kaspersky

Kaspersky Security Center 17 Linux

© 2026 AO Kaspersky Lab

Contenido

Ayuda de Kaspersky Security Center Linux

Novedades

Errores solucionados

Acerca del Kaspersky Security Center Linux

- Kit de distribución
- Requisitos de hardware y software
  - Requisitos del Servidor de administración
  - Requisitos de Web Console
  - Requisitos del Agente de red
- Aplicaciones y soluciones de Kaspersky compatibles
- Acerca de la compatibilidad de los componentes de Kaspersky Security Center Linux
- Comparación de Kaspersky Security Center: basado en Windows frente a basado en Linux
- Acerca de Kaspersky Next Expert View

Arquitectura y conceptos básicos

- Arquitectura
- Diagrama de despliegue del Servidor de administración de Kaspersky Security Center Linux y Kaspersky Security Center Web Console
- Puertos usados por Kaspersky Security Center Linux
- Puertos usados por Kaspersky Security Center Web Console
- Conceptos básicos
  - Servidor de administración
  - Jerarquía de Servidores de administración
  - Servidor de administración virtual
  - Servidor web
  - Servidor web de Kaspersky Security Center Linux
  - Agente de red
  - Grupos de administración
  - Dispositivo administrado
  - Dispositivo no asignado
  - Estación de trabajo del administrador
  - Complemento web de administración
  - Directivas
  - Perfiles de directivas
  - Tareas
  - Alcance de la tarea
  - Modo en que se relacionan las directivas y la configuración local de una aplicación
  - Punto de distribución
  - Puerta de enlace de conexión
  - Servidores de administración virtuales

Esquemas del tráfico de datos y de los puertos utilizados

- Servidor de administración y dispositivos administrados en una red de área local (LAN)
- Servidor de administración principal en una LAN y dos Servidores de administración secundarios
- Servidor de administración en una LAN, dispositivos administrados en Internet, se usa un proxy inverso

Servidor de administración en una LAN, dispositivos administrados en Internet, se usa una puerta de enlace de conexión
Servidor de administración en una DMZ, dispositivos administrados en Internet
Interacción entre los componentes de Kaspersky Security Center Linux y las aplicaciones de seguridad: más información
Convenciones utilizadas en esquemas de interacción
Servidor de administración y DBMS
Servidor de administración y dispositivo cliente: administración de la aplicación de seguridad
Actualización de software en un dispositivo cliente a través de un punto de distribución
Jerarquía de Servidores de administración: Servidor de administración principal y Servidor de administración secundario
Jerarquía de Servidores de administración con un Servidor de administración secundario en DMZ
Servidor de administración, una puerta de enlace de conexión en un segmento de red y un dispositivo cliente
Servidor de administración y dos dispositivos en DMZ: una puerta de enlace de conexión y un dispositivo cliente
Servidor de administración y Kaspersky Security Center Web Console
Guía de inicio rápido
Guía para reforzar la seguridad
Lista de comprobación de protección
Instalación del Servidor de administración
Seguridad de la conexión
Cuentas y autenticación
Administrar la protección del Servidor de administración
Administración de la protección del Agente de red
Administración de la protección de dispositivos cliente
Configurar la protección para aplicaciones administradas
Mantenimiento del Servidor de administración
Transferencia de eventos a sistemas de terceros
Recomendaciones de seguridad para sistemas de información de terceros
Recomendaciones para usar las aplicaciones de seguridad de Kaspersky
Escenario: autenticación del servidor MySQL
Escenario: autenticación TLS bidireccional de PostgreSQL para la base de datos del Servidor de administración y la base de datos de IAM
Preparativos para el despliegue
Seleccionar configuraciones estándares de Kaspersky Security Center Linux
Configuración estándar: oficina única
Configuración estándar: algunas oficinas a gran escala dirigidas por sus propios administradores
Configuración estándar: varias oficinas remotas pequeñas
Selección de una estructura para la protección de una empresa
Esquemas típicos para desplegar un sistema de protección
Selección de un DBMS
Suministro de acceso a Internet al Servidor de administración
Acceso a Internet: Servidor de administración en una red local
Acceso a Internet: Servidor de administración en la zona desmilitarizada (DMZ)
Instalación
Configurar el servidor MariaDB x64 para trabajar con Kaspersky Security Center Linux
Configurar un servidor de DBMS basado en PostgreSQL para que funcione con Kaspersky Security Center Linux
Configurar el servidor MySQL x64 para trabajar con Kaspersky Security Center Linux
Preparar un clúster de DBMS de alta disponibilidad para trabajar con Kaspersky Security Center Linux

Instalación de Kaspersky Security Center Linux
Instalación de Kaspersky Security Center Linux en modo silencioso
Instalación de Kaspersky Security Center Linux en Astra Linux en el modo de entorno de software cerrado
Instalación de Kaspersky Security Center Web Console
Parámetros de instalación de Kaspersky Security Center Web Console
Instalación de Kaspersky Security Center Web Console en Astra Linux en el modo de entorno de software cerrado
Instalación de Kaspersky Security Center Linux con un script
Despliegue del clúster de conmutación por error de Kaspersky Security Center Linux
Clúster de conmutación por error de Kaspersky Security Center Linux. Esquemas de despliegue
Clúster de conmutación por error de Kaspersky Security Center Linux
Procedimiento: Despliegue del clúster de conmutación por error de Kaspersky Security Center Linux
Clúster de conmutación por error de Kaspersky Security Center Linux. Requisitos de hardware y software
Preparación de un servidor de archivos para un clúster de conmutación por error de Kaspersky Security Center Linux
Preparación de nodos para un clúster de conmutación por error de Kaspersky Security Center Linux
Instalación de Kaspersky Security Center Linux en los nodos del clúster de conmutación por error de Kaspersky Security Center Linux
Iniciar y detener nodos del clúster manualmente
Reinstalación de un nodo del clúster de conmutación por error
Instalación de Kaspersky Security Center Web Console conectado al Servidor de administración instalado en nodos del clúster de conmutación por error de Kaspersky Security Center Linux
Clúster de conmutación por error de Kaspersky Security Center Linux distribuido geográficamente
Clúster distribuido geográficamente que ejecuta Ubuntu con DBMS de PostgreSQL
Preparación de un sistema de archivos de nodos de clúster
Configuración de un sistema de archivos de clúster replicado
Instalación y configuración de Corosync y Pacemaker en los nodos del clúster
Instalación y configuración del DBMS de PostgreSQL
Instalación de Kaspersky Security Center Linux en los nodos del clúster de conmutación por error distribuidos geográficamente
Clúster distribuido geográficamente que ejecuta SberLinux con DBMS de Platform V Pangolin
Preparación de un sistema de archivos de nodos de clúster
Configuración de un sistema de archivos de clúster replicado
Instalación y configuración de Corosync y Pacemaker en los nodos del clúster
Instalación y configuración del DBMS de Platform V Pangolin
Instalación de Kaspersky Security Center Linux en los nodos del clúster de conmutación por error distribuidos geográficamente
Instalación de Kaspersky Security Center Web Console en nodos de clúster de conmutación por error distribuidos geográficamente
Cuentas para trabajar con el DBMS
Creación de bases de datos y cuentas de usuario de MySQL y MariaDB
Creación de bases de datos basadas en PostgreSQL y cuentas de usuario
Mover datos desde un espacio de tabla compartido a un espacio de tabla por archivo en un DBMS MySQL o MariaDB
Certificados para trabajar con Kaspersky Security Center Linux
Acerca de los certificados de Kaspersky Security Center
Requisitos para los certificados personalizados utilizados en Kaspersky Security Center Linux
Reemisión de los certificados internos de Kaspersky Security Center Web Console
Reemplazo del certificado de Kaspersky Security Center Web Console
Conversión de un certificado PFX al formato PEM
Procedimiento: Especificación del certificado del Servidor de administración personalizado

Reemplazo del certificado del Servidor de administración mediante la utilidad klsetsrvcert
Conexión de los Agentes de red al Servidor de administración mediante la utilidad klmover
Volver a emitir el certificado del Servidor web
Cambiar el certificado predeterminado de IAM a uno personalizado
Agregar la dirección del Servidor de administración a la configuración del Servidor de IAM
Definición de una carpeta compartida
Iniciar y cerrar sesión en Kaspersky Security Center Web Console
Interfaz de Kaspersky Security Center Web Console
Cambiar el idioma de la interfaz de Kaspersky Security Center Web Console
Cambiar la página de inicio de Kaspersky Security Center Web Console
Añadir y eliminar marcadores
Eliminación de Kaspersky Security Center Web Console
Asistente de inicio rápido
Paso 1. Especificar la configuración de la conexión a Internet
Paso 2. Descargando actualizaciones requeridas
Paso 3. Selección de los activos para asegurar
Paso 4. Seleccionar el cifrado en las soluciones
Paso 5. Configurar la instalación de los complementos para las aplicaciones administradas
Paso 6. Descarga de paquetes de distribución y creación de paquetes de instalación
Paso 7. Configurar Kaspersky Security Network
Paso 8. Selección del método de activación de la aplicación
Paso 9. Especificar la configuración de administración de las actualizaciones de terceros
Paso 10. Creación de una configuración básica de protección de la red
Paso 11. Configuración de notificaciones por correo electrónico
Paso 12. Cierre del asistente de inicio rápido
Asistente de despliegue de la protección
Paso 1. Iniciar el Asistente de despliegue de la protección
Paso 2. Seleccionar el paquete de instalación
Paso 3. Selección de un método para la distribución del archivo de clave o código de activación
Paso 4. Seleccionar la versión del Agente de red
Paso 5. Seleccionar los dispositivos
Paso 6. Configurar la tarea de instalación remota
Paso 7. Opciones de reinicio
Paso 8. Eliminar aplicaciones incompatibles antes de la instalación
Paso 9. Mover los dispositivos a Dispositivos administrados
Paso 10. Seleccionar cuentas con acceso a los dispositivos
Paso 11. Inicio de la instalación
Actualización de Kaspersky Security Center Linux
Actualizar Kaspersky Security Center Linux versión 16 o posterior
Actualización de Kaspersky Security Center Linux de la versión 16 o posterior mediante el archivo de instalación
Actualización de Kaspersky Security Center Linux de la versión 16 o posterior mediante una copia de seguridad
Actualización de Kaspersky Security Center Linux de la versión 16 o posterior en los nodos del clúster de conmutación por error de Kaspersky Security Center Linux

- Actualizar Kaspersky Security Center Linux versión 15.4 o anterior
  - Actualización de Kaspersky Security Center Linux de la versión 15.4 o anterior mediante el archivo de instalación
  - Actualización de Kaspersky Security Center Linux de la versión 15.4 o anterior mediante una copia de seguridad
  - Actualización de Kaspersky Security Center Linux de la versión 15.4 o anterior en los nodos del clúster de conmutación por error de Kaspersky Security Center Linux
- Actualización de Kaspersky Security Center Web Console
- Actualización de Kaspersky Security Center Web Console en Astra Linux en el modo de entorno de software cerrado

Migración a Kaspersky Security Center Linux

- Guía general para migrar a un nuevo servidor de Kaspersky Security Center Linux
- Video tutorial: Migrar a Kaspersky Security Center Linux con un respaldo de los datos del Servidor de administración
- Migración a Kaspersky Security Center a través del Asistente de migración
  - Exportación de objetos de grupo desde Kaspersky Security Center Windows
  - Importar el archivo de exportación en Kaspersky Security Center Linux
  - Cambiar los dispositivos administrados para que estén bajo la administración de Kaspersky Security Center Linux

Configuración del Servidor de administración

- Configurar la dirección de conexión con el Servidor de administración
- Configuración de la conexión de Kaspersky Security Center Web Console al Servidor de administración
- Configurar una lista de direcciones IP autorizadas a iniciar sesión en Kaspersky Security Center Linux
- Configuración de las opciones de acceso a Internet para el Servidor de administración
- Jerarquía de Servidores de administración
- Creación de una jerarquía de servidores de administración: agregar un Servidor de administración secundario
- Ver la lista de servidores de administración secundarios
- Administración de servidores de administración virtuales
  - Crear un Servidor de administración virtual
  - Habilitación y deshabilitación de un Servidor de administración virtual
  - Asignar un administrador para un Servidor de administración virtual
  - Cambiar los dispositivos cliente de Servidor de administración
  - Eliminación de un Servidor de administración virtual
- Configurar el registro de eventos de conexiones del Servidor de administración
- Configuración del número máximo de eventos en el repositorio de eventos
- Mover el Servidor de administración a otro dispositivo
- Cambiar el nombre del Servidor de administración
  - Preservar las conexiones agregando un nuevo registro DNS
  - Conservación de las conexiones mediante el cambio a conectividad basada en direcciones IP
  - Restauración de conexiones interrumpidas después de cambiar el nombre del servidor
- Cambio de las credenciales de DBMS
- Copia de seguridad y restauración de los datos del Servidor de administración
  - Crear una tarea de copia de seguridad de los datos del Servidor de administración
  - Uso de la utilidad klbackup para realizar copias de seguridad y recuperar datos
  - Usar la utilidad klbackup para ceder el control de los dispositivos administrados a otro Servidor de administración
  - Cómo hacer copias de seguridad y restaurar datos del Servidor de administración si se usa MySQL o MariaDB
- Mantenimiento del Servidor de administración
- Eliminar una jerarquía de servidores de administración
- Acceso a servidores DNS públicos
- Configuración de la interfaz
- Conexión cifrada con un Servidor de administración
- Cifrar la comunicación con TLS

- Configuración de la red para interactuar con servicios externos
- Lista global de subredes
- Comprobar la integridad de los módulos mediante las utilidades klscmodchk e Integrity_checker

Descubrimiento de dispositivos conectados a la red

- Escenario: Descubrir dispositivos conectados a la red
- Sondeo de la red de Windows
- Sondeo de intervalos IP
- Agregar y modificar un intervalo IP
- Sondeo con Zeroconf
- Sondeo del controlador de dominio
- Autenticación y conexión a un controlador de dominio
- Configurar un controlador de dominio Samba
- Inventario de equipos
  - Agregar información sobre los dispositivos nuevos
  - Configurar criterios usados para los dispositivos de empresa
- Usar el modo dinámico para la Infraestructura de escritorio virtual (VDI) en los dispositivos cliente
  - Habilitación del modo dinámico de la Infraestructura de escritorio virtual (VDI) en las propiedades de un paquete de instalación para el Agente de red
  - Mover los dispositivos que forman parte de la VDI a un grupo de administración

Administración de dispositivos cliente

- Configuración de un dispositivo administrado
- Comprobación de la conexión entre un dispositivo administrado y el Servidor de administración (utilidad klnagchk)
- Reglas de movimiento de dispositivos
  - Crear reglas de movimiento de dispositivos
  - Copiar reglas de movimiento de dispositivos
  - Condiciones para una regla de movimiento de dispositivos
- Agregar dispositivos a un grupo de administración en forma manual
- Mover dispositivos o clústeres a un grupo de administración en forma manual
- Sobre clústeres y conjuntos de servidores
- Propiedades de un clúster o conjunto de servidores
- Ajuste de puntos de distribución y puertas de enlace de conexión
  - Acerca de los puntos de distribución
  - Configuración estándar de puntos de distribución: oficina única
  - Configuración estándar de puntos de distribución: varias oficinas remotas pequeñas
  - Cálculo de la cantidad de puntos de distribución y su configuración
  - Asignar puntos de distribución automáticamente
  - Designación manual de puntos de distribución
  - Agregar una puerta de enlace de conexión ubicada en una DMZ como punto de distribución
  - Modificar la lista de puntos de distribución para un grupo de administración
  - Habilitación de un servidor push
  - Aumento del límite de descriptores de archivos para el servicio klnagent
- Acerca de los estados del dispositivo
- Configurar cambios de estado para los dispositivos
- Selecciones de dispositivos
  - Ver la lista de dispositivos de una selección de dispositivos
  - Crear una selección de dispositivos
  - Configurar una selección de dispositivos

Exportar la lista de dispositivos de una selección de dispositivos

Eliminación de dispositivos de los grupos de administración en una selección

Etiquetas de dispositivo

Creación de una etiqueta de dispositivo

Cambiar el nombre de una etiqueta de dispositivo

Eliminar una etiqueta de dispositivo

Ver los dispositivos que tienen asignada una etiqueta

Ver las etiquetas asignadas a un dispositivo

Etiquetar un dispositivo manualmente

Quitarle una etiqueta a un dispositivo

Ver las reglas de etiquetado automático de dispositivos

Modificación de una regla para etiquetar dispositivos automáticamente

Creación de una regla para etiquetar dispositivos automáticamente

Ejecución de reglas para etiquetar dispositivos automáticamente

Eliminación de una regla para etiquetar dispositivos automáticamente

Administrar las etiquetas de los dispositivos con la utilidad klscflag

Protección y cifrado de datos

Ver la lista de unidades cifradas

Ver la lista de eventos de cifrado

Crear y ver informes de cifrado

Brindar acceso a una unidad cifrada en modo sin conexión

Transmisión de claves de cifrado entre Servidores de administración

Cambiar los dispositivos cliente de Servidor de administración

Evitar conflictos entre varios Servidores de administración

Mover dispositivos conectados a un Servidor de administración mediante puertas de enlace de conexión a otro Servidor de administración

Ver y configurar las acciones para dispositivos inactivos

Envío de mensajes a usuarios de dispositivos

Encendido, apagado y reinicio remoto de dispositivos cliente

Acceso remoto a dispositivos administrados

Acceso remoto desde un dispositivo basado en Linux con Kaspersky Security Center Web Console a un dispositivo administrado basado en Linux

Acceso remoto desde un dispositivo basado en Linux con Kaspersky Security Center Web Console a un dispositivo administrado basado en Windows

Acceso remoto desde un dispositivo basado en Windows con Kaspersky Security Center Web Console a un dispositivo administrado basado en Linux

Acceso remoto desde un dispositivo basado en Windows con Kaspersky Security Center Web Console a un dispositivo administrado basado en Windows

Administración de dispositivos móviles

Usar Firebase Cloud Messaging

Integración con una infraestructura de claves públicas

Administrar grupos de administración

Creación de grupos de administración

Instalación automática de aplicaciones en dispositivos de un grupo de administración

Traslado de grupos de administración

Eliminación de grupos de administración

Despliegue de las aplicaciones de Kaspersky
Procedimiento: despliegue de las aplicaciones de Kaspersky
Agregar complementos de administración para aplicaciones de Kaspersky
Paquetes
Descargar y crear paquetes de instalación para aplicaciones de Kaspersky
Crear paquetes de instalación a partir de un archivo
Creación de paquetes de instalación independientes
Ajustes del paquete de instalación del Agente de red
Ejecución de paquetes independientes creados por Kaspersky Security Center Linux
Instalación de aplicaciones con paquetes independientes
Conveniencia de actualizar las bases de datos en el paquete de instalación de una aplicación de seguridad
Modificación del límite de datos para paquetes de instalación personalizados
Distribución de paquetes de instalación a servidores de administración secundarios
Ver la lista de paquetes de instalación independientes
Instalar el Agente de red para Linux
Preparación de un dispositivo Linux para la instalación del Agente de red
Preparación de un dispositivo que ejecuta SUSE Linux Enterprise Server 15 para la instalación del Agente de red
Preparación de un dispositivo que ejecuta Astra Linux en el modo de entorno de software cerrado para la instalación del Agente de red
Preparación para instalar el Agente de red en un sistema operativo Linux con glibc 2.5 (SO heredado)
Preparación para instalar el Agente de red en un sistema operativo Linux con OpenSSH versión 6.4 (SO heredado)
Instalar el Agente de red en un dispositivo Linux de forma remota
Instalación del Agente de red para Linux en modo silencioso (con un archivo de respuestas)
Instalación del Agente de red para Linux en modo interactivo
Soporte de reversión del sistema de archivos para dispositivos con Agente de red
Instalar el Agente de red para Windows
Instalar el Agente de red para Windows en modo interactivo
Instalación del Agente de red para Windows en modo silencioso
Despliegue mediante la captura y copia de la imagen de un dispositivo
Modo de clonación de disco del Agente de red
Agente de red: parámetros de instalación
Instalar aplicaciones mediante la tarea de instalación remota
Acerca de las tareas de instalación remota en Kaspersky Security Center Linux
Instalación de una aplicación de forma remota
Instalación remota de aplicaciones en dispositivos macOS
Instalar aplicaciones en los Servidores de administración secundarios
Instalación remota de aplicaciones en dispositivos en los que se encuentra instalado el Agente de red
Opciones para controlar el reinicio de los dispositivos en la tarea de instalación remota
Despliegue forzado con la tarea de instalación remota de Kaspersky Security Center Linux
Instalación de aplicaciones en modo no interactivo
Preparación de un dispositivo de macOS para instalación remota de Agente de red
Infraestructura virtual
Sugerencias sobre la reducción de la carga en máquinas virtuales
Compatibilidad con máquinas virtuales dinámicas
Soporte de copia de máquinas virtuales
Definir ajustes para instalaciones remotas en dispositivos Unix
Supervisión del despliegue

- Iniciar y detener aplicaciones de Kaspersky
- Reemplazo de aplicaciones de seguridad de terceros
- Eliminación de aplicaciones o actualizaciones de software de forma remota
- Preparar un dispositivo Windows para la instalación remota
- Crear la tarea Ejecución remota de scripts
  - Crear un paquete de instalación basado en un archivo de manifiesto
  - Preparar un archivo para la tarea Ejecución remota de scripts
  - Instalar aplicaciones en dispositivos a distancia con la tarea Ejecución remota de scripts
  - Configurar notificaciones y supervisar la tarea Ejecución remota de scripts

Licencias

- Licencias de Kaspersky Security Center Linux
  - Acerca del Contrato de licencia de usuario final
  - Acerca de la licencia
  - Acerca del certificado de licencia
  - Acerca de la clave de licencia
  - Ver la Política de privacidad
  - Opciones de licencias de Kaspersky Security Center
  - Acerca del archivo de clave
  - Sobre la provisión de datos
  - Acerca de la suscripción
  - Activación de Kaspersky Security Center Linux
- Licencias de aplicaciones administradas de Kaspersky
  - Licencias de aplicaciones administradas
  - Agregar una clave de licencia al repositorio del Servidor de administración
  - Distribución de claves de licencia a dispositivos cliente
  - Distribución automática de una clave de licencia
  - Visualización de información sobre las claves de licencia en uso
  - Eventos sobre límites de licencia superados
  - Eliminar una clave de licencia del repositorio
  - Revocar la aceptación de un Contrato de licencia de usuario final
  - Renovación de licencias para aplicaciones de Kaspersky
  - Utilizar Kaspersky Marketplace para elegir soluciones empresariales de Kaspersky

Configuración de las aplicaciones de Kaspersky

- Procedimiento: Configurar la protección de la red
- Acerca de la administración de la seguridad centrada en el dispositivo y centrada en el usuario
- Configuración y propagación de directivas: enfoque centrado en el dispositivo
- Configuración y propagación de directivas: enfoque centrado en el usuario
- Directivas y perfiles de directivas
  - Acerca de las directivas y perfiles de directivas
  - Acerca del candado y el bloqueo de ajustes
  - Herencia en las directivas y los perfiles de directivas
    - Jerarquía de directivas
    - Perfiles de directivas en una jerarquía de directivas
    - Cómo se implementan los valores de configuración en un dispositivo administrado
  - Administración de directivas
    - Ver la lista de directivas
    - Crear una nueva directiva

Ajustes generales de una directiva
Modificar una directiva
Habilitar y deshabilitar una opción de herencia en las directivas
Copiar una directiva
Mover una directiva
Exportación de una directiva
Importación de una directiva
Sincronización forzada
Ver el gráfico de distribución de una directiva
Activar una directiva automáticamente ante un brote de virus
Eliminar una directiva
Administración de perfiles de directivas
Ver los perfiles de una directiva
Cambiar la prioridad de un perfil de directiva
Crear un perfil de directiva
Copiar un perfil de directiva
Crear una regla de activación para un perfil de directiva
Eliminar un perfil de directiva
Exportación e importación de un perfil de directiva
Ajustes de la directiva del Agente de red
Uso del Agente de red para Windows, Linux y macOS: comparación
Comparación de la configuración del Agente de red por sistemas operativos
Habilitar y deshabilitar el modo de bajo consumo de recursos para el Agente de red
Configurar la protección de las aplicaciones administradas
Configuración manual de la tarea de grupo para actualizar Kaspersky Endpoint Security
Instalación manual de la tarea de grupo para analizar un dispositivo con Kaspersky Endpoint Security
Kaspersky Security Network (KSN)
Acerca de KSN
Configurar el acceso a KSN
Habilitar y deshabilitar el uso de KSN
Ver la Declaración de KSN aceptada
Aceptar una Declaración de KSN actualizada
Verificar si el punto de distribución opera como servidor proxy de KSN
Ver las estadísticas del servidor proxy de KSN
Administración de tareas
Acerca de las tareas
Acerca del alcance de las tareas
Crear una tarea
Iniciar una tarea manualmente
Iniciar una tarea para dispositivos puntuales
Ver la lista de tareas
Configuración general de tareas
Exportar una tarea
Importar una tarea

Iniciar el Asistente para cambiar contraseñas de tareas
Paso 1. Especificar credenciales
Paso 2. Seleccionar una acción para realizar
Paso 3. Ver los resultados
Ver resultados de la ejecución de tareas almacenados en el Servidor de administración
Etiquetas de aplicación
Etiquetas de aplicación
Creación de una etiqueta de aplicación
Cambiar el nombre de una etiqueta de aplicación
Asignación de etiquetas a una aplicación
Quitarle una etiqueta a una aplicación
Eliminación de una etiqueta de aplicación
Usar la utilidad klscflag para abrir el puerto 13291
Registro de la aplicación Kaspersky Industrial CyberSecurity for Networks en Kaspersky Security Center Web Console
Administración de usuarios y roles de usuarios
Acerca de las cuentas de usuario
Acerca de los roles de usuario
Configurar los derechos de acceso a las funciones de la aplicación. Control de acceso basado en roles
Derechos de acceso a las funciones de la aplicación
Roles de usuario predefinidos
Asignación de derechos de acceso a objetos específicos
Asignar derechos de acceso a usuarios y grupos de seguridad
Agregar una cuenta de un usuario interno
Crear un grupo de seguridad
Editar una cuenta de un usuario interno
Editar un grupo de seguridad
Asignación de un rol a un usuario o a un grupo de seguridad
Agregar cuentas de usuario a un grupo interno de seguridad
Designación de un usuario como propietario de un dispositivo
Designación de un usuario como propietario de un dispositivo durante la instalación del Agente de red
Asignar a un usuario como propietario del dispositivo tras instalar el Agente de red
Anular la designación de un usuario como propietario de un dispositivo
Habilitación de la protección de una cuenta desde la modificación no autorizada
Configuración de la autenticación de dos factores
Acerca de la autenticación de dos factores para una cuenta
Configuración de una clave secreta de autenticación de dos factores al iniciar sesión en la consola web de Kaspersky Security Center
Permitir a los usuarios configurar la autenticación de dos factores
Restablecimiento y eliminación de una clave secreta de autenticación de dos factores
Excluir cuentas de la autenticación de dos factores
Editar el nombre del emisor de un código de seguridad
Cambiar el número de intentos de entrada de contraseña permitidos
Eliminar un usuario o un grupo de seguridad
Cambiar la contraseña de una cuenta de usuario
Creación de roles de usuario
Editar un rol de usuario
Editar el alcance de un rol de usuario

- Eliminar un rol de usuario
- Asociación de perfiles de directivas con roles
- Propagación de roles de usuario a Servidores de administración secundarios
- Cambiar la contraseña de una cuenta
- Revocar los derechos de administrador local
- Configuración de la autenticación de dominio Kerberos

Actualización de las bases de datos y las aplicaciones de Kaspersky

- Procedimiento: actualización regular de bases de datos y aplicaciones de Kaspersky
- Acerca de la actualización de las bases de datos, los módulos de software y las aplicaciones de Kaspersky
- Crear la Descarga de actualizaciones para la tarea del repositorio del Servidor de administración
- Comprobar actualizaciones descargadas
- Crear una tarea para descargar las actualizaciones en los repositorios de los puntos de distribución
- Adición de fuentes de actualizaciones para la tarea Descargar actualizaciones al repositorio del Servidor de administración
- Aprobar y rechazar actualizaciones de software
- Instalación automática de actualizaciones para Kaspersky Endpoint Security para Windows
- Acerca de la utilización de archivos diff para actualizar las bases de datos y los módulos de software de Kaspersky
- Habilitación de la función de descarga de archivos diff
- Descarga de actualizaciones por puntos de distribución
- Actualizar las bases de datos y los módulos de software de Kaspersky en dispositivos sin conexión

Supervisión, informes y auditoría

- Procedimiento: Supervisión y generación de informes
- Acerca de los tipos de funciones de supervisión y generación de informes
- Activación de reglas en modo Aprendizaje inteligente
  - Cómo ver y confirmar las detecciones realizadas con las reglas del Control de anomalías adaptativo
  - Adición de exclusiones para las reglas del Control de anomalías adaptativo
- Panel y widgets
  - Uso del panel
  - Agregar widgets al panel
  - Ocultar un widget del panel
  - Mover un widget en el panel
  - Cambiar el aspecto o el tamaño de un widget
  - Cambiar la configuración de un widget
  - Acerca del modo solo panel
  - Configuración del modo solo panel
- Informes de administración y protección
  - Utilización de informes
  - Creando una plantilla de informe
  - Ver y editar las propiedades de una plantilla de informe
  - Exportación de un informe a un archivo
  - Generar y ver un informe
  - Crear una tarea de entrega de informes
  - Eliminación de plantillas de informes
- Centro de refuerzo de seguridad
  - Aplicación de seguridad instalada
  - Directiva aplicada
  - Actualización de las bases de datos antivirus configurada
  - Copia de seguridad configurada

- Mantenimiento del Servidor de administración configurado
- Cifrado TLS habilitado
- Todos los dispositivos están administrados

Eventos y selecciones de eventos

- Acerca de los eventos en Kaspersky Security Center Linux
- Eventos de los componentes de Kaspersky Security Center Linux
  - Estructura de datos utilizada para describir los tipos de eventos
  - Eventos del Servidor de administración
    - Eventos del Servidor de administración: nivel Crítico
    - Eventos del Servidor de administración: nivel Error funcional
    - Eventos del Servidor de administración: nivel Advertencia
    - Eventos del Servidor de administración: nivel Información
  - Eventos del Agente de red
    - Eventos del Agente de red: nivel Error funcional
    - Eventos del Agente de red: nivel Advertencia
    - Eventos del Agente de red: nivel Información
- Utilización de selecciones de eventos
- Crear una selección de eventos
- Editar una selección de eventos
- Ver una lista de una selección de eventos
- Exportar una selección de eventos
- Importar una selección de eventos
- Visualización de las áreas de detalles del evento
- Exportar eventos a un archivo
- Acceder al historial de un objeto desde un evento
- Eliminar eventos
- Eliminación de selecciones de eventos
- Configuración del plazo de almacenamiento para un evento
- Bloquear eventos frecuentes
  - Acerca del bloqueo de eventos frecuentes
  - Administrar el bloqueo de eventos frecuentes
  - Eliminar el bloqueo de eventos frecuentes
- Almacenamiento y procesamiento de eventos en el Servidor de administración

Notificaciones y estados de los dispositivos

- Acerca de las notificaciones
- Visualización de notificaciones que requieren atención
- Visualización de notificaciones del sistema
- Visualización de novedades
- Dejar de recibir las novedades de Kaspersky
- Configurar cambios de estado para los dispositivos
- Configurar el envío de notificaciones
- Notificaciones de prueba
- Acerca de los estados del dispositivo
- Parámetros y variables de entorno para describir un evento

Ver información sobre la detección de amenazas

Integraciones para responder a alertas
Configurar la integración con Active Directory para realizar acciones de respuesta
Configuración de la integración con Kaspersky Automated Security Awareness Platform
Configurar la integración con Kaspersky Threat Intelligence Portal Sandbox
Agrupación de alertas por atributos
Cloud Discovery
Habilitar Cloud Discovery mediante el widget
Agregar el widget de Cloud Discovery al panel
Ver información sobre el uso de servicios en la nube
Nivel de riesgo de un servicio en la nube
Bloquear el acceso a servicios en la nube no deseados
Exportación de eventos a sistemas SIEM
Configurar la exportación de eventos a sistemas SIEM
Requisitos previos
Acerca de la exportación de eventos
Acerca de la configuración de la exportación de eventos en un sistema SIEM
Acerca de la exportación de eventos en formato CEF o LEEF
Conversión de eventos al formato CEF o LEEF
Marcar los eventos que se exportarán a un sistema SIEM en formato Syslog
Marcar eventos de una aplicación de Kaspersky para que se los exporte en formato Syslog
Marcar eventos generales para que se los exporte en formato Syslog
Acerca de la exportación de eventos en formato Syslog
Configurar Kaspersky Security Center Linux para exportar eventos a un sistema SIEM
Supervisión de cambios en directivas y perfiles de directiva
Exportación de eventos directamente desde la base de datos
Ejecución de una consulta SQL mediante la utilidad klsql2
Ejemplo de una consulta de SQL usando la utilidad klsql2
Visualización del nombre de la base de datos de Kaspersky Security Center Linux
Ver los resultados de la exportación
Administración de revisiones de objetos
Ver y guardar una revisión de la directiva
Comparar las revisiones de una directiva
Devolver un objeto a una revisión anterior
Amenazas activas
Desinfección de un archivo no procesado
Descarga de un archivo no procesado
Eliminar archivos desde la sección Amenazas activas
Eliminación de objetos
Descarga y eliminación de archivos de Cuarentena y Copias de seguridad del archivo
Descargar archivos de Cuarentena y Copia de seguridad de archivos
Acerca de la eliminación de objetos de los repositorios de Cuarentena, Copia de seguridad de archivos o Amenazas activas
Administrar la aplicación a través de SNMP
Configuración del servicio snmpd en el sistema operativo
Habilitación y deshabilitación de las notificaciones mediante SNMP
Habilitación y deshabilitación de SNMP en Kaspersky Security Center Linux
Valores de identificadores de objetos para SNMP

Trabajar con Kaspersky Security Center Linux con una licencia de Kaspersky Next XDR Optimum
Integraciones para responder a alertas
Configurar la integración con Active Directory para realizar acciones de respuesta
Configuración de la integración con Kaspersky Automated Security Awareness Platform
Configurar la integración con Kaspersky Threat Intelligence Portal Sandbox
Agrupación de alertas por atributos
Integración entre Kaspersky Security Center Web Console y otras soluciones de Kaspersky
Establecer una conexión en segundo plano
Configuración de la conexión del servidor proxy
Diagnóstico remoto de dispositivos cliente
Abrir la ventana de diagnóstico remoto
Habilitar y deshabilitar el seguimiento para las aplicaciones
Descargar los archivos de seguimiento de una aplicación
Eliminar archivos de seguimiento
Descargar la configuración de las aplicaciones
Descargar información del sistema desde un dispositivo cliente
Descargar registros de eventos
Iniciar, detener o reiniciar la aplicación
Realizar un diagnóstico remoto del Agente de red de Kaspersky Security Center Linux y descargar los resultados
Ejecutar una aplicación en un dispositivo cliente
Ejecución de diagnósticos remotos en un dispositivo cliente basado en Linux
Administrar aplicaciones y archivos ejecutables en dispositivos cliente
Uso de Control de aplicaciones para administrar archivos ejecutables
Obtención y visualización de una lista de archivos ejecutables almacenados en los dispositivos cliente
Creación de una categoría de aplicaciones con contenido agregado manualmente
Crear una categoría de aplicaciones con archivos ejecutables de dispositivos específicos
Creación de una categoría de aplicaciones que incluya archivos ejecutables de una carpeta seleccionada
Visualización de la lista de categorías de aplicaciones
Agregar archivos ejecutables vinculados a eventos a una categoría de aplicaciones
Configurar Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows
Obtener y ver una lista de aplicaciones instaladas en los dispositivos cliente
Acerca de las aplicaciones de terceros
Instalación de actualizaciones para software de terceros
Procedimiento: Actualización de software de terceros
Opciones para instalar actualizaciones de software de terceros
Configuración de la tarea Buscar vulnerabilidades y actualizaciones requeridas
Crear la tarea Buscar vulnerabilidades y actualizaciones requeridas
Ver información sobre las actualizaciones disponibles para el software de terceros
Exportar la lista de actualizaciones de software disponibles a un archivo
Aprobar y rechazar actualizaciones de software de terceros
Crear la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades
Agregar reglas de instalación de actualizaciones
Ajustes de la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades que se definen tras crearla
Actualización automática de aplicaciones de terceros
Reparación de vulnerabilidades en el software de terceros
Acerca de la búsqueda y reparación de vulnerabilidades de software
Procedimiento: búsqueda y reparación de vulnerabilidades de software de terceros

Reparación de vulnerabilidades en el software de terceros
Crear la tarea Reparar vulnerabilidades
Selección de soluciones de usuario para vulnerabilidades de software de terceros
Ver información sobre las vulnerabilidades de software detectadas en todos los dispositivos administrados
Ver información sobre las vulnerabilidades de software detectadas en un dispositivo administrado específico
Ver estadísticas de las vulnerabilidades presentes en los dispositivos administrados
Exportar la lista de vulnerabilidades de software a un archivo
Ignorar vulnerabilidades de software
Crear un paquete de instalación para una aplicación de terceros usando la base de datos de Kaspersky
Ver y modificar la configuración de un paquete de instalación de una aplicación de terceros de la base de datos de Kaspersky
Configurar el paquete de instalación de una aplicación de terceros incluida en la base de datos de Kaspersky
Reparar vulnerabilidades en una red aislada
Procedimiento: reparar vulnerabilidades en el software de terceros
Acerca de la reparación de vulnerabilidades en el software de terceros en una red aislada
Configurar el Servidor de administración con acceso a Internet para reparar vulnerabilidades en una red aislada
Configurar los servidores de administración aislados para reparar vulnerabilidades en una red aislada
Transmitir parches e instalar actualizaciones en una red aislada
Deshabilitar la transmisión de parches y la instalación de actualizaciones en una red aislada
Guía de referencia de API
Prácticas recomendadas para proveedores de servicios
Planificación del despliegue de Kaspersky Security Center Linux
Suministro de acceso a Internet al Servidor de administración
Configuración estándar de Kaspersky Security Center Linux
Acerca de los puntos de distribución
Jerarquía de Servidores de administración
Servidores de administración virtuales
Despliegue y configuración inicial
Recomendaciones sobre la instalación del Servidor de administración
Creación de cuentas para los servicios del Servidor de administración en un clúster de conmutación por error
Selección de un DBMS
Especificación de la dirección del Servidor de administración
Mantener conexiones inactivas
Desplegar el Agente de red y las aplicaciones de seguridad
Configuración de protección en la red de una organización cliente
Configuración manual de la directiva de Kaspersky Endpoint Security
Configuración de la directiva en la sección Protección avanzada contra amenazas
Configuración de la directiva en la sección Protección básica contra amenazas
Configuración de la directiva en la sección Configuración general
Configuración de la directiva en la sección Configuración de eventos
Configuración manual de la tarea de grupo para actualizar Kaspersky Endpoint Security
Instalación manual de la tarea de grupo para analizar un dispositivo con Kaspersky Endpoint Security
Programación de la tarea Buscar vulnerabilidades y actualizaciones requeridas
Configuración manual de la tarea de grupo para la instalación de actualizaciones y la reparación de vulnerabilidades
Creación de una estructura de grupos de administración y asignación de puntos de distribución
Configuración estándar de un cliente MSP: oficina única
Configuración estándar de un cliente MSP: varias pequeñas oficinas remotas

Jerarquía de directivas, usando perfiles de directivas
Jerarquía de directivas
Perfiles de directivas
Tareas
Reglas de movimiento de dispositivos
Categorización del software
Copia de seguridad y restauración de la configuración del Servidor de administración
Un dispositivo con el Servidor de administración es inoperable
La configuración del Servidor de administración o la base de datos es corrupta
Acerca de los perfiles de conexión para los usuarios fuera de la oficina
Acerca de cambiar el Agente de red a otros Servidores de administración
Creación de un perfil de conexión para usuarios fuera de la oficina
Acceso remoto a dispositivos administrados
Uso de la opción "No desconectarse del Servidor de administración" para proporcionar conectividad continua entre un dispositivo administrado y el Servidor de administración
Acerca de la comprobación de la hora de conexión entre un dispositivo y el Servidor de administración
Acerca de la sincronización forzada
Guía de dimensionamiento
Acerca de esta Guía
Limitaciones de Kaspersky Security Center Linux
Evaluaciones para Servidores de administración
Evaluación de recursos del hardware para el Servidor de administración
Requisitos de hardware para DBMS y el Servidor de administración
Evaluación de espacio de la base de datos
Evaluación de espacio en el disco
Evaluación del número y configuración de Servidores de administración
Recomendaciones para conectar máquinas virtuales dinámicas a Kaspersky Security Center
Cálculos para puntos de distribución y puertas de enlace de conexión
Requisitos para un punto de distribución
Cálculo de la cantidad de puntos de distribución y su configuración
Evaluación del número de pasarelas de conexión
Registro de información sobre eventos para tareas y directivas
Prácticas recomendadas para un Servidor de administración que administra una gran cantidad de dispositivos
Consideraciones específicas y configuración óptima de ciertas tareas
Frecuencia de descubrimiento de dispositivos
Tarea de copia de seguridad de datos del Servidor de administración y tarea de mantenimiento de la base de datos
Tareas de grupo para actualizar Kaspersky Endpoint Security
Tarea de inventario
Detalles de margen de la carga de la red entre Servidor de administración y dispositivos protegidos
Tasa de tráfico en diferentes escenarios
Uso promedio de tráfico por 24 horas
Problemas conocidos y limitaciones
Contacto con el Servicio de soporte técnico
Cómo obtener soporte técnico
Consultas mediante Kaspersky CompanyAccount al servicio de soporte técnico
Obtener archivos de volcado del Servidor de administración
Fuentes de información sobre la aplicación

Glosario
- Actualización
- Actualización disponible
- Administración centralizada de aplicaciones
- Administración directa de aplicaciones
- Administrador de Kaspersky Security Center Linux
- Administrador del cliente
- Administrador del proveedor de servicios
- Agente de actualización
- Agente de autenticación
- Agente de red
- Aplicación incompatible
- Archivo de clave
- Bases de datos antivirus
- Brote de virus
- Carpeta Copia de seguridad
- Certificado compartido
- Certificado del Servidor de administración
- Clave activa
- Clave de reserva
- Cliente del Servidor de administración (dispositivo cliente)
- Cloud Discovery
- Configuración de la aplicación
- Configuración de la tarea
- Consola de administración
- Copia de seguridad de los datos del Servidor de administración
- Derechos de administrador
- Directiva
- Dispositivo MDM con iOS
- Dispositivos administrados
- Dominio de difusión
- Estación de trabajo del administrador
- Estado de protección
- Estado de protección de la red
- FileTransferBridge
- Gravedad de un evento
- Grupo de administración
- Grupo de roles
- HTTPS
- Identity and Access Manager (IAM)
- Instalación local
- Instalación manual
- Instalación remota
- JavaScript
- Kaspersky Security Center System Health Validator (SHV)
- Nagent ligero (LWNGT)
- Nivel de importancia del parche

Operador de Kaspersky Security Center
Paquete de instalación
Perfil
Perfil de aprovisionamiento
Perfil de configuración
Periodo de vigencia de la licencia
Propietario del dispositivo
Proveedor de servicios de protección antivirus
Puerta de enlace de conexión
Repositorio de eventos
Restauración
Restauración de los datos del Servidor de administración
Seguridad antivirus de la red
Servidor de administración
Servidor de administración doméstico
Servidor de administración virtual
Servidor de MDM para iOS
Servidor web de Kaspersky Security Center Linux
Servidores de actualizaciones de Kaspersky
SSL
Subred de reconocimiento de ubicación de red (NLA)
Tarea
Tarea de grupo
Tarea local
Tarea para dispositivos específicos
Tienda de aplicaciones
Usuarios internos
Vulnerabilidad
Zona desmilitarizada (DMZ)
Información sobre código de terceros
Avisos de marcas registradas

Ayuda de Kaspersky Security Center Linux

Funciones nuevas

- Novedades

Requisitos de hardware y software

- Requisitos del Servidor de administración
- Requisitos de Web Console
- Requisitos del Agente de red

Guía de inicio rápido

- Instalación
- Asistente de inicio rápido
- Asistente de despliegue de la protección

Licencias y activación

- Activación de Kaspersky Security Center Linux
- Licencias de aplicaciones administradas

Despliegue y configuración

- Descubrimiento de dispositivos conectados a la red
- Ajuste de puntos de distribución y puertas de enlace de conexión
- Reemplazo de aplicaciones de seguridad de terceros
- Despliegue de la aplicación de Kaspersky Despliegue centralizado

- Configurar la protección de la red
- Despliegue de la aplicación de Kaspersky Actualización de las bases de datos y los módulos de software
- Configurar la dirección de conexión con el Servidor de administración
- Migración a Kaspersky Security Center Linux
- Acerca de las actualizaciones de Kaspersky Security Center Linux

Supervisión

- Supervisión e informes
- Cloud Discovery

Administración de dispositivos cliente

- Acceso remoto a dispositivos administrados

Administración de vulnerabilidades y parches

- Búsqueda y reparación de vulnerabilidades de software de terceros

Funciones adicionales

- Exportación de eventos a sistemas SIEM
- Ver las estadísticas del servidor proxy de KSN
- Guía de dimensionamiento (Ayuda en línea únicamente)

Novedades

Kaspersky Security Center 17 Linux

Kaspersky Security Center 17 Linux presenta un número de mejoras y características nuevas.

- Los certificados de Web Console, IAM y del Servidor de administración ahora se pueden agregar manualmente y reemplazar automáticamente sin reinstalar Web Console.
- Al ver el contenido de una revisión o comparar revisiones de directivas, ahora puede consultar los datos de los perfiles de directiva.
- Ahora, después de ejecutar una tarea para un dispositivo o dispositivos específicos, puede acceder a las propiedades de la tarea para ver los resultados.
- Se agregó un nuevo indicador del nivel de protección al Centro de fortalecimiento, que le permite realizar un seguimiento de los dispositivos sobre los que se pudo haber perdido el control.
- Se agregó la siguiente información sobre los dispositivos cliente a los eventos publicados por el Servidor de administración para los dispositivos administrados: nombre del DNS (FQDN), nombre NetBIOS, dirección IP y DisplayName.
- Se ampliaron las capacidades de auditoría:
  - Cuando el Agente de red cambia a otro Servidor de administración, ahora se registra un evento en el registro de eventos de Kaspersky. El evento indica la dirección del nuevo Servidor de administración y la dirección de la puerta de enlace, si corresponde.
  - Ahora se envían eventos extendidos al importar y copiar directivas, así como al revertir una directiva a una revisión seleccionada.
- Mejoras en la experiencia del usuario:
  - Se cambió el nombre de la sección **Etiquetas** a **Etiquetas de dispositivos**.
  - La sección **Etiquetas de dispositivos** y sus subsecciones se trasladaron de la sección **Administración de activos** a la sección **Repositorios**.
  - Ahora puede descargar en un archivo todos los eventos de un dispositivo o una selección de eventos de la lista de eventos.
- El script de instalación rápida de Kaspersky Security Center Linux ahora admite opciones de despliegue adicionales:
  - MySQL 8.4.10 con Ubuntu Server 26.04 LTS
  - MariaDB 10.11.18 con CentOS Stream 10
  - MariaDB 10.11.18 con RED OS 8
  - MariaDB 10.11.13 con Astra Linux 1.8.5

- El Servidor de administración ahora admite nuevas versiones de sistemas de gestión de bases de datos:
  - MariaDB 11.4
  - MariaDB 11.8
  - MariaDB 12.3
  - Platform V Pangolin 7.2.0.
  - Platform V Pangolin 7.2.0 (clúster de alta disponibilidad incorporado)
- El Servidor de administración y Web Console ahora son compatibles con las siguientes versiones nuevas de sistemas operativos:
  - ALT Server 11
  - MosOS 15.6
- El Agente de red ahora es compatible con las siguientes nuevas versiones de sistemas operativos:
  - Microsoft Windows 11 26H2 Home/Pro/Pro for Workstations/Enterprise/Education
  - Microsoft Windows 10 IoT Enterprise versión 1507
  - Debian GNU/Linux versiones 12.10, 12.11 y 12.14 (Bookworm) ARM
  - Astra Linux Special Edition RUSB.10015-16 (versión 2) (actualización operativa 8.1) E2K
  - Astra Linux Special Edition RUSB.10265-01 (actualización operativa 8.1) E2K
  - Elbrus 9.3.6 E2K
  - ALT Workstation 11.2 ARM
  - ALT Server 11.1 ARM
  - ALT SP Workstation 10 E2K
  - ALT SP Server 10 E2K
  - ALT 8 SP Workstation E2K
  - ALT SP Server 8 E2K
  - MSVSPHERE 9.5 SERVER
  - MSVSPHERE 9.5 ARM
  - Amazon Linux 2023
  - MosOS 15.6

Kaspersky Security Center 16.3 Linux

Kaspersky Security Center 16.3 Linux presenta un número de mejoras y características nuevas.

- Si modifica una directiva, se crea un evento de auditoría independiente por cada parámetro modificado. Los eventos se exportan a SIEM.
- Se agregó la compatibilidad con **Kaspersky SIEM** (KUMA) a la funcionalidad de exportación de eventos a sistemas SIEM.
- Kaspersky Security Center Linux ahora admite el uso de la solución Kaspersky Vulnerability Management.
- Para cumplir con la Guía para reforzar la seguridad, desarrollamos una configuración optimizada de Kaspersky Endpoint Security for Linux para instalarla en los dispositivos con Servidor de administración, Web Console y DBMS, así como para implementar el clúster de conmutación por error de Kaspersky Security Center Linux.
- Ahora puede especificar un esquema de base de datos personalizado al instalar Kaspersky Security Center Linux.
- En **Supervisión** → **Panel**, el indicador de nivel de protección le ayuda a evaluar la seguridad del Servidor de administración y de los puntos de distribución. Si el indicador está en amarillo o rojo, debe tomar medidas para resolver los problemas y que el estado del indicador cambie a verde.
- Hay disponible un método simplificado para el despliegue de Kaspersky Security Center Linux. Ahora puede usar un script de instalación.
- Hay disponible un paquete de distribución especial para el Agente de red de Kaspersky para Linux Legacy con glibc versión 2.5 para admitir los siguientes sistemas operativos obsoletos:
  - CentOS 5.2
  - CentOS 5.4
  - CentOS 6.4
  - CentOS 6.6
  - Astra Linux Special Edition RUSB.10015-01 (actualización operativa 1.4) (64 bits)
- El Agente de red ahora es compatible con las siguientes nuevas versiones de sistemas operativos:
  - Microsoft Windows 11 IoT Enterprise versión 25H2 (64 bits)
  - SberOS 3.6.1
  - Ubuntu Server 26.04 LTS
- Los siguientes DBMS ya no son compatibles:
  - MySQL 5.7
  - MariaDB 10.1.30

- Mejoras en la experiencia del usuario:
  - Se mejoró el filtrado de las tablas **Tareas** y **Directivas**. Ahora puede agregar varias condiciones mediante la lógica `OR`, así como usar un nuevo operador que le permite seleccionar varios valores para una sola propiedad y mostrar registros que coincidan con al menos uno de los criterios especificados.
  - En el menú principal:
    - Hay una nueva sección **Administración de software** disponible. Las siguientes secciones ahora se trasladaron a **Administración de software**: **Paquetes de instalación**, **Aplicaciones de Kaspersky**, **Aplicaciones de terceros**, **Catálogo de software de Kaspersky** y **Administración de parches**.
    - Las secciones **Dispositivos no asignados** y **Hardware** ahora se trasladaron a **Administración de activos**.
    - Las secciones **Tareas** y **Repositorios** se trasladaron al primer nivel del menú.
    - La sección **Copias de seguridad de complementos web** ya no se usa y se eliminó de Web Console.

Kaspersky Security Center 16.2 Linux



Descripción general de las nuevas funciones de la versión 16.2. Video

Kaspersky Security Center 16.2 Linux presenta un número de mejoras y características nuevas.

- En Kaspersky Security Center Web Console, ahora puede configurar una pasarela de conexión en la zona desmilitarizada (DMZ).

  Utilice la opción **Utilizar pasarela de conexión DMZ por dirección** para configurar una puerta de enlace de conexión.

- Se mejoró el algoritmo para conservar el identificador del dispositivo del Agente de red (el parámetro `Device ID`) en dispositivos Linux. Si el número de serie del BIOS, el número de serie de la placa base, los identificadores del disco de almacenamiento o la dirección MAC de un dispositivo coinciden con valores ya conocidos, el Servidor de administración identifica correctamente el dispositivo como detectado anteriormente después de una actualización del sistema operativo o un cambio de dirección MAC.

- Se agregó compatibilidad para un clúster de conmutación por error de Kaspersky Security Center Linux distribuido geográficamente con nodos ubicados en diferentes centros de datos. En la configuración del clúster distribuido geográficamente, todos los componentes son de conmutación por error.

- Ahora puede exportar eventos a un sistema SIEM en los formatos CEF o LEEF.
- Se agregó compatibilidad para el clúster de PostgreSQL de alta disponibilidad con Patroni para la conmutación por error automatizada y HAProxy para el equilibrio de carga.
- Puede comparar las revisiones de la directiva. La opción está disponible para las directivas del Servidor de administración, el Agente de red, Kaspersky Endpoint Security para Windows (a partir de la versión 14.0 del complemento web) y Kaspersky Endpoint Security for Mac (a partir de la versión 12.2.1 Parche A del complemento web). La lista de aplicaciones de Kaspersky que admiten esta función se ampliará en versiones futuras.
- Ahora se admite SNMP. Puede proporcionar información, estadísticas y eventos del Servidor de administración a aplicaciones cliente de terceros mediante SNMP.
- El sondeo de red de Windows ahora es compatible con los puntos de distribución basados en Windows.
- Ahora está disponible un paquete de instalación único para el Agente de red para Linux. Este paquete de instalación incluye versiones para diferentes administradores de paquetes y arquitecturas de CPU. Durante la instalación, el entorno se detecta automáticamente y se instala el paquete del Agente de red correspondiente.
- Los eventos ahora incluyen información sobre el iniciador de comandos ejecutados en los dispositivos móviles.
- El componente NSQ se elimina del paquete de distribución de Kaspersky Security Center Web Console. El servicio KSCWebConsoleMessageQueue.service ya no se utiliza y se eliminará después de la actualización de Kaspersky Security Center Web Console.
- Si el Servidor de administración no tiene acceso al repositorio de distribuciones de aplicaciones para la instalación remota, antes de crear paquetes de instalación a partir de un archivo para aplicaciones en dispositivos Windows, debe descargar módulos adicionales del sitio web de Kaspersky: Archivos para la instalación remota mediante Kaspersky Security Center (los archivos ri_utils_win32.zip y ri_utils_arm64.zip).
- El Agente de red ahora es compatible con la arquitectura de Windows ARM de 64 bits. La compatibilidad con las aplicaciones administradas se puede verificar en la documentación de Ayuda correspondiente.
- Kaspersky Security Center Linux es compatible con Kaspersky Sandbox.
- Mejoras en la experiencia del usuario:
  - Ahora puede eliminar todos los eventos de una selección de eventos y de una lista de eventos del dispositivo a la vez.

    Las opciones **Seleccionar todo** y **Seleccionar todo en la página actual** están disponibles en la selección de eventos y en la lista de eventos del dispositivo.
  - Ahora puede especificar la prioridad de una regla de movimiento manualmente.

    El botón **Cambiar prioridad** está disponible cuando selecciona una regla de movimiento y le permite especificar la nueva prioridad.
- Kaspersky Security Center Linux es compatible con Platform V SberLinux OS Server (SLO) 9.6.
- Kaspersky Security Center Linux ahora permite utilizar los siguientes DBMS:
  - MySQL Standard Edition 8.4
  - MySQL Enterprise Edition 8.4
  - PostgreSQL 18

- Postgres Pro 18 (todas las ediciones)
- Postgres Pro 18 Enterprise (clúster de alta disponibilidad incorporado)

- El Agente de red ahora es compatible con las siguientes nuevas versiones de sistemas operativos:
  - Microsoft Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education ARM
  - Platform V SberLinux OS Server (SLO) 9.6

Kaspersky Security Center 16.1 Linux

Kaspersky Security Center 16.1 Linux presenta un número de mejoras y características nuevas.

- La autenticación de dos factores ahora está habilitada de manera predeterminada. La opción global para deshabilitar la autenticación de dos factores ya no está disponible. Para asegurarse de que los usuarios puedan iniciar sesión en Kaspersky Security Center Web Console y continuar usando los scripts de automatización de OpenAPI, habilite la autenticación de dos factores para todos los usuarios antes de la actualización.
- Ahora puede guardar un perfil de directiva en un archivo KLPROF sin exportar una directiva y luego usar este archivo KLPROF para importar el perfil guardado a la directiva.
- El Agente de red ahora funciona en un Dispositivo que ejecuta ALT OS en el modo de entorno de software cerrado.
- Se agregó soporte para la autenticación de dominio basada en Kerberos para usuarios de dominio sin contraseña mediante el uso del protocolo SCRIL, que permite el inicio de sesión único (SSO) basado en certificados.
- Mejoras en la experiencia del usuario:
  - El filtrado de dispositivos cliente por versión del sistema operativo y operador de paquetes ahora incluye versiones del sistema operativo Linux.
  - Se mejoró el mecanismo de paginación de tablas en la consola web de Kaspersky Security Center: la cantidad predeterminada de elementos mostrados aumentó a 50 y ahora se conserva la cantidad personalizada de elementos mostrados entre sesiones.
  - Comentarios para categorías de aplicaciones que le permiten agregar descripciones de reglas para incluir y excluir aplicaciones dentro de una categoría.
  - De manera predeterminada, la lista de paquetes de instalación disponibles ahora solo muestra los paquetes de instalación de la aplicación de Kaspersky en el idioma de la interfaz de Kaspersky Security Center Web Console y en inglés.
- Kaspersky Security Center Linux es compatible con Kaspersky Endpoint Security for Linux 12.4.

- Kaspersky Security Center Linux es compatible con las siguientes nuevas versiones de sistemas operativos:
  - Debian GNU/Linux 13 (Trixie)
  - CentOS Stream 10
  - Red Hat Enterprise Linux Server 10.x
- El Agente de red ahora es compatible con las siguientes nuevas versiones de sistemas operativos:
  - ALT Workstation 11
  - ALT Server 11
  - ALT Education 11
  - AlterOS 2025
  - SberOS 3.4.0
  - SberOS 3.5.0
  - OSnova 3.*

Kaspersky Security Center 16 Linux

Kaspersky Security Center 16 Linux presenta un número de mejoras y características nuevas.

- Se admiten los controladores de dominio FreeIPA y ALD Pro.
- Se implementó la autenticación de dominio (inicio de sesión único). La función de inicio de sesión único le permite habilitar la autenticación segura en Kaspersky Security Center 16 Web Console sin tener que volver a ingresar la contraseña en la red corporativa. Para utilizar la autenticación de dominio, debe especificar los parámetros adicionales en el archivo de respuesta durante la instalación de Kaspersky Security Center Web Console.
- El Servidor de administración de Kaspersky Security Center 16 Linux solo es compatible con Kaspersky Security Center 16 Web Console. No se pueden utilizar versiones anteriores de Kaspersky Security Center Web Console.
- Ahora puede usar las funcionalidades de Kaspersky Next XDR Optimum con una licencia de prueba, siempre que haya agregado un Servidor de administración secundario, activado dicho servidor con la licencia de prueba e implementado la clave de licencia en los dispositivos administrados mediante el Servidor de administración secundario.
- Mejoras en la experiencia del usuario:
  - Se actualizó la navegación mediante los grupos de administración y los Servidores de administración. Ahora puede cambiar fácilmente entre grupos y Servidores desde un solo panel de navegación.
  - La configuración del perfil se movió al panel superior.

- Se modificó el nombre de las siguientes secciones del menú principal:
  - La sección **Activos (Dispositivos)** ahora se llama **Administración de activos**.
  - **Dispositivos administrados** ahora se llama **Dispositivos administrados**.
  - **Vínculos rápidos** ahora se llama **Navegación por la consola**.
- Si lo desea, puede minimizar el menú principal y visualizar íconos.
- Se eliminó la sección de **novedades de Kaspersky**, en **Supervisión → Notificaciones**.

- Los filtros que utiliza en las tablas en las secciones **Operaciones → Administración de parches → Vulnerabilidades de software** y **Operaciones → Administración de parches → Actualizaciones de software** ahora se guardan correctamente y no se modifican.
- Kaspersky Security Center Linux es compatible con:
  - Con Kaspersky NGFW
  - Estas versiones de los siguientes sistemas operativos (para los dispositivos administrados):
    - MosOS 15.5 Arbat
    - Microsoft Windows 11 25H2
    - CentOS 6.4
    - CentOS 6.6

Kaspersky Security Center 15.4 Linux

Kaspersky Security Center 15.4 Linux presenta un número de mejoras y características nuevas.

- Los perfiles de conexión para usuarios fuera de la oficina con dispositivos Linux ya están disponibles. A través de estos perfiles, puede configurar reglas que hagan que, dependiendo de la ubicación de los dispositivos Linux, las copias del Agente de red instaladas en esos equipos se conecten a un mismo Servidor de administración o a servidores de administración diferentes.
- Ahora se encuentra disponible la transmisión de claves de cifrado entre Servidores de administración.
- Kaspersky Thin Client ahora es compatible.
- El clúster de alta disponibilidad integrado de Platform V Pangolin ahora es compatible.
- Ahora se admite el clúster de alta disponibilidad integrado de Postgres Pro. Los nodos de este clúster de DBMS se especifican en la cadena de conexión al instalar Kaspersky Security Center Linux.

- Kaspersky Security Center Linux ahora permite utilizar los siguientes DBMS:
  - Platform V Pangolin 6.5.1
  - Tantor SE 1C para Astra Linux Special Edition RUSB.10015-01 (actualización operativa 1.8)
  - Jatoba 5
- Compatibilidad con Platform V SberLinux OS Server (SLO) versiones 8.10.1, 9.0.1, 9.5.1.
- El archivo KlAkOAPI.tar.gz se elimina de la Ayuda. El archivo KlAkOAPI.tar.gz se encuentra en la carpeta de instalación de Kaspersky Security Center Linux.
- El botón **Analizar** se elimina de la sección **Cuarentena**.
- La información sobre el tamaño, el hash del archivo y la ruta ya no está disponible en la lista de paquetes de instalación del paquete independiente del Agente de red o de cualquier paquete creado en los Servidores de administración virtuales, ya que estos paquetes independientes se generan en el momento de la descarga.

Kaspersky Security Center 15.4 Linux con licencia de Kaspersky Next XDR Optimum

Si activó el Servidor de administración con la licencia de Kaspersky Next XDR Optimum e implementó la clave de licencia de Kaspersky Next XDR Optimum en sus aplicaciones administradas, puede hacer lo siguiente:

- Agrupar alertas por atributos.
- Integraciones para responder a alertas.

Kaspersky Security Center 15.3 Linux

Kaspersky Security Center 15.3 Linux presenta un número de mejoras y características nuevas.

- La utilidad klcsngtgui se elimina del kit de distribución de Kaspersky Security Center Linux. Recomendamos usar la utilidad klnagchk en lugar de la utilidad klcsngtgui.
- El Agente de red ahora es compatible con las siguientes nuevas versiones de sistemas operativos:
  - Windows Server 2025
  - Fedora Linux Server 41
  - Fedora Linux Workstation 41
- Kaspersky Security Center Linux ahora permite utilizar los siguientes DBMS:
  - PostgreSQL 17
  - Postgres Pro 17

- Ahora puede descargar solo las actualizaciones requeridas de las bases de datos y los módulos de software para las aplicaciones de seguridad de Kaspersky mediante la Kaspersky Update Utility. En la ventana de propiedades de la tarea **Descargar actualizaciones en el repositorio del Servidor de administración**, active la opción **Descargar automáticamente el archivo de solicitud de actualización** y, a continuación, especifique la ruta donde Kaspersky Security Center Linux creará el archivo de solicitud de actualización con información sobre las actualizaciones que se descargarán.

- Ahora está disponible la visualización de estadísticas de uso del servidor proxy de KSN.

- Se actualizó la migración de los datos del Servidor de administración de Kaspersky Security Center Windows a Kaspersky Security Center Linux mediante la utilidad klbackup. Ahora puede migrar los datos del Servidor de administración almacenados en las bases de datos de Microsoft SQL Server a PostgreSQL o Postgres Pro.

- Ahora está disponible la configuración de la dirección de conexión del Servidor de Administración. La dirección de conexión del Servidor de administración se utiliza como dirección predeterminada al crear los paquetes de instalación del agente de red y como dirección del servidor proxy de KSN al conectar dispositivos administrados a KSN.

- Ahora puede reiniciar de forma central los dispositivos administrados.

- La información sobre los usuarios con sesión iniciada en el dispositivo administrado con Linux ahora se muestra en la sección **General** → **Sesiones** de la ventana de propiedades del dispositivo.

- Ahora puede obtener acceso remoto a los dispositivos administrados con Linux y Windows a través del Agente de red instalado en estos dispositivos. La conexión se establece mediante RDP, VNC o WDS. Al establecer una conexión con el dispositivo, el administrador obtiene acceso completo a la información almacenada en este dispositivo, de manera que puede administrar las aplicaciones instaladas en él.

- Cargue y ejecute una aplicación (o script) para realizar diagnósticos en un dispositivo administrado. Ahora puede cargar el directorio o el archivo comprimido que contiene el archivo ejecutable, o directamente el archivo ejecutable. Una vez ejecutada correctamente la aplicación, puede descargar los resultados de la ejecución.

- Mejoras en la experiencia del usuario, incluida la nueva sección **Vínculos rápidos**. En esta sección, se muestra el mapa del menú principal y le proporciona acceso rápido a todas las secciones de Kaspersky Security Center Web Console. De forma predeterminada, la sección **Vínculos rápidos** está configurada como página de inicio.

Kaspersky Security Center 15.2 Linux

Kaspersky Security Center 15.2 Linux presenta un número de mejoras y características nuevas.

- Nuevas funciones para la administración de contraseñas de las cuentas de usuarios internos:

  - Ahora puede requerir que un usuario interno cambie su contraseña en el próximo intento de inicio de sesión en Kaspersky Security Center Web Console.

  - Nueva opción para configurar el periodo de caducidad de las contraseñas de las cuentas de usuarios internos.

- Ahora puede hacer una copia de seguridad de los datos del Servidor de administración de Windows de Kaspersky Security Center y restaurarlos en Kaspersky Security Center Linux mediante la utilidad klbackup. La migración se puede realizar sin pérdida de datos entre DBMS del mismo tipo, o Microsoft SQL Server → MySQL o MariaDB.

- Kaspersky Security Center Linux ahora permite utilizar los siguientes DBMS:
  - PostgreSQL 16.x
  - Postgres Pro 16.x
- Kaspersky Security Center Linux ahora es compatible con algunos tipos de clústeres de PostgreSQL y Postgres Pro.
- Compatibilidad con nuevos sistemas operativos y nuevas versiones de sistemas operativos, entre ellos, los más recientes de OS MES (Moscow Electronic School), MosTech y MosTech Server.
- Mejoras en la experiencia del usuario, entre ellas:
  - Nuevo botón **Guardar** en la ventana de configuración de la directiva. Utilice este botón si desea guardar los cambios sin cerrar la ventana de configuración de la directiva.
- Ahora puede administrar el envío de archivos a dispositivos Android, eliminar los archivos enviados anteriormente y configurar sus ajustes en la nueva sección "Apps y archivos" del complemento Protección y administración de dispositivos móviles de Kaspersky.
- Ahora puede transferir paquetes de instalación de aplicaciones y perfiles de administración de dispositivos a dispositivos móviles sin conectarlos directamente al Servidor de administración mediante un nuevo servicio de servidor web en una pasarela de conexión.

Kaspersky Security Center 15.1 Linux

Kaspersky Security Center 15.1 Linux presenta un número de mejoras y características nuevas.

- Kaspersky Security Center Web Console ahora admite la administración de dispositivos móviles a través del complemento Kaspersky Mobile Devices Protection and Management.
- Ahora puede instalar y configurar servidores MDM de iOS a través del complemento de configuración del servidor MDM de iOS para administrar dispositivos MDM de iOS.
- Ahora puede administrar certificados de dispositivos móviles.
- Ahora se admite Kaspersky Endpoint Security for Android.
- Ahora se admite Kaspersky Security for iOS.
- Ahora se admite Kaspersky Endpoint Security for Aurora.
- Administración de vulnerabilidades y parches para dispositivos administrados basados en Windows. Puede administrar las actualizaciones del software de terceros instaladas en los dispositivos administrados basados en Windows y reparar las vulnerabilidades de dicho software mediante la instalación de las actualizaciones necesarias.
- Kaspersky Security Center Linux ahora sondea los controladores de dominio página por página en lugar de sondear todo el controlador de dominio a la vez. Esto le permite sondear controladores de dominio que incluyen una gran cantidad de entradas.

- Control de anomalías adaptativo. Esta es una función de Kaspersky Endpoint Security para Windows que utiliza un conjunto de reglas para rastrear comportamientos atípicos en los dispositivos cliente y le permite bloquear acciones anómalas.

- Actualizaciones sin interrupciones para las aplicaciones administradas de Kaspersky instaladas en dispositivos Windows y el Agente de red para Linux. Puede administrar el proceso de instalación de actualizaciones aprobando las actualizaciones que deben instalarse y rechazando las que no deben instalarse.

- Auditoría de directivas ampliada. Ahora puede ver el contenido de una revisión de la directiva y guardarla en un archivo. Actualmente, estas funciones solo están disponibles para la directiva del Servidor de administración y la directiva del Agente de red.

- Cloud Discovery. Es una función nueva que le permite supervisar el uso de los servicios en la nube en los dispositivos administrados con Windows y bloquear el acceso a los servicios en la nube que considere no deseados.

- Nueva subsección **Alertas** en la sección **Supervisión** del menú principal. En la subsección **Alertas**, podrá ver información sobre la detección de amenazas en los endpoints. Las aplicaciones de seguridad de Kaspersky detectan las amenazas.

- Kaspersky Security Center Linux ahora puede actuar como un componente de la solución Kaspersky Managed Detection and Response.

- Soporte para Kaspersky Security for Virtualization Light Agent.

- Inventario ampliado de hardware de dispositivos macOS. El Agente de red en un dispositivo macOS envía la dirección MAC y el número de serie del dispositivo al Servidor de administración.

- Ahora puede recibir un informe sobre la instalación remota cuando instale software en los dispositivos administrados mediante scripts personalizados.

- Cuando ejecuta varios scripts personalizados en un dispositivo administrado, puede establecer la prioridad de cada script para definir el orden de ejecución. Los scripts se ejecutarán de mayor a menor prioridad.

- Para reducir la cantidad de RAM consumida por Kaspersky Endpoint Security for Linux y el Agente de red para Linux, puede habilitar un modo de trabajo especial para el Agente de red para Linux. En este modo, el Agente de red para Linux requiere menos RAM, pero su funcionalidad es limitada.

- Puede desinstalar un software incompatible de los dispositivos administrados mediante la tarea *Desinstalar aplicación de forma remota*.

- El Informe de ataques de red ahora incluye la dirección MAC y el puerto del dispositivo atacante.

- La longitud máxima de la contraseña para un usuario interno aumentó a 256 caracteres.

- Mejoras en la experiencia del usuario, entre ellas:

  - Personalización del menú principal mediante la adición de secciones de Kaspersky Security Center Web Console a marcadores para un acceso rápido desde la sección **Marcadores**.

  - Trabajo optimizado con tablas. La vista predeterminada de cada tabla ahora contiene las columnas más usadas. Además, ahora puede seleccionar todos los elementos de la página actual o de toda la tabla, así como ordenar los elementos de toda la tabla.

  - Mejora en la configuración de la entrega de informes. Ahora puede especificar la programación de entrega del informe y hasta 20 direcciones de correo electrónico a las cuales enviar el informe.

- Soporte para nuevas versiones y una amplia variedad de sistemas operativos.
- Se desarrolló y publicó una nueva Guía de dimensionamiento en la Ayuda en línea.
- Como resultado de una revisión de la interfaz de usuario, se resolvió un problema que provocaba que la sección **Diagnóstico remoto** apareciera en la ventana de propiedades del Servidor de administración.
- Puede crear una tarea *Ejecutar scripts de forma remota* para ejecutar un paquete de instalación en un dispositivo cliente e instalar una aplicación de forma remota.
- Se puede asignar un usuario como propietario del dispositivo durante o después de la instalación del Agente de red en un dispositivo cliente en Linux.
- Puede configurar una selección de dispositivos o crear una regla de movimiento de dispositivo según el propietario, la pertenencia a un grupo de seguridad y el rol del dispositivo.
- Puede revocar los derechos de administrador local de las cuentas. Ello brinda una capa de control adicional sobre las cuentas de usuario. Los derechos de administrador local pueden revocarse, por ejemplo, una vez que finaliza un encargo puntual.
- Puede cambiar la contraseña de la cuenta local, por ejemplo, cuando el usuario olvida la contraseña de la cuenta local o para realizar un cambio de contraseña programado.
- En la subsección **Administración de certificados de usuario**, puede especificar qué certificados raíz instalar. Estos certificados se pueden utilizar, por ejemplo, para verificar la autenticidad de sitios web o servidores web.

Kaspersky Security Center 15 Linux

Kaspersky Security Center 15 Linux presenta un número de mejoras y características nuevas.

- El sondeo del controlador de dominio le permite sondear un controlador de dominio de Microsoft Active Directory y un controlador de dominio Samba. Puede utilizar el Servidor de administración o un punto de distribución para sondear Microsoft Active Directory. Puede sondear un controlador de dominio Samba solo a través de un punto de distribución basado en Linux. Cuando sondea un controlador de dominio, el Servidor de administración o un punto de distribución recupera información sobre la estructura del dominio, las cuentas de usuario, los grupos de seguridad y los nombres DNS de los dispositivos incluidos en el dominio.
- Kaspersky Security Center Linux ahora permite utilizar los siguientes DBMS:
  - PostgreSQL 15.x
  - Postgres Pro 15.x
- Si utiliza PostgreSQL o Postgres Pro como DBMS, Kaspersky Security Center Linux admite hasta 50 000 dispositivos administrados.
- Migración de Kaspersky Security Center Windows a Kaspersky Security Center Linux. Puede ejecutar un asistente para migrar objetos de Kaspersky Security Center, incluidas tareas, directivas y estructuras de grupos de administración. Después de eso, puede mover los dispositivos administrados importados para que estén bajo la administración de Kaspersky Security Center Linux.

- Kaspersky Security Center Linux ahora permite utilizar las siguientes aplicaciones de Kaspersky:
  - Kaspersky Security for Virtualization Light Agent
  - Kaspersky Embedded Systems Security para Windows
  - Kaspersky Embedded Systems Security para Linux
  - Kaspersky Industrial CyberSecurity for Nodes
  - Kaspersky Industrial CyberSecurity for Networks
  - Kaspersky Endpoint Security for Mac
  - Kaspersky Endpoint Agent
  - Kaspersky Security for Virtualization Light Agent
- Diagnóstico remoto de dispositivos administrados basados en Windows y Linux.
- Componente de control de aplicaciones mejorado. Ahora puede crear una categoría de aplicación basada en la lista de archivos ejecutables de una carpeta seleccionada o en función de una categoría de aplicación de Kaspersky. Luego, puede especificar si desea permitir o bloquear las aplicaciones de la categoría creada en su organización.
- Exportación e importación de selecciones de eventos. Puede exportar una selección de eventos definida por el usuario y su configuración a un archivo KLO y luego importar la selección de eventos guardada a Kaspersky Security Center Windows o Kaspersky Security Center Linux.
- En el Informe de amenazas, ahora puede abrir una cadena de desarrollo de amenazas haciendo clic en el vínculo **Ver alerta**.
- Kaspersky Security Center Linux ahora es compatible con tecnología de clústeres. Si un grupo de administración contiene clústeres o conjuntos de servidores, la página **Dispositivos administrados** muestra dos pestañas: una para dispositivos individuales, y otra para clústeres y conjuntos de servidores. Una vez que los dispositivos administrados se detectan como nodos de clúster, el clúster se agrega como un objeto individual a la pestaña **Clústeres y conjuntos de servidores**. Los nodos del clúster aparecen en la pestaña **Dispositivos**, junto con otros dispositivos administrados.
- Se discontinuó la compatibilidad de Kaspersky Security Center Linux con algunas plataformas porque sus proveedores ya no ofrecen el soporte.

Kaspersky Security Center 14.2 Linux

Kaspersky Security Center 14.2 Linux presenta un número de mejoras y características nuevas.

- Ahora, en una jerarquía de servidores de administración, un Servidor de administración instalado en Linux puede actuar como Servidor principal y administrar servidores secundarios instalados en Linux o Windows.
- Kaspersky Security Center Linux ahora es compatible con Kaspersky Security Network (KSN), con el servicio del proxy de KSN y con Kaspersky Private Security Network (KPSN).

- Kaspersky Security Center Linux ahora admite Kaspersky Endpoint Security para Windows como aplicación administrada.

  Para instalar el Agente de red para Windows en dispositivos cliente remotos, deben utilizarse las herramientas del sistema operativo a través de puntos de distribución basados en Windows.

- Ahora, la información almacenada en dispositivos Windows administrados puede cifrarse para reducir el riesgo de que se filtren datos corporativos o confidenciales ante el robo o extravío de un disco duro o una computadora portátil. Esta función se implementa a través de Kaspersky Endpoint Security para Windows.

- Kaspersky Security Center Linux permite descargar y actualizar tanto paquetes de distribución de aplicaciones Kaspersky como complementos web de administración directamente desde la interfaz de usuario de Kaspersky Security Center Linux.

- De manera predeterminada, se envía información al Servidor de administración sobre las aplicaciones instaladas en los dispositivos Windows y Linux administrados.

- Ahora, se verifica automáticamente que haya acceso a los servidores de Kaspersky. Si los servidores DNS configurados en el sistema no permiten acceder a los servidores de Kaspersky, la aplicación utiliza los servidores DNS públicos.

- Los datos confidenciales que se transfieren entre el Servidor de administración principal, los servidores de administración secundarios y los agentes de red ahora se protegen con el algoritmo de cifrado AES.

- Ahora es posible configurar derechos de usuario en un Servidor de administración virtual en cualquier momento y con independencia del Servidor de administración principal. Además, se pueden asignar a los usuarios de un Servidor principal los derechos necesarios para administrar un Servidor virtual.

- Kaspersky Security Center Linux ahora permite utilizar los siguientes DBMS:

  - PostgreSQL 13.x
  - PostgreSQL 14.x
  - Postgres Pro 13.x (todas las ediciones)
  - Postgres Pro 14.x (todas las ediciones)

- Puede usar Kaspersky Security Center Web Console para exportar directivas y tareas a un archivo y, luego, importar esas directivas y tareas en Kaspersky Security Center Windows o Kaspersky Security Center Linux.

- La opción **No usar servidor proxy** ya no está disponible en las siguientes tareas:

  - *Descargar actualizaciones en el repositorio del Servidor de administración*
  - *Descargar actualizaciones en los repositorios de los puntos de distribución*

Kaspersky Security Center 14 Linux

Kaspersky Security Center Linux presenta un número de mejoras y características nuevas:

- Además de con la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*, las bases de datos antivirus para las aplicaciones de seguridad de Kaspersky ahora se pueden descargar a través de la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución*.

- Las bases de datos antivirus y los módulos de aplicaciones en los dispositivos administrados se pueden propagar y actualizar a través del Servidor de administración o los puntos de distribución. Puede elegir un esquema de actualización óptimo para su organización, para reducir la carga en el Servidor de administración y optimizar el tráfico de datos en la red corporativa.

- Kaspersky Security Center Linux descarga de los servidores de actualización de Kaspersky solo aquellas actualizaciones solicitadas por las aplicaciones de seguridad de Kaspersky. Esto reduce el tamaño de los datos descargados.

- Ahora puede utilizar la función de archivos diff para descargar bases de datos antivirus y módulos de software. Un archivo diff describe las diferencias entre dos versiones de un archivo de una base de datos o de un módulo de software. El uso de archivos diff ahorra tráfico dentro de la red de su empresa porque los archivos diff ocupan menos espacio que los archivos completos de bases de datos y módulos de software.

- Se agregó la tarea *Verificación de actualizaciones*. Al utilizar esta tarea, puede verificar automáticamente la operatividad y los errores de las actualizaciones descargadas antes de instalar las actualizaciones en los dispositivos administrados.

- Kaspersky Security Center Linux ahora admite Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 como aplicación administrada.

Errores solucionados

En la siguiente tabla, se enumeran todos los problemas encontrados en versiones anteriores de Kaspersky Security Center Linux y resueltos en la versión actual.

Lista de problemas resueltos en Kaspersky Security Center Linux 17

Versión de Kaspersky Security Center Linux en la que apareció por primera vez el problema	ID del problema	Descripción del problema
16.2	10575601	Se solucionó el problema que impedía que la lista de grupos apareciera en la lista desplegable cuando estaba habilitada la opción **El dispositivo se encuentra en un subgrupo del grupo Dominios**.
16.3	10519188	Se solucionó un problema por el que la limpieza (`VACUUM`) de las tablas temporales ralentizaba el Servidor de administración.
16.3	10530831	Se solucionó el problema por el que los cambios realizados en la sección **Dispositivos administrados** no se guardaban después de cambiar el orden de las columnas.
16.3	10698217	Se solucionó el problema por el que, en las propiedades de un dispositivo administrado, al hacer clic en el vínculo **Registros de instalación remota** de la pestaña **Avanzado → Diagnóstico remoto → Registros de eventos**, la ventana que aparecía tenía el título **Registros de seguimiento del dispositivo**.
16.3	10696918	Se solucionó el problema por el que la ventana de búsqueda no se abría en el Servidor secundario, en la sección **Aplicaciones de terceros → Categorías de aplicaciones**, al acceder a las propiedades de una categoría en la pestaña **Condiciones**.
16.3	10720529	Se solucionó el problema por el que los datos se mostraban incorrectamente en la tabla de dispositivos administrados al usar el operador «≠» (distinto de) en el filtro **Última conexión con el Servidor de administración**.
16.3	10012561	Se solucionó el problema por el que el análisis de un dominio con SberLDAP no devolvía la estructura del dominio ni sus hosts.
16	9496192	Se solucionó el problema por el que, al hacer clic en el botón **Seleccionar todo** de la tabla **Selección de eventos** y luego exportar los eventos, solo se exportaban los de la página actual.
16.3	10292104	Se solucionó el problema por el que, en Kaspersky Security Center Web Console versión 15.1 o 15.2, si se actualizaba el complemento de Kaspersky Endpoint Detection and Response Optimum a la versión 16.3, la sección **Alertas** podía no mostrar las alertas.
16.3	10596319	Se solucionó el problema por el que, en la sección **Etiquetas** del formulario **Asignar etiqueta**, la lista de etiquetas se mostraba sin ordenar.
16.3	10127434	Se solucionó el problema por el que, al iniciar sesión en Kaspersky Security Center Web Console y acceder a la sección **Tareas** del Servidor de administración principal, el Servidor de administración virtual aparecía como el Servidor de administración principal en la ventana de jerarquía.
16.3	10252324	Se solucionó el problema por el que algunas aplicaciones de la selección de eventos generada por el componente **Control de apps** de la directiva de Kaspersky Endpoint Security no se agregaban a la sección **Categorías de aplicaciones**.
16.3	10308380	Se solucionó el problema por el que, después de crear una categoría de aplicaciones, no se abrían sus propiedades.
16.2	10698205	Se solucionó el problema por el que la sección **Clústeres y conjuntos de servidores** no se mostraba al seleccionar un clúster en la sección **Dispositivos administrados**, lo que impedía mover el clúster a un grupo.
16.3	10373324	Se solucionó el problema por el que no se tenía en cuenta el segundo nodo de clúster del clúster de conmutación por error de Kaspersky Security Center Linux al evaluar el estado del indicador de seguridad.

16.3	10563031	Se solucionó el problema que provocaba un error al actualizar el clúster de conmutación por error de Kaspersky Security Center Linux de la versión 16.2 a la 16.3 y de la versión 16 a la 16.3. El error era "Intento de cambiar el modo KLFOC durante la actualización. Se cancela".
16.3	10590796, 10590805	Se solucionó el problema por el que, al actualizar el nodo secundario del clúster de conmutación por error de Kaspersky Security Center, se producían los errores: "Error grave: ¡Está prohibido cambiar el modo de administración de KLFOC!" y "Error grave: No se puede obtener el nombre de la base de datos de KSC del almacenamiento de configuración".
16.3	10570574	Se solucionó el problema por el que, al reiniciar el servicio del Servidor de administración mientras se ejecutaba la tarea **Copia de seguridad de los datos del Servidor de administración**, la tarea se reiniciaba con el error "Ya hay una copia de seguridad en curso".
16.3	10085767	Se solucionó el problema por el que el alcance del informe podía mostrarse incorrectamente al migrar datos a Kaspersky Security Center Linux.
16.2	10135898	Se solucionó el problema por el que la sección **Configuración → Inicio de sesión único** no se cargaba si la sesión del usuario duraba más de una hora.
16.3	10542356	Se corrigió la validación errónea del campo **Dirección de correo electrónico** al editar un usuario en la sección **Usuarios y roles → Usuarios y grupos**.
16.3	10534809	Se solucionó el problema por el que los eventos de un dispositivo administrado tardaban mucho en cargarse. El tiempo de carga se redujo de 20 segundos a 2 segundos.
16.3	10537996	Se solucionó el problema por el que una pestaña del navegador con Kaspersky Security Center Web Console consumía más de 1,5 GB de RAM.
15.1	9067495	Se solucionó el problema por el que el botón **Comprobar conexión** estaba disponible al guardar la configuración de la conexión SIEM con el protocolo UDP.

Lista de problemas solucionados en Kaspersky Security Center Linux 16.3, actualización 1

Versión de Kaspersky Security Center Linux en la que apareció por primera vez el problema	ID del problema	Descripción del problema
16.3	10431901	Se solucionó un problema que hacía que la sección **Inicio de sesión único** no apareciera en el menú de Web Console. Por este motivo, los usuarios no podían configurar la autenticación de dominio mediante el protocolo Kerberos. La autenticación configurada previamente siguió funcionando.

Lista de problemas solucionados en Kaspersky Security Center Linux 16.3

Versión de Kaspersky Security Center Linux en la que apareció por primera vez el problema	ID del problema	Descripción del problema
16.2	9959974	Se solucionó el problema que hacía que la opción **Seleccionar todo** apareciera en la pestaña **Eventos** de la ventana de propiedades del dispositivo. Si se seleccionaba, podía provocar la eliminación de todos los eventos de la base de datos del Servidor de administración.
16.2	9392997	Se solucionó el problema que provocaba que se registrara un mensaje de error después de sondear correctamente un controlador de dominio ALD Pro o FreeIPA.
16.2	9504495	Se corrigió un problema que podía causar una asignación incorrecta de un usuario si el propietario del dispositivo se asignaba mediante los parámetros del paquete de instalación del Agente de red.
16.1	9316206	Se corrigió un problema por el cual los botones de control podían desaparecer de la pestaña **Autenticación de dos factores** al actualizar el navegador después de abrir la pestaña.
16.1	7555541	Se corrigió un problema que provocaba un error al iniciar sesión en Web Console si se habilitaba la opción **Establecer como contraseña de un solo uso (el usuario debe cambiar la contraseña después del primer inicio de sesión)** al crear la tarea *Cambiar contraseña de cuenta (solo Linux).*

15.4	7555788	Se corrigió un problema por el cual la tarea *Cambiar contraseña de cuenta* podía no funcionar correctamente si SELinux estaba habilitado en el dispositivo del usuario.
16.2	9603496	Se corrigió un problema por el cual era necesario instalar el Agente de red en el dispositivo del Servidor de administración para obtener información de diagnóstico sobre este dispositivo.
16.2	9704308	Se corrigió un problema por el cual abrir la sección **Jerarquía de grupos** durante la carga de la página en entornos con una gran cantidad de grupos de administración podía provocar un error `429 Too Many Requests`, interrumpir la conexión con el Servidor de administración y redirigir a los usuarios a la página de inicio de sesión.
16.2	9989231	Se corrigió un problema por el cual filtrar dispositivos por dirección IP de conexión podía devolver resultados incorrectos.
16.2	9990025	Se corrigió un problema por el cual la configuración de la vista de tabla en las secciones **Directivas** y **Tareas** no se conservaba al navegar entre páginas.
15.3	9632613	Se corrigió un problema por el cual el inicio de sesión de usuarios del dominio en Web Console podía retrasarse significativamente cuando los controladores de dominio LDAP no estaban disponibles o no contenían la cuenta de usuario.
15.1	9829027	Se corrigió un problema por el cual configurar el filtro **Estado de actualización** en el informe **Informe de uso de las bases de datos antivirus** podía producir un error.
15.1	9844707	Kaspersky Security Center y FCM (Firebase Cloud Messaging) interactuaban directamente, incluso si se había configurado un servidor proxy.

Lista de problemas solucionados en Kaspersky Security Center Linux 16.2

Versión de Kaspersky Security Center Linux en la que apareció por primera vez el problema	ID del problema	Descripción del problema
15.1	10071566	Se solucionó un problema por el cual los cambios realizados en una programación de tareas no se propagaban a los dispositivos administrados si la programación usaba la configuración "Por días de la semana".
15.4	9067754	Se solucionó un problema que causaba que los nuevos eventos se mostraran de forma incorrecta en una directiva creada anteriormente después de actualizar el complemento de Kaspersky Mobile Devices Protection and Management.
16	9329729	Se solucionó un problema por el cual aparecía un error en el Registro de eventos de Kaspersky después de actualizar Kaspersky Security Center Linux de la versión 16 a la versión 16.1 si la autenticación de dos factores se había configurado para ciertos usuarios antes de la actualización.
16.1	9256000	Se solucionó un problema por el cual la información acerca de los componentes de la aplicación administrada no estaba disponible si el Agente de red estaba instalado en Microsoft Windows XP.
16.1	9251629	Se solucionó un problema por el cual algunos encabezados de respuesta HTTP requeridos no se agregaban al iniciar sesión en Kaspersky Security Center Web Console.

Acerca del Kaspersky Security Center Linux

En esta sección, se brinda información sobre el objetivo, las características y los componentes principales de Kaspersky Security Center Linux. Se describen, además, las maneras en que se puede adquirir Kaspersky Security Center Linux.

Kaspersky Security Center Linux (también llamado Kaspersky Security Center) está diseñado para implementar y administrar la protección de dispositivos cliente mediante un Servidor de administración basado en Linux.

Kaspersky Security Center Linux le permite instalar aplicaciones de seguridad de Kaspersky en dispositivos mediante una red corporativa, ejecutar de forma remota tareas de análisis y actualización y administrar las directivas de seguridad de las aplicaciones administradas. Como administrador, puede utilizar un panel detallado que proporciona un panorama de los estados de los dispositivos corporativos, informes detallados y configuraciones granulares en las directivas de protección.

En comparación con la versión de Kaspersky Security Center que tiene un Servidor de administración basado en Windows®, Kaspersky Security Center Linux tiene un conjunto de características diferente.

Kaspersky Security Center Linux es una aplicación pensada para administradores de redes corporativas y empleados responsables de la protección de dispositivos para una amplia variedad de organizaciones.

Si utiliza Kaspersky Security Center, puede realizar lo siguiente:

- Crear una jerarquía de los Servidores de administración para administrar la red de la organización, como también las redes en las oficinas remotas o en las organizaciones cliente.

  La *organización cliente* es una organización cuya protección antivirus está garantizada por un proveedor de servicios.

- Crear una jerarquía de grupos de administración para administrar una selección de dispositivos cliente como si fueran una sola entidad.

- Administrar un sistema de protección antivirus desarrollado sobre la base de las aplicaciones de Kaspersky.

- Realizar la instalación remota de aplicaciones de Kaspersky y otros proveedores de software.

- Llevar a cabo el despliegue centralizado de las claves de licencia de las aplicaciones Kaspersky en dispositivos cliente, supervise su utilización y renueve las licencias.

- Recibir estadísticas e informes sobre el funcionamiento de las aplicaciones y dispositivos.

- Recibir notificaciones sobre eventos críticos en la operación de aplicaciones de Kaspersky.

- Administrar el cifrado de la información almacenada en unidades extraíbles y en los discos duros de los dispositivos Windows.

- Controlar el acceso de los usuarios a la información cifrada de dispositivos Windows.

- Realizar el inventario del hardware conectado a la red de la organización.

- Administrar de forma centralizada los archivos puestos en Cuarentena o Copia de seguridad por las aplicaciones de seguridad, y los archivos para los cuales se haya aplazado el procesamiento de parte de las aplicaciones de seguridad.

Puede comprar Kaspersky Security Center Linux a través de Kaspersky (por ejemplo, en https://latam.kaspersky.com/) o a través de empresas asociadas.

Si compra Kaspersky Security Center Linux a través de Kaspersky, puede copiar la aplicación de nuestro sitio web. La información requerida para la activación de la aplicación se envía por correo electrónico después del pago.

Es posible que la funcionalidad de las actualizaciones (incluida la provisión de actualizaciones de firmas antivirus y actualizaciones de base de código) y la funcionalidad de KSN no estén disponibles en el software en los EE. UU.

Kit de distribución

En el sitio web de Kaspersky, puede descargar todos los paquetes de distribución necesarios para la aplicación.

El kit de distribución de Kaspersky Security Center Linux incluye los siguientes archivos:

Servidor de administración de Kaspersky Security Center Linux:

- Servidor de administración que se instalará en un dispositivo que ejecuta el sistema operativo Debian:
  ksc64_17.0.0-<build>_amd64.deb
- Servidor de administración que se instalará en un dispositivo que ejecuta el sistema operativo Red Hat Enterprise Linux:
  ksc64-17.0.0-<build>.x86_64.rpm

Kaspersky Security Center Web Console:

- Web Console que se instalará en un dispositivo que ejecuta el sistema operativo Debian:
  ksc-web-console-17.0.<build>.x86_64.deb
- Web Console que se instalará en un dispositivo que ejecuta el sistema operativo Red Hat Enterprise Linux:
  ksc-web-console-17.0.<build>.x86_64.rpm

Script de instalación de Kaspersky Security Center:

- ksc_fast_install.tar.gz

Agente de red para Windows:

- Agente de red que se instalará en un dispositivo con arquitectura Arm:
  klnagent_winarm64-17.0.0.<build>-win_<localization>.zip
- Archivos para la instalación remota del Agente de red en un dispositivo con arquitectura x86-32 o x64:
  ksc_17_17.0.0.<build>_NetAgent_<localization>.zip
- Archivos para la instalación remota del Agente de red en un dispositivo con arquitectura Arm:
  ksc_17_17.0.0.<build>_NetAgent_arm64_<localization>.zip

- Archivos para la instalación remota mediante Kaspersky Security Center en un dispositivo con arquitectura Arm:

  ri_utils_arm64.zip

- Archivos para la instalación remota mediante Kaspersky Security Center en un dispositivo con arquitectura x86-32 o x64:

  ri_utils_win32.zip

Agente de red para Linux:

- Agente de red que se instalará en un dispositivo que ejecuta el sistema operativo Debian:

  klnagent64_17.0.0-<build>_<architecture>.deb

- Agente de red que se instalará en un dispositivo que ejecuta el sistema operativo Red Hat Enterprise Linux:

  klnagent64-17.0.0-<build>_<architecture>.rpm

- Archivos para la instalación remota del Agente de red en un dispositivo que ejecuta el sistema operativo Debian:

  klnagent-<architecture>-17.0.0.<build>-deb_<localization>.tar.gz

- Archivos para la instalación remota del Agente de red en un dispositivo que ejecuta el sistema operativo Red Hat Enterprise Linux:

  klnagent-<architecture>-17.0.0.<build>-rpm_<localization>.tar.gz

- Archivos para la instalación remota del Agente de red Elbrus Edition en un dispositivo que ejecuta un sistema operativo basado en Debian o Red Hat Enterprise Linux:

  klnagent-e2k-17.0.0.<build>-all-<localization>.tar.gz

- Paquete de distribución único para la instalación remota de los Agentes de red para Linux:

  klnagent-all-17.0.0.<build>-all_<localization>.tar.gz

  El paquete de distribución único puede ser útil si tiene muchos dispositivos cliente con diferente arquitectura de CPU y diferentes sistemas operativos basados en Linux. Las versiones requeridas de los Agentes de red se seleccionarán automáticamente para su posterior instalación en los dispositivos.

- Archivos para la instalación remota del Agente de red en un dispositivo que ejecuta un sistema operativo heredado basado en Debian o Red Hat Enterprise Linux con glibc 2.5:

  klnagent-all-17.0.0.<build>-glibc2.5-all-<localization>.tar.gz

Complemento web de Kaspersky Endpoint Detection and Response Optimum:

- signed_irp.zip

  Solo puede descargar el complemento web desde el Repositorio de paquetes de distribución de aplicaciones para la instalación remota.

Si le resulta difícil elegir un paquete de instalación para un Agente de red para Linux, consulte el artículo: Cómo elegir el paquete de instalación para el Agente de red para Linux.

Requisitos de hardware y software

- Requisitos del Servidor de administración
- Requisitos de Web Console
- Requisitos del Agente de red

Para conocer los requisitos de la versión de Android e iOS en el despliegue de la protección y administración de los dispositivos móviles, consulte la ayuda de Kaspersky Security para dispositivos móviles y la ayuda de Kaspersky Secure Mobility Management.

Requisitos del Servidor de administración

Este artículo enumera las versiones de software en las que se probó la aplicación y para las que se garantiza que funciona correctamente. La aplicación también puede funcionar con otras versiones de software, pero esas configuraciones no se sometieron a un ciclo de prueba completo y no se incluyen en la lista de versiones compatibles garantizadas.

Requisitos de hardware mínimos:

- CPU con frecuencia de operación de 2,5 GHz o superior, 2 núcleos.
- RAM: 6 GB

  Debe habilitar el archivo de intercambio en el dispositivo con el Servidor de administración instalado. El tamaño mínimo del archivo de intercambio debe ser 1.5 veces mayor que el volumen de RAM.
- Espacio disponible en disco: se requieren 10 GB para la carpeta donde se almacenan los datos del Servidor de administración (/var/opt/kaspersky/klnagent_srv).

Para obtener más información sobre los requisitos de hardware, consulte la sección Requisitos de hardware del DBMS y del Servidor de administración.

Recomendamos que, después de instalar el Servidor de administración en un dispositivo, instale Kaspersky Endpoint Security for Linux en ese dispositivo.
Para la instalación simultánea, debe tener un mínimo de 300 IOPS, así como agregar 1,5 GB de RAM y un 15 % de CPU a los requisitos del Servidor de administración.
Para conocer los requisitos de hardware de Kaspersky Endpoint Security, consulte la Ayuda de Kaspersky Endpoint Security for Linux.
Para obtener información sobre la configuración de seguridad necesaria para trabajar con Kaspersky Security Center Linux, consulte la Ayuda de Kaspersky Endpoint Security for Linux.

Se admiten los siguientes sistemas operativos:

Para la comunicación entre procesos en el sistema operativo, la interfaz de bucle invertido debe estar disponible.

- Debian GNU/Linux 12.0, 12.1, 12.2, 12.4, 12.5, 12.6, 12.7, 12.8, 12.9, 12.10, 12.11, 12.12, 12.13 (Bookworm) de 64 bits
- Debian GNU/Linux 13.0, 13.1, 13.2, 13.3 (Trixie) de 64 bits
- Ubuntu Server 22.04 LTS (Jammy Jellyfish) (64 bits)
- Ubuntu Server 24.04 LTS (Noble Numbat) (64 bits)
- Ubuntu Server 26.04 LTS (Resolute Raccoon) (64 bits)
- CentOS Stream 9 64 bits
- CentOS Stream 10 64 bits
- Red Hat Enterprise Linux Server 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 de 64 bits
- Red Hat Enterprise Linux Server 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10 de 64 bits
- Red Hat Enterprise Linux Server 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6 de 64 bits
- Red Hat Enterprise Linux Server 10.0, 10.1 de 64 bits
- SUSE Linux Enterprise Server 12.5, 12.6, 12.7 de 64 bits
- SUSE Linux Enterprise Server 15.0, 15.1, 15.2, 15.3, 15.4, 15.5, 15.6, 15.7 de 64 bits
- Astra Linux Special Edition RUSB.10015-01 (actualización operativa 1.6) (64 bits)
- Astra Linux Special Edition RUSB.10015-01 (actualización operativa 1.7) (64 bits)
- Astra Linux Special Edition RUSB.10015-01 (actualización operativa 1.8) (64 bits)
- Astra Linux Special Edition RUSB.10015-16 (versión 1) (actualización operativa 1.6) (64 bits)
- Astra Linux Special Edition RUSB.10015-17 (actualización operativa 1.7.3) (64 bits)
- Astra Linux Special Edition RUSB.10015-03 (actualización operativa 7.6) de 64 bits
- Astra Linux Special Edition RUSB.10015-37 (actualización operativa 7.7) (64 bits)
- Astra Linux Common Edition (actualización operativa 2.12) (64 bits)
- ALT Server 11 64 bits
- ALT SP Server 10 (64 bits)
- ALT SP Workstation 10 (64 bits)
- Oracle Linux 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 de 64 bits

- Oracle Linux 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9 de 64 bits
- Oracle Linux 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6 de 64 bits
- Platform V SberLinux OS Server (SLO) 8.10.1 (64 bits)
- Platform V SberLinux OS Server (SLO) 9.5.1 (64 bits)
- Platform V SberLinux OS Server (SLO) 9.6 (64 bits)
- Platform V SberLinux OS Server (SLO) 9.7 (64 bits)
- RED OS 7.3 Server (64 bits)
- RED OS 7.3 Certified Edition (64 bits)
- RED OS 8 (64 bits)
- ROSA COBALT 7.9 (64 bits)
- M OS (Moscow Electronic School) 12 Server de 64 bits
- Mostech Server de 64 bits
- MosOS 15.5 Arbat (64 bits)
- MosOS 15.6 (64 bits)

Le recomendamos que utilice el sistema de archivos EXT4 con su configuración predeterminada.

Se admiten los siguientes servidores de bases de datos (el servidor de bases de datos puede estar en un dispositivo diferente):

- MySQL Standard Edition 8.0 (versión 8.0.20 y posterior) de 32 bits o 64 bits
- MySQL Enterprise Edition 8.0 (versión 8.0.20 y posterior) de 32 bits o 64 bits
- MySQL Standard Edition 8.4 (32 bits o 64 bits)
- MySQL Enterprise Edition 8.4 (32 bits o 64 bits)
- MariaDB 10.11 (compilación 10.11.10 y versiones posteriores) (32 bits o 64 bits)
- MariaDB 11.4 (64 bits)
- MariaDB 11.8 (64 bits)
- MariaDB 12.3 (64 bits)
- MariaDB Galera Cluster 4 (32 bits o 64 bits)
- PostgreSQL 15.x (64 bits)
- PostgreSQL 15.x (64 bits) (clúster Corosync/Pacemaker)

- PostgreSQL 16.x de 64 bits
- PostgreSQL 17 (64-bits)
- PostgreSQL 18 (64 bits)
- Postgres Pro 15.x (64 bits) (todas las ediciones)
- Postgres Pro 15.x (64 bits) (clúster Corosync/Pacemaker)
- Postgres Pro 16.x de 64 bits (todas las ediciones)
- Postgres Pro 16.x Enterprise 64 bits (clúster de alta disponibilidad incorporado)
- Postgres Pro 17.x de 64 bits (todas las ediciones)
- Postgres Pro 17.x Enterprise 64 bits (clúster de alta disponibilidad incorporado)
- Postgres Pro 18.x de 64 bits (todas las ediciones)
- Postgres Pro 18.x Enterprise 64 bits (clúster de alta disponibilidad incorporado)
- Platform V Pangolin 6.5.1 (64 bits)
- Platform V Pangolin 6.5.1 (64 bits) (alta disponibilidad integrada en el clúster)
- Platform V Pangolin 7.2.0 (64 bits)
- Platform V Pangolin 7.2.0 (64 bits) (clúster de alta disponibilidad incorporado)
- Jatoba 4 (64 bits)
- Jatoba 5 (64 bits)
- Tantor SE 1C (64 bits)

Se admiten los clústeres PostgreSQL de alta disponibilidad. Consulte el siguiente artículo para obtener más información: Preparación de un clúster de DBMS de alta disponibilidad para trabajar con Kaspersky Security Center Linux.

Para obtener información sobre las plataformas de virtualización compatibles, consulte la Ayuda de Kaspersky Security for Virtualization Light Agent.

Requisitos de Web Console

Este artículo enumera las versiones de software en las que se probó la aplicación y para las que se garantiza que funciona correctamente. La aplicación también puede funcionar con otras versiones de software, pero esas configuraciones no se sometieron a un ciclo de prueba completo y no se incluyen en la lista de versiones compatibles garantizadas.

Servidor de Kaspersky Security Center Web Console

Requisitos de hardware mínimos:

- CPU: 2 núcleos, frecuencia de funcionamiento de 2.5 GHz.
- RAM: 4 GB
- Espacio disponible en disco: se requieren 40 GB para la carpeta donde se almacenan los datos de Web Console (/var/opt/kaspersky).

Le recomendamos que, después de instalar Kaspersky Security Center Web Console en un dispositivo, instale Kaspersky Endpoint Security for Linux en ese dispositivo. Para conocer los requisitos de hardware de Kaspersky Endpoint Security, consulte la Ayuda de Kaspersky Endpoint Security for Linux.

Uno de los siguientes sistemas operativos (**solo versiones de 64 bits**):

> Para la comunicación entre procesos en el sistema operativo, la interfaz de bucle invertido debe estar disponible.

- Debian GNU/Linux 12.0, 12.1, 12.2, 12.4, 12.5, 12.6, 12.7, 12.8, 12.9, 12.10, 12.11, 12.12, 12.13 (Bookworm)
- Debian GNU/Linux 13.0, 13.1, 13.2, 13.3 (Trixie)
- Ubuntu Server 22.04 LTS (Jammy Jellyfish)
- Ubuntu Server 24.04 LTS (Noble Numbat)
- Ubuntu Server 26.04 LTS (Resolute Raccoon)
- CentOS Stream 9
- CentOS Stream 10
- Red Hat Enterprise Linux Server 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9
- Red Hat Enterprise Linux Server 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10
- Red Hat Enterprise Linux Server 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6
- Red Hat Enterprise Linux Server 10.0, 10.1
- SUSE Linux Enterprise Server 12.5, 12.6, 12.7
- SUSE Linux Enterprise Server 15.0, 15.1, 15.2, 15.3, 15.4, 15.5, 15.6, 15.7
- Astra Linux Special Edition RUSB.10015-01 (actualización operativa 1.6)
- Astra Linux Special Edition RUSB.10015-16 (versión 1) (actualización operativa 1.6)
- Astra Linux Special Edition RUSB.10015-01 (actualización operativa 1.7)

- Astra Linux Special Edition RUSB.10015-17 (actualización operativa 1.7.3)
- Astra Linux Special Edition RUSB.10015-01 (actualización operativa 1.8)
- Astra Linux Special Edition RUSB.10015-03 (actualización 7.6)
- Astra Linux Special Edition RUSB.10015-37 (actualización operativa 7.7)
- Astra Linux Common Edition (actualización operativa 2.12)
- ALT Server 11
- ALT SP Server 10
- ALT SP Workstation 10
- Oracle Linux 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9
- Oracle Linux 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9
- Oracle Linux 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6
- Platform V SberLinux OS Server (SLO) 8.10.1
- Platform V SberLinux OS Server (SLO) 9.5.1
- Platform V SberLinux OS Server (SLO) 9.6
- Platform V SberLinux OS Server (SLO) 9.7
- RED OS 7.3 Server
- RED OS 7.3 Certified Edition
- RED OS 8
- ROSA COBALT 7.9
- M OS (Moscow Electronic School) 12 Server
- Mostech Server
- MosOS 15.5 Arbat
- MosOS 15.6

Para obtener información sobre las plataformas de virtualización compatibles, consulte la Ayuda de Kaspersky Security for Virtualization Light Agent.

Dispositivos cliente

Para un dispositivo cliente, el uso de Kaspersky Security Center Web Console solo requiere un navegador.

La resolución de pantalla mínimas es 1366x768 píxeles.

Los requisitos de hardware y software del dispositivo son los mismos que los del navegador utilizado con Kaspersky Security Center Web Console.

Navegadores:

- Google Chrome 149.0.7827.115 o versiones posteriores
- Microsoft Edge 149.0.4022.62 o versiones posteriores
- Safari 18.6 (20621.3.11.11.3) en macOS
- Yandex Browser 26.4.4.799 o versiones posteriores
- Versión de soporte extendido de Mozilla Firefox 140.11.0 o versiones posteriores

Requisitos del Agente de red

Este artículo enumera las versiones de software en las que se probó la aplicación y para las que se garantiza que funciona correctamente. La aplicación también puede funcionar con otras versiones de software, pero esas configuraciones no se sometieron a un ciclo de prueba completo y no se incluyen en la lista de versiones compatibles garantizadas.

Requisitos de hardware mínimos:

- CPU con una frecuencia operativa de 1 GHz o superior. Para sistemas operativos de 64 bits, la frecuencia mínima admisible es de 1.4 GHz.
- RAM: 512 MB.
- Espacio libre en disco: 1 GB.

Requisito de software para dispositivos basados en Linux: debe estar instalado el intérprete de lenguaje Perl versión 5.10 o superior.

Agente de red. Plataformas compatibles

Sistemas operativos. Estaciones de trabajo con Microsoft Windows	Microsoft Windows Embedded POSReady 2009 con el Service Pack más reciente (32 bits) Microsoft Windows Embedded 7 Standard con Service Pack 1 (32 bits o 64 bits) Microsoft Windows Embedded 8.1 Industry Pro (32 bits o 64 bits) Microsoft Windows 10 Enterprise 2015 LTSB (32 bits o 64 bits) Microsoft Windows 10 Enterprise 2016 LTSB (32 bits o 64 bits) Microsoft Windows 10 Enterprise 2019 LTSC (32 bits o 64 bits) Microsoft Windows 10 IoT Enterprise versión 1507, 1607, 1703, 1709, 1803, 1809, 1909 (32 bits o 64 bits) Microsoft Windows 10 20H2, 21H2 IoT Enterprise (32 bits o 64 bits) Microsoft Windows 10 TH1 (julio de 2015) Home/Pro/Pro for Workstations/Enterprise/Education (32 o 64 bits) Microsoft Windows 10 TH2 (noviembre de 2015) Home/Pro/Pro for Workstations/Enterprise/Education (32 o 64 bits) Microsoft Windows 10 RS1 (agosto de 2016) Home/Pro/Pro for Workstations/Enterprise/Education (32 o 64 bits) Microsoft Windows 10 RS2 (abril de 2017) Home/Pro/Pro for Workstations/Enterprise/Education (32 o 64 bits) Microsoft Windows 10 RS3 (Fall Creators Update, v1709) Home/Pro/Pro for Workstations/Enterprise/Education (32 bits o 64 bits) Microsoft Windows 10 RS4 (actualización de abril de 2018, 17134) Home/Pro/Pro for Workstations/Enterprise/Education (32 bits o 64 bits) Microsoft Windows 10 RS5 (octubre de 2018) Home/Pro/Pro for Workstations/Enterprise/Education (32 bits o 64 bits) Microsoft Windows 10 RS6 (mayo de 2019) Home/Pro/Pro for Workstations/Enterprise/Education (32 o 64 bits) Microsoft Windows 10 19H1, 19H2 Home/Pro/Pro for Workstations/Enterprise/Education (32 bits o 64 bits) Microsoft Windows 10 20H1 (actualización de mayo de 2020) Home/Pro/ Pro for Workstations/Enterprise/Education (32 bits o 64 bits) Microsoft Windows 10 20H2 (actualización de octubre de 2020) Home/Pro/Pro for Workstations/Enterprise/Education (32 bits o 64 bits) Microsoft Windows 10 21H1 (actualización de mayo de 2021) Home/Pro/Pro for Workstations/Enterprise/Education (32 bits o 64 bits) Microsoft Windows 10 21H2 (actualización de octubre de 2021) Home/Pro/Pro for Workstations/Enterprise/Education (32 bits o 64 bits) Microsoft Windows 10 22H2 (actualización de octubre de 2023) Home/Pro/Pro for Workstations/Enterprise/Education (32 bits o 64 bits) Microsoft Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education ARM (64 bits) Microsoft Windows 11 IoT Enterprise versión 25H2 (64 bits) Microsoft Windows 11 22H2 Home/Pro/Pro for Workstations/Enterprise/Education (64 bits) Microsoft Windows 11 23H2 Home/Pro/Pro for Workstations/Enterprise/Education (64 bits) Microsoft Windows 11 24H2 Home/Pro/Pro for Workstations/Enterprise/Education (64 bits) Microsoft Windows 11 25H2 Home/Pro/Pro for Workstations/Enterprise/Education (64 bits) Microsoft Windows 11 26H2 Home/Pro/Pro for Workstations/Enterprise/Education (64 bits) Microsoft Windows 8.1 Pro/Enterprise (32 bits o 64 bits) Microsoft Windows 8 Pro/Enterprise (32 bits o 64 bits) Microsoft Windows 7 Professional/Enterprise/Ultimate/Home Basic/Premium con Service Pack 1 y versiones posteriores (32 bits o 64 bits) Microsoft Windows XP Professional con Service Pack 2 de 32 bits o 64 bits (compatible solo con el Agente de red versión 10.5.1781) Microsoft Windows XP Professional con Service Pack 3 y versiones posteriores de 32 bits (compatible con la versión 14.0.0.20023 del Agente de red, requiere la actualización de seguridad para Windows XP KB2868626) Microsoft Windows XP Professional para sistemas integrados con Service Pack 3 de 32 bits (compatible con la versión 14.0.0.20023 del Agente de red)

Sistemas operativos. Servidores de Microsoft Windows	Microsoft Windows MultiPoint Server 2011 Standard/Premium (64 bits) Microsoft Windows Server 2003 SP1 de 32 o 64 bits (compatible solo con la versión 10.5.1781 del Agente de red, que puede solicitar al Soporte técnico) Microsoft Windows Server 2003 SP2 Standard/Enterprise 32 bits / 64 bits (compatible solo con la versión 10.5.1781 del Agente de red) Microsoft Windows Server 2003 R2 Standard/Enterprise con SP2 de 32 bits / 64 bits (compatible solo con la versión 10.5.1781 del Agente de red) Microsoft Windows Server 2008 Standard/Enterprise con Service Pack 2 (32 bits o 64 bits) Microsoft Windows Server 2008 R2 Datacenter/Enterprise/Foundation/Standard con Service Pack 1 y versiones posteriores (64 bits) Microsoft Windows Server 2012 Server Core/Datacenter/Essentials/Foundation/Standard (64 bits) Microsoft Windows Server 2012 R2 Server Core/Datacenter/Essentials/Foundation/Standard (64 bits) Microsoft Windows Server 2016 Datacenter/Standard/Server Core (opción de instalación) (LTSB) (64 bits) Microsoft Windows Server 2019 Standard/Datacenter/Core (64 bits) Microsoft Windows Server 2019 RS5 Essentials/Standard (64 bits) Microsoft Windows Server 2022 Standard/Datacenter/Core (64 bits) Microsoft Windows Server 2025 Standard/Datacenter/Core (64 bits) Microsoft Windows Server 2022 21H2 Standard/Datacenter (64 bits) Microsoft Windows Small Business Server 2011 Standard (64 bits) Microsoft Windows Small Business Server 2011 Essentials (64 bits)

Sistemas operativos. Linux	Debian GNU/Linux 10.0, 10.1, 10.2, 10.3, 10.4, 10.5, 10.6, 10.7, 10.8, 10.9, 10.10, 10.11, 10.12 (Buster) (32 o 64 bits) Debian GNU/Linux 11.0, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 11.7, 11.8, 11.9, 11.10, 11.11 (Bullseye) (32 o 64 bits) Debian GNU/Linux 12.0, 12.1, 12.2, 12.4, 12.5, 12.6, 12.7, 12.8, 12.9, 12.10, 12.11, 12.12, 12.13 (Bookworm) (32 o 64 bits) Debian GNU/Linux 12.10, 12.11, 12.14 (Bookworm) ARM (64 bits) Debian GNU/Linux 13.0, 13.1, 13.2, 13.3 (Trixie) de 64 bits Ubuntu Server 10.04 LTS (Lucid Lynx) (32 o 64 bits) Ubuntu Server 16.04 LTS (Xenial Xerus) (32 bits o 64 bits) Ubuntu Server 18.04 LTS (Bionic Beaver) (64 bits) Ubuntu Server 20.04 LTS (Focal Fossa) (64 bits) Ubuntu Server 22.04 LTS (Jammy Jellyfish) (64 bits) Ubuntu Server 22.04 LTS ARM (64 bits) Ubuntu Server 24.04 LTS (Noble Numbat) (64 bits) Ubuntu Server 26.04 LTS (Resolute Raccoon) (64 bits) Ubuntu Server 26.04 LTS ARM (64 bits) Ubuntu Desktop 10.04 LTS (Lucid Lynx) (32 o 64 bits) Ubuntu Desktop 16.04 LTS (Xenial Xerus) (32 bits o 64 bits) CentOS 5.2 (64 bits) (compatible solo con el Agente de red para Linux Legacy, que puede descargar mediante la interfaz de Web Console o desde el sitio web de Kaspersky) CentOS 5.4 (64 bits) (compatible solo con el Agente de red para Linux Legacy, que puede descargar mediante la interfaz de Web Console o desde el sitio web de Kaspersky) CentOS 6.4 (64 bits) (compatible solo con el Agente de red para Linux Legacy, que puede descargar mediante la interfaz de Web Console o desde el sitio web de Kaspersky) CentOS 6.6 (32 o 64 bits) (compatible solo con el Agente de red para Linux Legacy, que puede descargar mediante la interfaz de Web Console o desde el sitio web de Kaspersky) CentOS 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 (64 bits) CentOS Stream 8 (64 bits) CentOS Stream 9 (64 bits) CentOS Stream 9 ARM (64 bits) CentOS Stream 10 (64 bits) Red Hat Enterprise Linux Server 6.5, 6.6, 6.7, 6.8, 6.9, 6.10 (32 o 64 bits) Red Hat Enterprise Linux Server 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 (64 bits) Red Hat Enterprise Linux Server 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10 de 64 bits Red Hat Enterprise Linux Server 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6 de 64 bits Red Hat Enterprise Linux Server 10.0, 10.1 de 64 bits SUSE Linux Enterprise Server 12.5, 12.6, 12.7 de 64 bits SUSE Linux Enterprise Server 15.0, 15.1, 15.2, 15.3, 15.4, 15.5, 15.6, 15.7 de 64 bits SUSE Linux Enterprise Server 15.4, 15.5, 15.6, 15.7 ARM (64 bits) openSUSE Leap 15.0, 15.1, 15.2, 15.3, 15.4, 15.5, 15.6 (64 bits) EulerOS 2.0 SP10 (64 bits) EulerOS 2.0 SP10 ARM (64 bits) Astra Linux Special Edition RUSB.10015-01 (actualización operativa 1.4) (32 bits) Astra Linux Special Edition RUSB.10015-01 (actualización operativa 1.4) (64 bits) (compatible únicamente con el Agente de red para Linux Legacy, que puede descargar mediante la interfaz de Web Console o desde el sitio web de Kaspersky) Astra Linux Special Edition RUSB.10015-01 (actualización operativa 1.5) (64 bits) Astra Linux Special Edition RUSB.10015-01 (actualización operativa 1.6) (64 bits) Astra Linux Special Edition RUSB.10015-16 (versión 1) (actualización operativa 1.6) (64 bits) Astra Linux Special Edition RUSB.10015-16 (versión 2) (actualización operativa 8.1) E2K Astra Linux Special Edition RUSB.10015-17 (actualización operativa 1.7.3) (64 bits) Astra Linux Special Edition RUSB.10015-01 (actualización operativa 1.7) (64 bits) Astra Linux Special Edition RUSB.10015-01 (actualización operativa 1.8) (64 bits) Astra Linux Special Edition RUSB.10015-03 (actualización operativa 7.6) de 64 bits Astra Linux Special Edition RUSB.10015-37 (actualización operativa 7.7) (64 bits) Astra Linux Special Edition RUSB.10152-02 (actualización operativa 4.7) ARM (64 bits) Astra Linux Special Edition RUSB.10265-01 (actualización operativa 8.1) E2K Astra Linux Common Edition (actualización operativa 2.12) (64 bits) ALT Workstation 11.2 ARM (64 bits)

ALT Workstation 11 64 bits
ALT Server 11.1 ARM (64 bits)
ALT Server 11 64 bits
ALT Education 11 64 bits
ALT Workstation 10.1 (64 bits)
ALT Server 10.1 (64 bits)
ALT Education 10.1 (64 bits)
ALT SP Server 10 (32 bits o 64 bits)
ALT SP Server 10 ARM (64 bits)
ALT SP Server 10 E2K
ALT SP Workstation 10 (32 bits o 64 bits)
ALT SP Workstation 10 ARM (64 bits)
ALT SP Workstation 10 E2K
ALT 8 SP Server (LKNV.11100-01) (32 bits o 64 bits)
ALT 8 SP Server (LKNV.11100-02) (32 bits o 64 bits)
ALT 8 SP Server (LKNV.11100-03) (32 bits o 64 bits)
ALT SP Server 8 E2K
ALT 8 SP Workstation (LKNV.11100-01) (32 bits o 64 bits)
ALT 8 SP Workstation (LKNV.11100-02) (32 bits o 64 bits)
ALT 8 SP Workstation (LKNV.11100-03) (32 bits o 64 bits)
ALT 8 SP Workstation E2K
Oracle Linux 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 de 64 bits
Oracle Linux 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10 de 64 bits
Oracle Linux 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7 de 64 bits
Linux Mint 21.1, 21.2, 21.3 de 64 bits
Linux Mint 22.0, 22.1, 22.2 de 64 bits
AlterOS 7.5 64 bits
AlterOS 2025 64 bits
SberOS 3.4.0 64 bits
SberOS 3.5.0 64 bits
SberOS 3.6.1 (64 bits)
Platform V SberLinux OS Server (SLO) 8.10.1 (64 bits)
Platform V SberLinux OS Server (SLO) 9.1 (64 bits)
Platform V SberLinux OS Server (SLO) 9.5.1 (64 bits)
Platform V SberLinux OS Server (SLO) 9.6 (64 bits)
Platform V SberLinux OS Server (SLO) 9.7 (64 bits)
RED OS 7.3 Server (64 bits)
RED OS 7.3 Certified Edition (64 bits)
RED OS 8 (64 bits)
RED OS 8 ARM (64 bits)
ROSA Enterprise Linux Server 7.9 (64 bits)
ROSA Enterprise Linux Desktop 7.9 (64 bits)
ROSA COBALT 7.9 (64 bits)
ROSA CHROME 12 (64 bits)
AlmaLinux 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10 (64 bits)
AlmaLinux 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6 (64 bits)
Rocky Linux 8.5, 8.6, 8.7, 8.8, 8.9, 8.10 (64 bits)
Rocky Linux 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6 (64 bits)
Atlant, compilación Alcyone, versión 2022.02 (64 bits)
Msvsphere 9.2 Server (64 bits)
Msvsphere 9.2 ARM (64 bits)
MSVSPHERE 9.4 SERVER de 64 bits
MSVSPHERE 9.4 ARM (64 bits)
Msvsphere 9.5 Server (64 bits)
Msvsphere 9.5 ARM (64 bits)
SynthesisM Server 8.6 (64 bits)

	SynthesisM Client 8.6 (64 bits) OSnova 2.9, 2.14 (64 bits) OSnova 3.0.5, 3.1 (64 bits) Kylin 10 (64 bits) EMIAS 1.0 (64 bits) Amazon Linux 2 (64 bits) Amazon Linux 2023 (64 bits) MosOS 15.5 Arbat (64 bits) MosOS 15.6 (64 bits) OS MES 12 para escuelas de Moscú para computadoras de escritorio y portátiles (con telemetría y soporte de DIT) (64 bits). OS MES 12 para escuelas de Moscú para paneles interactivos (con telemetría y soporte de DIT) (64 bits). M OS (Moscow Electronic School) 12 Server de 64 bits Mostech (64 bits) Mostech Server de 64 bits Fedora Linux Server 41 (64 bits) Fedora Linux Workstation 41 (64 bits) Elbrus 9.3.6 E2K
Sistemas operativos. macOS	Para obtener una lista de los sistemas operativos compatibles, consulte la Ayuda de Kaspersky Endpoint Security for Mac.
Plataformas de virtualización	Para obtener información sobre las plataformas de virtualización compatibles, consulte la Ayuda en línea de Kaspersky Security for Virtualization Light Agent.

En versiones de Windows anteriores a Microsoft Windows Server 2008 R2 (versiones de servidor) y Microsoft Windows 7 (versiones de escritorio), el Agente de red no admite las siguientes funciones:

- Redifusión de actualizaciones (utilizada por los puntos de distribución)
- Proxy KSN (utilizado por los puntos de distribución)
- Tarea de análisis de vulnerabilidades

En dispositivos con Microsoft Windows 10 versiones RS4 o RS5, puede que Kaspersky Security Center no detecte algunas vulnerabilidades en las carpetas en las que esté habilitada la distinción entre mayúsculas y minúsculas.

Antes de instalar el Agente de red en dispositivos con Windows 7, Windows Server 2008, Windows Server 2008 R2 o Windows MultiPoint Server 2011, asegúrese de haber instalado la actualización de seguridad KB3063858 para el sistema operativo de Windows (Actualización de seguridad para Windows 7 [KB3063858], Actualización de seguridad para Windows 7 para sistemas de 64 bits [KB3063858], Actualización de seguridad para Windows Server 2008 [KB3063858], Actualización de seguridad para Windows Server 2008 x64 Edition [KB3063858], Actualización de seguridad para Windows Server 2008 R2 x64 Edition [KB3063858]).

En Microsoft Windows XP, el Agente de red podría no realizar algunas operaciones correctamente.

Puede instalar o actualizar el Agente de red para Windows XP solo en Microsoft Windows XP. Las ediciones compatibles de Microsoft Windows XP y sus versiones correspondientes del Agente de red se enumeran en la lista de sistemas operativos compatibles. Puede descargar la versión que necesite del Agente de red para Microsoft Windows XP desde esta página.

Le recomendamos que instale la misma versión del Agente de red para Linux que en Kaspersky Security Center Linux.

Kaspersky Security Center Linux es totalmente compatible con el Agente de red de la misma versión o versiones más recientes.

Network Agent para macOS se proporciona junto con la aplicación de seguridad Kaspersky para este sistema operativo.

Aplicaciones y soluciones de Kaspersky compatibles

Puede usar Kaspersky Security Center Linux para desplegar y administrar cualquier aplicación o solución de Kaspersky que hoy sea compatible. Para conocer los números de versión de estas aplicaciones y soluciones, consulte la página web sobre el ciclo de vida del soporte para aplicaciones.

Aplicaciones compatibles de Kaspersky:

- Kaspersky Endpoint Security para Windows (compatible con servidores de archivos)
- Kaspersky Endpoint Security for Linux (compatible con servidores de archivos)
- Kaspersky Endpoint Security for Linux Elbrus Edition
- Kaspersky Endpoint Security for Mac
- Kaspersky Endpoint Security para Android
- Kaspersky Endpoint Security for Aurora
- Kaspersky Security for iOS
- Kaspersky Industrial CyberSecurity for Linux Nodes
- Kaspersky Industrial CyberSecurity for Nodes
- Kaspersky Industrial CyberSecurity for Networks
- Kaspersky Endpoint Agent
- Kaspersky Embedded Systems Security para Windows
- Kaspersky Embedded Systems Security para Linux
- Kaspersky Security for Virtualization Light Agent
- KATA Sandbox (uno de los componentes de Kaspersky Anti Targeted Attack Platform)
- Kaspersky Thin Client

- Kaspersky NGFW
- Kaspersky Sandbox
- Kaspersky Password Manager for Business
- Kaspersky Vulnerability Management

Kaspersky Security Center Linux se incluye en las siguientes soluciones:

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

Para conocer los números de versión de estas aplicaciones y soluciones, consulte la página web sobre el ciclo de vida del soporte para aplicaciones.

Problemas conocidos y limitaciones

El inicio de sesión único (SSO) no es compatible con Kaspersky Industrial CyberSecurity for Networks.

Acerca de la compatibilidad de los componentes de Kaspersky Security Center Linux

En la siguiente tabla, puede encontrar información sobre la compatibilidad de los componentes de Kaspersky Security Center Linux.

Compatibilidad de los componentes de Kaspersky Security Center Linux

Componente	Compatible con
Servidor de administración de Kaspersky Security Center 17 Linux	• Kaspersky Security Center Web Console de las siguientes versiones: 17, 16.3, 16.2 • Agente de red de Kaspersky Security Center de las siguientes versiones: 17, 16.3, 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1, 14*, 10.5**
Kaspersky Security Center 17 Web Console	Servidor de administración de Kaspersky Security Center Linux de las siguientes versiones: 17, 16.3, 16.2
Servidor de administración principal de Kaspersky Security Center 17 Linux	Servidores de administración secundarios: • Kaspersky Security Center Linux de las siguientes versiones: 17, 16.3, 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1 • Kaspersky Security Center Windows de las siguientes versiones: 15.1
Servidor de administración secundario de Kaspersky Security Center 17 Linux	Servidores de administración principales: • Kaspersky Security Center Linux de las siguientes versiones: 17, 16.3, 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1 • Kaspersky Security Center Windows de las siguientes versiones: 15.1

Componente	Compatible con
Agente de red de Kaspersky Security Center 17	Servidores de administración: • Kaspersky Security Center Linux de las siguientes versiones: 17, 16.3, 16.2, 16.1, 16.0, 15.4, 15.3, 15.2, 15.1 • Kaspersky Security Center Windows de las siguientes versiones: 15.1
Copia de seguridad y restauración de los datos del Servidor de administración de Kaspersky Security Center	La copia de seguridad y la restauración de datos son compatibles con las siguientes versiones del Servidor de administración de Kaspersky Security Center Linux: 16.3, 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1

*Esta versión es compatible con Microsoft Windows XP Professional con Service Pack 3. Puede descargar esta versión del Agente de red desde esta página.

**Esta versión es compatible con Microsoft Windows XP Professional con Service Pack 2. Puede solicitar esta versión del Agente de red a través del servicio de Soporte técnico.

Le recomendamos que utilice la última versión del Servidor de administración de Kaspersky Security Center y de Kaspersky Security Center Web Console. De lo contrario, la funcionalidad de Kaspersky Security Center puede verse limitada. Puede instalar y actualizar el Servidor de administración de Kaspersky Security Center y Kaspersky Security Center Web Console de forma independiente. Si lo hace, asegúrese de que la versión de Kaspersky Security Center Web Console instalada sea compatible con la versión del Servidor de administración al que busque conectarse:

Si tiene la última versión de Kaspersky Security Center Web Console y la versión anterior de Kaspersky Security Center, y se produce un error durante la autenticación del dominio, el texto del error contendrá un mensaje predeterminado.

Comparación de Kaspersky Security Center: basado en Windows frente a basado en Linux

Kaspersky proporciona Kaspersky Security Center como una solución local para dos plataformas: Windows y Linux. En la solución para Windows, se instala el Servidor de administración en un dispositivo que ejecuta un sistema operativo Windows. La solución para Linux tiene una versión del Servidor de administración que se puede instalar en un dispositivo Linux. Esta ayuda en línea contiene información sobre Kaspersky Security Center. Si desea obtener información detallada sobre la solución para Windows, consulte la Ayuda de Kaspersky Security Center Windows.

La siguiente tabla le permite comparar las características principales de Kaspersky Security Center como solución basada en Windows y como solución basada en Linux.

Comparación de funciones de Kaspersky Security Center que funciona como una solución basada en Windows y una solución basada en Linux

Característica o propiedad	Kaspersky Security Center 15.1 Windows	Kaspersky Security Center 16.3 Linux
Servidor de administración		
Ubicación del sistema de administración de bases de datos (DBMS)	Local	Local (Microsoft SQL no es compatible)
Sistema operativo para instalar el Servidor de administración en	Windows	Linux
Jerarquía de Servidores de administración	✓	✓
Compatibilidad con Servidores de administración virtuales	✓	✓

Característica o propiedad	Kaspersky Security Center 15.1 Windows	Kaspersky Security Center 16.3 Linux
Despliegue del clúster de conmutación por error de Kaspersky Security Center	✓ Solo un clúster de sitio único	✓ A partir de Kaspersky Security Center 16.2 Linux, se admite el clúster de conmutación por error distribuido geográficamente
Transmisión de estadísticas del Servidor de administración a aplicaciones de terceros mediante SNMP	✓	✓
Servidor web para publicar paquetes de instalación y otros archivos	✓	✓
Consola de administración		
Tipo de Consola de administración	Basada en MMC y basada en la web	Basado en la web
Sistema operativo donde instalar la consola de administración web	Windows o Linux	Linux
Inicio de sesión en la consola mediante la autenticación del dominio	✓	✓
Administración de dispositivos cliente y grupos de administración		
Número máximo de dispositivos administrados (por servidor de administración)	100 000 (con Microsoft SQL Server)	50 000 (con PostgreSQL y Postgres Pro)
Sondeo de red	✓	✓
Protección de dispositivos administrados: Windows, Linux y macOS	✓	✓
Protección de dispositivos móviles	✓ Administración básica de dispositivos móviles	✓ MDM y uso de la funcionalidad Kaspersky Secure Mobility Management (con la licencia)
Administración de la protección de máquinas virtuales	✓	✓
Protección de infraestructuras de nubes públicas	✓	—
Conexión remota al escritorio de un dispositivo cliente	✓	✓
Protección y cifrado de datos	✓ En dispositivos administrados basados en Windows con Kaspersky Endpoint Security para Windows o Kaspersky Endpoint Security for Mac instalados	✓ En dispositivos administrados basados en Windows con Kaspersky Endpoint Security para Windows o Kaspersky Endpoint Security for Mac instalados
Compatibilidad con clústeres y matrices de servidores en grupos de administración	✓	✓
Jerarquía de grupos de administración	✓	✓
Agregar una puerta de enlace de conexión ubicada en una DMZ como punto de distribución	✓ (no es compatible con Web Console)	✓
Trabajar con los usuarios		
Creación y gestión de cuentas de usuario	✓	✓
Administrar aplicaciones de Kaspersky		
Directivas para aplicaciones	✓	✓
Tareas para aplicaciones de Kaspersky	✓	✓
Kaspersky Security Network	✓	✓
Servidor proxy de KSN	✓	✓
Kaspersky Private Security Network	✓	✓

Característica o propiedad	Kaspersky Security Center 15.1 Windows	Kaspersky Security Center 16.3 Linux
Despliegue centralizado de claves de licencia para aplicaciones de Kaspersky	✓	✓
Diagnóstico remoto de dispositivos cliente	✓	✓
Actualización automática de aplicaciones de Kaspersky	✓	✓
Compatibilidad con el Control de anomalías adaptativo	✓	✓
Administración de la seguridad centrada en el dispositivo	✓	✓
Gestión de seguridad centrada en el usuario	✓	✓
Administración de sistemas		
Instalar sistemas operativos en dispositivos cliente	✓	—
Administración de licencias de terceros	✓	Se implementará en 2026
Uso del Servidor de administración como servidor WSUS	✓	✓ (solo el modo de búsqueda pasiva de Windows Update)
Administración de aplicaciones de terceros en dispositivos cliente		
Instalar actualizaciones de software de terceros y reparar vulnerabilidades de software de terceros	✓	✓
Importación y exportación de categorías de aplicaciones	✓ (no es compatible con Web Console)	Se implementará en 2026
Supervisión, informes y auditoría		
Administración de revisiones de objetos	✓	✓
Comparar las revisiones de una directiva	✓	✓
Visualización y trabajo con alertas detectadas por Kaspersky Endpoint Detection and Response Optimum	✓	✓
Notificaciones sobre eventos ocurridos en dispositivos administrados	✓	✓
Supervisión del estado de las directivas y el estado de las tareas	✓	✓
Integraciones		
Integración de Kaspersky Managed Detection and Response	✓	✓
Integración con sistemas SIEM	✓	✓
Agrupación de alertas y realización de acciones de respuesta mediante Active Directory, KASAP y Kaspersky TIP Sandbox	—	✓ Debe activar el Servidor de administración con una licencia de Kaspersky Next XDR Optimum y, a continuación, desplegar la clave de licencia de Kaspersky Next XDR Optimum en sus aplicaciones administradas

Acerca de Kaspersky Next Expert View

El uso de Kaspersky Security Center como una aplicación local significa que usted instala Kaspersky Security Center, incluido el Servidor de administración, en un dispositivo local y administra el sistema de seguridad de red a través de la Consola de administración basada en Microsoft Management Console (disponible solo en Kaspersky Security Center Windows) o de Kaspersky Security Center Web Console.

Sin embargo, puede usar Kaspersky Security Center como un servicio en la nube. En este caso, los expertos de Kaspersky instalan y mantienen Kaspersky Security Center para usted en el entorno de nube, y Kaspersky le proporciona acceso al Servidor de administración como un servicio. Para administrar el sistema de seguridad de su red, utilizará una Consola de administración basada en la nube, llamada Kaspersky Security Center Cloud Console. La interfaz de esta consola se asemeja a la de Kaspersky Security Center Web Console.

La interfaz y la documentación de Kaspersky Next Expert View están disponibles en los siguientes idiomas:

- Inglés
- Francés
- Alemán
- Italiano
- Japonés
- Portugués (Brasil)
- Ruso
- Chino simplificado
- Español
- Español (Latinoamérica)
- Chino tradicional

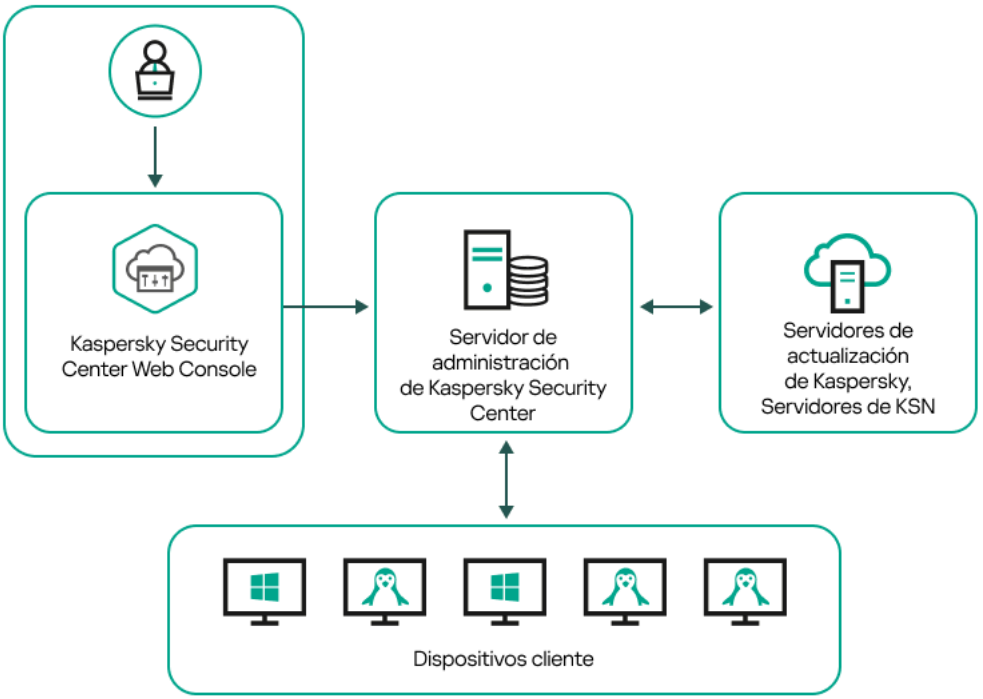
Puede obtener más información sobre Kaspersky Next Expert View y sus características en la documentación de Kaspersky Next Expert View y en la documentación de Kaspersky Endpoint Security for Business.

Arquitectura y conceptos básicos

Esta sección explica la arquitectura de la aplicación y los conceptos básicos relacionados con Kaspersky Security Center Linux.

Arquitectura

Esta sección proporciona una descripción de los componentes de Kaspersky Security Center y su interacción.



Arquitectura de Kaspersky Security Center Linux

Kaspersky Security Center Linux está formado por los siguientes componentes básicos:

- **Kaspersky Security Center Web Console**. Proporciona una interfaz web para crear y mantener el sistema de protección de la red de una organización cliente que es administrada por Kaspersky Security Center.
- **Servidor de administración de Kaspersky Security Center** (también denominado *Servidor*). Centraliza el almacenamiento de información sobre las aplicaciones instaladas en la red de la organización y sobre cómo administrarlas.
- **Servidores de actualizaciones de Kaspersky**. Servidores HTTP(S) de Kaspersky desde los que las aplicaciones de Kaspersky descargan actualizaciones para sus bases de datos y módulos de software.
- **Servidores de KSN**. Servidores que contienen una bases de datos de Kaspersky con información actualizada constantemente sobre la reputación de los archivos, recursos web y software. Kaspersky Security Network permite que las aplicaciones de Kaspersky respondan más rápido a las amenazas, mejora el rendimiento de algunos componentes de protección y reduce la probabilidad de enfrentar falsos positivos.
- **Dispositivos cliente.** Dispositivos de la empresa cliente protegidos por Kaspersky Security Center Linux. Cada dispositivo que debe protegerse debe tener instalada una de las aplicaciones de seguridad de Kaspersky.

Diagrama de despliegue del Servidor de administración de Kaspersky Security Center Linux y Kaspersky Security Center Web Console

En la siguiente imagen, se muestra el diagrama de despliegue del Servidor de administración de Kaspersky Security Center Linux y Kaspersky Security Center Web Console.

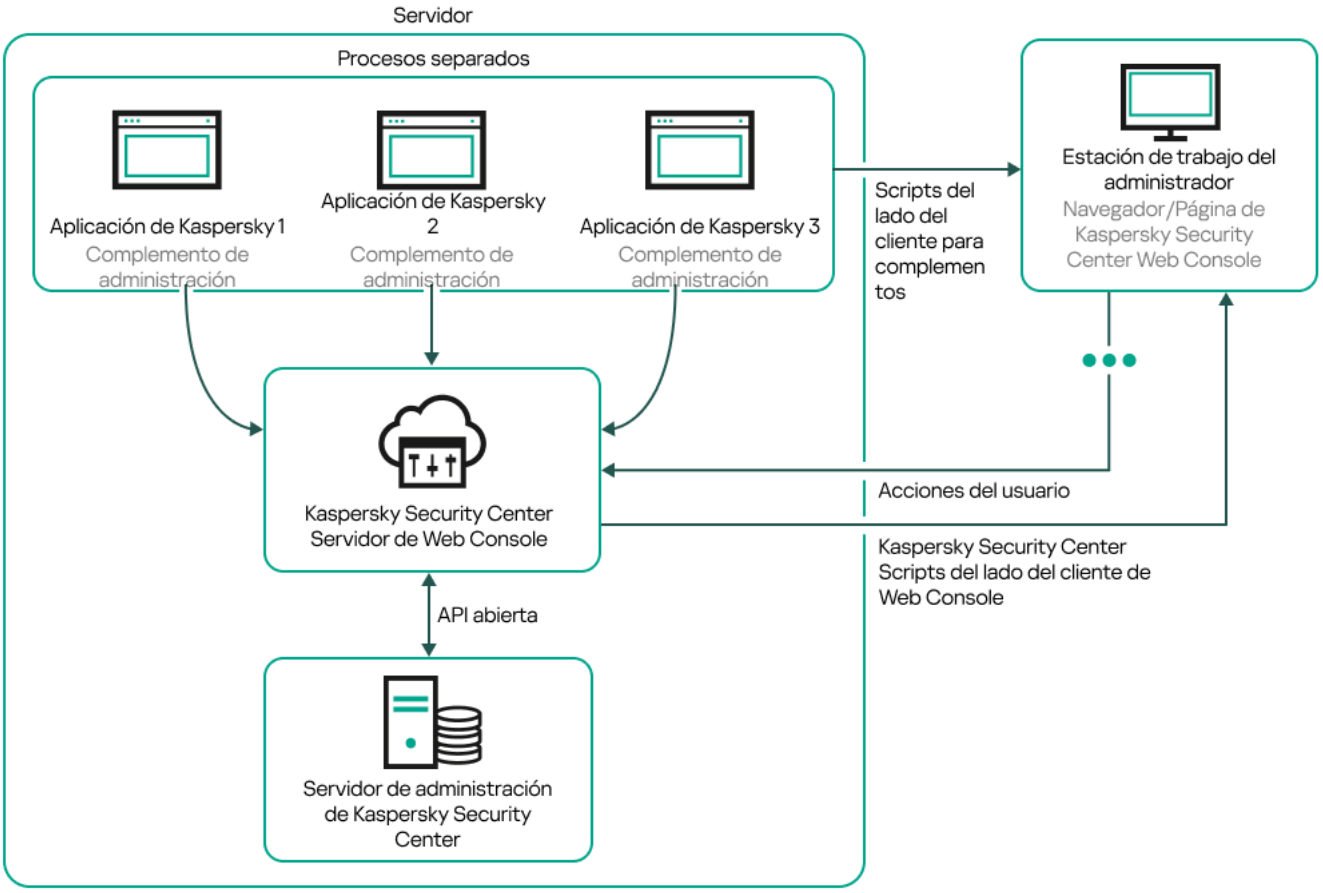


Diagrama de despliegue del Servidor de administración de Kaspersky Security Center Linux y Kaspersky Security Center Web Console

Los complementos de administración para aplicaciones de Kaspersky instaladas en dispositivos protegidos (un complemento para cada aplicación) se despliegan juntos con el Servidor de Kaspersky Security Center Web Console.

Como administrador, accede a Kaspersky Security Center Web Console usando un navegador en su estación de trabajo.

Cuando usted realiza acciones específicas en Kaspersky Security Center Web Console, el Servidor de Kaspersky Security Center Web Console se comunica con el Servidor de administración de Kaspersky Security Center Linux a través de OpenAPI. El Servidor de Kaspersky Security Center Web Console solicita la información necesaria al Servidor de administración de Kaspersky Security Center Linux y muestra los resultados de las operaciones en Kaspersky Security Center Web Console.

Puertos usados por Kaspersky Security Center Linux

Las siguientes tablas muestran los puertos predeterminados que utilizan el Servidor de administración y los dispositivos cliente. Si lo desea, puede cambiar los números de puerto predeterminados.

Puertos usados por el servidor administración de Kaspersky Security Center Linux

Número de puerto	Nombre del proceso que abre el puerto	Protocolo	Objetivo del puerto	Alcance
8060	klcsweb	TCP	Transmisión de paquetes de instalación publicados a dispositivos cliente	Publicación de paquetes de instalación. Puede cambiar el número de puerto predeterminado en la sección **Servidor web** de la ventana de propiedades del Servidor de administración. Este puerto es opcional. Por razones de seguridad, recomendamos utilizar el puerto TCP 8061.
8061	klcsweb	TCP (TLS)	Transmisión de paquetes de instalación publicados a dispositivos cliente	Publicación de paquetes de instalación. Puede cambiar el número de puerto predeterminado en la sección **Servidor web** de la ventana de propiedades del Servidor de administración.
13000	klserver	TCP (TLS)	Recepción de conexiones de los agentes de red y de los servidores de administración secundarios. Los servidores de administración secundarios también usan este puerto para recibir conexiones del Servidor de administración principal (por ejemplo, si el Servidor de administración secundario está en una DMZ).	Administración de dispositivos cliente y servidores de administración secundarios. Puede cambiar el número de puerto predeterminado para las conexiones entrantes de los Agentes de red al configurar los puertos de conexión durante la instalación de Kaspersky Security Center Linux. Puede cambiar el puerto predeterminado para las conexiones entrantes de los servidores de administración secundarios al crear la jerarquía de servidores de administración.
13000	klserver	UDP	Recepción de información sobre dispositivos que se han apagado mediante los agentes de red	Administración de dispositivos cliente. Puede cambiar el número de puerto predeterminado en la ventana de propiedades del Agente de red.
13291	klserver	TCP (TLS)	Uso de la utilidad klakaut para automatizar el funcionamiento de Kaspersky Security Center Linux	Trabajar con la utilidad klakaut. La utilidad klakaut y un sistema de ayuda para ello se encuentran en la carpeta de instalación de Kaspersky Security Center Linux. La aplicación cierra este puerto de manera predeterminada. Si desea usar la utilidad klakaut para automatizar el funcionamiento de Kaspersky Security Center Linux, abra el puerto 13291 con la utilidad klscflag.
13299	klserver	TCP (TLS)	Recepción de conexiones de Identity and Access Manager (IAM) con el Servidor de administración. Recepción de conexiones con el Servidor de administración a través de OpenAPI	Administre el Servidor de administración mediante Kaspersky Security Center Web Console; trabajando con OpenAPI. Puede cambiar el número de puerto predeterminado en la ventana de propiedades del Servidor de administración (en la subsección **Puertos de conexión** de la sección **General**), o cuando está creando una jerarquía de Servidores de administración.
14000	klserver	TCP	Recepción de conexiones de los agentes de red	Administración de dispositivos cliente. Si desea cambiar el número de puerto predeterminado, puede hacerlo al configurar los puertos de conexión durante la instalación de Kaspersky Security Center Linux o al momento de conectar un dispositivo cliente al Servidor de administración de forma manual. Este puerto es opcional y está cerrado de manera predeterminada. Por razones de seguridad, recomendamos utilizar el puerto TCP 13000.

Número de puerto	Nombre del proceso que abre el puerto	Protocolo	Objetivo del puerto	Alcance
13111 (solo si el servicio del proxy de KSN se ejecuta en el dispositivo)	ksnproxy	TCP	Recepción de solicitudes enviadas por los dispositivos administrados al servidor proxy de KSN	Servidor proxy de KSN. Puede cambiar el número de puerto predeterminado en la ventana de propiedades del Servidor de administración.
15111 (solo si el servicio del proxy de KSN se ejecuta en el dispositivo)	ksnproxy	UDP	Recepción de solicitudes enviadas por los dispositivos administrados al servidor proxy de KSN	Servidor proxy de KSN. Puede cambiar el número de puerto predeterminado en la ventana de propiedades del Servidor de administración.
17111 (solo si el servicio del proxy de KSN se ejecuta en el dispositivo)	ksnproxy	HTTPS	Recepción de solicitudes enviadas por los dispositivos administrados al servidor proxy de KSN	Servidor proxy de KSN. Puede cambiar el número de puerto predeterminado en la ventana de propiedades del Servidor de administración.
17000	klactprx	TCP (TLS)	Recepción de conexiones para la activación de la aplicación de dispositivos móviles	Servidor proxy de activación para dispositivos móviles. Puede cambiar el número de puerto predeterminado solamente a través de la Consola de administración, desde la ventana de propiedades del Servidor de administración (específicamente, desde la subsección **Puertos adicionales** de la sección **General**).
13292 (solo si administra dispositivos móviles)	klserver	TCP (TLS)	Recepción de conexiones de dispositivos móviles	Administración de dispositivos móviles. Puede cambiar el número de puerto predeterminado en la ventana de propiedades del Servidor de administración en la Consola de administración o en Kaspersky Security Center Web Console.
19170	klserver	HTTPS (TLS)	Túneles de conexión establecidos con la utilidad klsctunnel para comunicarse con los dispositivos administrados	Conexiones establecidas con dispositivos administrados remotos a través de Kaspersky Security Center Web Console. Puede cambiar el número de puerto predeterminado en la ventana de propiedades del Servidor de administración (**General → Puertos de conexión → Tunelización de conexiones RDP**).
4444	kliam	HTTPS	Autenticación mediante el protocolo OpenID Connect	Intercambio de tokens de autentificación entre el navegador y Identity and Access Manager (IAM).
9050	kliam	HTTPS	Conexión con el Servidor de administración mediante IAM	Intercambio de tokens de autentificación entre Kaspersky Security Center Web Console e IAM.

Si instala el Servidor de administración y la base de datos en dispositivos diferentes, debe asegurarse de que los puertos necesarios estén disponibles en el dispositivo en el que se encuentra la base de datos (por ejemplo, el puerto 3306 para un servidor MariaDB). Consulte la documentación del DBMS para obtener la información necesaria.

La siguiente tabla muestra el puerto que utiliza el Servidor de MDM para iOS™ (solo si administra dispositivos móviles).

Puerto utilizado por el servidor de MDM para iOS

Número de puerto	Nombre del proceso que abre el puerto	Protocolo	Objetivo del puerto	Alcance
443	kliosmdmservicesrv	TCP (TLS)	Recepción de conexiones procedentes de dispositivos móviles iOS	Administración de dispositivos móviles. Puede cambiar el número de puerto predeterminado durante la instalación del Servidor de MDM para iOS.

La siguiente tabla muestra el puerto que utiliza el servidor de Kaspersky Security Center Web Console. Este servidor puede estar en el mismo dispositivo que el Servidor de administración o en otro diferente.

Puerto usado por Kaspersky Security Center Web Console

Número de puerto	Nombre del proceso que abre el puerto	Protocolo	Objetivo del puerto	Alcance
8080	Node.js: JavaScript del lado del servidor	TCP (TLS)	Recepción de conexiones del navegador web destinadas a Kaspersky Security Center Web Console	Kaspersky Security Center Web Console. Puede cambiar el número de puerto predeterminado durante la instalación de Kaspersky Security Center Web Console. Si instala Kaspersky Security Center Web Console en el sistema operativo ALT Linux, deberá indicar un número de puerto distinto del 8080: el puerto 8080 es utilizado por el sistema operativo.

La siguiente tabla muestra el puertos que utilizan los dispositivos administrados en los que está instalado el Agente de red.

Puertos usados por el Agente de red

Número de puerto	Nombre del proceso que abre el puerto	Protocolo	Objetivo del puerto	Alcance
15000	klnagent	UDP	Señales de administración enviadas del Servidor de administración o del punto de distribución a los Agentes de red	Administración de dispositivos cliente. Puede cambiar el número de puerto predeterminado en la ventana de propiedades del Agente de red.
15000	klnagent	Difusión UDP	Obtención de datos sobre otros agentes de red dentro del mismo dominio de difusión (los datos se envían luego al Servidor de administración)	Distribución de actualizaciones y paquetes de instalación.
15001	klnagent	UDP	Recepción de solicitudes multidifusión de un punto de distribución (si se lo utiliza)	Recepción de actualizaciones y paquetes de instalación de un punto de distribución. Puede cambiar el número de puerto predeterminado en la ventana de propiedades del punto de distribución.
30522, 30523 (puertos en la interfaz de localhost)	klnagent	TCP	Transferencia de actualizaciones de las aplicaciones desde el Agente de red a las aplicaciones de Kaspersky instaladas localmente mediante el componente FileTransferBridge	Dispositivos administrados que reciben actualizaciones de la aplicación de Kaspersky del Servidor de administración especificado como origen de actualizaciones de las bases de datos.

Tenga en cuenta que el proceso klnagent también puede solicitar puertos libres que pertenezcan al grupo de puertos dinámicos del sistema operativo instalado en el endpoint. El sistema operativo asigna estos puertos a klnagent en forma automática; por este motivo, el proceso klnagent podría tomar puertos utilizados por otras aplicaciones. Si el proceso klnagent afecta el funcionamiento de otras aplicaciones, cambie la configuración de puertos en esas aplicaciones o excluya los puertos afectados del grupo de puertos dinámicos del sistema operativo.

También tenga en cuenta que las recomendaciones sobre la compatibilidad de Kaspersky Security Center Linux con software de terceros se describen solo como referencia, y es posible que no se apliquen a nuevas versiones de software de terceros. Las recomendaciones descritas para configurar puertos se basan en las experiencias de Soporte técnico y en nuestras prácticas recomendadas.

La siguiente tabla muestra los puertos que utiliza un dispositivo administrado con Agente de red instalado actuando como punto de distribución. Los puertos enumerados los utilizan los dispositivos del punto de distribución además de los puertos utilizados por los Agentes de red (consulte la tabla anterior).

Puertos usados por el Agente de red cuando opera como punto de distribución

Número de puerto	Nombre del proceso que abre el puerto	Protocolo	Objetivo del puerto	Alcance
13000	klnagent	TCP (TLS)	Recepción de conexiones de agentes de red y puertas de enlace de conexión	Administración de dispositivos cliente y distribución de actualizaciones y paquetes de instalación. Puede cambiar el número de puerto predeterminado en las propiedades del punto de distribución.
13111 (solo si el servicio del proxy de KSN se ejecuta en el dispositivo)	ksnproxy	TCP	Recepción de solicitudes enviadas por los dispositivos administrados al servidor proxy de KSN	Servidor proxy de KSN. Puede cambiar el número de puerto predeterminado en las propiedades del punto de distribución.
15111 (solo si el servicio del proxy de KSN se ejecuta en el dispositivo)	ksnproxy	UDP	Recepción de solicitudes enviadas por los dispositivos administrados al servidor proxy de KSN	Servidor proxy de KSN. Puede cambiar el número de puerto predeterminado en las propiedades del punto de distribución.
17111 (solo si el servicio del proxy de KSN se ejecuta en el dispositivo)	ksnproxy	HTTPS	Recepción de solicitudes enviadas por los dispositivos administrados al servidor proxy de KSN	Servidor proxy de KSN. Puede cambiar el número de puerto predeterminado en las propiedades del punto de distribución.
13295 (solo si utiliza el punto de distribución como servidor push)	klnagent	TCP (TLS)	Recepción de conexiones de dispositivos cliente	Servidor push. Puede cambiar el número de puerto predeterminado en las propiedades del punto de distribución.
8060	klcsweb	TCP	Transmisión de paquetes de instalación publicados a dispositivos cliente	Publicación de paquetes de instalación. Puede cambiar el número de puerto predeterminado en la sección **Servidor web** de la ventana de propiedades del Servidor de administración.
8061	klcsweb	TCP (TLS)	Transmisión de paquetes de instalación publicados a dispositivos cliente	Publicación de paquetes de instalación. Puede cambiar el número de puerto predeterminado en la sección **Servidor web** de la ventana de propiedades del Servidor de administración.

En la siguiente tabla, se muestran los puertos que utiliza un dispositivo controlador de dominio.

Puertos que utiliza un dispositivo controlador de dominio

Número de puerto	Protocolo	Objetivo del puerto	Alcance
389	LDAP sobre TCP o UDP	Conexión a un servidor LDAP	Sondeo del controlador de dominio
636	LDAP sobre TLS	Conexión a un servidor LDAP	Sondeo del controlador de dominio

En la siguiente tabla, se enumeran los puertos que deben estar abiertos en los dispositivos cliente con el Agente de red instalado.

Puerto utilizado en el dispositivo cliente no asignado

Número de puerto	Protocolo	Objetivo del puerto	Alcance
22	SSH	Conexión a un dispositivo cliente a través de SSH	Instalación remota de aplicaciones de Kaspersky.

Puertos usados por Kaspersky Security Center Web Console

El dispositivo en el que instale el Servidor de Kaspersky Security Center Web Console (también denominado Kaspersky Security Center Web Console) debe tener abiertos los puertos que se indican en la siguiente tabla.

Puertos usados por Kaspersky Security Center Web Console

Número de puerto	Nombre del servicio	Protocolo	Objetivo del puerto	Alcance
2001	Kaspersky Security Center Product Plugins Server	HTTPS	Puerto de la API. Lo utilizan los procesos del complemento de administración para recibir solicitudes del Servicio de administración de Kaspersky Security Center Web Console.	Ejecución de los procesos "node" de los complementos de administración
1329, 2003	Servicio de administración de Kaspersky Security Center Web Console	HTTPS	Puertos de la API. Se utilizan para recibir las solicitudes del Servicio de administración de Kaspersky Security Center Web Console que se ejecutan en el mismo dispositivo.	Actualización de los componentes de Kaspersky Security Center Web Console
2005	Kaspersky Security Center Web Console	HTTPS	Puerto de la API. Se utiliza para recibir las solicitudes del Servicio de administración de Kaspersky Security Center Web Console que se ejecutan en el mismo dispositivo.	Ejecución de los procesos "node" de Kaspersky Security Center Web Console
4222	NATS de Kaspersky Security Center Web Console	HTTPS	Los puertos de la API del agente de mensajes basado en NATS se utilizan para la comunicación entre los procesos de Kaspersky Security Center Web Console y los complementos de administración. El puerto 8222 se utiliza para supervisar NATS.	Interacción entre Kaspersky Security Center Web Console y los complementos de administración
4444	Identity and Access Manager (IAM)	HTTPS	Puerto que utiliza el protocolo de autenticación OpenID Connect.	Intercambio de tokens de autentificación entre Kaspersky Security Center Web Console y Identity and Access Manager (IAM)
9050	IAM	HTTPS	Puerto que utiliza IAM.	Interacción entre Kaspersky Security Center Web Console e IAM

Conceptos básicos

Esta sección explica los conceptos básicos relacionados con Kaspersky Security Center Linux.

Servidor de administración

Los componentes de Kaspersky Security Center Linux permiten la administración remota de las aplicaciones Kaspersky instaladas en dispositivos cliente.

Los dispositivos con el componente Servidor de administración instalado serán mencionados como *Servidores de administración* (también denominados *Servidores*). Los Servidores de administración deben estar protegidos, incluida la protección física, contra cualquier acceso no autorizado.

El Servidor de administración se instala en un dispositivo como un servicio con el siguiente conjunto de atributos:

- Con el nombre `kladminserver_srv`
- Configurado para iniciarse automáticamente junto con el sistema operativo
- Con la cuenta `ksc` o la cuenta de usuario seleccionada durante la instalación del Servidor de Administración

Consulte el siguiente artículo para obtener la lista completa de configuraciones de instalación: Instalación de Kaspersky Security Center Linux.

El Servidor de administración cumple las siguientes funciones:

- Almacena la estructura de los grupos de administración.
- Almacena información sobre la configuración de los dispositivos cliente.
- Organizar los repositorios para paquetes de distribución de aplicaciones.
- Instalar de manera remota aplicaciones en dispositivos cliente y eliminarlas.
- Permite actualizar las bases de datos y los módulos de software de las aplicaciones de Kaspersky.
- Permite administrar directivas y tareas en los dispositivos cliente.
- Almacenar información sobre eventos producidos en dispositivos cliente.
- Generación de informes sobre el funcionamiento de aplicaciones Kaspersky.
- Permite distribuir claves de licencia a los dispositivos cliente y puede almacenar información sobre estas claves.
- Puede reenviar notificaciones sobre el progreso de las tareas (por ejemplo, sobre la detección de virus en un dispositivo cliente).

Asignación de nombres a los Servidores de administración en la interfaz de la aplicación

En la interfaz de Kaspersky Security Center Web Console, los servidores de administración pueden tener los siguientes nombres:

- Nombre del dispositivo del Servidor de administración, por ejemplo: "*nombre_del_dispositivo*" o "Servidor de administración: *nombre_del_dispositivo*".
- Dirección IP del dispositivo del Servidor de administración, por ejemplo: "*Dirección IP*" o "Servidor de administración: *Dirección IP*".
- Los Servidores de administración secundarios y los Servidores de administración virtuales tienen nombres personalizados que usted especifica cuando conecta un Servidor de administración virtual o secundario al Servidor de administración principal.
- Si usa Kaspersky Security Center Web Console instalado en un dispositivo Linux, la aplicación mostrará los nombres de los servidores de administración que haya marcado como confiables en el archivo de respuesta.

Puede conectarse al Servidor de administración a través de Kaspersky Security Center Web Console.

Jerarquía de Servidores de administración

Los Servidores de administración se pueden organizar en una jerarquía. Cada Servidor de administración puede tener varios Servidores de administración secundarios (denominados *Servidores secundarios*) en diferentes niveles de anidamiento de la jerarquía. El nivel de anidamiento para los Servidores secundarios no está restringido. Por tanto, los grupos de administración del Servidor de administración principal incluirán los dispositivos cliente de todos los Servidores de administración secundarios. De esta manera, secciones independientes y aisladas de redes pueden ser administradas por diferentes Servidores de administración que, a su vez, están administrados por el Servidor principal.

En una jerarquía, un Servidor de administración instalado en Linux puede funcionar como servidor principal o como servidor secundario. Un Servidor de administración principal instalado en Linux puede administrar servidores secundarios instalados tanto en Linux como en Windows. Un servidor principal basado en Windows puede administrar un servidor secundario basado en Linux.

Los Servidores de administración virtuales son un caso particular de Servidores de administración secundarios.

La jerarquía de Servidores de administración se puede usar para realizar lo siguiente:

- Disminuir la carga en el Servidor de administración (en comparación con un único Servidor de administración instalado para toda la red).
- Disminuir el tráfico de intranet y simplificar el trabajo con las oficinas remotas. No es necesario establecer conexiones entre el Servidor de administración principal y todos los dispositivos de red, que pueden estar ubicados, por ejemplo, en diferentes regiones. Es suficiente instalar, en cada segmento de red, un Servidor de administración secundario, distribuir los dispositivos entre grupos de administración de Servidores secundarios y establecer conexiones entre los Servidores secundarios y el Servidor principal sobre canales de comunicación rápida.

- Distribuir las responsabilidades entre los administradores de seguridad antivirus. Todas las capacidades para la administración centralizada y el control de la seguridad antivirus en las redes corporativas permanecen disponibles.

- Uso de Kaspersky Security Center Linux por parte de los proveedores de servicios. El proveedor de servicios únicamente necesita instalar Kaspersky Security Center Linux y Kaspersky Security Center Web Console. Para administrar un gran número de dispositivos cliente de distintas organizaciones, los proveedores pueden agregar servidores de administración secundarios (los cuales pueden ser virtuales) a la jerarquía de servidores de administración.

Cada dispositivo incluido en la jerarquía de grupos de administración puede estar conectado a un único Servidor de administración. Deberá monitorear la conexión entre dispositivos y servidores de administración independientemente. Use la función para la búsqueda de dispositivos en los grupos de administración de diferentes Servidores en función de los atributos de red.

Servidor de administración virtual

El Servidor de administración virtual (también llamado *Servidor virtual*) es un componente de Kaspersky Security Center Linux cuyo propósito es administrar la protección antivirus de la red de la organización cliente.

El Servidor de administración virtual es una clase particular de Servidor de administración secundario. En comparación con un Servidor de administración físico, los servidores de administración virtuales tienen las siguientes restricciones:

- El Servidor de administración virtual puede crearse solamente en un Servidor de administración principal.

- El Servidor de administración virtual usa la base de datos del Servidor de administración principal. Los servidores de administración virtuales no son compatibles con la tarea de copia de seguridad y restauración de datos ni con la tarea de búsqueda y descarga de actualizaciones.

- El Servidor virtual no admite la creación de Servidores de administración secundarios (incluidos Servidores virtuales).

Además, el Servidor de administración virtual está sujeto a las siguientes restricciones:

- En la ventana de propiedades de los servidor de administración virtuales, el número de secciones está restringido.

- Para instalar aplicaciones de Kaspersky de manera remota en dispositivos cliente administrados por un Servidor de administración virtual, es necesario que uno de esos dispositivos tenga instalado el Agente de red. Esto se necesita para garantizar la comunicación con el Servidor de administración virtual. Luego de la primera conexión con el Servidor de administración virtual, ese dispositivo se designa automáticamente como punto de distribución y, por lo tanto, funciona como puerta de enlace para la conexión entre los dispositivos cliente y el Servidor de administración virtual.

- Un Servidor virtual solo puede sondear la red utilizando puntos de distribución.

- Para reiniciar un Servidor virtual que funciona incorrectamente, Kaspersky Security Center Linux reinicia el Servidor de administración principal y todos los Servidores de administración virtuales.
- A los usuarios creados en un Servidor virtual no se les puede asignar una función en el Servidor de administración.

El administrador de un Servidor de administración virtual tiene todos los privilegios en este Servidor virtual particular.

Servidor web

El *Servidor web* de Kaspersky Security Center (en adelante también denominado *Servidor web*) es un componente de Kaspersky Security Center que se instala junto con el Servidor de administración. El Servidor web está diseñado para transmitir paquetes de instalación independientes y archivos de una carpeta compartida a través de una red.

Al crear un paquete de instalación independiente, éste se publica automáticamente en el servidor web. En la lista de paquetes de instalación independiente creados se muestra un enlace para descargar el paquete independiente. De ser necesario, puede cancelar la publicación del paquete independiente o publicarlo nuevamente en el servidor web.

La carpeta compartida se utiliza para el almacenamiento de información disponible para todos los usuarios cuyos dispositivos se administren a través del Servidor de administración. Si el usuario no posee un acceso directo a la carpeta compartida, puede obtener información sobre esa carpeta en el servidor web.

Para brindar a los usuarios información de la carpeta compartida por medio del Servidor web, el administrador debe crear una subcarpeta llamada "Pública" en la carpeta compartida y pegar la información relevante en ella.

La sintaxis del enlace de transferencia de información es la siguiente:

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

donde:

- `<Web Server name>` es el nombre de Kaspersky Security Center Web Server.
- `<HTTPS port>` es un puerto HTTPS del servidor web que ha sido definido por el administrador. El puerto HTTPS se puede configurar en la sección **Servidor web** de la ventana de propiedades del Servidor de administración. El número de puerto predeterminado es 8061.
- `<object>` es la subcarpeta o archivo al que el usuario tiene acceso.

El administrador puede enviar el nuevo enlace al usuario de cualquier manera que le resulte conveniente (por ejemplo, por correo electrónico).

Mediante este enlace, el usuario puede descargar la información solicitada a un dispositivo local.

Servidor web de Kaspersky Security Center Linux

El Servidor web de Kaspersky Security Center Linux (denominado en lo sucesivo "Servidor web") es un componente de Kaspersky Security Center Linux. El Servidor web está diseñado para publicar paquetes de instalación independientes y archivos de la carpeta compartida.

Los paquetes de instalación creados se publican en el Servidor web automáticamente y se eliminan después de la primera descarga. El administrador puede enviar el nuevo enlace al usuario de cualquier manera que le resulte conveniente (por ejemplo, por correo electrónico).

Al hacer clic en este enlace, el usuario puede descargar la información solicitada a un dispositivo móvil.

Configuración del Servidor web

Si necesita ajustar los parámetros del Servidor web, puede modificar sus propiedades para cambiar los puertos utilizados para HTTP (8060) y HTTPS (8061). Además de cambiar los puertos, puede reemplazar el certificado HTTPS del Servidor y cambiar el nombre de dominio (FQDN) utilizado por el Servidor web para el acceso mediante HTTP.

Configuración del servidor web en una puerta de enlace de conexión

En el punto de distribución se implementa un servicio de servidor web independiente en el modo de puerta de enlace de conexión, lo que permite trabajar con dispositivos móviles conectados a Kaspersky Security Center Linux. Este servicio es responsable de transferir paquetes de instalación de apps y perfiles de administración de dispositivos a los dispositivos administrados sin conectarlos directamente al Servidor de administración. Los archivos se transfieren a medida de que el servicio procesa solicitudes de archivos HTTP/HTTPS en una puerta de enlace de conexión.

El servicio de servidor web en una puerta de enlace de conexión se instala junto con el Agente de red Linux. Para utilizar esta funcionalidad, debe asignar un dispositivo que actuará como punto de distribución en modo de puerta de enlace de conexión para ser utilizado como servidor web y luego especificar las configuraciones correspondientes. Para obtener información detallada sobre cómo configurar los parámetros del servidor web en una puerta de enlace de conexión, consulte la Ayuda de Kaspersky Secure Mobility Management.

Agente de red

La interacción entre el Servidor de administración y los dispositivos está a cargo de un componente de Kaspersky Security Center Linux llamado *Agente de red*. El Agente de red debe instalarse en todos los dispositivos en los que se utiliza Kaspersky Security Center Linux para administrar las aplicaciones de Kaspersky.

Un dispositivo que tiene el Agente de red instalado se denomina *dispositivo administrado* o *dispositivo*. Puede descargar el paquete de instalación del Agente de red desde las siguientes fuentes:

- Almacenamiento del Servidor de administración (debe tener instalado el Servidor de administración)
- Sitio web de Kaspersky

El Agente de red para Linux se instala en un dispositivo como un servicio con el siguiente conjunto de atributos:

- El nombre "Agente de red de Kaspersky".
- Configurado para iniciarse automáticamente junto con el sistema operativo.
- Se ejecuta utilizando la cuenta root.

El Agente de red para Windows se instala en un dispositivo como un servicio con el siguiente conjunto de atributos:

- El nombre "Agente de red de Kaspersky Security Center".
- Configurado para iniciarse automáticamente junto con el sistema operativo.
- Se ejecuta utilizando la cuenta LocalSystem.

El Agente de red para macOS se instala en un dispositivo como un servicio con el siguiente conjunto de atributos:

- El nombre "com.kaspersky.klnagent.core".
- Configurado para iniciarse automáticamente junto con el sistema operativo.
- Se ejecuta utilizando la cuenta root.

Los nombres de los procesos del servicio:

- Para Linux:
  - klnagent64.service (para un sistema operativo de 64 bits)
  - klnagent32.service (para un sistema operativo de 32 bits)
- Para Windows:
  - klnagent
- For macOS:
  - com.kaspersky.klnagent

De forma predeterminada, el Agente de red se instala en las siguientes ubicaciones:

- Para Linux:
  - Sistemas de 32 bits: /opt/kaspersky/klnagent/
  - Sistemas de 64 bits: /opt/kaspersky/klnagent64/
- Para Windows:
  - Sistemas de 32 bits: C:\Archivos de programa\Kaspersky Lab\NetworkAgent
  - Sistemas de 64 bits: C:\Archivos de programa (x86)\Kaspersky Lab\NetworkAgent

- For macOS:
  - Sistemas de 64 bits: /Library/Application Support/Kaspersky Lab/klnagent/Binaries/klnagent

Para los dispositivos Windows, puede especificar una carpeta diferente para la instalación del Agente de red en la configuración del paquete de instalación. Sin embargo, para los dispositivos con Linux, el instalador de Agente de red solo se puede instalar en el directorio predeterminado.

La carpeta de instalación del Agente de red también contiene utilidades para administrar y diagnosticar el funcionamiento del Agente de red, como las utilidades klmover y klnagchk.

Cuando instala el Servidor de administración, la versión del servidor del Agente de red se instala automáticamente junto con el Servidor de administración. Sin embargo, para administrar el dispositivo del Servidor de administración como cualquier otro dispositivo administrado, instale el Agente de red para Linux en el dispositivo del Servidor de administración. En este caso, el Agente de red para Linux se instala y funciona independientemente de la versión del servidor del Agente de red que instaló junto con el Servidor de administración.

El Agente de red se encarga de sincronizar el dispositivo administrado con el Servidor de administración. Recomendamos que el intervalo de sincronización (también llamado *latido*) se fije en 15 minutos por cada 10 000 dispositivos administrados.

Grupos de administración

Un *grupo de administración* (o, en lo sucesivo, *grupo*) es un conjunto lógico de dispositivos que se han combinado sobre la base de un rasgo específico para administrarlos como si fueran una sola entidad dentro de Kaspersky Security Center Linux.

Todos los dispositivos administrados que pertenecen a un grupo de administración están configurados para lo siguiente:

- Ejecutar aplicaciones con una configuración en común. La configuración puede definirse mediante directivas de grupo.
- Usar un modo común de funcionamiento de las aplicaciones, mediante la creación de tareas de grupo con parámetros específicos. Puede usar tareas de grupo para, por ejemplo, crear e instalar un paquete de instalación común, actualizar las bases de datos y los módulos de una aplicación, realizar análisis a pedido y activar la protección en tiempo real.

Un dispositivo administrado puede pertenecer a un solo grupo de administración.

Los grupos y los servidores de administración se pueden organizar en jerarquías sin límites de anidamiento. Cada nivel de una jerarquía puede incluir servidores de administración secundarios y virtuales, grupos y dispositivos administrados. Puede mover dispositivos de un grupo a otro sin trasladar esos equipos físicamente. Por ejemplo, si un empleado de su empresa pasa del departamento de Contabilidad al departamento de Desarrollo, puede mover el dispositivo que utiliza esa persona del grupo de administración Contadores al grupo de administración Desarrolladores. Al efectivizarse el traspaso, el dispositivo recibirá automáticamente la configuración que los desarrolladores requieren para sus aplicaciones.

Dispositivo administrado

Un *dispositivo administrado* es un dispositivo que ejecuta Linux, Windows o macOS, y que tiene instalado el Agente de red. Puede administrar dichos dispositivos creando tareas y directivos para las aplicaciones instaladas en estos dispositivos. También puede recibir informes de dispositivos administrados.

Puede hacer que un dispositivo administrado funcione como un punto de distribución y como una puerta de enlace de conexión.

Un dispositivo puede estar administrado por un solo Servidor de administración. La cantidad de dispositivos que puede administrar un Servidor de administración depende de la configuración del dispositivo que aloja el Servidor de administración y de las restricciones del DBMS.

Dispositivo no asignado

Un *dispositivo no asignado* es un dispositivo en la red que no se ha incluido en ningún grupo de administración. Puede realizar algunas acciones en los dispositivos no asignados, por ejemplo, moverlos a grupos de administración o instalar aplicaciones.

Cuando se detecta un nuevo dispositivo en su red, este dispositivo va al grupo de administración de **Dispositivos no asignados**. Puede configurar reglas para que los dispositivos se muevan automáticamente a otros grupos de administración una vez que se detecten los dispositivos.

Estación de trabajo del administrador

Cada dispositivo que tiene instalado el Servidor de Kaspersky Security Center Web Console se denomina *estación de trabajo del administrador*. Los administradores pueden usar esos dispositivos para la administración remota centralizada de aplicaciones de Kaspersky instaladas en dispositivos cliente.

No hay restricciones sobre el número de equipos administrador. Desde cualquier estación de trabajo del administrador, puede administrar grupos de administración de varios Servidores de administración en la red, al mismo tiempo. Puede conectar la estación de trabajo del administrador a un Servidor de administración (ya sea físico o virtual) de cualquier nivel de jerarquía.

Puede incluir la estación de trabajo del administrador en un grupo de administración como dispositivo cliente.

Dentro de los grupos de administración de cualquier Servidor de administración, el mismo dispositivo puede actuar como un cliente del Servidor de administración, un Servidor de administración o una estación de trabajo del administrador.

Complemento web de administración

Para administrar las aplicaciones de Kaspersky en forma remota a través de Kaspersky Security Center Web Console, se utiliza un componente especial, llamado *complemento web de administración*. En lo sucesivo, el término *complemento de administración* hará referencia a un complemento web de administración. Un complemento de administración es una interfaz entre Kaspersky Security Center Web Console y una aplicación específica de Kaspersky. El complemento de administración permite configurar tareas y directivas para esa aplicación.

Puede descargar los complementos web de administración desde el sitio web de Kaspersky.

Un complemento de administración hace lo siguiente:

- Brinda una interfaz para crear y editar tareas y ajustes para una aplicación
- Brinda una interfaz para crear y editar las directivas y los perfiles de directivas que se utilizan para configurar los dispositivos y las aplicaciones de Kaspersky en forma remota y centralizada
- Transmite los eventos generados por una aplicación
- Brinda las funciones que permiten a Kaspersky Security Center Web Console mostrar los datos de funcionamiento y los eventos de una aplicación, así como las estadísticas transmitidas por los dispositivos cliente

Directivas

Una *directiva* es un conjunto de valores de configuración de la aplicación de Kaspersky que se aplica a un grupo de administración y sus subgrupos. Puede instalar varias aplicaciones de Kaspersky en los dispositivos de un grupo de administración. Con Kaspersky Security Center, puede crear una única directiva para cada aplicación de Kaspersky disponible en un grupo de administración. Cada directiva puede tener uno de los siguientes estados:

Estado de la directiva

Estado	Descripción
Activa	La directiva que se encuentra vigente en un dispositivo. Solo puede haber una directiva activa para cada aplicación de Kaspersky en cada grupo de administración. Los dispositivos aplican los valores configurados en la directiva activa a la aplicación de Kaspersky.
Inactiva	Una directiva que no se encuentra vigente en un dispositivo.
Fuera de la oficina	Una directiva "fuera de la oficina" entra en vigor (es decir, se activa) cuando el dispositivo sale de la red corporativa.

Las directivas funcionan de acuerdo con las siguientes reglas:

- Es posible configurar más de una directiva, con distintos valores, para una misma aplicación.
- Solo puede haber una directiva activa para la aplicación actual.
- Una directiva puede tener directivas secundarias.

En general, puede usar las directivas como preparativos para situaciones de emergencia, como un ataque de virus. Si sufriera un ataque a través de unidades USB, por ejemplo, podría activar una directiva que bloqueara el acceso a ese tipo de unidades. Al hacerlo, la directiva que se encontrara activa hasta ese momento se desactivaría automáticamente.

Para poder hacer frente a distintas situaciones sin tener que mantener un grupo de directivas que difieran entre sí en unos pocos valores de configuración, puede usar perfiles de directivas.

Un *perfil* de *directiva* es un subconjunto de valores de configuración que se agrupan bajo un nombre y reemplazan los valores de configuración de una directiva. Un perfil de directiva afecta la constitución de los ajustes vigentes de un dispositivo administrado. Los *ajustes vigentes* de un dispositivo son aquellos que se encuentran en vigor en el mismo en un momento dado como resultado de aplicar la directiva, el perfil de directiva y la configuración local de una aplicación.

Los perfiles de directivas funcionan de acuerdo con las siguientes reglas:

- Un perfil de directiva entra en vigor cuando se cumple una condición de activación específica.
- Los perfiles de directivas contienen valores de configuración que difieren de los especificados en la directiva.
- La activación de un perfil de directiva modifica los ajustes vigentes del dispositivo administrado.
- Una directiva puede tener un máximo de 100 perfiles de directiva.

Perfiles de directivas

Puede que a veces necesite crear varias versiones de una misma directiva para diferentes grupos de administración. En ese caso, probablemente quiera tener la capacidad de modificar la configuración de esas directivas centralmente. Las versiones de la directiva podrían diferir en uno o dos valores de configuración únicamente. Suponga, por ejemplo, que todos los contadores de su empresa están sujetos a una misma directiva, pero existe una diferencia: los contadores sénior tienen permiso para usar unidades de almacenamiento extraíbles, mientras que los contadores junior lo tienen prohibido. En tal caso, no será práctico valerse únicamente de la jerarquía de grupos de administración para aplicar las directivas a los dispositivos.

Para que no tenga que crear varias versiones de las mismas directivas, Kaspersky Security Center Linux le permite crear *perfiles de directivas*. Los perfiles de directivas permiten que los dispositivos de un mismo grupo de administración operen con diferentes configuraciones de directiva.

Un perfil de directiva es un subconjunto nominado de los valores de configuración definidos en una directiva. Este subconjunto de valores, que se distribuye a los dispositivos de destino junto con la propia directiva, entra en vigor cuando se presenta una condición específica, llamada *condición de activación del perfil*. Un perfil contiene solamente los valores de configuración que difieren de los de la directiva "básica" que se encuentra activa en el dispositivo administrado. Cuando el perfil se activa, se modifican los valores de configuración que la directiva "básica" había impuesto inicialmente en el dispositivo. La configuración toma los valores especificados en el perfil.

Tareas

Para administrar las aplicaciones de seguridad de Kaspersky instaladas en los dispositivos a través de Kaspersky Security Center Linux, es necesario crear y ejecutar *tareas*. Las tareas son el medio que se utiliza para instalar, iniciar y detener aplicaciones, analizar archivos, actualizar bases de datos y módulos de software y realizar otras acciones en las aplicaciones.

Las tareas para una aplicación específica solo se pueden crear si el complemento de administración para esa aplicación está instalado.

Una tarea se puede ejecutar en el Servidor de administración o en un dispositivo.

Las siguientes tareas se realizan en el Servidor de administración:

- Distribución automática de informes
- Descarga de actualizaciones en el repositorio del Servidor de administración
- Copia de seguridad de los datos del Servidor de administración
- Mantenimiento de la base de datos

Los siguientes tipos de tareas se ejecutan en los dispositivos:

- *Tareas locales*. Son tareas que se ejecutan en un dispositivo específico.

  Las tareas locales pueden ser modificadas por el administrador (mediante Kaspersky Security Center Web Console) o por el usuario de un dispositivo remoto (mediante la interfaz de su aplicación de seguridad, por ejemplo). Si el administrador y el usuario del dispositivo administrado modifican una tarea local al mismo tiempo, los cambios realizados por el administrador se consideran prioritarios y son los que entran en vigor.

- *Tareas de grupo*. Son tareas que se ejecutan en todos los dispositivos de un grupo específico.

  A menos que se especifique lo contrario en las propiedades de la tarea, una tarea de grupo también afecta a todos los subgrupos del grupo seleccionado. Una tarea de grupo también afecta (opcionalmente) a los dispositivos que se han conectado a Servidores de administración secundarios y virtuales incluidos en el grupo o en cualquiera de sus subgrupos.

- *Tareas globales*. Son tareas que se ejecutan en un conjunto de dispositivos que pueden o no pertenecer a un grupo.

Para cada aplicación, puede crear cualquier número de tareas de grupo, tareas globales o tareas locales.

Puede copiar, importar, exportar y eliminar tareas, consultar el progreso de su ejecución y modificar su configuración.

Para que una tarea se inicie en un dispositivo, la aplicación para la que se la ha creado debe estar en ejecución.

Los resultados de las tareas se guardan en el registro de eventos y en el registro de eventos de Kaspersky Security Center Linux, tanto centralmente en el Servidor de administración como localmente en cada dispositivo.

No incluya datos privados en la configuración de las tareas. Por ejemplo, evite especificar la contraseña del administrador del dominio.

Alcance de la tarea

El *alcance de una tarea* es el conjunto de dispositivos en los que se realiza esa tarea. Los tipos de alcance son los siguientes:

- Para una *tarea local*, el alcance es el propio dispositivo.
- Para una *tarea del Servidor de administración*, el alcance es el Servidor de administración.
- Para una *tarea de grupo*, el alcance es la lista de dispositivos incluidos en el grupo.

Al crear una *tarea global*, puede usar los siguientes métodos para especificar su alcance:

- Especificar dispositivos puntuales manualmente.

  Puede utilizar una dirección IP (o un intervalo IP) o un nombre de DNS. También puede seleccionar los dispositivos de la red que detecta el servidor de administración.

- Importar una lista de dispositivos de un archivo .txt que contenga, en líneas separadas, la dirección de cada dispositivo que se quiera agregar.

  Si importa una lista almacenada en un archivo o crea una lista manualmente y elige identificar los dispositivos por nombre, tenga en cuenta que la lista únicamente podrá incluir dispositivos sobre los que ya haya información en la base de datos del Servidor de administración. Dicha información deberá haberse cargado durante la conexión o el descubrimiento de los dispositivos.

- Especificar una selección de dispositivos.

  El alcance de una tarea cambia con el tiempo, según cambia el conjunto de dispositivos incluidos en la selección. Puede generar una selección de dispositivos basada en los atributos de los dispositivos que quiera incluir (por ejemplo, el software instalado) o en las etiquetas asignadas a esos dispositivos. Una selección de dispositivos es la opción más flexible para especificar el alcance de una tarea.

  Las tareas para selecciones de dispositivos siempre son ejecutadas por el Servidor de administración en forma programada. Estas tareas no se pueden ejecutar en dispositivos que carecen de conexión con el Servidor de administración. Las tareas cuyo alcance se especifica mediante otros métodos se ejecutan directamente en los dispositivos y, por lo tanto, no dependen de la conexión del dispositivo al Servidor de administración.

  Las tareas para selecciones de dispositivos no se ejecutan según la hora local del dispositivo, sino según la hora local del Servidor de administración. Cuando el alcance se especifica por otros medios, la tarea se ejecuta según la hora local del dispositivo.

Modo en que se relacionan las directivas y la configuración local de una aplicación

Puede usar directivas para que una aplicación opere con los mismos valores de configuración en todos los dispositivos de un grupo.

Si necesita redefinir los valores de configuración especificados por una directiva para ciertos dispositivos de un grupo, puede hacerlo modificando la configuración local de la aplicación. Tenga en cuenta que solo podrá modificar los valores de configuración que la directiva permita modificar, es decir, los de aquellos ajustes o parámetros que se encuentren desbloqueados.

El valor que una aplicación utiliza para un parámetro en un dispositivo cliente depende de si dicho parámetro está o no bloqueado (🔒) en la directiva:

- Cuando no está permitido modificar un parámetro, todos los dispositivos cliente utilizan el mismo valor (el que se ha fijado en la directiva).
- Cuando está permitido modificar un parámetro, en lugar del valor exigido por la directiva, la aplicación usa el valor definido localmente en el dispositivo cliente. Ello significa que el valor puede modificarse en la configuración local de la aplicación.

Así, cuando se ejecuta una tarea en un dispositivo cliente, la aplicación aplica valores configurados por dos vías diferentes:

- por medio de la configuración de la tarea y la configuración local de la aplicación, si la directiva no prohíbe los cambios en el parámetro correspondiente;
- por medio de la directiva de grupo, si la directiva prohíbe los cambios en el parámetro correspondiente.

La configuración local de una aplicación toma los valores definidos en una directiva la primera vez que se aplica esa directiva.

Punto de distribución

Un *punto de distribución* (anteriormente conocido como agente de actualización) es un dispositivo con el Agente de red instalado que se utiliza para distribuir actualizaciones, instalar de forma remota las aplicaciones y recuperar información sobre los dispositivos en red.

Las funciones y los casos de uso del Agente de red instalado en un dispositivo utilizado como punto de distribución varían según el sistema operativo.

Un punto de distribución puede realizar las siguientes funciones:

- Distribuir las actualizaciones y los paquetes de instalación recibidos del Servidor de administración a los dispositivos cliente dentro del grupo (incluida la multidifusión a través de UDP). Las actualizaciones se pueden recibir desde el Servidor de administración o desde los servidores de actualización de Kaspersky. En el segundo caso, se debe crear una tarea de actualización para el punto de distribución.

  Los puntos de distribución aceleran la distribución de actualizaciones y liberan recursos en el Servidor de administración.

- Distribuir directivas y tareas de grupo mediante la multidifusión con UDP.

- Ejercer de gateway de conexión para el Servidor de administración para los dispositivos de un grupo de administración.

  Cuando los dispositivos administrados de un grupo no se pueden conectar de forma directa con el Servidor de administración, el punto de distribución puede actuar como puerta de enlace para el grupo y facilitar la conexión con el Servidor de administración. Los dispositivos administrados se conectan a la puerta de enlace de conexión, y esta, a su vez, se conecta al Servidor de administración.

  Aun cuando existe un punto de distribución configurado como puerta de enlace de conexión, los dispositivos administrados siempre tienen la opción de conectarse en forma directa con el Servidor de administración. Si sucede que la puerta de enlace no está disponible, pero establecer una conexión directa con el Servidor de administración es técnicamente posible, los dispositivos administrados se conectan directamente al Servidor de administración.

- Sondear la red para detectar nuevos dispositivos y actualizar la información disponible sobre los dispositivos de los que ya se tenía conocimiento. Un punto de distribución puede aplicar los mismos métodos de descubrimiento de dispositivos que el Servidor de administración.

- Realice la instalación remota de aplicaciones de Kaspersky y otros proveedores de software, incluida la instalación en dispositivos cliente sin Agente de red.

  Esta función permite transferir en forma remota paquetes de instalación del Agente de red a dispositivos cliente ubicados en redes a las que el Servidor de administración no tiene acceso.

- Actuar como servidor proxy vinculado a Kaspersky Security Network (KSN).

  Puede habilitar el servidor proxy de KSN en el punto de distribución para que el dispositivo actúe como proxy de KSN. Si habilita esta función, se ejecutará el servicio del proxy de KSN en el dispositivo.

La transmisión de archivos del Servidor de administración al punto de distribución se realiza mediante el protocolo HTTP o, si la conexión SSL está habilitada, el protocolo HTTPS. La utilización de HTTP o HTTPS genera un rendimiento más alto en comparación con SOAP, debido a la reducción de tráfico.

Los dispositivos con el Agente de red instalado pueden ser designados como puntos de distribución de forma manual (por el administrador) o automáticamente (por el Servidor de administración). La lista completa de puntos de distribución para los grupos de administración especificados se muestra en el informe sobre la lista de puntos de distribución.

El alcance de un punto de distribución se compone del grupo de administración para el que ha sido designado y de todos los subgrupos de ese grupo, sin límite de anidamiento. Cuando existe más de un punto de distribución en la jerarquía de grupos de administración, el Agente de red del dispositivo administrado se conecta con el punto de distribución que más cerca se encuentra en esa jerarquía.

Si el Servidor de administración asigna puntos de distribución automáticamente, los asigna por dominios de difusión, no por grupos de administración. Esto ocurre cuando se conocen todos los dominios de difusión. El Agente de red intercambia mensajes con otros Agentes de red en la misma subred y luego envía información al Servidor de administración acerca de sí mismo y los demás Agentes de red. El Servidor de administración puede usar esa información para agrupar los Agentes de red por dominios de difusión. El Servidor de administración conoce los dominios de difusión cuando sondea más del 70 % de los Agentes de red en los grupos de administración. El Servidor de administración sondea los dominios de difusión cada dos horas. Una vez que se asignan puntos de distribución mediante dominios de difusión, no se pueden reasignar por grupos de administración.

Si el administrador asigna manualmente puntos de distribución, se pueden asignar a grupos de administración o ubicaciones de red.

Los Agentes de red con el perfil de conexión activo no participan en la detección de dominios de difusión.

Kaspersky Security Center Linux asigna a cada Agente de red una dirección de multidifusión IP única que se diferencia de todas las demás direcciones. Esto le permite evitar la sobrecarga de la red que podría ocurrir debido a superposiciones de IP. Las direcciones de multidifusión IP que se asignaron en versiones anteriores de la aplicación no se cambiarán.

Cuando hay dos o más puntos de distribución asignados a una misma área de red o a un mismo grupo de administración, uno de ellos se convierte en el punto de distribución activo y el restante (o los restantes) en punto(s) de distribución en espera. El punto de distribución activo descarga las actualizaciones y los paquetes de instalación directamente del Servidor de administración; los puntos de distribución en espera únicamente reciben actualizaciones del punto de distribución activo. Así, los archivos se descargan una sola vez del Servidor de administración y luego se distribuyen entre los puntos de distribución. Si el punto de distribución activo no se encuentra disponible por alguna razón, uno de los puntos de distribución en espera se vuelve activo. El Servidor de administración determina automáticamente que un punto de distribución debe quedar en espera.

El estado del punto de distribución (*Activo*/*En espera*) se muestra con una casilla en el informe klnagchk.

El punto de distribución debe tener un mínimo de 4 GB de espacio libre en su disco. Si el espacio libre en disco del punto de distribución es inferior a 2 GB, Kaspersky Security Center Linux crea un problema de seguridad con el nivel de importancia *Advertencia*. El problema de seguridad se publicará en las propiedades del dispositivo, en la sección **Problemas de seguridad**.

La ejecución de tareas de instalación remotas en un dispositivo asignado como un punto de distribución requiere espacio libre adicional. El volumen de espacio libre debe superar el tamaño total de los paquetes de instalación que se instalarán.

La ejecución de tareas de actualización (instalación de parches) y de reparación de la vulnerabilidad en un dispositivo asignado como un punto de distribución requiere espacio libre adicional. El volumen de espacio libre debe ser de al menos el doble del tamaño total de los parches que se instalarán.

Los dispositivos designados como puntos de distribución deben protegerse contra el acceso no autorizado por medios virtuales y físicos.

Puerta de enlace de conexión

Una *puerta de enlace de conexión* es un Agente de red que opera de un modo especial. Las puertas de enlace de conexión aceptan conexiones de otros agentes de red y las hacen llegar al Servidor de administración a través de la conexión que mantiene con el mismo. A diferencia de un Agente de red normal, una puerta de enlace de conexión no se encarga de establecer conexión con el Servidor de administración, sino que espera a que el Servidor de administración se conecte a ella.

Una puerta de enlace de conexión puede recibir conexiones de hasta 10 000 dispositivos.

Cuenta con dos opciones para utilizar las puertas de enlace de conexión:

- Le recomendamos que instale una puerta de enlace de conexión en una zona desmilitarizada (DMZ). En caso de otros Agentes de red que estén instalados en dispositivos fuera de la oficina, debe configurar específicamente una conexión al Servidor de administración mediante la puerta de enlace de conexión.

  Una puerta de enlace de conexión no modifica ni procesa de ninguna manera los datos que se transmiten desde los Agentes de red al Servidor de administración. Además, no escribe los datos en ningún búfer y, por lo tanto, no puede aceptar datos de un Agente de red para luego reenviarlos al Servidor de administración. Si el Agente de red intenta conectarse al Servidor de administración mediante la puerta de enlace de conexión, pero esta no puede conectarse al Servidor de administración, el Agente de red lo percibe como si el Servidor de administración no estuviera accesible. Todos los datos permanecen en el Agente de red (no en la puerta de enlace de conexión).

  Una puerta de enlace de conexión no puede conectarse al Servidor de administración mediante otra puerta de enlace de conexión. Esto significa que el Agente de red no puede simultáneamente ser una puerta de enlace de conexión y utilizar una puerta de enlace de conexión para conectarse al Servidor de administración.

  En la lista de puntos de distribución en las propiedades del Servidor de administración, se incluyen todas las puertas de enlace de conexión.

- También puede utilizar puertas de enlace de conexión dentro de la red. Por ejemplo, los puntos de distribución asignados automáticamente también se convierten en puertas de enlace de conexión en su propio ámbito. Sin embargo, dentro de una red interna, las puertas de enlace de conexión no brindan un beneficio significativo. Reducen la cantidad de conexiones de red que recibe el Servidor de administración, pero no reducen el volumen de los datos entrantes. Incluso sin las puertas de enlace de conexión, todos los dispositivos podrían conectarse al Servidor de administración.

Servidores de administración virtuales

Sobre la base de un Servidor de administración físico, se pueden crear varios Servidores de administración virtual, los que serán similares a los Servidores de administración secundarios. En comparación con el modelo de acceso discrecional, que se basa en listas de control de acceso (ACL), el modelo del Servidor de administración virtual es más funcional y proporciona un mayor nivel de aislamiento. Además de una estructura dedicada de grupos de administración para dispositivos asignados con directivas y tareas, cada Servidor de administración virtual presenta su propio grupo de dispositivos no asignados, sus propios conjuntos de informes, dispositivos seleccionados y eventos, paquetes de instalación, reglas de traslado, etc. El alcance funcional de los Servidores de administración virtuales puede ser utilizado tanto por proveedores de servicios (xSP) para maximizar el aislamiento de los clientes como por organizaciones a gran escala con flujos de trabajo sofisticados y numerosos administradores.

Los Servidores de administración virtual son muy similares a los Servidores de administración secundarios, pero con las distinciones siguientes:

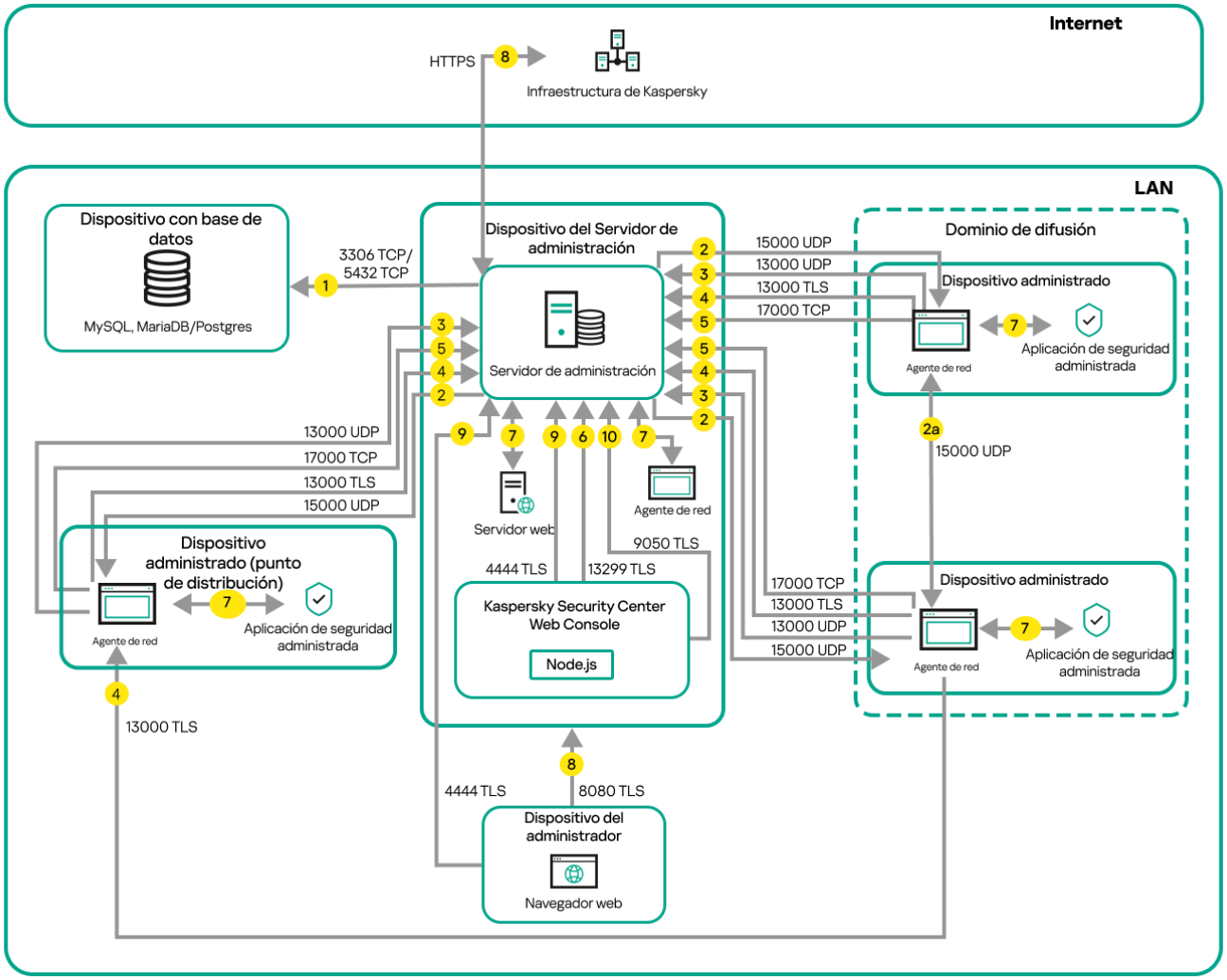
- Un Servidor de administración virtual carece de la mayoría de las configuraciones globales y sus propios puertos TCP.
- Un Servidor de administración virtual no tiene Servidores de administración secundarios.
- Un Servidor de administración virtual no tiene otros Servidores de administración virtuales.
- En un Servidor de administración físico se ven los dispositivos, grupos, eventos y objetos de los dispositivos administrados (elementos en Cuarentena, registro de aplicaciones, etc.) de todos sus Servidores de administración virtuales.
- Un Servidor de administración virtual solo puede analizar la red con puntos de distribución conectados.

Esquemas del tráfico de datos y de los puertos utilizados

En esta sección encontrará una serie de esquemas en los que se representa el tráfico de datos entre los componentes de Kaspersky Security Center Linux, las aplicaciones de seguridad administradas y los servidores externos bajo distintas configuraciones. Los esquemas tienen numerados los puertos que deben estar disponibles en los dispositivos locales.

Servidor de administración y dispositivos administrados en una red de área local (LAN)

La siguiente imagen es una representación del tráfico de datos cuando Kaspersky Security Center se ha desplegado únicamente en una red de área local (LAN).



Servidor de administración y dispositivos administrados en una red de área local (LAN)

La figura muestra cómo los diferentes dispositivos administrados se conectan al Servidor de administración de diferentes maneras: directamente o a través de un punto de distribución. Los puntos de distribución reducen la carga en el Servidor de administración durante la distribución de actualizaciones y optimizan el tráfico de red. Sin embargo, los puntos de distribución solo son necesarios si la cantidad de dispositivos administrados es lo suficientemente grande. Si la cantidad de dispositivos administrados es pequeña, todos los dispositivos administrados pueden recibir actualizaciones del Servidor de administración directamente.

Las flechas indican el inicio del tráfico: cada flecha apunta desde un dispositivo que inicia la conexión al dispositivo que "responde" a la llamada. También contienen el número de puerto y el nombre del protocolo con que se transfiere la información. Los números con los que están etiquetadas las flechas se corresponden con los tipos de tráfico que se detallan a continuación:

1. El Servidor de administración envía información a la base de datos. Si instala el Servidor de administración y la base de datos en dispositivos diferentes, debe asegurarse de que los puertos necesarios estén disponibles en el dispositivo donde se encuentra la base de datos (por ejemplo, el puerto 3306 para un servidor MySQL o MariaDB, o el puerto 5432 para un servidor PostgreSQL o Postgres Pro). Consulte la documentación del DBMS para obtener la información necesaria.

2. Cuando el Servidor de administración necesita comunicarse con los dispositivos administrados no móviles, envía la solicitud correspondiente a través del puerto UDP 15000.

   Los agentes de red se envían solicitudes entre sí dentro de un dominio de transmisión. Luego, los datos se envían al Servidor de administración y se utilizan para definir los límites del dominio de transmisión y para la asignación automática de puntos de distribución (si esta opción está activada).

   Si el Servidor de administración no tiene acceso directo a los dispositivos administrados, las solicitudes de comunicación del Servidor de administración a estos dispositivos no se envían directamente.

   2a. Los Agentes de red en dispositivos administrados no móviles intercambian datos sobre otros Agentes de red dentro del mismo dominio de transmisión (los datos luego se envían al Servidor de administración).

3. Cuando un dispositivo administrado se apaga, el Agente de red se lo comunica al Servidor de administración a través del puerto UDP 13000.

4. Los Agentes de red y los Servidores de administración secundarios se conectan con el Servidor de administración a través del puerto TLS 13000.

   Si usó una versión anterior de Kaspersky Security Center, el Servidor de administración de su red puede recibir conexiones de Agentes de red a través del puerto (no de TLS) 14000. Kaspersky Security Center también admite la conexión de Agentes de red a través del puerto 14000, aunque se recomienda utilizar el puerto TLS 13000.

5. Los dispositivos administrados (exceptuados los dispositivos móviles) envían sus solicitudes de activación a través del puerto TCP 17000. Esto solo es necesario cuando los dispositivos no tienen acceso propio a Internet; cuando pueden hacerlo, los dispositivos envían los datos directamente a los servidores de Kaspersky por Internet.

6. El Servidor de Kaspersky Security Center Web Console utiliza el puerto TLS 13299 para comunicarse con el Servidor de administración, que puede estar instalado en el mismo dispositivo o en otro separado.

   El componente Identity and Access Manager (IAM) se conecta al Servidor de administración a través del puerto TLS 13299.

7. Las aplicaciones instaladas en un mismo dispositivo intercambian tráfico local (esto es válido tanto para el Servidor de administración como para los dispositivos administrados). No se deben abrir puertos externos.

8. Los datos del Servidor de administración a los servidores de Kaspersky (como los datos de KSN o la información sobre licencias) y los datos de los servidores de Kaspersky al Servidor de administración (como las actualizaciones de aplicaciones y las actualizaciones de las bases de datos antivirus) se transfieren mediante el protocolo HTTPS.

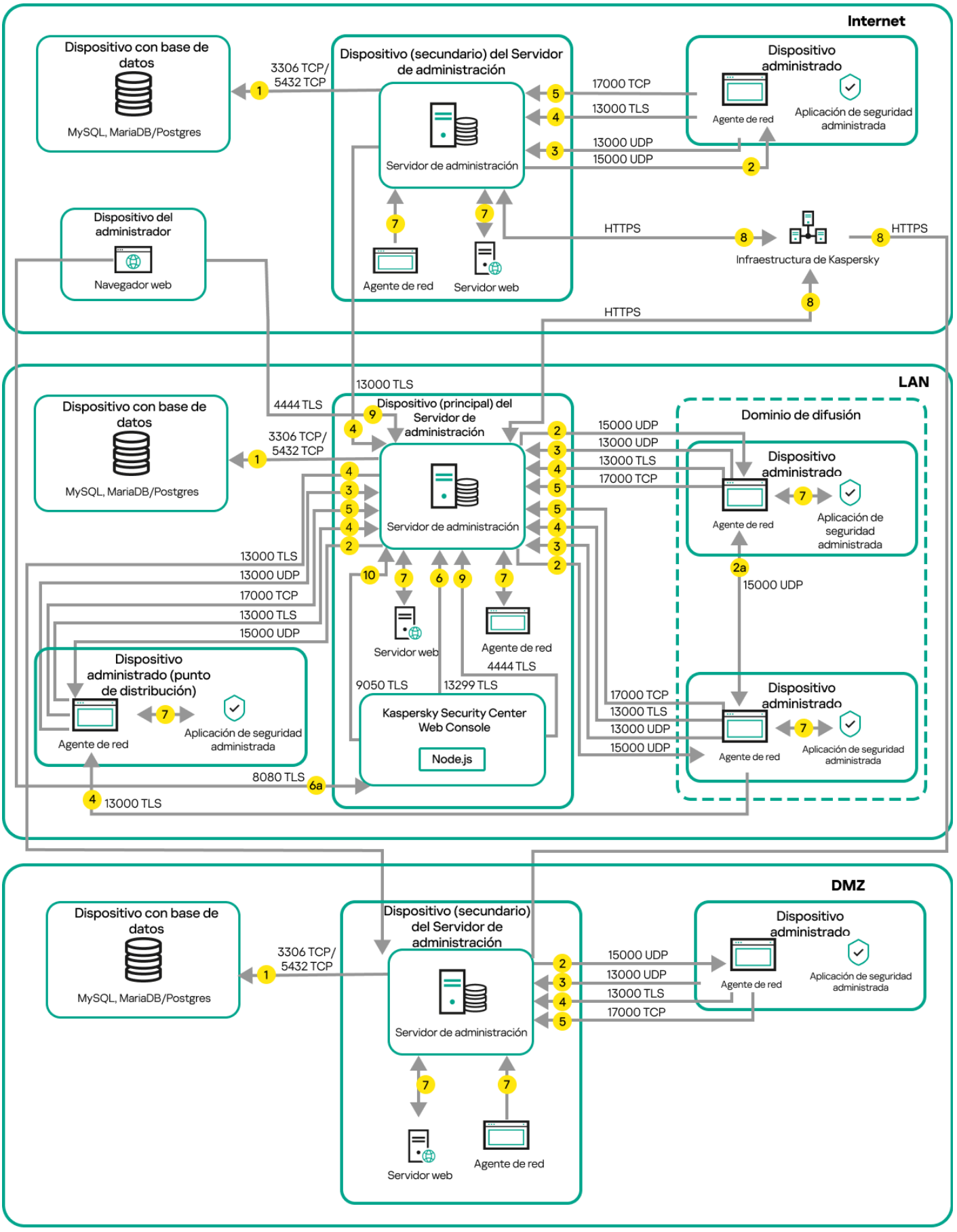
   Si no quiere que el Servidor de administración tenga acceso a Internet, deberá administrar estos datos manualmente.

9. El Servidor de Kaspersky Security Center Web Console y el navegador (que se utiliza con Kaspersky Security Center Web Console) se conectan con el Servidor de administración a través del protocolo de autenticación OpenID Connect mediante el puerto TLS 4444.

10. Kaspersky Security Center Web Console se conecta a un Servidor de administración a través del puerto TLS 9050.

Servidor de administración principal en una LAN y dos Servidores de administración secundarios

La siguiente imagen es una representación de la jerarquía de Servidores de administración. El Servidor de administración principal se encuentra en una red de área local. Hay un Servidor de administración secundario en la zona desmilitarizada (DMZ) y otro Servidor de administración secundario en Internet.



Jerarquía de Servidores de administración: Servidor de administración principal y dos Servidores de administración secundarios

Las flechas indican el inicio del tráfico: cada flecha apunta desde un dispositivo que inicia la conexión al dispositivo que "responde" a la llamada. También contienen el número de puerto y el nombre del protocolo con que se transfiere la información. Los números con los que están etiquetadas las flechas se corresponden con los tipos de tráfico que se detallan a continuación:

1. El Servidor de administración envía información a la base de datos. Si instala el Servidor de administración y la base de datos en dispositivos diferentes, debe asegurarse de que los puertos necesarios estén disponibles en el dispositivo donde se encuentra la base de datos (por ejemplo, el puerto 3306 para un servidor MySQL o MariaDB, o el puerto 5432 para un servidor PostgreSQL o Postgres Pro). Consulte la documentación del DBMS para obtener la información necesaria.

2. Cuando el Servidor de administración necesita comunicarse con los dispositivos administrados no móviles, envía la solicitud correspondiente a través del puerto UDP 15000.

   Los agentes de red se envían solicitudes entre sí dentro de un dominio de transmisión. Luego, los datos se envían al Servidor de administración y se utilizan para definir los límites del dominio de transmisión y para la asignación automática de puntos de distribución (si esta opción está activada).

   Si el Servidor de administración no tiene acceso directo a los dispositivos administrados, las solicitudes de comunicación del Servidor de administración a estos dispositivos no se envían directamente.

3. Cuando un dispositivo administrado se apaga, el Agente de red se lo comunica al Servidor de administración a través del puerto UDP 13000.

4. Los Agentes de red y los Servidores de administración secundarios se conectan con el Servidor de administración a través del puerto TLS 13000.

   Si usó una versión anterior de Kaspersky Security Center, el Servidor de administración de su red puede recibir conexiones de Agentes de red a través del puerto (no de TLS) 14000. Kaspersky Security Center Linux también admite la conexión de Agentes de red a través del puerto 14000, aunque se recomienda utilizar el puerto TLS 13000.

5. Los dispositivos administrados (exceptuados los dispositivos móviles) envían sus solicitudes de activación a través del puerto TCP 17000. Esto solo es necesario cuando los dispositivos no tienen acceso propio a Internet; cuando pueden hacerlo, los dispositivos envían los datos directamente a los servidores de Kaspersky por Internet.

6. El Servidor de Kaspersky Security Center Web Console utiliza el puerto TLS 13299 para comunicarse con el Servidor de administración, que puede estar instalado en el mismo dispositivo o en otro separado.

   El componente Identity and Access Manager (IAM) se conecta al Servidor de administración a través del puerto TLS 13299.

   6a. El tráfico del navegador, instalado en un dispositivo independiente que utiliza el administrador, se transfiere al Servidor de Kaspersky Security Center Web Console a través del puerto TLS 8080. El Servidor de Kaspersky Security Center Web Console se puede instalar en el mismo dispositivo que el Servidor de administración o en uno separado.

7. Las aplicaciones instaladas en un mismo dispositivo intercambian tráfico local (esto es válido tanto para el Servidor de administración como para los dispositivos administrados). No se deben abrir puertos externos.

8. Los datos del Servidor de administración a los servidores de Kaspersky (como los datos de KSN o la información sobre licencias) y los datos de los servidores de Kaspersky al Servidor de administración (como las actualizaciones de aplicaciones y las actualizaciones de las bases de datos antivirus) se transfieren mediante el protocolo HTTPS.

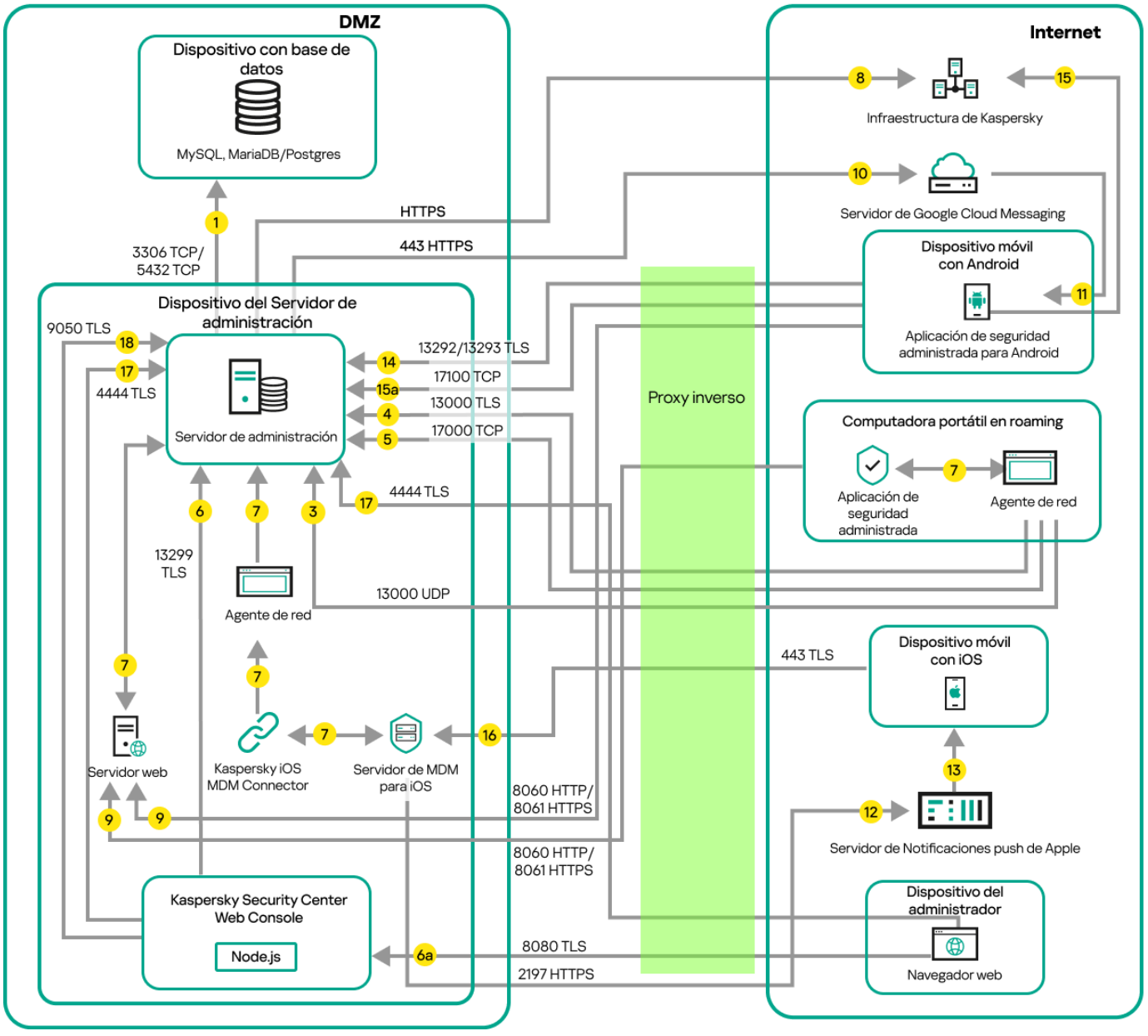
   Si no quiere que el Servidor de administración tenga acceso a Internet, deberá administrar estos datos manualmente.

9. El Servidor de Kaspersky Security Center Web Console y el navegador (que se utiliza con Kaspersky Security Center Web Console) se conectan con el Servidor de administración a través del protocolo de autenticación OpenID Connect mediante el puerto TLS 4444.

10. Kaspersky Security Center Web Console se conecta a un Servidor de administración a través del puerto TLS 9050.

Servidor de administración en una LAN, dispositivos administrados en Internet, se usa un proxy inverso

La siguiente imagen es una representación del tráfico de datos cuando el Servidor de administración está ubicado en una red de área local (LAN), y los dispositivos administrados están en Internet. En esta figura, se está utilizando un proxy inverso de su elección. Consulte la documentación de la aplicación para obtener más información.



Servidor de administración en una red de área local; los dispositivos administrados se conectan con el Servidor de administración a través de un proxy inverso

Recomendamos que siga este esquema de despliegue cuando los dispositivos móviles no deban conectarse en forma directa con el Servidor de administración y no quiera asignar una puerta de enlace de conexión dentro de la DMZ.

Las flechas indican el inicio del tráfico: cada flecha apunta desde un dispositivo que inicia la conexión al dispositivo que "responde" a la llamada. También contienen el número de puerto y el nombre del protocolo con que se transfiere la información. Los números con los que están etiquetadas las flechas se corresponden con los tipos de tráfico que se detallan a continuación:

1. El Servidor de administración envía información a la base de datos. Si instala el Servidor de administración y la base de datos en dispositivos diferentes, debe asegurarse de que los puertos necesarios estén disponibles en el dispositivo donde se encuentra la base de datos (por ejemplo, el puerto 3306 para un servidor MySQL o MariaDB, o el puerto 5432 para un servidor PostgreSQL o Postgres Pro). Consulte la documentación del DBMS para obtener la información necesaria.

2. Cuando el Servidor de administración necesita comunicarse con los dispositivos administrados no móviles, envía la solicitud correspondiente a través del puerto UDP 15000.

   Los agentes de red se envían solicitudes entre sí dentro de un dominio de transmisión. Luego, los datos se envían al Servidor de administración y se utilizan para definir los límites del dominio de transmisión y para la asignación automática de puntos de distribución (si esta opción está activada).

   Si el Servidor de administración no tiene acceso directo a los dispositivos administrados, las solicitudes de comunicación del Servidor de administración a estos dispositivos no se envían directamente.

3. Cuando un dispositivo administrado se apaga, el Agente de red se lo comunica al Servidor de administración a través del puerto UDP 13000.

4. Los Agentes de red y los Servidores de administración secundarios se conectan con el Servidor de administración a través del puerto TLS 13000.

   Si usó una versión anterior de Kaspersky Security Center, el Servidor de administración de su red puede recibir conexiones de Agentes de red a través del puerto (no de TLS) 14000. Kaspersky Security Center Linux también admite la conexión de Agentes de red a través del puerto 14000, aunque se recomienda utilizar el puerto TLS 13000.

5. Los dispositivos administrados (exceptuados los dispositivos móviles) envían sus solicitudes de activación a través del puerto TCP 17000. Esto solo es necesario cuando los dispositivos no tienen acceso propio a Internet; cuando pueden hacerlo, los dispositivos envían los datos directamente a los servidores de Kaspersky por Internet.

6. El Servidor de Kaspersky Security Center Web Console utiliza el puerto TLS 13299 para comunicarse con el Servidor de administración, que puede estar instalado en el mismo dispositivo o en otro separado.

   El componente Identity and Access Manager (IAM) se conecta al Servidor de administración a través del puerto TLS 13299.

   6a. El tráfico del navegador, instalado en un dispositivo independiente que utiliza el administrador, se transfiere al Servidor de Kaspersky Security Center Web Console a través del puerto TLS 8080. El Servidor de Kaspersky Security Center Web Console se puede instalar en el mismo dispositivo que el Servidor de administración o en uno separado.

7. Las aplicaciones instaladas en un mismo dispositivo intercambian tráfico local (esto es válido tanto para el Servidor de administración como para los dispositivos administrados). No se deben abrir puertos externos.

8. Los datos del Servidor de administración a los servidores de Kaspersky (como los datos de KSN o la información sobre licencias) y los datos de los servidores de Kaspersky al Servidor de administración (como las actualizaciones de aplicaciones y las actualizaciones de las bases de datos antivirus) se transfieren mediante el protocolo HTTPS.

   Si no quiere que el Servidor de administración tenga acceso a Internet, deberá administrar estos datos manualmente.

9. Las solicitudes de paquetes de los dispositivos administrados, incluidos los dispositivos móviles, se transfieren al Servidor web, que se encuentra en el mismo dispositivo que el Servidor de administración.

10. Dispositivos móviles Android únicamente: el Servidor de administración se comunica con los servidores de Google. La conexión se utiliza para indicar a los dispositivos móviles Android que deben conectarse con el Servidor de administración. Las notificaciones push se envían entonces a los dispositivos móviles.

11. Dispositivos móviles Android únicamente: las notificaciones push de los servidores de Google se envían al dispositivo móvil. La conexión se utiliza para indicar a los dispositivos móviles que deben conectarse con el Servidor de administración.

12. Solo para dispositivos móviles iOS: los datos del Servidor de MDM para iOS se transfieren a los servidores de notificaciones push de Apple. Las notificaciones push se envían entonces a los dispositivos móviles.

13. Solo para dispositivos móviles iOS: las notificaciones push se envían desde los servidores de Apple al dispositivo móvil. La conexión se utiliza para indicar a los dispositivos móviles iOS que deben conectarse con el Servidor de MDM para iOS.

14. Solo para dispositivos móviles: los datos de la aplicación administrada se transfieren al Servidor de administración (o a la puerta de enlace de conexión) a través de los puertos TLS 13292 o 13293, ya sea en forma directa o a través de un proxy inverso.

15. Dispositivos móviles únicamente: datos enviados por el dispositivo móvil a la infraestructura de Kaspersky.

    Si un dispositivo móvil no tiene acceso a Internet, los datos se transfieren al Servidor de administración a través del puerto 17100, y el Servidor de administración los envía a la infraestructura de Kaspersky. Sin embargo, esta situación es muy poco frecuente.

16. Solo para dispositivos móviles iOS: los datos de los dispositivos móviles se transfieren a través del puerto TLS 443 al servidor de MDM para iOS, que se encuentra en el mismo dispositivo que el Servidor de administración o en la puerta de enlace de conexión.

17. El Servidor de Kaspersky Security Center Web Console y el navegador (que se utiliza con Kaspersky Security Center Web Console) se conectan con el Servidor de administración a través del protocolo de autenticación OpenID Connect mediante el puerto TLS 4444.

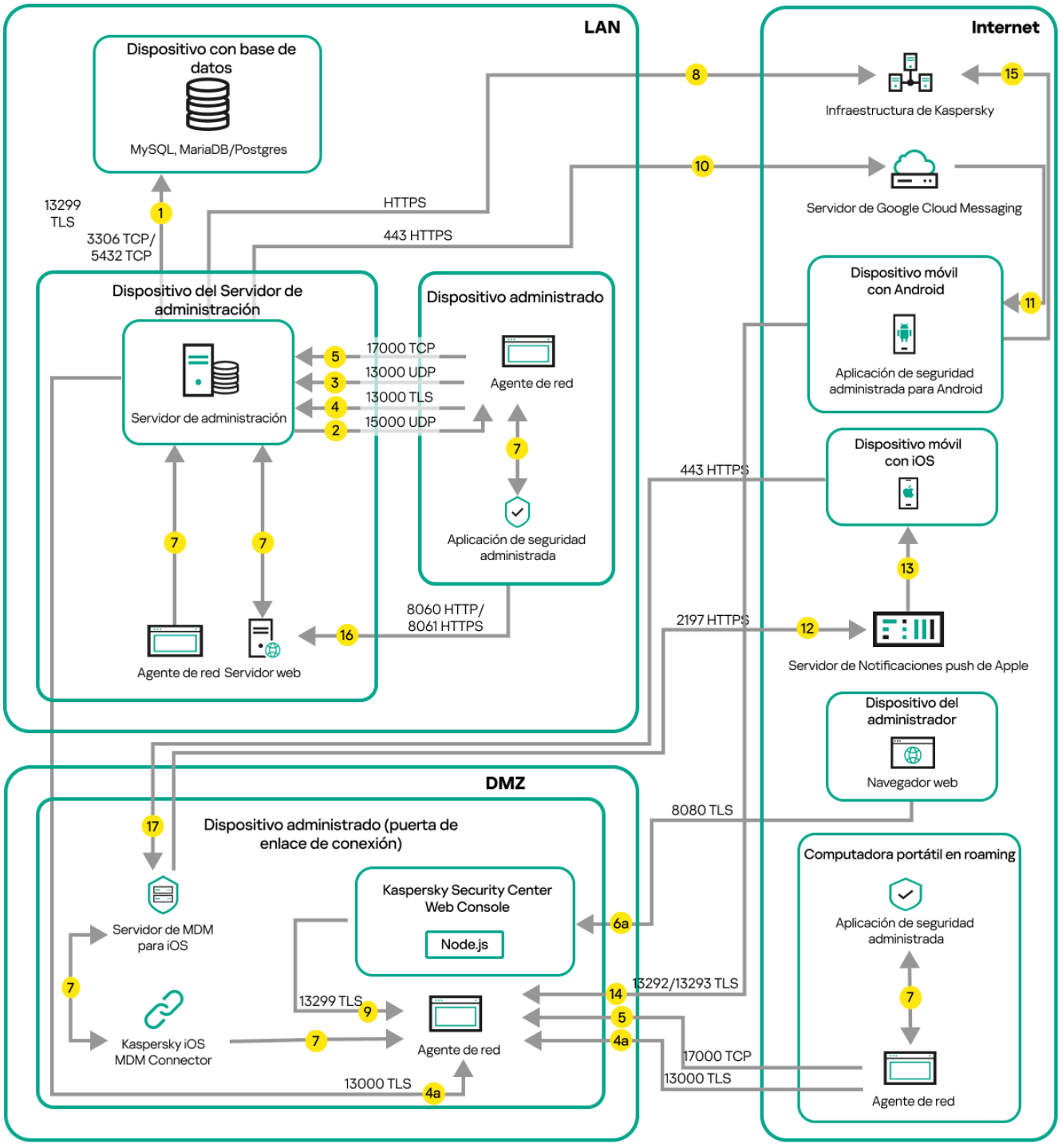
18. Kaspersky Security Center Web Console se conecta a un Servidor de administración a través del puerto TLS 9050.

Servidor de administración en una LAN, dispositivos administrados en Internet, se usa una puerta de enlace de conexión

La siguiente imagen es una representación del tráfico de datos cuando el Servidor de administración está ubicado en una red de área local (LAN), y los dispositivos administrados están en Internet. Se utiliza una puerta de enlace de conexión.

Se recomienda este esquema de despliegue si no desea que los dispositivos administrados se conecten directamente al Servidor de administración ni desea usar un proxy inverso o un firewall corporativo.

Para este esquema de despliegue, no es compatible la autenticación de dominio (inicio de sesión único) que proporciona Identity and Access Manager (IAM).



Dispositivos móviles administrados que se conectan al Servidor de administración a través de una puerta de enlace de conexión

En la imagen de arriba, los dispositivos administrados se conectan con el Servidor de administración a través de una puerta de enlace de conexión, la cual se encuentra en una DMZ. No se utiliza ni un proxy inverso ni un firewall corporativo.

Las flechas indican el inicio del tráfico: cada flecha apunta desde un dispositivo que inicia la conexión al dispositivo que "responde" a la llamada. También contienen el número de puerto y el nombre del protocolo con que se transfiere la información. Los números con los que están etiquetadas las flechas se corresponden con los tipos de tráfico que se detallan a continuación:

1. El Servidor de administración envía información a la base de datos. Si instala el Servidor de administración y la base de datos en dispositivos diferentes, debe asegurarse de que los puertos necesarios estén disponibles en el dispositivo donde se encuentra la base de datos (por ejemplo, el puerto 3306 para un servidor MySQL o MariaDB, o el puerto 5432 para un servidor PostgreSQL o Postgres Pro). Consulte la documentación del DBMS para obtener la información necesaria.

2. Cuando el Servidor de administración necesita comunicarse con los dispositivos administrados no móviles, envía la solicitud correspondiente a través del puerto UDP 15000.

   Los agentes de red se envían solicitudes entre sí dentro de un dominio de transmisión. Luego, los datos se envían al Servidor de administración y se utilizan para definir los límites del dominio de transmisión y para la asignación automática de puntos de distribución (si esta opción está activada).

   Si el Servidor de administración no tiene acceso directo a los dispositivos administrados, las solicitudes de comunicación del Servidor de administración a estos dispositivos no se envían directamente.

3. Cuando un dispositivo administrado se apaga, el Agente de red se lo comunica al Servidor de administración a través del puerto UDP 13000.

4. Los Agentes de red y los Servidores de administración secundarios se conectan con el Servidor de administración a través del puerto TLS 13000.

   Si usó una versión anterior de Kaspersky Security Center, el Servidor de administración de su red puede recibir conexiones de Agentes de red a través del puerto (no de TLS) 14000. Kaspersky Security Center Linux también admite la conexión de Agentes de red a través del puerto 14000, aunque se recomienda utilizar el puerto TLS 13000.

   4a. Si existe una puerta de enlace de conexión en la DMZ, también recibe las conexiones del Servidor de administración a través del puerto TLS 13000. El Servidor de administración crea y mantiene una conexión permanente —denominada conexión de señal— con la puerta de enlace. Esto es necesario porque la puerta de enlace, al encontrarse en la DMZ, no puede acceder a los puertos del Servidor. La conexión de señal no se utiliza para transferir información, sino para que una parte le indique a la otra que desea entablar un contacto de red sucesivo. Cuando la puerta de enlace necesita conectarse con el Servidor de administración, se lo hace saber a través de esta conexión; el Servidor, tras recibir este aviso, establece una conexión que permite el intercambio de datos.

   Los dispositivos que se encuentran fuera de la oficina también utilizan el puerto TLS 13000 para conectarse con la puerta de enlace de conexión.

5. Los dispositivos administrados (exceptuados los dispositivos móviles) envían sus solicitudes de activación a través del puerto TCP 17000. Esto solo es necesario cuando los dispositivos no tienen acceso propio a Internet; cuando pueden hacerlo, los dispositivos envían los datos directamente a los servidores de Kaspersky por Internet.

6. El Servidor de Kaspersky Security Center Web Console utiliza el puerto TLS 13299 para comunicarse con el Servidor de administración, que puede estar instalado en el mismo dispositivo o en otro separado.

   6a. El tráfico del navegador, instalado en un dispositivo independiente que utiliza el administrador, se transfiere al Servidor de Kaspersky Security Center Web Console a través del puerto TLS 8080. El Servidor de Kaspersky Security Center Web Console se puede instalar en el mismo dispositivo que el Servidor de administración o en uno separado.

7. Las aplicaciones instaladas en un mismo dispositivo intercambian tráfico local (esto es válido tanto para el Servidor de administración como para los dispositivos administrados). No se deben abrir puertos externos.

8. Los datos del Servidor de administración a los servidores de Kaspersky (como los datos de KSN o la información sobre licencias) y los datos de los servidores de Kaspersky al Servidor de administración (como las actualizaciones de aplicaciones y las actualizaciones de las bases de datos antivirus) se transfieren mediante el protocolo HTTPS.

   Si no quiere que el Servidor de administración tenga acceso a Internet, deberá administrar estos datos manualmente.

9. Las solicitudes de paquetes de los dispositivos administrados, incluidos los dispositivos móviles, se transfieren al Servidor web, que se encuentra en el mismo dispositivo que el Servidor de administración.

10. Dispositivos móviles Android únicamente: el Servidor de administración se comunica con los servidores de Google. La conexión se utiliza para indicar a los dispositivos móviles Android que deben conectarse con el Servidor de administración. Las notificaciones push se envían entonces a los dispositivos móviles.

11. Dispositivos móviles Android únicamente: las notificaciones push de los servidores de Google se envían al dispositivo móvil. La conexión se utiliza para indicar a los dispositivos móviles que deben conectarse con el Servidor de administración.

12. Solo para dispositivos móviles iOS: los datos del Servidor de MDM para iOS se transfieren a los servidores de notificaciones push de Apple. Las notificaciones push se envían entonces a los dispositivos móviles.

13. Solo para dispositivos móviles iOS: las notificaciones push se envían desde los servidores de Apple al dispositivo móvil. La conexión se utiliza para indicar a los dispositivos móviles iOS que deben conectarse con el Servidor de MDM para iOS.

14. Solo para dispositivos móviles: los datos de la aplicación administrada se transfieren al Servidor de administración (o a la puerta de enlace de conexión) a través de los puertos TLS 13292 o 13293, ya sea en forma directa o a través de un proxy inverso.

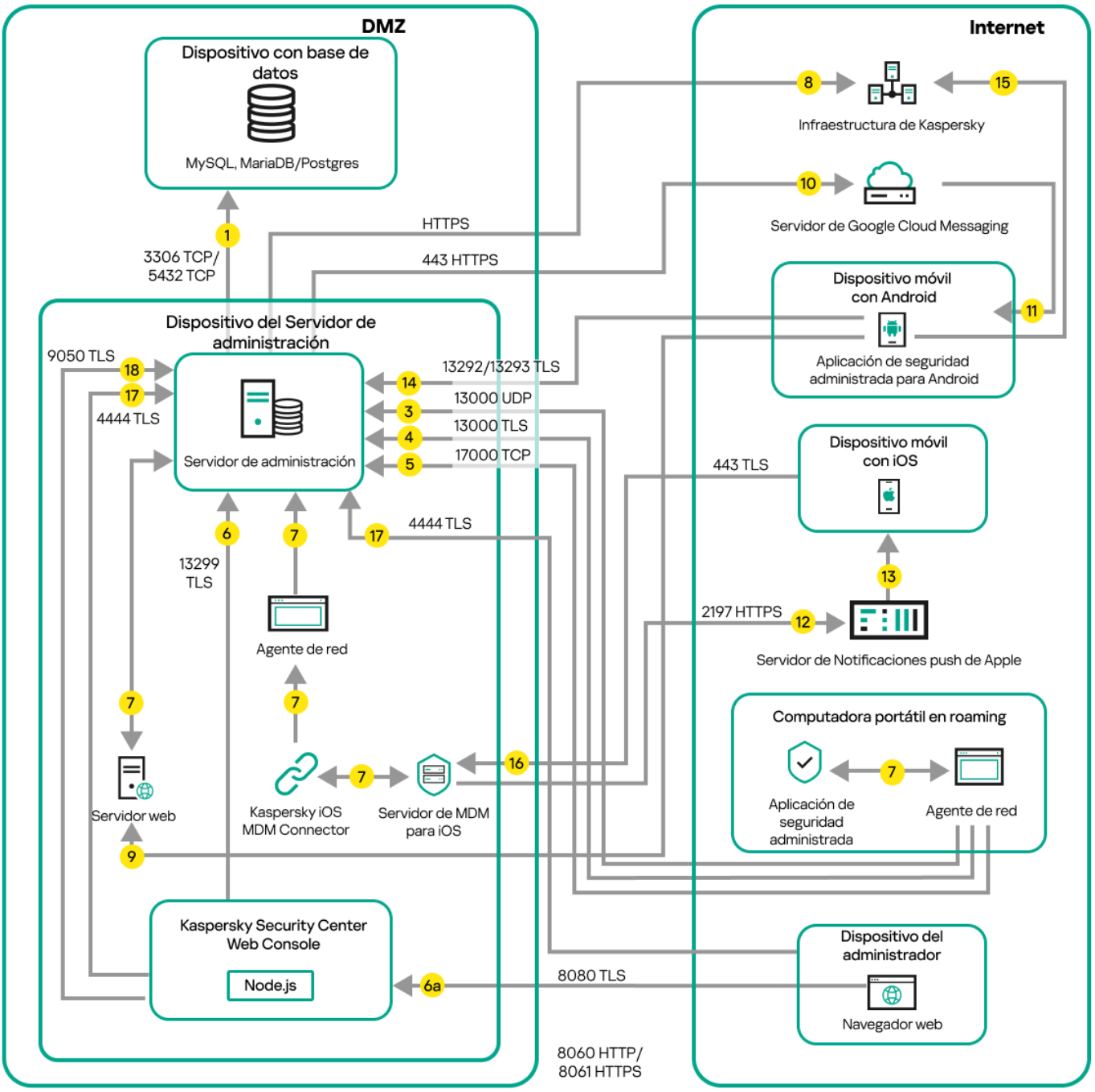
15. Dispositivos móviles únicamente: datos enviados por el dispositivo móvil a la infraestructura de Kaspersky.

    Si un dispositivo móvil no tiene acceso a Internet, los datos se transfieren al Servidor de administración a través del puerto 17100, y el Servidor de administración los envía a la infraestructura de Kaspersky. Sin embargo, esta situación es muy poco frecuente.

16. Solo para dispositivos móviles iOS: los datos de los dispositivos móviles se transfieren a través del puerto TLS 443 al servidor de MDM para iOS, que se encuentra en el mismo dispositivo que el Servidor de administración o en la puerta de enlace de conexión.

Servidor de administración en una DMZ, dispositivos administrados en Internet

La siguiente imagen es una representación del tráfico de datos cuando el Servidor de administración está ubicado en una zona desmilitarizada (DMZ) y los dispositivos administrados están en Internet.



Servidor de administración en la DMZ, dispositivos móviles administrados en Internet

En el esquema de la imagen, no se utiliza una puerta de enlace de conexión; los dispositivos móviles establecen una conexión directa con el Servidor de administración.

Las flechas indican el inicio del tráfico: cada flecha apunta desde un dispositivo que inicia la conexión al dispositivo que "responde" a la llamada. También contienen el número de puerto y el nombre del protocolo con que se transfiere la información. Los números con los que están etiquetadas las flechas se corresponden con los tipos de tráfico que se detallan a continuación:

1. El Servidor de administración envía información a la base de datos. Si instala el Servidor de administración y la base de datos en dispositivos diferentes, debe asegurarse de que los puertos necesarios estén disponibles en el dispositivo donde se encuentra la base de datos (por ejemplo, el puerto 3306 para un servidor MySQL o MariaDB, o el puerto 5432 para un servidor PostgreSQL o Postgres Pro). Consulte la documentación del DBMS para obtener la información necesaria.

2. Cuando el Servidor de administración necesita comunicarse con los dispositivos administrados no móviles, envía la solicitud correspondiente a través del puerto UDP 15000.

   Los agentes de red se envían solicitudes entre sí dentro de un dominio de transmisión. Luego, los datos se envían al Servidor de administración y se utilizan para definir los límites del dominio de transmisión y para la asignación automática de puntos de distribución (si esta opción está activada).

   Si el Servidor de administración no tiene acceso directo a los dispositivos administrados, las solicitudes de comunicación del Servidor de administración a estos dispositivos no se envían directamente.

3. Cuando un dispositivo administrado se apaga, el Agente de red se lo comunica al Servidor de administración a través del puerto UDP 13000.

4. Los Agentes de red y los Servidores de administración secundarios se conectan con el Servidor de administración a través del puerto TLS 13000.

   Si usó una versión anterior de Kaspersky Security Center, el Servidor de administración de su red puede recibir conexiones de Agentes de red a través del puerto (no de TLS) 14000. Kaspersky Security Center Linux también admite la conexión de Agentes de red a través del puerto 14000, aunque se recomienda utilizar el puerto TLS 13000.

5. Los dispositivos administrados (exceptuados los dispositivos móviles) envían sus solicitudes de activación a través del puerto TCP 17000. Esto solo es necesario cuando los dispositivos no tienen acceso propio a Internet; cuando pueden hacerlo, los dispositivos envían los datos directamente a los servidores de Kaspersky por Internet.

6. El Servidor de Kaspersky Security Center Web Console utiliza el puerto TLS 13299 para comunicarse con el Servidor de administración, que puede estar instalado en el mismo dispositivo o en otro separado.

   El componente Identity and Access Manager (IAM) se conecta al Servidor de administración a través del puerto TLS 13299.

   6a. El tráfico del navegador, instalado en un dispositivo independiente que utiliza el administrador, se transfiere al Servidor de Kaspersky Security Center Web Console a través del puerto TLS 8080. El Servidor de Kaspersky Security Center Web Console se puede instalar en el mismo dispositivo que el Servidor de administración o en uno separado.

7. Las aplicaciones instaladas en un mismo dispositivo intercambian tráfico local (esto es válido tanto para el Servidor de administración como para los dispositivos administrados). No se deben abrir puertos externos.

8. Los datos del Servidor de administración a los servidores de Kaspersky (como los datos de KSN o la información sobre licencias) y los datos de los servidores de Kaspersky al Servidor de administración (como las actualizaciones de aplicaciones y las actualizaciones de las bases de datos antivirus) se transfieren mediante el protocolo HTTPS.

   Si no quiere que el Servidor de administración tenga acceso a Internet, deberá administrar estos datos manualmente.

9. Las solicitudes de paquetes de los dispositivos administrados se transfieren al Servidor web, que se encuentra en el mismo dispositivo que el Servidor de administración.

10. Dispositivos móviles Android únicamente: el Servidor de administración se comunica con los servidores de Google. La conexión se utiliza para indicar a los dispositivos móviles Android que deben conectarse con el Servidor de administración. Las notificaciones push se envían entonces a los dispositivos móviles. El servicio FCM también opera en el puerto 443 HTTPS.

11. Dispositivos móviles Android únicamente: las notificaciones push de los servidores de Google se envían al dispositivo móvil. La conexión se utiliza para indicar a los dispositivos móviles que deben conectarse con el Servidor de administración.

12. Solo para dispositivos móviles iOS: los datos del Servidor de MDM para iOS se transfieren a los servidores de notificaciones push de Apple. Las notificaciones push se envían entonces a los dispositivos móviles.

13. Solo para dispositivos móviles iOS: las notificaciones push se envían desde los servidores de Apple al dispositivo móvil. La conexión se utiliza para indicar a los dispositivos móviles iOS que deben conectarse con el Servidor de MDM para iOS.

14. Solo para dispositivos móviles: los datos de la aplicación administrada se transfieren al Servidor de administración (o a la puerta de enlace de conexión) a través de los puertos TLS 13292 o 13293, ya sea en forma directa o a través de un proxy inverso.

15. Dispositivos móviles únicamente: datos enviados por el dispositivo móvil a la infraestructura de Kaspersky.

    Si un dispositivo móvil no tiene acceso a Internet, los datos se transfieren al Servidor de administración a través del puerto 17100, y el Servidor de administración los envía a la infraestructura de Kaspersky. Sin embargo, esta situación es muy poco frecuente.

16. Solo para dispositivos móviles iOS: los datos de los dispositivos móviles se transfieren a través del puerto TLS 443 al servidor de MDM para iOS, que se encuentra en el mismo dispositivo que el Servidor de administración o en la puerta de enlace de conexión.

17. El Servidor de Kaspersky Security Center Web Console y el navegador (que se utiliza con Kaspersky Security Center Web Console) se conectan con el Servidor de administración a través del protocolo de autenticación OpenID Connect mediante el puerto TLS 4444.

18. Kaspersky Security Center Web Console se conecta a un Servidor de administración a través del puerto TLS 9050.

Interacción entre los componentes de Kaspersky Security Center Linux y las aplicaciones de seguridad: más información

Esta sección proporciona los esquemas para la interacción de componentes Kaspersky Security Center Linux y aplicaciones de seguridad administradas. Los esquemas proporcionan los números de los puertos que deben estar abiertos y los nombres de los procesos que abren esos puertos.

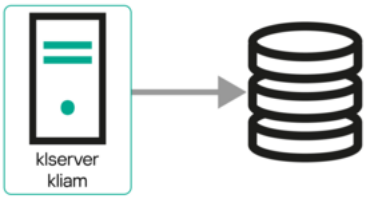
Convenciones utilizadas en esquemas de interacción

La siguiente tabla proporciona las convenciones usadas en los esquemas.

Icono	Valor
	Servidor de administración
	Servidor de administración secundario
	DBMS
	El dispositivo cliente (que tiene Agente de red y una aplicación de la familia de Kaspersky Endpoint Security instalada o tiene una aplicación de seguridad diferente instalada que Kaspersky Security Center Linux puede administrar)
	Puerta de enlace de conexión
	Punto de distribución
	Navegador en el dispositivo del usuario
	Proceso que se ejecuta en el dispositivo y que abre un puerto
	Puerto y su número
	Tráfico de TCP (la dirección de la flecha muestra la dirección del flujo de tráfico)
	Tráfico de UDP (la dirección de la flecha muestra la dirección de flujo del tráfico)
	Transporte de DBMS
	Límite de DMZ

Servidor de administración y DBMS

Los datos del Servidor de administración y de Identity and Access Manager (IAM) se almacenan en bases de datos independientes en el mismo DBMS.



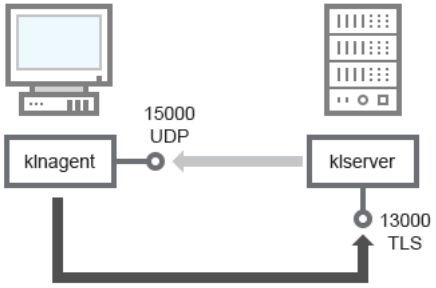
Servidor de administración, Identity and Access Manager y DBMS

Si instala el Servidor de administración y la base de datos en dispositivos diferentes, debe asegurarse de que los puertos necesarios estén disponibles en el dispositivo en el que se encuentra la base de datos (por ejemplo, el puerto 3306 para un servidor MariaDB). Consulte la documentación del DBMS para obtener la información necesaria.
Un usuario especifica el puerto para que IAM se conecte al DBMS durante la instalación de Kaspersky Security Center Linux.

El Servidor de administración no elimina automáticamente la base de datos del Servidor de administración y la base de datos de IAM cuando se desinstala o traslada el servidor a otro dispositivo. Si es necesario, debe eliminar las bases de datos manualmente.

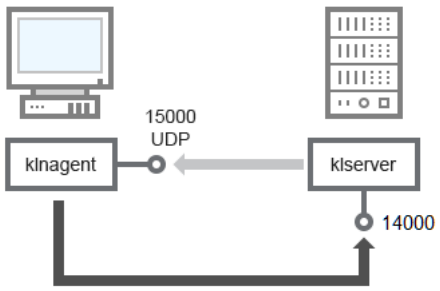
Servidor de administración y dispositivo cliente: administración de la aplicación de seguridad

El Servidor de administración recibe la conexión de los Agentes de red a través del puerto TLS 13000 (consulte la figura a continuación).



Servidor de administración y dispositivo cliente: administración de la aplicación de seguridad, conexión a través del puerto 13000 (recomendado)

Si usó una versión anterior de Kaspersky Security Center Linux, el Servidor de administración de su red puede recibir conexiones de Agentes de red a través del puerto (no de SSL) 14000 (consulte la figura a continuación). Kaspersky Security Center Linux también admite la conexión de Agentes de red a través del puerto 14000, aunque se recomienda utilizar el puerto SSL 13000.



Servidor de administración y dispositivo cliente: administración de la aplicación de seguridad, conexión a través del puerto 14000 (menor seguridad)

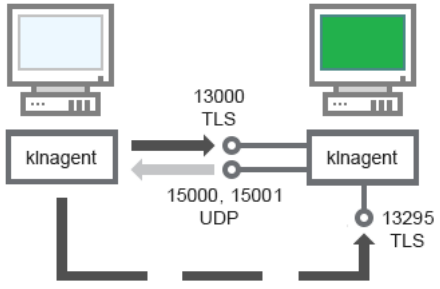
Para explicaciones sobre los esquemas, consulte la tabla a continuación.

Servidor de administración y dispositivo cliente: administración de la aplicación de seguridad (tráfico)

Dispositivo	Número de puerto	Nombre del proceso que abre el puerto	Protocolo	Objetivo del puerto
Agente de red	15000	klnagent	UDP	Multidifusión para Agentes de red
Servidor de administración	13000	klserver	TCP (TLS)	Recepción de conexiones de los agentes de red
Servidor de administración	14000	klserver	TCP	Recepción de conexiones de los agentes de red

Actualización de software en un dispositivo cliente a través de un punto de distribución

El dispositivo cliente se conecta al punto de distribución mediante el puerto 13000 y, si utiliza el punto de distribución como servidor push, también mediante el puerto 13295. Se realiza la multidifusión del punto de distribución hacia el Agente de red mediante el puerto 15000 (consulte la imagen siguiente). Las actualizaciones y los paquetes de instalación se reciben desde un punto de distribución a través del puerto 15001.



Actualización de software en un dispositivo cliente a través de un punto de distribución

Para aclaraciones del esquema, consulte la tabla a continuación.

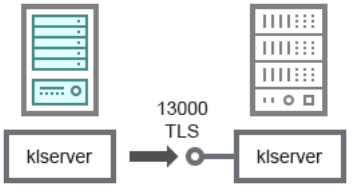
Actualización de software mediante un punto de distribución (tráfico)

Dispositivo	Número de puerto	Nombre del proceso que abre el puerto	Protocolo	Objetivo del puerto
Agente de red	15000	klnagent	UDP	Multidifusión para Agentes de red
Agente de red	15001	klnagent	UDP	Recepción de actualizaciones y paquetes de instalación de un punto de distribución
Punto de distribución	13000	klnagent	TCP (TLS)	Recepción de conexiones de los agentes de red
Punto de distribución	13295	klnagent	TCP (TLS)	Recepción de conexiones de dispositivos cliente (servidor push)

Jerarquía de Servidores de administración: Servidor de administración principal y Servidor de administración secundario

El esquema (vea la figura a continuación) muestra cómo usar el puerto 13000 para asegurar la interacción entre los Servidores de administración combinados en una jerarquía.

Posteriormente, cuando los Servidores de administración se combinen en una jerarquía, podrá administrarlos mediante Kaspersky Security Center Web Console conectado al Servidor de administración principal. Por lo tanto, la accesibilidad del puerto 13299 del Servidor de administración principal es el único requisito previo.



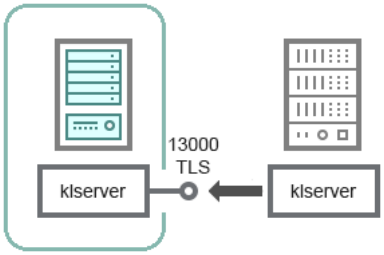
Jerarquía de Servidores de administración: Servidor de administración principal y Servidor de administración secundario

Para aclaraciones del esquema, consulte la tabla a continuación.

Jerarquía de Servidores de administración (tráfico)

Dispositivo	Número de puerto	Nombre del proceso que abre el puerto	Protocolo	Objetivo del puerto
Servidor de administración principal	13000	klserver	TCP (TLS)	Recepción de conexiones de Servidores de administración secundarios

Jerarquía de Servidores de administración con un Servidor de administración secundario en DMZ



Jerarquía de Servidores de administración con un Servidor de administración secundario en DMZ

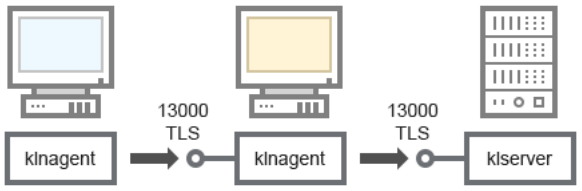
El esquema muestra una jerarquía de Servidores de administración en la que el Servidor de administración secundario ubicado en la "zona desmilitarizada" (DMZ) recibe una conexión del Servidor de administración principal (consulte la tabla a continuación para explicaciones sobre esquemas). Al combinar dos Servidores de administración en una jerarquía, asegúrese de que el puerto 13299 esté accesible en ambos Servidores de administración. Kaspersky Security Center Web Console se conecta a un Servidor de administración a través del puerto 13299.

Posteriormente, cuando los Servidores de administración se combinen en una jerarquía, podrá administrarlos mediante Kaspersky Security Center Web Console conectado al Servidor de administración principal. Por lo tanto, la accesibilidad del puerto 13299 del Servidor de administración principal es el único requisito previo.

Jerarquía de Servidores de administración con un Servidor de administración secundario en DMZ (tráfico)

Dispositivo	Número de puerto	Nombre del proceso que abre el puerto	Protocolo	Objetivo del puerto
Servidor de administración secundario	13000	klserver	TCP (TLS)	Recepción de conexiones del Servidor de administración principal

Servidor de administración, una puerta de enlace de conexión en un segmento de red y un dispositivo cliente



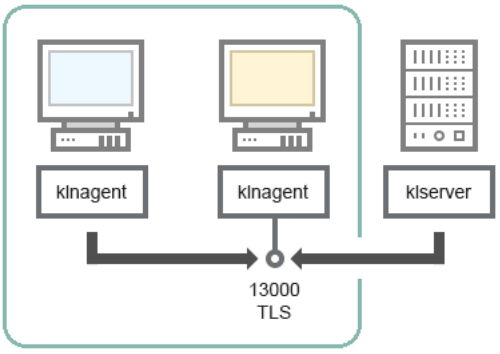
Servidor de administración, una puerta de enlace de conexión en un segmento de red y un dispositivo cliente

Para aclaraciones del esquema, consulte la tabla a continuación.

Servidor de administración con una puerta de enlace de conexión en un segmento de red y un dispositivo cliente (tráfico)

Dispositivo	Número de puerto	Nombre del proceso que abre el puerto	Protocolo	Objetivo del puerto
Servidor de administración	13000	klserver	TCP (TLS)	Recepción de conexiones de los agentes de red
Agente de red	13000	klnagent	TCP (TLS)	Recepción de conexiones de los agentes de red

Servidor de administración y dos dispositivos en DMZ: una puerta de enlace de conexión y un dispositivo cliente



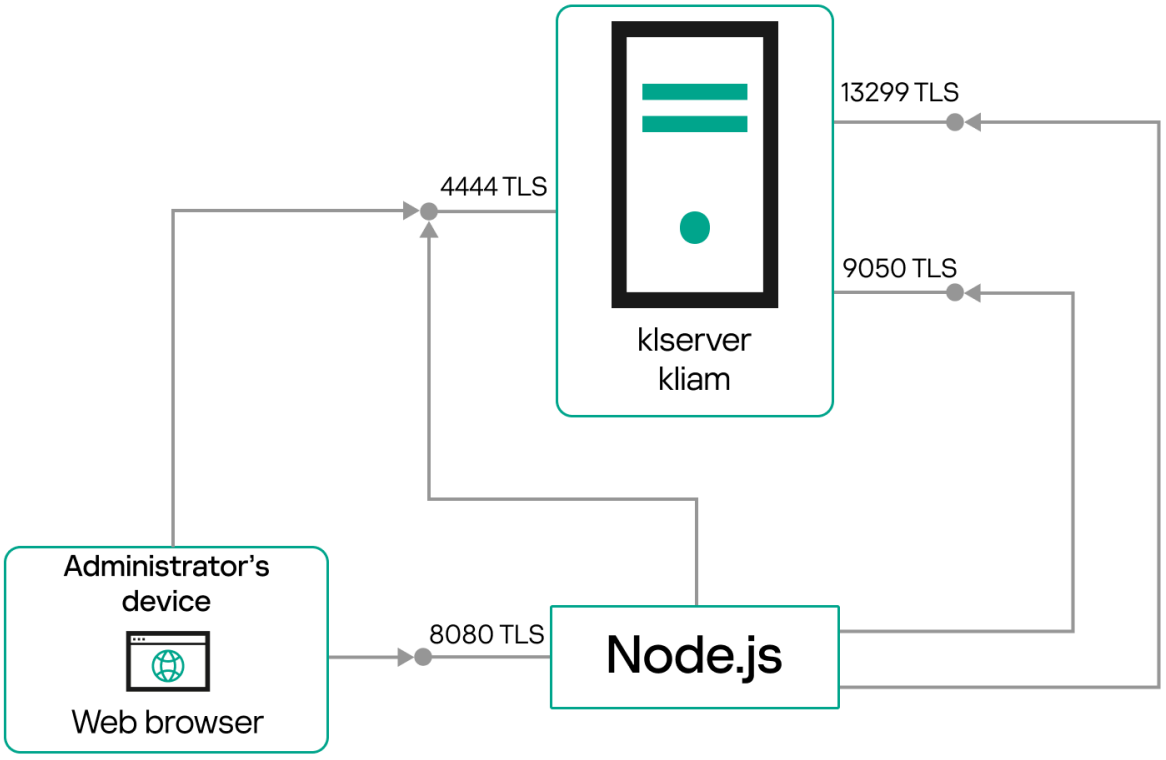
Servidor de administración con una puerta de enlace de conexión y un dispositivo cliente en DMZ

Para aclaraciones del esquema, consulte la tabla a continuación.

Servidor de administración con una puerta de enlace de conexión en un segmento de red y un dispositivo cliente (tráfico)

Dispositivo	Número de puerto	Nombre del proceso que abre el puerto	Protocolo	Objetivo del puerto
Agente de red	13000	klnagent	TCP (TLS)	Recepción de conexiones de los agentes de red

Servidor de administración y Kaspersky Security Center Web Console



Servidor de administración y Kaspersky Security Center Web Console

Para aclaraciones del esquema, consulte la tabla a continuación.

Servidor de administración y Kaspersky Security Center Web Console (tráfico)

Dispositivo	Número de puerto	Nombre del proceso que abre el puerto	Protocolo	Objetivo del puerto
Servidor de administración	13299	klserver	TCP (TLS)	Recepción de conexiones de Kaspersky Security Center Web Console y Identity and Access Manager (IAM) con el Servidor de administración a través de OpenAPI
Servidor de administración o Servidor de Kaspersky Security Center Web Console	8080	Node.js: JavaScript del lado del servidor	TCP (TLS)	Recibiendo conexiones de Kaspersky Security Center Web Console
Servidor de administración	4444	kliam	TCP (TLS)	Recepción de conexiones del Servidor de Kaspersky Security Center Web Console y el navegador (utilizado con Kaspersky Security Center Web Console) con el Servidor de administración mediante IAM y el protocolo de autenticación OpenID Connect
Servidor de administración	9050	kliam	TCP (TLS)	Recepción de conexiones de Kaspersky Security Center Web Console con IAM

Kaspersky Security Center Web Console se puede instalar en el Servidor de administración o en otro dispositivo.

Guía de inicio rápido

Aquí se describe cómo instalar el Servidor de administración de Kaspersky Security Center Linux y Kaspersky Security Center Web Console, realizar la configuración inicial del Servidor de administración con el asistente de inicio rápido e instalar las aplicaciones de Kaspersky en los dispositivos administrados utilizando el Asistente de despliegue de la protección.

Requisitos previos

Asegúrese de contar con una clave de licencia (código de activación) para Kaspersky Endpoint Security for Business o con claves de licencia (códigos de activación) para las aplicaciones de seguridad de Kaspersky.

Si primero desea probar Kaspersky Security Center Linux, puede obtener una versión de prueba sin costo en el sitio web de Kaspersky para evaluar el producto durante 30 días.

Etapas

El escenario de instalación principal se desarrolla en etapas:

1 Selección de una estructura para la protección de una empresa

Antes que nada, lea sobre los componentes de Kaspersky Security Center Linux. Basándose en la configuración de su red y en la capacidad de sus canales de comunicación, defina cuántos servidores de administración usará y cómo los distribuirá entre sus oficinas (si tiene una red distribuida). Siga las recomendaciones para elegir la estructura de la red.

Decida si usará una jerarquía de servidores de administración en su organización. Para hacer esto, debe evaluar si es posible y oportuno abarcar todos los dispositivos cliente con un solo Servidor de administración o si es necesario construir una jerarquía de Servidores de administración.

2 Preparación para el uso de certificados personalizados

Si la infraestructura de claves públicas (PKI) de su organización exige el uso de certificados personalizados emitidos por una entidad de certificación (CA) específica, prepare esos certificados y asegúrese de que reúnan todos los requisitos.

3 Configuración del acceso a la red

Configure la interacción de los componentes en la red de su organización de acuerdo con la estructura de protección elegida en el paso 1.

Para ello, debe:

- Abrir el acceso a la red según sea necesario.
- Garantizar la posibilidad de conectarse a los servidores de Kaspersky o establecer un flujo de trabajo de actualización con otro origen de actualizaciones.
- Para conectar los dispositivos administrados al Servidor de administración desde Internet, configure el acceso mediante pasarelas de conexión o ubique el Servidor de administración en la DMZ.

4 Dimensionamiento del hardware y planificación de la instalación de los componentes

Si tiene previsto instalar todos los componentes de Kaspersky Security Center Linux en el mismo servidor, use los cálculos de dimensionamiento predefinidos del archivo de configuración del script de instalación rápida (klfi_netsize). Asegúrese de que todos los requisitos para usar el script de despliegue automatizado de componentes se ajusten a su infraestructura.

De lo contrario, realice un cálculo completo de los recursos de hardware necesarios para el Servidor de administración, el DBMS y Web Console. Para desplegar la solución manualmente, componente por componente, tenga en cuenta los requisitos de hardware y software y la sección sobre el cálculo de recursos de hardware.

Para aumentar el nivel de protección de Kaspersky Security Center Linux, asegúrese de incluir en sus cálculos los requisitos de hardware de la aplicación Kaspersky Endpoint Security for Linux.

5 Instalación de los componentes de Kaspersky Security Center Linux

Instale un sistema operativo compatible con el Servidor de administración y Kaspersky Security Center Web Console en los dispositivos de destino en los que desea desplegar la solución.

Instale Kaspersky Security Center Linux según el tipo de despliegue planificado:

- Usar el script de instalación rápida automatizada
- Seguir las instrucciones para instalar y configurar manualmente los componentes Servidor de administración y Web Console.

6 Instalación de Kaspersky Endpoint Security para Linux y el Agente de red en el dispositivo del Servidor de administración

De manera predeterminada, la aplicación no considera el dispositivo del Servidor de administración como un dispositivo administrado. Para proteger el Servidor de administración y administrar este dispositivo, instale Kaspersky Endpoint Security for Linux y el Agente de red para Linux en el dispositivo del Servidor de administración. En este caso, el Agente de red para Linux se instala y funciona independientemente de la versión del servidor del Agente de red que instaló junto con el Servidor de administración.

Administre la configuración de seguridad necesaria para Kaspersky Security Center Linux de acuerdo con las recomendaciones de la Ayuda de Kaspersky Endpoint Security for Linux.

Para obtener más información, consulte el paso "Configuración de la protección antivirus del Servidor de administración" en la sección que describe el escenario de migración a Kaspersky Security Center Linux mediante el script de instalación rápida.

7 Realizar la configuración inicial

Cuando se conecta al Servidor de administración a través de Web Console por primera vez, el asistente de inicio rápido se inicia automáticamente.

Durante la etapa de configuración inicial, el asistente usará los ajustes predeterminados para crear las directivas y tareas necesarias para desplegar la protección. Estos ajustes podrían no ser los ideales para su organización. Puede cambiar la configuración de directivas y tareas si es necesario.

8 Detección de dispositivos de red

Configure y sondee la red para detectar los dispositivos manualmente. Kaspersky Security Center Linux recibe las direcciones y nombres de todos los dispositivos detectados en la red. Puede usar a continuación Kaspersky Security Center Linux para instalar Aplicaciones de Kaspersky y software desde otros proveedores en los dispositivos detectados. Kaspersky Security Center Linux realiza un descubrimiento de dispositivos periódicamente, lo que significa que, si aparece alguna instancia nueva en la red, se la detectará automáticamente.

9 Organización de dispositivos en grupos de administración

En algunos casos, para desplegar la protección en los dispositivos de la red con mayor facilidad, tendrá que repartir la totalidad de los dispositivos en grupos de administración con arreglo a la estructura de su organización. Puede crear reglas de movimiento que organicen los dispositivos en grupos o puede distribuir los dispositivos manualmente. Puede asignar tareas de grupo para grupos de administración, definir el alcance de directivas y asignar puntos de distribución.

Asegúrese de que todos los dispositivos administrados se hayan asignado correctamente a los grupos de administración apropiados y que no queden dispositivos no asignados en la red.

10 Designar los puntos de distribución

Se recomienda usar puntos de distribución en redes de gran escala, pues ayudan a reducir la carga del Servidor de administración. También son recomendables en redes con una estructura distribuida, ya que pueden brindarle al Servidor de administración acceso a dispositivos (o grupos de dispositivos) que se comuniquen a través de canales con un ancho de banda limitado. Los puntos de distribución para los grupos de administración se pueden asignar automáticamente o manualmente.

Puede asignar pasarelas de conexión solo cuando asigne los puntos de distribución manualmente.

Para hacerlo, realice los siguientes pasos:

- Asegúrese de tener suficientes puntos de distribución después de cambiar el modo de asignación a manual.
- Configure las conexiones necesarias del Servidor de administración y las pasarelas de conexión antes de proceder con el despliegue de los Agentes de red en los dispositivos de las localizaciones de red en las que deban conectarse al Servidor de administración a través de una pasarela de conexión.

11 Instalación del Agente de red y aplicaciones de seguridad en dispositivos en red

Desplegar la protección en la red de una organización implica instalar el Agente de red y las aplicaciones de seguridad en los dispositivos que el Servidor de administración encontró durante el proceso de descubrimiento de dispositivos.

Para instalar las aplicaciones de forma remota, ejecute el Asistente de despliegue de la protección.

Las aplicaciones de seguridad se encargan de proteger a los dispositivos contra virus y otros programas riesgosos. El Agente de red garantiza la comunicación entre el dispositivo y el Servidor de administración. La configuración de Agente de red se ajusta automáticamente de forma predeterminada.

Antes de iniciar la instalación de Agente de red y las aplicaciones de seguridad en dispositivos en red, asegúrese de que estos dispositivos estén accesibles (encendidos).

12 Despliegue de claves de licencia a los dispositivos cliente

Despliegue claves de licencia a los dispositivos cliente para activar las aplicaciones de seguridad administradas en esos dispositivos.

13 Configuración de directivas de la aplicación de Kaspersky

Para aplicar diferentes configuraciones de aplicaciones a diferentes dispositivos, puede usar la administración de seguridad centrada en el dispositivo o la administración de seguridad centrada en el usuario. La administración de la seguridad centrada en el dispositivo se puede implementar mediante el uso de directivas y tareas. Solo puede aplicar tareas a aquellos dispositivos que cumplan condiciones específicas. Para establecer las condiciones para filtrar dispositivos, use selecciones de dispositivos y etiquetas.

14 Supervisión del estado de protección de la red

Puede supervisar su red utilizando widgets en el panel, generar informes desde las aplicaciones de Kaspersky, configurar y ver selecciones de eventos recibidos de las aplicaciones en los dispositivos administrados y ver listas de notificaciones.

El almacenamiento a largo plazo de eventos, la recepción oportuna de eventos, el procesamiento y la correlación deben realizarse en un sistema externo especializado en tareas de SIEM.

Los indicadores de los componentes de la solución se supervisan mediante el protocolo SNMP en sistemas de supervisión de infraestructura de TI y otras soluciones de agentes de terceros.

La supervisión continua del estado de la protección está disponible en la sección **Centro de refuerzo de seguridad** de Web Console.

Guía para reforzar la seguridad

Kaspersky Security Center Linux está diseñado para ejecutar tareas de administración y mantenimiento básicas en la red de una organización de forma centralizada. La aplicación proporciona al administrador acceso a información detallada sobre el nivel de seguridad de la red de la organización. Kaspersky Security Center Linux le permite configurar todos los componentes de protección creados con las aplicaciones de Kaspersky.

El Servidor de administración de Kaspersky Security Center Linux tiene acceso completo a la administración de protección de los dispositivos cliente y es el componente más importante del sistema de seguridad de la organización. Por lo tanto, se requieren métodos de mayor protección para el Servidor de administración.

Antes de realizar la configuración, cree una copia de seguridad del Servidor de administración de Kaspersky Security Center Linux con la tarea Copia de seguridad de los datos del Servidor de administración o la utilidad klbackup. Guarde la copia de seguridad de los datos en un lugar seguro.

La Guía para reforzar la seguridad describe recomendaciones y funciones para configurar Kaspersky Security Center Linux y sus componentes, con el objetivo de reducir los riesgos.

La Guía para reforzar la seguridad contiene la siguiente información:

- Selección de la arquitectura del Servidor de administración
- Configuración de una conexión segura al Servidor de administración
- Configuración de las cuentas para acceder al Servidor de administración
- Administrar la protección del Servidor de administración
- Administración de la protección de dispositivos cliente
- Configurar la protección para aplicaciones administradas
- Mantenimiento del Servidor de administración
- Transferencia de información a aplicaciones de terceros

- Recomendaciones de seguridad para sistemas de información de terceros

Lista de comprobación de protección

Instalación del Servidor de administración

- Instale el Servidor de administración en un servidor físico o virtual dedicado.
- No utilice el servidor dedicado para ejecutar otros servicios.
- No instale el Servidor de administración (en adelante, el Servidor) en UN:
  - Controlador de dominio
  - Servidor de terminales
  - Dispositivo de usuario

Seguridad de la conexión

- Configure un firewall para restringir el acceso al dispositivo del Servidor en todos los puertos y protocolos, excepto en los puertos requeridos por el Servidor. Permita el acceso al dispositivo del Servidor solo desde dispositivos de confianza.
- Configure una lista de admitidos de direcciones IP para los puertos del Servidor que se utilizan para conectar Kaspersky Security Center Web Console (también denominada Web Console) al Servidor.
- Configure el firewall para permitir el acceso al Servidor a través de Kaspersky Security Center Web Console solo desde dispositivos de confianza.
- Configure la versión 1.2 o superior del protocolo TLS en el Servidor.
- Configure un firewall para restringir el acceso al dispositivo con el DBMS del Servidor instalado.
- Configure la autenticación SSL entre el Servidor y el DBMS (MySQL o PostgreSQL).

Cuentas y autenticación

- Configure la autenticación de dos factores (TOTP, RFC 6238) para el acceso al servidor.
- No instale la app de autenticación en el mismo dispositivo desde el que se establece la conexión con el Servidor a través de Web Console.
- Utilice la autenticación multifactor (MFA) para acceder al Servidor mediante un token, una tarjeta inteligente u otro método.

- Cree un grupo de administración exclusivo para el dispositivo del Servidor y cree una directiva de seguridad especial para él.
- Restrinja el número de usuarios que tienen el rol de Administrador principal.
- Configure los derechos de acceso a las funciones del Servidor según los roles de usuarios y grupos.
- Permita la instalación remota de aplicaciones solo para una cuenta de usuario independiente.
- Realice una auditoría periódica de todos los usuarios del dispositivo del Servidor.

Administrar la protección del Servidor de administración

- Instale una aplicación de seguridad en el dispositivo del Servidor:
  - Para un servidor físico: Kaspersky Endpoint Security
  - Para un servidor virtual: Kaspersky Security for Virtualization
- Cree y aplique una directiva independiente para la protección del Servidor (distinta a las directivas de seguridad para otros dispositivos administrados).
- Cree y aplique una contraseña independiente para la protección del Servidor (distinta de la contraseña para otros dispositivos administrados).
- Habilite todos los módulos de protección disponibles en la aplicación de seguridad (para obtener información sobre la configuración de seguridad necesaria para usar el Servidor de administración, consulte la Ayuda de Kaspersky Endpoint Security for Linux).

Configurar directivas y tareas para las aplicaciones de Kaspersky administradas.

- Cree y aplique directivas a todos los dispositivos administrados o al grupo con nuevos dispositivos administrados para las siguientes aplicaciones:
  - Agente de red
  - Kaspersky Endpoint Security para Windows/Linux/macOS
  - Kaspersky Endpoint Agent (u otras aplicaciones de Kaspersky)
- Habilite la protección con contraseña para no deshabilitar la protección o desinstalar aplicaciones de Kaspersky.
- Bloquee la configuración de la directiva (cierre el "candado") para evitar la reasignación de esta configuración en los dispositivos administrados.
- Cree una tarea de análisis completo programada de todos los dispositivos.
- Habilite el uso de Kaspersky Security Network (KSN) y acepte la última Declaración de KSN.

- Configure el descubrimiento de dispositivos y especifique el grupo de administración predeterminado para los dispositivos recién descubiertos.
- Restrinja el uso de reglas automáticas para mover dispositivos entre grupos de administración.
- Proteja los puntos de distribución del acceso no autorizado.
- Evite asignar puntos de distribución automáticamente en redes pequeñas o redes de alta importancia.

Mantenimiento del Servidor de administración

- No elimine ni deshabilite las siguientes tareas:
  - Copia de seguridad
  - Mantenimiento del Servidor de administración
- Instale regularmente el SO y las actualizaciones de software de terceros.

Transferencia de eventos a sistemas de terceros

- Configure el control y la notificación de eventos de seguridad.
- Configurar la exportación de eventos a un sistema SIEM.
- Configure las notificaciones del Servidor para:
  - Eventos de auditoría
  - Eventos críticos
  - Eventos de falla y advertencias

Recomendaciones de seguridad para sistemas de información de terceros

- Aplique las recomendaciones de seguridad de CIS Benchmarks a los sistemas operativos, DBMS e hipervisores utilizados.
- Para Astra Linux, siga las recomendaciones de seguridad de la versión correspondiente del Libro rojo.
- Para RED OS, siga las recomendaciones proporcionadas en la documentación oficial de RED OS.

Instalación del Servidor de administración

Arquitectura del Servidor de administración

En general, la elección de una arquitectura de administración centralizada depende de la ubicación de los dispositivos protegidos, el acceso desde redes adyacentes, los esquemas de entrega de actualizaciones de bases de datos, etc.

En la etapa inicial del desarrollo de la arquitectura, recomendamos familiarizarse con los componentes de Kaspersky Security Center Linux y su interacción entre sí, así como con esquemas de tráfico de datos y uso de puertos.

Basándose en esta información, puede formar una arquitectura que especifique:

- la ubicación del Servidor de administración y las conexiones de red.
- la organización de los espacios de trabajo del administrador y los métodos de conexión al Servidor de administración.
- métodos de despliegue del Agente de red y el software de protección.
- el uso de puntos de distribución.
- el uso de Servidores de administración virtuales.
- usar una jerarquía de Servidores de administración.
- esquema de actualización de la base de datos antivirus.
- otros flujos de información.

la selección de un dispositivo para la instalación del Servidor de administración.

Recomendamos instalar el Servidor de administración en un servidor dedicado en la infraestructura de la organización. Si no hay otro software de terceros instalado en el servidor, puede configurar los ajustes de seguridad según los requisitos de Kaspersky Security Center Linux, sin depender de los requisitos del software de terceros.

Puede desplegar el Servidor de administración en un servidor físico o en un servidor virtual. Asegúrese de que el dispositivo seleccionado cumple los requisitos de hardware y software.

Restricción de despliegue del Servidor de administración en un controlador de dominio, un servidor de terminal o un dispositivo de usuario

Desaconsejamos instalar el Servidor de administración en un controlador de dominio, un servidor de terminales o un dispositivo de usuario.

Le recomendamos que proporcione una separación funcional de los nodos clave de la red. Este enfoque le permite mantener la operatividad de diferentes sistemas cuando un nodo falla o se ve comprometido. Al mismo tiempo, puede crear diferentes políticas de seguridad para cada nodo.

Cuentas para instalar y ejecutar el Servidor de administración

Durante el despliegue del Servidor de administración, es necesario crear dos cuentas sin privilegios. Los servicios incluidos en el Servidor de administración funcionarán con estas cuentas sin privilegios. A la hora de asignar derechos y permisos a las cuentas, limítese a lo justo y necesario. Evite incluir cuentas innecesarias en el grupo "kladmins".

También debe crear una cuenta interna del DBMS. El Servidor de administración utiliza esta cuenta interna del DBMS para acceder al DBMS seleccionado.

El conjunto de cuentas requeridas y sus derechos depende del tipo de DBMS seleccionado y el método de creación de la base de datos del Servidor de administración.

Seguridad de la conexión

Uso de TLS

Recomendamos prohibir las conexiones no seguras al Servidor de administración. Por ejemplo, puede prohibir las conexiones que usan HTTP en la configuración del Servidor de administración.

Tenga en cuenta que, de forma predeterminada, varios puertos HTTP del Servidor de administración están cerrados. El puerto restante se utiliza para el servidor web del Servidor de administración (8060). Este puerto puede estar limitado por la configuración del firewall del dispositivo del Servidor de Administración.

Configuración estricta de TLS

Le recomendamos usar el protocolo TLS de la versión 1.2 y posteriores, y restringir o prohibir los algoritmos de cifrado inseguros.

Puede configurar los protocolos de cifrado (TLS) usados por el Servidor de administración. Tenga en cuenta que, en el momento de lanzar una versión del Servidor de administración, la configuración del protocolo de cifrado está configurada de manera predeterminada para garantizar una transferencia de datos segura.

Restricción del acceso a la base de datos del Servidor de administración

Recomendamos restringir el acceso a la base de datos del Servidor de administración. Por ejemplo, conceda el acceso solo desde el dispositivo del Servidor de administración. Esto reduce la probabilidad de que la base de datos del Servidor de administración se vea comprometida debido a vulnerabilidades conocidas.

Puede configurar los parámetros de acuerdo con las instrucciones de funcionamiento de la base de datos usada, así como proporcionar puertos cerrados en los firewalls.

Interacción de seguridad con un SGBD externo

Si el SGBD se instala en un dispositivo independiente durante la instalación del Servidor de Administración (SGBD externo), recomendamos configurar los parámetros para una interacción y autenticación seguras con este SGBD. Para obtener más información sobre cómo configurar la autenticación SSL, consulte Autenticación del servidor PostgreSQL y Escenario: autenticación del servidor MySQL.

Configuración de una lista de admitidos de direcciones IP para conectarse al Servidor de administración

De manera predeterminada, los usuarios de Kaspersky Security Center Linux pueden iniciar sesión en Kaspersky Security Center Linux desde cualquier dispositivo donde estén instalados Kaspersky Security Center Web Console o aplicaciones de OpenAPI. Puede hacer que el Servidor de administración únicamente acepte conexiones de dispositivos que tengan una dirección IP permitida. Por ejemplo, si un intruso intenta conectarse a Kaspersky Security Center Linux a través del Servidor de Kaspersky Security Center Web Console instalado en un dispositivo que no está incluido en la lista de admitidos, no podrá iniciar sesión en Kaspersky Security Center Linux.

Configurar una lista de direcciones IP permitidas para conectarse con Kaspersky Security Center Web Console

De manera predeterminada, los usuarios de Kaspersky Security Center Linux pueden conectarse a Kaspersky Security Center Web Console desde cualquier dispositivo. En un dispositivo con Kaspersky Security Center Web Console, debe configurar el firewall (integrado en el sistema operativo o en uno de terceros) para que los operadores puedan conectarse a Kaspersky Security Center Web Console solo desde las direcciones IP permitidas.

Seguridad de la conexión al controlador de dominio durante el sondeo

Para sondear el controlador de dominio, el Servidor de administración o un punto de distribución de Linux intenta conectarse a este dominio a través de LDAPS. De forma predeterminada, la verificación del certificado no es obligatoria al conectarse. Para hacer verificar el certificado, establezca el indicador `KLNAG_LDAP_TLS_REQCERT` en 1. Además, puede especificar una ruta personalizada a la autoridad de certificación (CA) para acceder a la cadena de certificados utilizando el indicador `KLNAG_LDAP_SSL_CACERT`.

Cuentas y autenticación

Antes de seguir estos pasos, cree una copia de seguridad de los datos del Servidor de administración de Kaspersky Security Center Linux mediante la tarea Copia de seguridad de los datos del Servidor de administración o la utilidad klbackup y guarde la copia de seguridad en una localización segura. Guarde la copia de seguridad de los datos en un lugar seguro.

Uso de la autenticación de dos factores con el Servidor de administración

Kaspersky Security Center Linux utiliza autenticación de dos factores al iniciar sesión en Kaspersky Security Center Web Console, según el estándar RFC 6238 (TOTP: algoritmo de contraseña de un solo uso basado en el tiempo).

Cada vez que inicia sesión en Kaspersky Security Center Web Console, ingresa su nombre de usuario, contraseña y un código de seguridad de un solo uso adicional. Para recibir un código de seguridad de un solo uso, debe instalar una app de autenticación en su computadora o dispositivo móvil.

Existen autenticadores de software y de hardware (tokens) que admiten el estándar RFC 6238. Algunos ejemplos de autenticadores de software son Kaspersky Password Manager for Business, Google Authenticator, Microsoft Authenticator y FreeOTP.

No recomendamos en absoluto instalar la app de autenticación en el mismo dispositivo desde el que se establece la conexión con el Servidor de administración. Puede instalar una app de autenticación en su dispositivo móvil.

Uso de la autenticación de dos factores para un sistema operativo

Para garantizar una protección integral mediante el uso de la autenticación de dos factores, es necesario proteger no solo el Servidor de administración, sino también el dispositivo en el que está instalado.

Al conectarse al dispositivo donde está instalado el Servidor de administración (a través de SSH, RDP u otros protocolos), recomendamos usar la autenticación multifactor (MFA) con un token, tarjeta inteligente u otro método de autenticación.

Prohibición de guardar la contraseña de administrador

Si utiliza Kaspersky Security Center Web Console, no recomendamos guardar la contraseña de administrador en el navegador instalado en el dispositivo del usuario.

Autenticación de una cuenta de usuario interna

Por defecto, la contraseña de una cuenta de usuario interna del Servidor de Administración debe cumplir con las siguientes reglas:

- La contraseña debe tener entre 8 y 256 caracteres.
- La contraseña debe incluir caracteres de al menos tres de los grupos enumerados a continuación:
  - Letras mayúsculas (A–Z)
  - Letras minúsculas (a-z)
  - Números (0–9)
  - Caracteres especiales (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- La contraseña no debe contener espacios en blanco, caracteres Unicode o la combinación de "." y "@" cuando "." está colocado delante de "@".

De manera predeterminada, el número máximo de intentos permitidos es 10. Puede cambiar el número de intentos de entrada de contraseña permitidos.

El usuario de Kaspersky Security Center Linux puede introducir una contraseña no válida un número limitado de veces. Una vez que se alcanza el límite, la cuenta de usuario se bloquea durante una hora.

Configurar las opciones para cambiar la contraseña de una cuenta de usuario interno

Recomendamos configurar las siguientes opciones para cambiar la contraseña de una cuenta de usuario interno:

- Período de rotación de contraseñas
- Tiempo de la advertencia preliminar sobre la necesidad de cambiar la contraseña
- Valor de la opción **El usuario debe cambiar la contraseña la primera vez que inicie sesión**

Protección de una cuenta contra modificaciones sin autorización

Recomendamos habilitar una opción adicional para proteger una cuenta de usuario interno del Servidor de administración contra modificaciones no autorizadas. Esta protección debe configurarse por separado para cada usuario interno.

Grupo de administración dedicado para el Servidor de administración

Para el Servidor de administración

Recomendamos crear un grupo de administración dedicado. Otorgue a este grupo derechos de acceso especiales y cree una directiva de seguridad especial para él.

Para evitar bajar intencionadamente el nivel de seguridad del Servidor de administración, recomendamos restringir la lista de cuentas que puede administrar el grupo de administración dedicado.

Restricción de la asignación del rol de Administrador principal

Al usuario creado por la utilidad kladduser se le asigna el rol de Administrador principal en la lista de control de acceso (ACL) del Servidor de Administración o del Servidor de Administración virtual. Recomendamos evitar la asignación del rol de Administrador principal a un gran número de usuarios.

Configurar los derechos de acceso a las funciones de la aplicación

Recomendamos utilizar una configuración flexible de los derechos de acceso a las funciones de Kaspersky Security Center Linux para cada usuario o grupo de usuarios.

El control de acceso basado en funciones permite la creación de funciones de usuario estándar con un conjunto de derechos preestablecido y la asignación de esas funciones a los usuarios según su ámbito de responsabilidad.

Las principales ventajas del modelo de control de acceso basado en funciones:

- Facilidad de administración
- Jerarquía de funciones
- Enfoque de privilegios mínimos
- Segregación de deberes

Puede asignar funciones integradas a ciertos empleados en función de sus puestos o crear funciones completamente nuevas.

Al configurar funciones, preste atención a los privilegios asociados con el cambio del estado de protección del dispositivo del Servidor de administración y la instalación remota de software de terceros:

- Administrar grupos de administración
- Operaciones con el Servidor de administración
- Instalación remota
- Cambiar los parámetros para almacenar eventos y enviar notificaciones.

  Este privilegio le permite configurar notificaciones que ejecutan un script o un módulo ejecutable en el dispositivo del Servidor de administración cuando ocurra un evento.

Cuenta separada para la instalación remota de aplicaciones

Además de la diferenciación básica de derechos de acceso, recomendamos restringir la instalación remota de aplicaciones para todas las cuentas (excepto para el Administrador principal u otra cuenta especializada).

Recomendamos usar una cuenta aparte para la instalación remota de aplicaciones. Puede asignar un rol o permisos a la cuenta separada.

Auditoría periódica de todos los usuarios y las acciones de los usuarios

Recomendamos realizar una auditoría regular de todos los usuarios en el dispositivo del Servidor de administración. Esto le permite responder a ciertos tipos de amenazas de seguridad asociadas con el posible compromiso de un dispositivo.

Además, puede realizar un seguimiento de las acciones de los usuarios, como conectarse y desconectarse del Servidor de administración, conectarse al Servidor de administración con un error y modificar los objetos (para los objetos que admiten la administración de revisiones).

Administrar la protección del Servidor de administración

Selección de un software de protección del Servidor de administración

Según el tipo de instalación del Servidor de administración y la estrategia de protección general, seleccione la aplicación para proteger el dispositivo del Servidor de administración.

Si despliega el Servidor de administración en un dispositivo dedicado, le recomendamos que seleccione la aplicación Kaspersky Endpoint Security para proteger el dispositivo del Servidor de administración. Esto permite aplicar todas las tecnologías disponibles para proteger el dispositivo del Servidor de administración, incluidos los módulos de análisis de comportamiento.

Si el Servidor de administración está instalado en un dispositivo que existe en la infraestructura y se ha utilizado previamente para otras tareas, recomendamos considerar el siguiente software de protección:

- Kaspersky Industrial CyberSecurity for Nodes. Recomendamos instalar esta aplicación en dispositivos que estén incluidos en una red industrial. Kaspersky Industrial CyberSecurity for Nodes es una aplicación que cuenta con certificados de compatibilidad con varios fabricantes de software industrial.

- Aplicaciones de seguridad recomendadas. Si el Servidor de administración está instalado en un dispositivo con otro software, recomendamos tener en cuenta las recomendaciones de ese proveedor de software sobre la compatibilidad de los productos de seguridad (puede que ya haya recomendaciones para seleccionar una solución de seguridad, y quizá deba configurar la zona de confianza).

Creación de una directiva de seguridad independiente para la aplicación de protección

Recomendamos crear una directiva de seguridad independiente para la aplicación que protege el dispositivo del Servidor de administración. Esta directiva debe ser diferente de la política de seguridad para dispositivos cliente. Esto permite especificar la configuración de seguridad más adecuada para el Servidor de administración, sin afectar el nivel de protección de otros dispositivos.

Recomendamos dividir los dispositivos en grupos y luego colocar el dispositivo del Servidor de administración en un grupo separado, para el cual puede crear una directiva de seguridad especial.

Módulos de protección

Si no hay recomendaciones especiales del proveedor del software de terceros instalado en el mismo dispositivo que el Servidor de administración, recomendamos activar y configurar todos los módulos de protección disponibles (tras comprobar el funcionamiento de los mismos durante un tiempo determinado).

Configuración del firewall del dispositivo del Servidor de administración

En el dispositivo del Servidor de administración, recomendamos configurar el firewall para restringir el número de dispositivos que los administradores pueden conectar al Servidor de administración a través de Kaspersky Security Center Web Console.

De manera predeterminada, el Servidor de administración utiliza el puerto 13299 para recibir conexiones desde Kaspersky Security Center Web Console. Recomendamos restringir la cantidad de dispositivos desde los que se puede administrar el Servidor de administración mediante el uso de este puerto.

Administración de la protección del Agente de red

Para evitar que los atacantes saquen los dispositivos del control de su Servidor de administración, se recomienda encarecidamente seguir estas prácticas:

Uso de la contraseña de desinstalación

En la configuración del paquete de instalación del Agente de red, especifique la contraseña que se solicitará al desinstalar el Agente de red.

Esta funcionalidad solo está disponible para el Agente de red en dispositivos Windows.

Fortalecimiento del Agente de red

En la configuración del paquete de instalación del Agente de red, active la opción **Evitar que el servicio del Agente de red se detenga o se elimine sin autorización e impedir cambios en su configuración**. Después de instalar el Agente de red en un dispositivo administrado, el componente no se puede desinstalar ni modificar sin los privilegios necesarios. El servicio del Agente de red no se podrá detener.

Esta funcionalidad solo está disponible para el Agente de red en dispositivos Windows.

Seguimiento de la dirección del Servidor de administración al que se conecta el Agente de red

Para detectar cualquier cambio no autorizado del Agente de red a un Servidor de administración externo, utilice el registro de eventos de Kaspersky. El registro de eventos de Kaspersky es una sección del registro de eventos almacenado en el sistema operativo de los dispositivos administrados. En Windows, puede consultar el contenido del registro con el Lector de eventos y, en Linux, con la utilidad journalctl. Cuando el Agente de red se conecta al Servidor de administración, se escriben una o dos entradas en el registro de eventos de Kaspersky con la siguiente información:

- Dirección del Servidor de administración:
  - **Intentar conectarse al Servidor de administración en <dirección del Servidor de administración>**.
  - **Conectado al Servidor de administración en <dirección del Servidor de administración>**.
- La dirección del Servidor de administración y la pasarela de conexión, cuando la conexión se realiza a través de una pasarela:
  - **Intentar conectarse al Servidor de administración en <dirección del Servidor de administración> mediante CG <dirección de la pasarela de conexión>**.
  - **Conectado al Servidor de administración en <dirección del Servidor de administración> mediante CG <dirección de la pasarela de conexión>**.

Se registra un evento con la dirección del Servidor de administración en los siguientes casos:

- Cada vez que se reinicia el servicio del Agente de red
- Cuando el Agente de red se conecta a otro Servidor de administración
- Una vez al día durante el funcionamiento normal del dispositivo, aunque el servicio del Agente de red no se haya reiniciado ni el Agente de red se haya conectado a otro Servidor de administración (en este caso, solo se vuelve a escribir la segunda entrada en el registro).

Para mayor comodidad, recomendamos configurar la carga de eventos del registro de eventos de Kaspersky en un sistema SIEM y generar una alerta si la dirección del Servidor indicada en el evento no coincide con la dirección actual de su Servidor.

Administración de la protección de dispositivos cliente

Restricción al agregar claves de licencia a paquetes de instalación

Los paquetes de instalación se almacenan en la carpeta compartida del Servidor de administración, en la subcarpeta Paquetes. Si agrega una clave de licencia a un paquete de instalación, todos los usuarios con derechos de lectura en esta carpeta podrán acceder a ella (de manera directa o mediante el Servidor web integrado en el Servidor de administración).

Para no poner en riesgo la clave de licencia, no recomendamos agregar claves de licencia a los paquetes de instalación.

Recomendamos usar la distribución automática de claves de licencia a los dispositivos administrados, el despliegue al ejecutar la tarea de agregar una clave de licencia a una aplicación administrada, y agregar manualmente un código de activación o un archivo clave a los dispositivos.

Reglas automáticas para trasladar dispositivos automáticamente entre los grupos de administración

Recomendamos restringir el uso de reglas automáticas para mover dispositivos entre grupos de administración.

Si usa reglas automáticas para mover dispositivos, puede conducir a la propagación de directivas que otorguen más privilegios al dispositivo movido que los que tenía antes de la reubicación.

Además, mover un dispositivo cliente a otro grupo de administración puede provocar la propagación de la configuración de políticas. Estas configuraciones de políticas pueden ser indeseables para su distribución a dispositivos invitados y no confiables.

Esta recomendación no se aplica a la asignación inicial única de dispositivos a grupos de administración.

Requisitos de seguridad para puntos de distribución y puertas de enlace de conexión

Los dispositivos con Network Agent instalado pueden actuar como punto de distribución y realizar las siguientes funciones:

- Distribuir actualizaciones y paquetes de instalación recibidos del Servidor de administración a los dispositivos cliente dentro del grupo.
- Realizar la instalación remota de software de terceros y aplicaciones de Kaspersky en dispositivos cliente.
- Sondear la red para detectar nuevos dispositivos y actualizar la información disponible sobre los dispositivos de los que ya se tenía conocimiento. Un punto de distribución puede aplicar los mismos métodos de descubrimiento de dispositivos que el Servidor de administración.

Colocar puntos de distribución en la red de la organización que se utilizan para:

- reducir la carga del Servidor de administración
- optimizar el tráfico
- proporcionar al Servidor de administración acceso a dispositivos en puntos poco accesibles de la red de la organización

Teniendo en cuenta las capacidades disponibles, recomendamos proteger los dispositivos que actúan como puntos de distribución de cualquier tipo de acceso no autorizado (incluido el físico).

Restricción de la asignación automática de los puntos de distribución

Para simplificar la administración y mantener la operatividad de la red, recomendamos utilizar la asignación automática de puntos de distribución. Sin embargo, para redes industriales y redes pequeñas, le recomendamos que no asigne puntos de distribución automáticamente, ya que, por ejemplo, la información privada de las cuentas utilizadas para forzar tareas de instalación remota, puede transferirse a puntos de distribución por medio del sistema operativo.

Para redes industriales y redes pequeñas, puede asignar dispositivos manualmente para que actúen como puntos de distribución.

También puede ver el Informe de actividad de puntos de distribución.

Requisitos de seguridad para los dispositivos de los usuarios de Kaspersky Security Center Linux

Se deben aplicar requisitos de seguridad especiales a los dispositivos de los usuarios de Kaspersky Security Center Linux. Recomendamos proteger estos dispositivos contra cualquier tipo de acceso no autorizado (incluso físicamente).

Los dispositivos de usuarios de Kaspersky Security Center Linux incluyen los siguientes:

- Dispositivos desde los cuales los usuarios de Kaspersky Security Center Linux se conectan a Kaspersky Security Center Web Console mediante un navegador.
- Dispositivos desde los cuales las aplicaciones que interactúan con el Servidor de administración a través de OpenAPI están conectadas a Kaspersky Security Center Linux.

Requisitos de seguridad para dispositivos con Kaspersky Security Center Web Console instalado

Los dispositivos con Kaspersky Security Center Web Console instalado se utilizan para administrar Kaspersky Security Center Linux, por lo que deben aplicarse requisitos especiales a la seguridad de estos dispositivos. Recomendamos proteger estos dispositivos contra cualquier tipo de acceso no autorizado (incluso físicamente).

Configurar la protección para aplicaciones administradas

Políticas de aplicaciones administradas

Recomendamos crear una directiva para cada tipo de aplicaciones y componentes de Kaspersky Security Center Linux que se utilice (Agente de red, Kaspersky Endpoint Security para Windows, Kaspersky Endpoint Security for Linux, Kaspersky Endpoint Agent y otros). Esta directiva debe aplicarse a todos los dispositivos administrados (el grupo de administración raíz) o a un grupo aparte al que se mueven automáticamente los nuevos dispositivos administrados de acuerdo con las reglas de movimiento configuradas.

Especificar la contraseña para desactivar la protección y desinstalar la aplicación

Recomendamos encarecidamente habilitar la protección con contraseña para evitar que los intrusos deshabiliten o desinstalen las aplicaciones de seguridad de Kaspersky. En plataformas donde se admite la protección con contraseña, puede establecer la contraseña, por ejemplo, para Kaspersky Endpoint Security, Agente de red y otras aplicaciones de Kaspersky. Después de habilitar la protección con contraseña, recomendamos bloquear la configuración correspondiente al cerrar el "candado".

Especificación de la contraseña para la conexión manual de un dispositivo cliente al Servidor de administración (utilidad klmover)

La utilidad klmover le permite conectar manualmente un dispositivo cliente al Servidor de administración. La utilidad klmover se encuentra en la carpeta de instalación del Agente de red.

Para evitar que los intrusos muevan los dispositivos fuera del control de su Servidor de administración, recomendamos que active la protección con contraseña para ejecutar la utilidad klmover. Para habilitar la protección con contraseña, seleccione la opción **Utilizar contraseña de desinstalación** en la configuración de la directiva del Agente de red.

La utilidad klmover requiere derechos de administrador local.

Si pierde u olvida la contraseña del Agente de red protegido con contraseña, que está instalado en el dispositivo y que Kaspersky Security Center Linux ya no administra, no podrá eliminar el Agente de red mediante la utilidad klmover o la línea de comando. En este caso, deberá reinstalar el sistema operativo en el dispositivo que tiene instalado el Agente de red protegido con contraseña.

Al activar la opción **Utilizar contraseña de desinstalación** en los dispositivos Windows, también se activa la protección con contraseña para la herramienta Cleaner (cleaner.exe).

Usar Kaspersky Security Network

En todas las directivas de las aplicaciones administradas y en las propiedades del Servidor de administración, recomendamos habilitar el uso de Kaspersky Security Network (KSN) y aceptar la Declaración de KSN. Cuando actualiza el Servidor de administración, puede aceptar la Declaración de KSN actualizada. En algunos casos, cuando el uso de servicios de nube está prohibido por la ley u otras regulaciones, puede deshabilitar KSN.

Análisis periódico de dispositivos administrados

Recomendamos, para todos los grupos de dispositivos, crear una tarea que ejecute periódicamente un análisis completo de los dispositivos.

Detección de nuevos dispositivos

Recomendamos establecer correctamente la configuración de detección de dispositivos: configure la integración con controladores de dominio y especifique intervalos de direcciones IP para detectar nuevos dispositivos.

Por motivos de seguridad, puede utilizar el grupo de administración predeterminado que incluye todos los dispositivos nuevos y las directivas predeterminadas que afectan a este grupo.

Mantenimiento del Servidor de administración

Copia de seguridad de los datos del Servidor de administración

Las copias de seguridad de datos le permiten restaurar los datos del Servidor de administración sin pérdida de datos.

De forma predeterminada, se crea una tarea de copia de seguridad de datos automáticamente después de la instalación del Servidor de administración y se ejecuta periódicamente, guardando las copias de seguridad en el directorio adecuado.
La configuración de la tarea de copia de seguridad de datos se puede cambiar de la siguiente manera:

- La frecuencia de la copia de seguridad aumenta
- Se especifica un directorio especial para guardar copias
- Se modifican las contraseñas de las copias de seguridad

Si almacena copias de seguridad en un directorio especial distinto al directorio predeterminado, le recomendamos que limite la lista de control de acceso (ACL) de este directorio. Las cuentas del Servidor de administración y las cuentas de la base de datos del Servidor de administración deben tener acceso de escritura a este directorio.

Mantenimiento del Servidor de administración

El mantenimiento del Servidor de administración le permite reducir el volumen de la base de datos y mejorar el rendimiento y la fiabilidad del funcionamiento de la aplicación. Le recomendamos realizar un mantenimiento del Servidor de administración por lo menos una vez a la semana.

El mantenimiento del Servidor de administración se lleva a cabo a través de la tarea especializada. La aplicación realiza las acciones siguientes durante el mantenimiento del Servidor de administración:

- Reorganiza los índices de la base de datos
- Actualiza las estadísticas de la base de datos
- Reduce la base de datos si es necesario

Instalación de actualizaciones del sistema operativo y actualizaciones de software de terceros

Enfatizamos nuestra recomendación de que instale regularmente actualizaciones de software para el sistema operativo y el software de terceros en el dispositivo del Servidor de administración.

Los dispositivos cliente no requieren una conexión continua al Servidor de administración, por lo que es seguro reiniciar el dispositivo del Servidor de administración después de instalar las actualizaciones. Todos los eventos registrados en los dispositivos cliente durante el tiempo de inactividad del Servidor de administración se envían al mismo una vez que se restablece la conexión.

Transferencia de eventos a sistemas de terceros

Supervisión e informes

Para dar una respuesta oportuna a los problemas de seguridad, recomendamos configurar las funciones de supervisión y generación de informes.

Exportación de eventos a sistemas SIEM

Para obtener una detección rápida de problemas de seguridad antes de que se produzcan daños significativos, recomendamos usar la exportación de eventos en un sistema SIEM.

Notificaciones por correo electrónico de eventos de auditoría

Kaspersky Security Center Linux le permite recibir información sobre los eventos que ocurren durante el funcionamiento del Servidor de administración y aplicaciones de Kaspersky instaladas en dispositivos administrados. Para obtener una respuesta oportuna ante emergencias, recomendamos configurar el Servidor de administración para enviar notificaciones sobre los eventos de auditoría, eventos críticos, eventos de fallos y advertencias que publica.

Dado que estos eventos tienen lugar dentro del sistema, se puede esperar que no sean muchos, algo que resulta muy cómodos para enviarlos por correo.

Recomendaciones de seguridad para sistemas de información de terceros

Recomendaciones de seguridad de CIS Benchmarks

Al usar versiones de sistemas operativos, plataformas de virtualización o servidores de bases de datos compatibles con el Servidor de administración y el Agente de red, sugerimos que, de existir, aplique las prácticas de seguridad de la información recomendadas por el Center for Internet Security (CIS) para ajustar la configuración de estos sistemas de información

El Center for Internet Security (CIS) es una organización sin fines de lucro dedicada a mejorar la seguridad en el campo de la tecnología de la información. En particular, el CIS desarrolla y distribuye estándares de seguridad como CIS Controls y CIS Benchmarks. Estos estándares incluyen un conjunto de recomendaciones y prácticas para garantizar la seguridad de los sistemas de información.

El portal del CIS contiene recomendaciones para las versiones de los siguientes sistemas de información compatibles con el Servidor de administración y el Agente de red:

- Sistemas operativos de las siguientes familias:
  - Windows para equipos de escritorio
  - Windows para servidores
  - Debian
  - Ubuntu
  - CentOS
  - Oracle Linux
  - Red Hat Enterprise Linux
  - SUSE Linux Enterprise Server
  - macOS

- Plataformas de virtualización VMware
- Servidores de bases de datos:
  - Microsoft SQL Server
  - MySQL
  - MariaDB
  - PostgreSQL

Recomendaciones de seguridad para el sistema operativo Astra Linux

Si utiliza el sistema operativo Astra Linux, siga las recomendaciones de seguridad descritas en el "libro rojo" correspondiente a su versión de Astra Linux.

Recomendaciones de seguridad para el sistema operativo RED OS

Si utiliza el sistema operativo RED OS, siga las recomendaciones de seguridad de la guía del administrador descritas en la documentación oficial de RED OS.

Recomendaciones para usar las aplicaciones de seguridad de Kaspersky

Usar la contraseña de KLAdmin en Kaspersky Endpoint Security para Windows

La cuenta KLAdmin es una cuenta de administrador con acceso irrestricto a Kaspersky Endpoint Security para Windows. La cuenta KLAdmin tiene permiso para realizar cualquier acción protegida con contraseña en Kaspersky Endpoint Security para Windows y puede, incluso, desinstalar la aplicación. Los permisos de la cuenta KLAdmin no se pueden revocar. Puede configurar la contraseña de la cuenta KLAdmin en las propiedades de la directiva de Kaspersky Endpoint Security para Windows. El administrador de Kaspersky Endpoint Security para Windows es totalmente responsable del uso seguro de esta contraseña. Si su organización tiene una política de contraseñas propias, siga las directrices de esa política. Cuanto más larga y compleja sea la contraseña, más fiable será.

Estas son nuestras recomendaciones para proteger a una organización contra el robo de la contraseña de KLAdmin:

- **Requisitos generales**

  No utilice el nombre de la cuenta o parte del nombre como contraseña.

- **Requisitos mínimos sobre la longitud de la contraseña**

  Cree una contraseña de 10 caracteres o más.

- **Requisitos sobre el uso de varios tipos de caracteres**

  Establezca una contraseña compleja que contenga caracteres de diferentes categorías: letras minúsculas y mayúsculas, números y caracteres especiales.

- **Requisitos sobre la caducidad de la contraseña**

  Establezca la fecha mínima de caducidad de la contraseña en 90 días. Una nueva contraseña no debe coincidir con ninguna de las 24 contraseñas anteriores.

Escenario: autenticación del servidor MySQL

Le recomendamos que utilice un certificado TLS para autenticar el servidor MySQL. Puede usar un certificado de una autoridad de certificación (AC) de confianza o un certificado autofirmado.

El Servidor de administración admite autenticación SSL unidireccional y bidireccional para MySQL.

Habilitación de la autenticación SSL unidireccional

Siga estos pasos a fin de configurar la autenticación SSL unidireccional para MySQL:

1. **Cree un certificado TLS autofirmado para el servidor MySQL**

   Ejecute el siguiente comando:

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

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

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

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

2. **Cree un archivo de indicador del servidor**

   Use la utilidad klscflag para crear el indicador del servidor KLSRV_MYSQL_OPT_SSL_CA y especifique la ruta al certificado como su valor: La utilidad klscflag se encuentra en el directorio en el que está instalado el Servidor de administración. La ruta de instalación predeterminada es /opt/kaspersky/ksc64/sbin.

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <ruta a ca-cert.pem> -t d
   ```

3. **Configure las bases de datos**

   Especifique los certificados en el archivo my.cnf. Abra el archivo my.cnf en un editor de texto y agregue las siguientes líneas en la sección [mysqld]:

   ```
   [mysqld]
   ```

   ```
   ssl-ca=".../mysqlcerts/ca-cert.pem"
   ```

   ```
   ssl-cert=".../mysqlcerts/server-cert.pem"
   ```

   ```
   ssl-key=".../mysqlcerts/server-key.pem"
   ```

Habilitación de la autenticación SSL bidireccional

Siga estos pasos a fin de configurar la autenticación SSL bidireccional para MySQL:

1. **Cree archivos de indicador del servidor**

   Use la utilidad klscflag para crear indicadores del servidor y especifique la ruta a los archivos de certificados como sus valores:

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <ruta a ca-cert.pem> -t s
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CERT -v <ruta a server-cert.pem> -t s
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_KEY -v <ruta a server-key.pem> -t s
   ```

   La utilidad klscflag se encuentra en el directorio en el que está instalado el Servidor de administración. La ruta de instalación predeterminada es /opt/kaspersky/ksc64/sbin.

2. **Especifique la frase de contraseña (opcional)**

   Si server-key.pem requiere una frase de contraseña, cree un indicador KLSRV_MARIADB_OPT_TLS_PASPHRASE y especifique la frase de contraseña como su valor:

   ```
   klscflag -fset -pv klserver -n KLSRV_MARIADB_OPT_TLS_PASPHRASE -v <frase de contraseña> -t s
   ```

3. **Configure las bases de datos**

   Especifique los certificados en el archivo my.cnf. Abra el archivo my.cnf en un editor de texto y agregue las siguientes líneas en la sección [mysqld]:

   ```
   [mysqld]
   ssl-ca=".../mysqlcerts/ca-cert.pem"
   ssl-cert=".../mysqlcerts/server-cert.pem"
   ssl-key=".../mysqlcerts/server-key.pem"
   ```

Escenario: autenticación TLS bidireccional de PostgreSQL para la base de datos del Servidor de administración y la base de datos de IAM

En Kaspersky Security Center Linux, puede configurar el cifrado y la validación mutua de certificados entre el servidor PostgreSQL y los clientes, es decir, el Servidor de administración e IAM. Cada base de datos utiliza un usuario y un certificado de cliente independientes. Además de TLS, se utiliza la autenticación mediante contraseña `scram-sha-256`.

La autenticación del servidor PostgreSQL se realiza por etapas:

1. **Preparación del DBMS y creación de roles**

   Ejecute el siguiente comando:

   ```
   sudo -u postgres psql
   CREATE DATABASE kav;
   CREATE DATABASE iam;
   CREATE USER myuserksc WITH PASSWORD '*password*';
   ```

```
ALTER ROLE myuserksc WITH LOGIN CREATEDB;
ALTER DATABASE kav OWNER TO myuserksc;
CREATE USER myuseriam WITH PASSWORD '*password*';
ALTER ROLE myuseriam WITH LOGIN CREATEDB;
ALTER DATABASE iam OWNER TO myuseriam;
```

2. Creación de su propia CA y de un certificado de servidor (autenticación SSL unidireccional)

`subjectAltName` (SAN) es un parámetro obligatorio del certificado de servidor. El valor de este parámetro debe coincidir con el FQDN del host.

Ejecute el siguiente comando:

```
sudo openssl req -x509 -nodes -newkey rsa:4096 -keyout
/etc/ssl/private/postgresql_ca.key -out /etc/ssl/certs/postgresql_ca.crt -days 365 -
addext "subjectAltName=DNS:*FQDN*" -subj "/CN=mysrvca"
sudo openssl req -new -nodes -newkey rsa:4096 -keyout
/etc/ssl/private/postgresql_leaf.key -out /tmp/postgresql_leaf.csr -addext
"subjectAltName=DNS:< FQDN >" -subj "/CN=*FQDN*"
sudo openssl x509 -req -in /tmp/postgresql_leaf.csr -CA
/etc/ssl/certs/postgresql_ca.crt -CAkey /etc/ssl/private/postgresql_ca.key -
CAcreateserial -out /etc/ssl/certs/postgresql_leaf.crt -days 365 -sha256 -
copy_extensions copy
sudo cat /etc/ssl/certs/postgresql_leaf.crt /etc/ssl/certs/postgresql_ca.crt | sudo
tee /etc/ssl/certs/postgresql.crt
sudo chmod 600 /etc/ssl/private/postgresql_leaf.key
sudo chown postgres:postgres /etc/ssl/private/postgresql_leaf.key
sudo chmod 644 /etc/ssl/certs/postgresql_leaf.crt
sudo chown ksc:kladmins /etc/ssl/certs/postgresql_ca.crt
sudo chmod 644 /etc/ssl/certs/postgresql_ca.crt
sudo chmod 644 /etc/ssl/certs/postgresql.crt
```

3. Creación de una autoridad de certificación (CA) de cliente y certificados para la base de datos del Servidor de administración y la base de datos de IAM (autenticación SSL bidireccional)

Ejecute el siguiente comando:

```
sudo openssl req -x509 -nodes -newkey rsa:4096 -keyout
/etc/ssl/private/postgresql_cli_ca.key -out /etc/ssl/certs/postgresql_cli_ca.crt -days
365 -subj "/CN=myclica"
openssl x509 -in /etc/ssl/certs/postgresql_cli_ca.crt -text -noout
sudo chmod 600 /etc/ssl/private/postgresql_cli_ca.key
sudo chmod 644 /etc/ssl/certs/postgresql_cli_ca.crt
openssl req -new -nodes -newkey rsa:4096 -keyout $HOME/postgresql_cli_myuserksc.key -
out /tmp/postgresql_cli_myuserksc.csr -subj "/CN=myuserksc"
sudo openssl x509 -req -in /tmp/postgresql_cli_myuserksc.csr -CA
/etc/ssl/certs/postgresql_cli_ca.crt -CAkey /etc/ssl/private/postgresql_cli_ca.key -
CAcreateserial -out $HOME/postgresql_cli_myuserksc.crt -days 365
openssl req -new -nodes -newkey rsa:4096 -keyout $HOME/postgresql_cli_myuseriam.key -
out /tmp/postgresql_cli_myuseriam.csr -subj "/CN=myuseriam"
sudo openssl x509 -req -in /tmp/postgresql_cli_myuseriam.csr -CA
/etc/ssl/certs/postgresql_cli_ca.crt -CAkey /etc/ssl/private/postgresql_cli_ca.key -
CAcreateserial -out $HOME/postgresql_cli_myuseriam.crt -days 365
```

4. Copia de certificados de cliente al Servidor de administración y al host de IAM y configuración de permisos

Ejecute el siguiente comando:

```
sudo cp $HOME/postgresql_cli_myuserksc.crt   /home/ksc/
sudo cp $HOME/postgresql_cli_myuserksc.key   /home/ksc/
sudo cp $HOME/postgresql_cli_myuseriam.crt   /home/ksciam/
sudo cp $HOME/postgresql_cli_myuseriam.key   /home/ksciam/
sudo chown ksc:kladmins /home/ksc/*.crt /home/ksc/*.key
sudo chown ksciam:kladmins /home/ksciam/*.crt /home/ksciam/*.key
sudo chmod 644 /home/ksc/*.crt
```

```
sudo chmod 600 /home/ksc/*.key
sudo chmod 644 /home/ksciam/*.crt
sudo chmod 600 /home/ksciam/*.key
```

5. **Configuración de PostgreSQL**

   Edite el archivo postgresql.conf de la siguiente manera:

   ```
   listen_addresses = '*'
   ssl = on
   ssl_cert_file = '*path to postgresql.crt*'
   ssl_key_file = '*path to postgresql_leaf.key*'
   ssl_ca_file = '*path to postgresql_cli_ca.crt*'
   ```

   Modifique el archivo pg_hba.conf de la siguiente manera:

   ```
   hostssl    kav    myuserksc    *Administration Server IP address*    scram-sha-256
   clientcert=verify-full
   hostssl    iam    myuseriam    *Administration Server IP address*    scram-sha-256
   clientcert=verify-full
   ```

   Si el Servidor de administración y PostgreSQL están en el mismo dispositivo, utilice la dirección `127.0.0.1/32` y `listen_addresses = 'localhost'`.

   Asegúrese de que pg_hba.conf no incluya un registro que comience con `host`.

6. **Reiniciar el servicio en segundo plano PostgreSQL**

   Ejecute el siguiente comando:

   ```
   systemctl restart postgresql
   ```

7. **Especificar el indicador de servidor para el Servidor de administración**

   Use la utilidad klscflag para crear indicadores del servidor y especifique la ruta a los archivos de certificados como sus valores.

   La utilidad klscflag se encuentra en la carpeta donde está instalado el Servidor de administración. La ruta de instalación predeterminada es `/opt/kaspersky/ksc64/sbin/`.

   Ejecute el siguiente comando:

   ```
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CERT -v *path to
   postgresql_cli_myuserksc.crt* -t s
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_KEY -v *path to
   postgresql_cli_myuserksc.key* -t s
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v *path to
   postgresql_ca.crt* -t s
   ```

   Si postgres_leaf.key requiere una frase de contraseña, cree un indicador KLSRV_POSTGRES_OPT_TLS_PASPHRASE y especifique la frase de contraseña como su valor:

   ```
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_TLS_PASPHRASE -v *pasphrase* -t s
   ```

8. **Configurar IAM**

   Edite el archivo iam_config.yaml de la siguiente manera:

   ```
   dbms_tl_opt_ssl_ca: "/etc/ssl/certs/postgresql_ca.crt"
   dbms_tl_opt_ssl_verify_server_cn: "1"
   dbms_tl_opt_ssl_cert: "/home/ksc/postgresql_cli_myuseriam.crt"
   dbms_tl_opt_ssl_key:  "/home/ksc/postgresql_cli_myuseriam.key"
   ```

9. **Reiniciar los servicios del Servidor de administración**

   Ejecute el siguiente comando:

   ```
   sudo systemctl restart kl*
   ```

Preparativos para el despliegue

En esta sección se describe cómo elegir la opción de despliegue de Kaspersky Security Center Linux, la configuración de Kaspersky Security Center Linux y un DBMS según las necesidades de su organización.

Hay varias opciones para el despliegue de componentes de Kaspersky Security Center Linux en la red de una organización, y su elección depende de los siguientes criterios:

- Número total de dispositivos.
- Unidades (oficinas locales, sucursales) que se separan a nivel organizacional o geográfico.
- Redes independientes conectadas por canales estrechos.
- Necesidad de acceso por Internet al Servidor de administración.

Un Servidor de administración puede admitir hasta 50 000 dispositivos (con PostgreSQL o Postgres Pro como DBMS). Cuando el número total de dispositivos en la red de una organización supera los 50 000, resulta necesario instalar varios Servidores de administración en esa red y combinarlos en una jerarquía para lograr una administración centralizada conveniente.

Si una organización incluye oficinas locales remotas a gran escala (sucursales) con sus propios administradores, es útil instalar Servidores de administración en dichas oficinas. De otra forma, esas oficinas se deben ver como redes separadas conectadas por canales de bajo rendimiento, consulte la sección "Configuración estándar: pocas oficinas a gran escala ejecutadas por sus propios administradores".

Al usar redes separadas conectadas a canales estrechos, puede ahorrarse tráfico al asignar uno o varios Agentes de red para que funcionen como puntos de distribución (consulte tabla para la evaluación del número de puntos de distribución). En este caso, todos los dispositivos en una red separada recuperan actualizaciones desde tales centros de actualización locales. Los puntos de distribución reales pueden descargar actualizaciones tanto desde el Servidor de administración (escenario predeterminado) como desde servidores de Kaspersky en Internet (ver la sección "Configuración estándar: varias oficinas pequeñas remotas").

La sección "Configuraciones estándares de Kaspersky Security Center Linux" proporciona descripciones detalladas de las configuraciones estándares de Kaspersky Security Center Linux. Al planificar el despliegue, elija la configuración estándar más conveniente, según la estructura de la organización.

En la etapa de planificación del despliegue, es necesario tener en cuenta la asignación del certificado especial X.509 al Servidor de administración. La asignación del certificado X.509 al Servidor de administración puede ser útil en los casos siguientes (lista parcial):

- Inspección del tráfico de la capa de sockets seguros (SSL) por medio de un proxy de cancelación de la SSL, o para usar un proxy inverso
- Integración con la infraestructura de claves públicas (PKI) de una organización
- Para especificar los valores requeridos de los campos del certificado
- Para proporcionar la solidez de cifrado deseada del certificado

Seleccionar configuraciones estándares de Kaspersky Security Center Linux

Esta sección describe las configuraciones estándares siguientes usadas para la distribución de componentes de Kaspersky Security Center Linux en la red de la organización:

- Oficina única
- Unas pocas oficinas a gran escala, que están geográficamente separadas y son dirigidas por sus propios administradores
- Varias oficinas pequeñas, que están geográficamente separadas.

Configuración estándar: oficina única

Puede haber uno o varios Servidores de administración instalados en la red de la organización. El número de Servidores de administración se puede seleccionar según el hardware disponible o el número total de dispositivos administrados.

Un Servidor de administración puede admitir hasta 50 000 dispositivos (con PostgreSQL o Postgres Pro como DBMS). Considere la posibilidad de aumentar el número de dispositivos administrados en el futuro próximo: puede ser útil conectar un número levemente menor de dispositivos a un solo Servidor de administración.

Los Servidores de administración pueden instalarse en la red interna o en la DMZ; la decisión dependerá de si se necesita o no acceder a los Servidores de administración por Internet.

Si se utilizan varios servidores, se recomienda que los combine en una jerarquía. La utilización de una jerarquía de Servidores de administración le permite evitar directivas y tareas duplicadas y gestionar el conjunto entero de dispositivos administrados como si estuvieran administrados por un Servidor de administración único (es decir, buscar dispositivos, crear selecciones de dispositivos y crear informes).

Configuración estándar: algunas oficinas a gran escala dirigidas por sus propios administradores

Si la organización tiene unas pocas oficinas grandes geográficamente separadas, debe considerar la opción de desplegar Servidores de administración en cada una de ellas. Se pueden desplegar uno o varios Servidores de administración por oficina, según la cantidad de dispositivos cliente y el hardware disponibles. En este caso, cada una de las oficinas se puede ver como una "Configuración estándar: oficina única". Para facilitar la administración, le recomendamos que combine todos los Servidores de administración en una jerarquía (de ser posible, de varios niveles).

Si hay empleados que se mueven entre distintas oficinas con sus dispositivos (computadoras portátiles), cree perfiles de conexión del Agente de red en la directiva del Agente de red.

Configuración estándar: varias oficinas remotas pequeñas

Esta configuración estándar es útil para una oficina central y muchas oficinas remotas pequeñas que pueden comunicarse con la oficina central por Internet. Cada una de las oficinas remotas puede localizarse detrás de la Traducción de la Dirección de red (NAT), es decir, no puede establecerse ninguna conexión entre dos oficinas remotas, dado que están aisladas.

Debe desplegarse un Servidor de administración en la oficina central y deben asignarse uno o varios puntos de distribución al resto de las oficinas. Si las oficinas están conectadas a través de Internet, puede ser útil crear una tarea *Descargar actualizaciones a los repositorios de puntos de distribución* para los puntos de distribución, de modo que descarguen las actualizaciones directamente desde los servidores de Kaspersky, carpeta local o de la red, no desde el Servidor de administración.

Si algunos dispositivos en una oficina remota no tienen acceso directo al Servidor de administración (por ejemplo, el acceso al Servidor de administración se proporciona mediante Internet, pero algunos dispositivos no tienen acceso a Internet), los puntos de distribución se deben cambiar al modo de puerta de enlace de conexión. En este caso, los Agentes de red de los dispositivos en la oficina remota se conectarán, para realizar una sincronización adicional, con el Servidor de administración, pero a través de la puerta de enlace, no directamente.

Como es muy probable que el Servidor de administración no pueda realizar un sondeo de la red de la oficina remota, puede ser útil transferir esta función a un punto de distribución.

El Servidor de administración no podrá enviar notificaciones al puerto UDP 15000 a dispositivos administrados ubicados detrás de la NAT en la oficina remota. Para resolver este problema, puede habilitar el modo de conexión continua al Servidor de administración en las propiedades de los dispositivos que actúan como puntos de distribución (casilla **No desconectar del Servidor de administración**). Este modo está disponible si el número total de puntos de distribución no supera los 300. Utilice servidores push para asegurarse de que haya una conectividad continua entre un dispositivo administrado y el Servidor de administración. Consulte el siguiente artículo para obtener más detalles: Habilitación de un servidor push.

Selección de una estructura para la protección de una empresa

La selección de una estructura para la protección de una organización depende de los siguientes factores:

- Topología de red de la organización.
- Estructura organizativa.
- Número de empleados a cargo de la protección de la red y asignación de sus responsabilidades.
- Recursos de hardware que se pueden asignar a los componentes de administración de protección.
- Volumen de trabajo de los canales de comunicación que se puede asignar para el mantenimiento de los componentes de protección en la red de la organización.
- Límites de tiempo para ejecutar las operaciones administrativas críticas en la red de la organización. Las operaciones administrativas críticas incluyen, por ejemplo, la distribución de bases de datos antivirus y la modificación de las directivas de los dispositivos cliente.

Al seleccionar una estructura de protección, se recomienda que, en primer lugar, se estimen los recursos de red y hardware disponibles que se pueden usar para la operación de un sistema de protección centralizado.

Para analizar la red e infraestructura del hardware, se recomienda que siga el proceso a continuación:

1. Defina la siguiente configuración de la red en la que se desplegará la protección:
   - Número de segmentos de red.
   - Velocidad de los canales de comunicación entre segmentos de red individuales.
   - Número de dispositivos administrados en cada segmento de red.
   - Volumen de trabajo de cada canal de comunicación que se puede asignar para mantener operativa la protección.
2. Determina el tiempo máximo permitido para la ejecución de operaciones administrativas clave para todos los dispositivos administrados.
3. Analice la información de los pasos 1 y 2, así como los datos de las pruebas de carga del sistema de administración. Según el análisis, responda las siguientes preguntas:
   - ¿Es posible prestar servicio a todos los clientes con un solo Servidor de administración o se requiere una jerarquía de Servidores de administración?
   - ¿Qué configuración de hardware de los Servidores de administración se requiere para manejar todos los clientes dentro de los plazos especificados en el paso 2?
   - ¿Es preciso usar los puntos de distribución para reducir la carga en los canales de comunicación?

Si obtiene las respuestas a las preguntas del paso 3 anterior, podrá compilar un conjunto de estructuras permitidas de protección de la organización.

En la red de la organización, puede usar una de las siguientes estructuras de protección estándares:

- Un Servidor de administración. Todos los dispositivos cliente están conectados a un solo Servidor de administración. El Servidor de administración funciona como el punto de distribución.
- Un Servidor de administración con puntos de distribución. Todos los dispositivos cliente están conectados a un solo Servidor de administración. Algunos de los dispositivos cliente conectados a una red funcionan como puntos de distribución.
- Jerarquía de Servidores de administración. Se asigna un Servidor de administración a cada uno de los segmentos de la red y estos pasan a formar una jerarquía general de Servidores de administración. El Servidor de administración principal funciona como punto de distribución.
- Jerarquía de Servidores de administración con puntos de distribución. Se asigna un Servidor de administración a cada uno de los segmentos de la red y estos pasan a formar una jerarquía general de Servidores de administración. Algunos de los dispositivos cliente conectados a una red funcionan como puntos de distribución.

Esquemas típicos para desplegar un sistema de protección

Esta sección describe los esquemas estándares de distribución de un sistema de protección con Kaspersky Security Center.

El sistema se debe proteger contra cualquier tipo del acceso no autorizado. Le recomendamos que instale todas las actualizaciones de seguridad disponibles para su sistema operativo antes de instalar la aplicación en su dispositivo y que proteja físicamente los Servidores de administración y los puntos de distribución.

Puede usar Kaspersky Security Center para distribuir un sistema de protección en una red corporativa por medio de los siguientes esquemas de distribución:

- Despliegue de un sistema de protección a través de Kaspersky Security Center Web Console.

  Las aplicaciones de Kaspersky se instalan de manera automática en los dispositivos cliente, que a su vez se conectan automáticamente al Servidor de administración mediante Kaspersky Security Center.

- Distribución de un sistema de protección de manera manual mediante los paquetes de instalación independientes creados en Kaspersky Security Center.

  La instalación de las aplicaciones de Kaspersky en los dispositivos cliente y en la estación de trabajo del administrador se realiza manualmente; la configuración para conectar los dispositivos cliente al Servidor de administración se define durante la instalación del Agente de red.

  Este método de despliegue se recomienda cuando no existe la posibilidad de realizar instalaciones remotas.

Kaspersky Security Center no admite la implementación mediante políticas de grupo de Microsoft Active Directory®.

Selección de un DBMS

La siguiente tabla enumera las opciones de DBMS válidas, así como las recomendaciones y las restricciones en su uso.

Recomendaciones y restricciones en DBMS

DBMS	Recomendaciones y restricciones
MySQL (ver versiones compatibles)	Utilice este DBMS si planea ejecutar un solo Servidor de administración para menos de 20 000 dispositivos.
MariaDB (ver versiones compatibles)	Utilice este DBMS si planea ejecutar un solo Servidor de administración para menos de 20 000 dispositivos.
PostgreSQL, Postgres Pro (ver versiones compatibles)	Utilice este DBMS si planea ejecutar un solo Servidor de administración para menos de 50 000 dispositivos.
Tantor (consulte las versiones compatibles)	Utilice este DBMS si planea ejecutar un solo Servidor de administración para menos de 50 000 dispositivos. El DBMS de Tantor solo es compatible con Astra Linux Special Edition RUSB.10015-01 (actualización operativa 1.8).

Para obtener información sobre cómo instalar el DBMS seleccionado, consulte su documentación.

Se recomienda deshabilitar la Tarea del inventario del software y deshabilitar (en la configuración de directivas de Kaspersky Endpoint Security) las notificaciones del Servidor de administración en las aplicaciones iniciadas.

Si decide instalar PostgreSQL o Postgres Pro, asegúrese de especificar la contraseña del superusuario. Si no especifica esta contraseña, es posible que el Servidor de administración no pueda conectarse a la base de datos.

Si instala MySQL, MariaDB, PostgreSQL, o Postgres Pro, use la configuración recomendada para garantizar que el DBMS funcione correctamente.

Si usa un DBMS PostgreSQL, MariaDB o MySQL, la pestaña **Eventos** puede mostrar una lista incompleta de eventos para el dispositivo cliente seleccionado. Esto ocurre cuando el DBMS almacena una gran cantidad de eventos. Realice una de las siguientes acciones si desea aumentar la cantidad de eventos mostrados:

- Eliminación de eventos innecesarios.
- Reducción del plazo de almacenamiento para eventos innecesarios.

Para ver una lista completa de eventos registrados en el Servidor de administración para el dispositivo, use Informes.

Suministro de acceso a Internet al Servidor de administración

Los casos siguientes requieren acceso a Internet para el Servidor de administración:

- Actualizar periódicamente las bases de datos, los módulos de software y las aplicaciones de Kaspersky
- Actualización de software de terceros

  De forma predeterminada, el Servidor de administración no requiere conexión a Internet para instalar las actualizaciones de software de Microsoft en los dispositivos administrados. Los dispositivos administrados pueden descargar las actualizaciones de software de Microsoft directamente de los servidores de Microsoft Update, por ejemplo, o de un servidor Windows Server que esté desplegado en la red de la organización y que tenga Windows Server Update Services (WSUS) habilitado. El Servidor de administración debe tener conexión a Internet en los siguientes casos:

  - Al usar un Servidor de administración como servidor WSUS
  - Para instalar actualizaciones de software de terceros que no sean software de Microsoft
- Reparación de vulnerabilidades en el software de terceros

  Existe una conexión a Internet que le permita al Servidor de administración realizar las siguientes tareas:

  - Hacer una lista de reparaciones recomendadas para vulnerabilidades en el software de Microsoft. Los especialistas de Kaspersky crean y actualizan periódicamente esta lista.
  - Reparar vulnerabilidades en software de terceros que no sean Microsoft.
- Administración de dispositivos (portátiles) de usuarios fuera de la oficina
- Administración de dispositivos en oficinas remotas
- Interacción con Servidores de administración principales o secundarios localizados en oficinas remotas
- Administración de dispositivos móviles

Esta sección describe modos habituales de proporcionar acceso al Servidor de administración a través de Internet. Cada uno de los casos que se centra en proporcionar acceso a Internet al Servidor de administración puede requerir un certificado dedicado para el Servidor de administración.

Acceso a Internet: Servidor de administración en una red local

Si el Servidor de administración está ubicado en la red interna de una organización, puede hacer que el puerto TCP 13000 del Servidor de administración sea accesible desde fuera mediante el redireccionamiento de puertos.

Acceso a Internet: Servidor de administración en la zona desmilitarizada (DMZ)

Si el Servidor de administración está ubicado en la DMZ de la red de la organización, no tiene acceso a la red interna de la organización. Por lo tanto, las limitaciones siguientes se aplican:

- El Servidor de administración no puede detectar dispositivos nuevos.
- El Servidor de administración no puede realizar el despliegue inicial del Agente de red a través de la instalación forzada en dispositivos en la red interna de la organización.

  Esto solo se aplica a la instalación inicial del Agente de red. Algunas otras actualizaciones del Agente de red o la instalación de la aplicación de seguridad pueden ser, sin embargo, realizadas por el Servidor de administración.

Tenga en cuenta que Kaspersky Security Center Linux no admite la implementación mediante políticas de grupo de Microsoft Windows.

Puede utilizar puntos de distribución ubicados en la red de la organización. Para realizar el despliegue inicial en dispositivos sin el Agente de red, primero instale el Agente de red en uno de los dispositivos y luego asígnele el estado de punto de distribución. Como resultado, la instalación inicial del Agente de red en otros dispositivos será realizada por el Servidor de administración a través de este punto de distribución.

Para garantizar el envío correcto de notificaciones al puerto UDP 15000 en dispositivos administrados ubicados dentro de la intranet de la organización, debe abarcar la red completa de puntos de distribución. En las propiedades de los puntos de distribución que se asignaron, seleccione la casilla de verificación **No desconectar del Servidor de administración**. Como resultado, el Servidor de administración establecerá una conexión continua con los puntos de distribución y estos podrán enviar notificaciones al puerto UDP 15 000 en dispositivos dentro de la red interna de la organización (puede ser una red IPv4 o IPv6).

Instalación

En esta sección, se describe la instalación de Kaspersky Security Center Linux y Kaspersky Security Center Web Console.

Configurar el servidor MariaDB x64 para trabajar con Kaspersky Security Center Linux

Para configurar correctamente el servidor MariaDB x64 para que funcione con Kaspersky Security Center, debe usar los parámetros del servidor predeterminados, con la excepción de los parámetros del servidor que se especifican en este artículo.

Valores recomendados para el archivo my.cnf

Para obtener más información sobre la configuración de DBMS, consulte también el procedimiento de configuración de la cuenta. Para obtener información sobre la instalación de DBMS, consulte el procedimiento de instalación de un DBMS.

Para configurar el archivo my.cnf:

1. Abra el archivo my.cnf en un editor de texto.

2. Ingrese las siguientes líneas en la sección [mysqld] del archivo my.cnf:

```
sort_buffer_size=10M
join_buffer_size=100M
join_buffer_space_limit=300M
join_cache_level=8
tmp_table_size=512M
max_heap_table_size=512M
key_buffer_size=200M
innodb_buffer_pool_size=< 80 % de la RAM asignada al DBMS; consulte la documentación
de su DBMS para obtener recomendaciones >
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
sql_mode="STRICT_TRANS_TABLES,NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION"
```

   Tenga en cuenta que la memoria especificada en el valor `innodb_buffer_pool_size` se asigna al inicio del servidor. Si el tamaño de la base de datos es más pequeño que el tamaño del búfer especificado, solo se asigna la memoria necesaria. Si utiliza MariaDB 10.4.3 o una versión anterior, la cantidad de memoria asignada será, en la práctica, aproximadamente un 10 % superior al tamaño especificado para el búfer. Para obtener recomendaciones sobre cómo configurar `innodb_buffer_pool_size` y otra información adicional, consulte la documentación de MySQL.

   Se recomienda utilizar el valor del parámetro `innodb_flush_log_at_trx_commit=0`, porque los valores "1" o "2" afectan negativamente la velocidad de funcionamiento de MariaDB. Asegúrese de que el parámetro `innodb_file_per_table` esté establecido en `1`.

   Para MariaDB 10.1, ingrese adicionalmente las siguientes líneas en la sección [mysqld]:

```
innodb_file_format='Barracuda'
innodb_default_row_format=dynamic
innodb_large_prefix=1
```

Para MariaDB 10.6, ingrese adicionalmente las siguientes líneas en la sección [mysqld]:

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

De forma predeterminada, los complementos del optimizador `join_cache_incremental`, `join_cache_hashed`, `join_cache_bka` están habilitados. Si estos complementos no están habilitados, debe habilitarlos.

Para comprobar si los complementos optimizadores están habilitados o no:

1. En la consola cliente MariaDB, ejecute el comando:

   ```
   SELECT @@optimizer_switch;
   ```

2. Compruebe que la salida contenga las siguientes líneas:

   ```
   join_cache_incremental=on
   join_cache_hashed=on
   join_cache_bka=on
   ```

   Si estas líneas están presentes y tienen los valores `on`, luego se habilitan los complementos del optimizador.

   Si estas líneas faltan o tienen valores `off`, debe hacer lo siguiente:

   a. Abra el archivo my.cnf en un editor de texto.

   b. Agregue las siguientes líneas en el archivo my.cnf:

   ```
   optimizer_switch='join_cache_incremental=on'
   optimizer_switch='join_cache_hashed=on'
   optimizer_switch='join_cache_bka=on'
   ```

Los complementos `join_cache_incremental`, `join_cache_hash` y `join_cache_bka` están habilitados.

Aumente el límite predeterminado de archivos que se pueden abrir (descriptores de archivo) para que el servicio systemd de MariaDB garantice la estabilidad bajo carga.

Para aumentar el límite de descriptores de archivos, siga estos pasos:

1. Ejecute el siguiente comando:

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

2. Especifique el límite de los descriptores de archivo en el parámetro `LimitNOFILE` de la sección `[Service]`:

   ```
   LimitNOFILE=1048576
   ```

3. Ejecute el siguiente comando para asegurarse de que los parámetros se especificaron correctamente:

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

4. Ejecute el siguiente comando para volver a cargar el proceso systemd:

   ```
   sudo systemctl daemon-reload
   ```

5. Ejecute el siguiente comando para reiniciar el servicio de MariaDB:

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

   Se aumentó el límite de descriptores de archivos.

Configurar un servidor DBMS basado en PostgreSQL para que funcione con Kaspersky Security Center Linux

En este artículo se describe cómo configurar un Servidor de administración implementado en un solo dispositivo. Si utiliza un clúster de DBMS de alta disponibilidad, lea el artículo Preparación de un clúster de DBMS de alta disponibilidad para que funcione con Kaspersky Security Center Linux.

Kaspersky Security Center Linux es compatible con los DBMS basados en PostgreSQL. Para configurar un servidor de base de datos PostgreSQL para que funcione con Kaspersky Security Center Linux, utilice la configuración predeterminada del servidor, excepto los ajustes que se indican en este artículo.

> La ruta predeterminada al archivo de configuración es `/etc/postgresql/<VERSION>/main/postgresql.conf`.
> En el sistema operativo ALT Linux, la ruta predeterminada es `/var/lib/pgsql/data/postgresql.conf`

Para preparar el DBMS para la instalación de Kaspersky Security Center Linux:

1. Configure los ajustes necesarios del servidor de DBMS de acuerdo con la documentación del DBMS.
2. Para integrar de manera óptima el DBMS con Kaspersky Security Center Linux, especifique los siguientes ajustes:
   - `max_connections = 151`
   - `shared_buffers = N`

     N = 25 % del tamaño de la RAM estimado para el DBMS. Si el DBMS se instala en un dispositivo junto con el servidor de administración, el cálculo debe basarse en la RAM asignada para el DBMS, no en la RAM total del dispositivo.

     Si el dispositivo tiene menos de 1 GB de memoria RAM, deje el valor predeterminado.
   - `temp_buffers = 24MB`
   - `work_mem = 16MB`
   - `maintenance_work_mem = 128MB`
   - `max_stack_depth` =tamaño máximo de la pila (ejecute el comando "`ulimit -s`" comando para obtener este valor en KB) menos el margen de seguridad de 1 MB
   - `max_parallel_workers_per_gather = 0`
   - `standard_conforming_strings = on`

   Si utiliza Postgres Pro 15.7 o Postgres Pro 15.7.1, desactive el parámetro `enable_compound_index_stats`:

   `enable_compound_index_stats = off`

   Vuelva a cargar la configuración o reinicie el servidor del DBMS después de actualizar el archivo de configuración mediante el siguiente comando:

   `sudo systemctl restart postgresql-<version>`

o

```
sudo systemctl restart postgresql
```

3. Cree bases de datos y cuentas de usuario.

   Para obtener instrucciones sobre cómo crear bases de datos y configurar cuentas de usuario para un DBMS basado en PostgreSQL, consulte el artículo Creación de bases de datos basadas en PostgreSQL y cuentas de usuario.

El DBMS está listo para la instalación de Kaspersky Security Center Linux.

Configurar el servidor MySQL x64 para trabajar con Kaspersky Security Center Linux

Para configurar correctamente el servidor MySQL x64 para que funcione con Kaspersky Security Center, debe usar los parámetros del servidor predeterminados, con la excepción de los parámetros del servidor que se especifican en este artículo.

Si utiliza el servidor MySQL para Kaspersky Security Center, habilite la compatibilidad con los sistemas de almacenamiento InnoDB y MEMORY. Habilite también las codificaciones UTF-8 y UCS-2.

Valores recomendados para el archivo my.cnf

Para obtener más información sobre la configuración de DBMS, consulte también el procedimiento de configuración de la cuenta. Para obtener información sobre la instalación de DBMS, consulte el procedimiento de instalación de un DBMS.

Para configurar el archivo my.cnf:

1. Abra el archivo my.cnf en un editor de texto.

2. Añada las siguientes líneas en la sección `[mysqld` del archivo my.cnf:

```
sort_buffer_size=10M
join_buffer_size=20M
tmp_table_size=600M
max_heap_table_size=600M
key_buffer_size=200M
innodb_buffer_pool_size=< 80 % de la RAM asignada al DBMS; consulte la documentación
de su DBMS para obtener recomendaciones >
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0 (en la mayoría de los casos, el servidor utiliza
transacciones pequeñas)
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
```

Tenga en cuenta que la memoria especificada en el valor `innodb_buffer_pool_size` se asigna al inicio del servidor. Si el tamaño de la base de datos es más pequeño que el tamaño del búfer especificado, solo se asigna la memoria necesaria. El tamaño real de la memoria asignada es aproximadamente un 10 por ciento mayor que el tamaño del búfer especificado. Para obtener recomendaciones sobre cómo configurar `innodb_buffer_pool_size` y otra información adicional, consulte la documentación de MySQL.

Se recomienda utilizar el valor del parámetro `innodb_flush_log_at_trx_commit = 0`, porque los valores "1" o "2" afectan negativamente la velocidad de funcionamiento de MySQL. Asegúrese de que el parámetro `innodb_file_per_table` esté establecido en `1`.

Preparar un clúster de DBMS de alta disponibilidad para trabajar con Kaspersky Security Center Linux

En este artículo se describen los pasos para preparar un clúster de DBMS de alta disponibilidad para Kaspersky Security Center Linux. Si el Servidor de administración se implementa en un solo dispositivo, consulte el artículo Configuración de un servidor de DBMS basado en PostgreSQL para trabajar con Kaspersky Security Center Linux.

Kaspersky Security Center Linux es compatible con los siguientes clústeres de alta disponibilidad:

- Platform V Pangolin
- Clúster de alta disponibilidad integrado de Postgres Pro
- Patroni (con equilibrador de carga HAProxy opcional)

Como mínimo, la configuración recomendada de un clúster de DBMS de alta disponibilidad debe incluir tres nodos.

A fin de preparar un clúster de DBMS de alta disponibilidad para trabajar con Kaspersky Security Center Linux:

1. Establezca el tipo de replicación en síncrona.

   Si utiliza la plantilla de Patroni versión 3.3.1 o anterior para PostgreSQL, asegúrese de que el parámetro `synchronous_standby_names` se aplica correctamente.

   Para comprobar que se utiliza la replicación síncrona, ejecute la siguiente consulta en el nodo primario:

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

   Si la columna `sync_state` de cualquier nodo muestra valores distintos a `sync` o `potential`, el clúster utiliza la replicación asincrónica, que no es compatible. Para resolver este problema, realice una de las siguientes acciones:

   Actualice Patroni a la versión 3.3.2 o posterior.

   En el archivo de configuración de Patroni, busque la subsección `dcs` de la sección `bootstrap` y establezca el parámetro `synchronous_mode` como `true`:

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

2. En cada nodo del clúster de DBMS, configure el archivo de configuración siguiendo los pasos 1 y 2 de las instrucciones Configuración de un servidor DBMS basado en PostgreSQL para que funcione con Kaspersky Security Center Linux.

3. Cree las bases de datos y las cuentas de usuario según las instrucciones del artículo Creación de bases de datos basadas en PostgreSQL y cuentas de usuario.

4. Configure la detección de los nodos del clúster de DBMS de una de las siguientes maneras:

   - Especifique manualmente todos los nodos del clúster de DBMS durante la instalación de Kaspersky Security Center Linux.

   - Para la detección automática de los nodos del clúster, especifique únicamente el nombre del DNS o la dirección IP del nodo de control o del nodo de réplica durante la instalación de Kaspersky Security Center Linux.

     Para hacerlo:

     a. En todos los nodos del clúster de DBMS de alta disponibilidad, agregue la siguiente línea al archivo de configuración `postgresql`:

     `log_hostname=1`

     b. Después de editar el archivo de configuración, reinicie el servicio del clúster de DBMS en todos los nodos del clúster de DBMS de alta disponibilidad.

     c. Asegúrese de que el usuario de la base de datos tenga el privilegio `pg_read_all_stats`.

     Puede conceder este privilegio ejecutando el siguiente comando:

     `GRANT pg_read_all_stats TO "<kscdbadmin>";`

     Donde `<kscdbadmin>` es el nombre del usuario de la base de datos.

     El nombre de usuario de la base de datos del Servidor de administración se especifica durante la instalación de Kaspersky Security Center Linux.

     d. Configure el equilibrador de carga para la base de datos de IAM.

El clúster de DBMS de alta disponibilidad está listo para funcionar con Kaspersky Security Center Linux.

Instalación de Kaspersky Security Center Linux

A continuación, se describe el procedimiento de instalación de Kaspersky Security Center Linux.

Antes de instalar la aplicación, siga estos pasos:

- Diseñe el despliegue de Kaspersky Security Center Linux de acuerdo con las recomendaciones del escenario Primeros pasos.

  Si cumplió con los requisitos previos y completó los pasos del 1 al 4 del escenario, continúe con la instalación del Servidor de administración de Kaspersky Security Center Linux.

  > Si utiliza el sistema operativo RED OS 7.3.4 o posterior, o MSVSPHERE 9.2 o posterior, instale el paquete libxcrypt-compat para el correcto funcionamiento del Servidor de administración.

- Instale el DBMS para Kaspersky Security Center Linux. Puede elegir uno de los DBMS compatibles.

  Si su distribución de Linux no incluye un DBMS compatible, puede instalar el DBMS desde un repositorio de paquetes de terceros del proveedor o desde otra fuente confiable.

Después de instalar el DBMS, siga las instrucciones correspondientes:

- Configurar un servidor DBMS basado en PostgreSQL para que funcione con Kaspersky Security Center Linux
- Configurar el servidor MariaDB x64 para trabajar con Kaspersky Security Center Linux
- Configuración del servidor MySQL x64 para trabajar con Kaspersky Security Center Linux

- Asegúrese de que el servidor DNS esté disponible en la red.

  Asegúrese de que las direcciones FQDN y los nombres del DNS de los componentes de servidor de Kaspersky Security Center Linux se conviertan correctamente en direcciones IP en los sistemas operativos de los componentes de la aplicación y en los dispositivos de red.

- Descargue el archivo de instalación con la localización necesaria del sitio web de Kaspersky.

  Elija el archivo de instalación que corresponda a la distribución de Linux instalada en su dispositivo: ksc64_<número_de_versión>_amd64.deb o ksc64-<número_de_versión>.x86_64.rpm.

  > El idioma del Servidor de administración instalado depende de la localización del paquete de distribución descargado.

Para instalar Kaspersky Security Center Linux:

1. Cree un grupo de seguridad para los servicios de Kaspersky Security Center, un usuario sin privilegios para iniciar los servicios del Servidor de administración y un usuario sin privilegios para iniciar los servicios de IAM.

   Estos usuarios deben pertenecer al grupo de seguridad de Kaspersky Security Center.

   Para ello, ejecute los siguientes comandos en orden (en este ejemplo, el grupo de seguridad es "kladmins", el usuario para ejecutar los servicios del Servidor de administración es "ksc" y el usuario para iniciar los servicios de IAM es "ksciam"):

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

2. De ser necesario, aumente el límite predeterminado de archivos que se pueden abrir (descriptores de archivo) para las cuentas utilizadas para el funcionamiento de los servicios del Servidor de administración.

   Para hacer esto, abra el archivo /etc/security/limits.conf y especifique los límites duros y blandos de los descriptores de archivos de la siguiente manera:

   ```
   ksc soft nofile <max_number_of_opened_files>
   ksc hard nofile <max_number_of_opened_files>
   ```

   De forma predeterminada, los límites de los descriptores de archivos se especifican durante la instalación. El límite suave de archivos es de 32 768, mientras que el límite duro es de 131 072.

3. Realice la instalación de Kaspersky Security Center Linux.

   Dependiendo de su distribución de Linux, ejecute uno de los siguientes comandos:

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

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

4. Ejecute el script de configuración inicial de Kaspersky Security Center Linux:

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

5. Leer el Contrato de licencia de usuario final (EULA) y la Política de privacidad. El texto se muestra en la ventana de la línea de comandos. Presione la barra espaciadora para ver el siguiente segmento de texto. Luego, cuando se le solicite, ingrese los siguientes valores:

   a. Ingrese `y` si comprende y acepta los términos del EULA. Ingrese `n` si no acepta los términos del EULA. Para utilizar Kaspersky Security Center Linux, debe aceptar los términos del EULA.

   b. Ingrese `y` si comprende y acepta los términos de la Política de privacidad, y si acepta que sus datos se manejen y transmitan (incluso a terceros países) como se describe en la Política de privacidad. Ingrese `n` si no acepta los términos de la Política de privacidad. Para utilizar Kaspersky Security Center Linux, debe aceptar los términos de la Política de privacidad.

6. Cuando se le solicite, ingrese la siguiente configuración:

   a. Seleccione **Estándar** como un modo de instalación del Servidor de administración.

   b. Ingrese el FQDN o el nombre del DNS del Servidor de administración. Otros dispositivos utilizarán este nombre para conectarse al Servidor de administración.

   c. Ingrese el número de puerto SSL del Servidor de administración. El número de puerto predeterminado es 13000.

   d. Evalúe el número aproximado de dispositivos que pretende administrar:

   - Si tiene de 1 a 100 dispositivos administrados, ingrese 1.
   - Si tiene de 101 a 1000 dispositivos administrados, ingrese 2.
   - Si tiene más de 1000 dispositivos administrados, ingrese 3.

   Esta configuración se utiliza para el retardo aleatorio automático para el inicio de tareas a fin de optimizar la carga de la red. En la siguiente lista se muestra el intervalo dentro del cual se calcula el retardo:

   - De 1 a 100 dispositivos administrados, valor 1. No se utiliza el retardo.
   - De 101 a 1000 dispositivos administrados, valor 2. El retardo es de 5 minutos.
   - Más de 1000 dispositivos administrados, valor 3. El retardo es de 10 minutos.

   e. Ingrese el nombre del grupo de seguridad creado en el paso 1 (en el ejemplo, el grupo es `kladmins`).

   f. Ingrese el nombre del usuario que iniciará el servicio del Servidor de administración creado en el paso 1 (en el ejemplo, el usuario es `ksc`).

   El usuario debe ser miembro del grupo de seguridad que especificó en el paso 8e.

   g. Ingrese el nombre de usuario que iniciará otros servicios (en el ejemplo, el grupo es `kladmins`).

   El usuario debe ser miembro del grupo de seguridad que especificó en el paso 8e.

h. Seleccione el DBMS que haya instalado para trabajar con Kaspersky Security Center Linux:

- Si instaló MySQL o MariaDB, ingrese 1.
- Si instaló un DBMS basado en PostgreSQL, ingrese 2.

i. Ingrese el nombre del DNS o la dirección IP del dispositivo en el que está instalada la base de datos del Servidor de administración. Para una instalación local del DBMS, especifique 127.0.0.1.

Para usar un clúster de conmutación por error de alta disponibilidad, realice una de las siguientes acciones:

- Ingrese los nombres DNS o las direcciones IP y los puertos de todos los nodos en el siguiente formato: `<fqdn1>:<port>,<fqdn2>:<port>,<...><fqdnX>:<port>;`
- Especifique solo el nombre DNS o la dirección IP del nodo principal o del nodo de réplica.

j. Introduzca el número de puerto de la base de datos. Este puerto se utiliza para comunicarse con el Servidor de administración. Este paso se omite si ingresó los nombres del DNS o las direcciones IP y los puertos de todos los nodos del clúster de alta disponibilidad en el paso 8i.

De forma predeterminada, se utilizan los siguientes puertos:

- Puerto `3306` para MySQL o MariaDB
- Puerto `5432` para PostgreSQL o Postgres Pro

k. Ingrese el nombre de la base de datos del Servidor de administración (en el ejemplo de los artículos, la base de datos `kav`) que creó siguiendo las instrucciones de Creación de bases de datos y cuentas de usuario basadas en PostgreSQL o Configuración del servidor MariaDB x64 para trabajar con Kaspersky Security Center Linux.

l. Ingrese el nombre de la cuenta de administrador de la base de datos que se utiliza para acceder a la base de datos del Servidor de administración (en el ejemplo de estos artículos del paso 8k, `kscdbadmin`).

m. Ingrese la contraseña de la cuenta de administrador de la base de datos que utiliza para acceder a la base de datos del Servidor de administración.

n. Si instaló una base de datos basada en PostgreSQL, puede especificar el esquema de la base de datos que utilizará el Servidor de administración. Para hacerlo, especifique el nombre del esquema.

> El nombre del esquema distingue entre mayúsculas y minúsculas: debe usar solo letras minúsculas.

Si no desea utilizar un esquema personalizado, presione INTRO. En este caso, se utiliza el esquema predeterminado seleccionado en el DBMS.

o. Ingrese el FQDN o el nombre del DNS del servidor de IAM. Si no especifica esta variable, se utiliza el nombre DNS del dispositivo que tiene el Servidor de administración instalado.

Ingrese el valor que especificó en el paso 8b.

p. Ingrese el nombre de la cuenta que iniciará el servicio IAM creado en el paso 1. El usuario debe pertenecer al grupo de seguridad que especificó en el paso 8e (en el ejemplo del paso 1, `ksciam`).

q. Seleccione el DBMS que haya instalado para trabajar con el servicio IAM:

- Si instaló MySQL o MariaDB, ingrese 1.
- Si instaló PostgreSQL o Postgres Pro SQL, ingrese 2.

r. Ingrese la dirección de DBMS de IAM que utilizará el servicio de IAM.

Para usar un clúster de alta disponibilidad, realice una de las siguientes acciones:

- Ingrese los nombres DNS o las direcciones IP y los puertos de todos los nodos en el siguiente formato: `<fqdn1>:<port>,<fqdn2>:<port>,<...><fqdnX>:<port>;`
- Especifique solo el nombre DNS o la dirección IP del equilibrador de carga.

s. Ingrese el número de puerto de DBMS de IAM. Este puerto se utiliza para comunicarse con el servicio IAM. Este paso se omite si ingresó los nombres del DNS o las direcciones IP y los puertos de todos los nodos del clúster de alta disponibilidad en el paso 8r.

De forma predeterminada, se utilizan los siguientes puertos:

- Puerto 3306 para MySQL y MariaDB.
- Puerto 5432 para PostgreSQL y Postgres Pro.

t. Ingrese el nombre de la base de datos de IAM que utilizará el servicio de IAM (en el ejemplo, `iam`).

u. Ingrese el nombre de usuario de la cuenta de administrador de la base de datos que utiliza para acceder a la base de datos (en el ejemplo, `iamdbadmin`).

v. Ingrese la contraseña de la cuenta de administrador de la base de datos que utiliza para acceder a la base de datos de IAM.

Espere a que los servicios se agreguen e inicien automáticamente:

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

w. Si instaló PostgreSQL o Postgres Pro, puede especificar el esquema de base de datos que usará IAM. Para hacerlo, especifique el nombre del esquema.

Si no desea utilizar un esquema personalizado, presione INTRO. En este caso, se utiliza el esquema 'public'.

> El nombre del esquema distingue entre mayúsculas y minúsculas: debe usar solo letras minúsculas.
> No especifique los nombres de esquema reservados de IAM: client, iam, ksc, locker, pat, scope, voltron.

x. Cree una cuenta que actuará como administrador del Servidor de administración. Ingrese el nombre de usuario y la contraseña.

La contraseña debe cumplir con las siguientes reglas:

- La contraseña de usuario no puede tener menos de 8 ni más de 256 caracteres.
- La contraseña debe incluir caracteres de al menos tres de los grupos enumerados a continuación:
  - Letras mayúsculas (A–Z)
  - Letras minúsculas (a-z)
  - Números (0–9)
  - Caracteres especiales (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

Si omite este paso, puede usar el siguiente comando para crear un nuevo usuario más adelante:

```
/opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p
```

Se agregará el usuario y Kaspersky Security Center Linux quedará instalado.

Continúe con la instalación de Kaspersky Security Center Web Console.

Si el Servidor de administración no tiene acceso al repositorio de paquetes de distribución de aplicaciones para la instalación remota, descargue las dependencias necesarias para crear paquetes de instalación para instalar aplicaciones en dispositivos Windows de la siguiente manera:

1. Cree el indicador RlUtilsArchiveDirUsed mediante el siguiente comando:

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

2. Ejecute el siguiente comando para reiniciar el servicio del Servidor de administración:

   `systemctl restart kladminserver_srv.service`

3. Descargue los módulos adicionales "Archivos para la instalación remota mediante Kaspersky Security Center" del sitio web de Kaspersky.

   Los archivos comprimidos descargados tienen los siguientes nombres:

   - ri_utils_win32.zip
   - ri_utils_arm64.zip

   No cambie el nombre de los archivos comprimidos.

4. Coloque los archivos comprimidos en el directorio /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives.

El Servidor de administración ahora tiene las dependencias necesarias.

Verificación del servicio

Use los siguientes comandos para verificar si un servicio se está ejecutando o no:

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

Instalación de Kaspersky Security Center Linux en modo silencioso

Puede instalar Kaspersky Security Center Linux en dispositivos Linux mediante el uso de un archivo de respuesta para ejecutar una instalación en modo silencioso, es decir, sin la participación del usuario. El archivo de respuesta contiene un conjunto personalizado de parámetros de instalación: variables y sus respectivos valores.

Antes de la instalación:

- Instale el DBMS para Kaspersky Security Center Linux. Puede elegir uno de los DBMS compatibles. Para obtener información sobre cómo instalar el DBMS seleccionado, consulte su documentación.

  Si su distribución del sistema operativo Linux no contiene un DBMS compatible, puede utilizar el repositorio de paquetes de un tercero para instalar el DBMS.

  Después de instalar el DBMS, siga las instrucciones correspondientes:

  - Configurar el servidor PostgreSQL o Postgres Pro para que funcione con Kaspersky Security Center Linux

    Configuración de la cuenta para trabajar con PostgreSQL y Postgres Pro

    Si desea que el Servidor de administración descubra automáticamente las direcciones de los nodos de clúster, solo tiene que especificar el nombre del DNS o la dirección IP del nodo de control o del nodo de réplica durante la instalación. Para ello, asegúrese de haber completado el paso 2 de las instrucciones Preparación de un clúster de DBMS de alta disponibilidad para trabajar con Kaspersky Security Center Linux.

  - Configurar el servidor MariaDB x64 para trabajar con Kaspersky Security Center Linux

    Configuración de la cuenta de DBMS para trabajar con MySQL y MariaDB

  - Configurar el servidor MySQL x64 para trabajar con Kaspersky Security Center Linux

    Configuración de la cuenta de DBMS para trabajar con MySQL y MariaDB

- Asegúrese de que su dispositivo con el DBMS instalado no tenga cuentas de usuario de DBMS con los siguientes nombres:

  - client
  - iam

- ksc
- locker
- pat
- scope
- voltron

- Asegúrese de que el dispositivo en el que desee instalar Kaspersky Security Center Linux cuente con una de las distribuciones de Linux compatibles.

  Si utiliza el sistema operativo RED OS 7.3.4 o posterior, o MSVSPHERE 9.2 o posterior, instale el paquete libxcrypt-compat para el correcto funcionamiento del Servidor de administración.

- Descargue el archivo de instalación con la localización necesaria desde el sitio web de Kaspersky. Elija el archivo de instalación que corresponda a la distribución de Linux instalada en su dispositivo: ksc64_[número_de_versión]_amd64.deb o ksc64-[número_de_versión].x86_64.rpm.

Para instalar Kaspersky Security Center Linux en modo silencioso, siga estos pasos:

1. Lea el Contrato de licencia de usuario final. Siga los pasos a continuación únicamente si comprende y acepta los términos del Contrato de licencia de usuario final.

2. Cree un grupo "kladmins" y una cuenta sin privilegios "ksc" y "ksciam", que debe ser miembro del grupo "kladmins". Para hacerlo, ejecute secuencialmente los siguientes comandos en una cuenta con privilegios raíz:

   `adduser ksc`

   `groupadd kladmins`

   `gpasswd -a ksc kladmins`

   `usermod -g kladmins ksc`

   `adduser ksciam`

   `gpasswd -a ksciam kladmins`

   `usermod -g kladmins ksciam`

3. En el servidor de DBMS, cree una base de datos para IAM. El nombre de la base de datos debe ser diferente al de la base de datos que instaló para trabajar con Kaspersky Security Center Linux. El Servidor de administración no elimina la base de datos de IAM automáticamente al desinstalar o mover el servidor a otro dispositivo; debe eliminarla de forma manual.

   - En el caso de PostgreSQL, ejecute el siguiente comando:

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

   - En el caso de MariaDB, ejecute el siguiente comando:

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

4. Cree el archivo de respuesta (en formato TXT) y agregue una lista de variables en el formato `VARIABLE_NAME=variable_value` al archivo de respuesta. Agregue cada variable en una línea separada. El archivo de respuesta debe incluir las variables enumeradas en la tabla a continuación.

5. Establezca el valor de la variable de entorno `KLAUTOANSWERS` en el entorno raíz que contiene el nombre completo del archivo de respuesta, incluida la ruta; por ejemplo, con el siguiente comando:

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

6. Ejecute la instalación de Kaspersky Security Center Linux en modo silencioso; según la distribución de Linux, ejecute uno de los siguientes comandos:

   En el entorno raíz:

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

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

   En el entorno del usuario:

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

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

7. Cree un usuario para trabajar con Kaspersky Security Center Web Console. Para ello, ejecute el siguiente comando con una cuenta con privilegios de root y especifique una contraseña de al menos 8 caracteres:

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

8. Instale Kaspersky Security Center Web Console.

Variables del archivo de respuesta utilizadas como parámetros de instalación de Kaspersky Security Center Linux en modo silencioso

Nombre de la variable	Obligatoria	Descripción	Valores posibles
`EULA_ACCEPTED`	Sí	Confirma que entiende y acepta los términos del Contrato de licencia de usuario final.	1
`PP_ACCEPTED`	Sí	Confirma que entiende y acepta los términos de la Política de privacidad.	1
`KLSRV_UNATT_SERVERADDRESS`	Sí	El nombre de DNS o la dirección IP estática del Servidor de administración.	Nombre de DNS o dirección IP
`KLSRV_UNATT_PORT_SRV`	No	El número de puerto del Servidor de administración. Configuración opcional. El valor predeterminado es 14000.	Número de puerto
`KLSRV_UNATT_PORT_SRV_SSL`	No	El número de puerto SSL del Servidor de administración. Configuración opcional. El valor predeterminado es 13000.	Número de puerto
`KLSRV_UNATT_PORT_KLOAPI`	No	El número del puerto para trabajar con OpenAPI. Además, este puerto se utiliza para recibir conexiones de Kaspersky Security Center Web Console. Configuración opcional. El valor predeterminado es 13299.	Número de puerto

KLSRV_UNATT_PORT_GUI	No	El número del puerto para trabajar con la utilidad klakaut. Configuración opcional. El valor predeterminado es 13291. La utilidad klakaut y un sistema de ayuda para ello se encuentran en la carpeta de instalación de Kaspersky Security Center Linux. La aplicación cierra este puerto de manera predeterminada. Si desea usar la utilidad klakaut para automatizar el funcionamiento de Kaspersky Security Center Linux, abra el puerto 13291 con la utilidad klscflag.	Número de puerto
KLSRV_UNATT_NETRANGETYPE	No	El número aproximado de dispositivos que desea administrar. Esta configuración se utiliza para optimizar la carga de la red. Configuración opcional. El valor predeterminado es 1.	1 para 1 a 100 dispositivos administrados. 2 para 101 a 1000 dispositivos administrados. 3 para más de 1000 dispositivos administrados.
KLSRV_UNATT_DBMS_TYPE	Sí	El tipo de sistema de administración de bases de datos: MySQL (MariaDB) o Postgres.	mysql o postgres
KLSRV_UNATT_DBMS_INSTANCE	Sí	La dirección del servidor de la base de datos. Para usar un clúster de alta disponibilidad incorporado de PostgreSQL o Postgres Pro, o un clúster de DBMS de Platform V Pangolin, ingrese los nombres DNS o las direcciones IP y los puertos de todos los nodos en el siguiente formato: <fqdn1>:<port>,<fqdn2>:<port>,<...><fqdnX>:<port>; De forma alternativa, si desea utilizar un clúster de DBMS de Platform V Pangolin, puede especificar solo el nombre del DNS o la dirección IP del nodo principal, o el nodo de réplica, al especificar la dirección del DBMS.	Nombre del DNS o dirección IP estática del servidor de la base de datos.
KLSRV_UNATT_DBMS_PORT	Sí	Puerto del servidor de la base de datos. El valor predeterminado para MySQL (MariaDB) es 3306; el valor predeterminado para Postgres es 5432.	3306 o 5432
KLSRV_UNATT_DB_NAME	Sí	El nombre de la base de datos. El nombre de la base de datos debe ser diferente del nombre de la base de datos de IAM que especificó en la variable KLSRV_UNATT_DB_IAM_NAME.	kav
KLSRV_UNATT_DBMS_LOGIN	Sí	El nombre de usuario de un usuario que tiene acceso a la base de datos.	
KLSRV_UNATT_DBMS_PASSWORD	Sí	La contraseña de un usuario que tiene acceso a la base de datos.	
KLSRV_UNATT_DBMS_SCHEMA	No	El esquema de DBMS personalizado. Si no especifica un esquema personalizado, el Servidor de administración usará uno predeterminado. El nombre del esquema distingue entre mayúsculas y minúsculas: debe usar solo letras minúsculas. Solo puede especificar un esquema personalizado si se utiliza PostgreSQL o Postgres Pro como DBMS. De lo contrario, se ignora la variable.	database_schema

KLSRV_UNATT_IAM_ADDRESS	Sí	Los navegadores de los usuarios se redirigirán a esta dirección mediante OpenID Connect. Ingrese el nombre DNS del servidor de FQDN. Debe utilizar el nombre DNS del Servidor de administración que se especificó en el parámetro KLSRV_UNATT_SERVERADDRESS.	FQDN
KLSRV_UNATT_KLIAMUSER	Sí	El nombre de la cuenta para iniciar el servicio de IAM. La cuenta debe ser miembro del grupo de seguridad especificado en la variable KLSRV_UNATT_KLADMINSGROUP.	ksciam
KLSRV_UNATT_DBMS_IAM_TYPE	Sí	El tipo de sistema de administración de bases de datos de IAM: MySQL (MariaDB) o Postgres.	mysql o postgres
KLSRV_UNATT_DBMS_IAM_INSTANCE	Sí	La dirección del servidor de la base de datos IAM. Para usar un clúster de alta disponibilidad incorporado de PostgreSQL o Postgres Pro, o un clúster de DBMS de Platform V Pangolin, ingrese los nombres DNS o las direcciones IP y los puertos de todos los nodos en el siguiente formato: <fqdn1>:<port>,<fqdn2>:<port>,<...> <fqdnX>:<port>; De forma alternativa, si desea utilizar un clúster de DBMS de Platform V Pangolin, puede especificar solo el nombre del DNS o la dirección IP del nodo principal, o el nodo de réplica, al especificar la dirección del DBMS.	Dirección IP
KLSRV_UNATT_DBMS_IAM_PORT	Sí	El puerto del servidor de la base de datos de IAM. El valor predeterminado para MySQL (MariaDB) es 3306; el valor predeterminado para Postgres es 5432.	3306 o 5432
KLSRV_UNATT_DBMS_IAM_LOGIN	Sí	El nombre de usuario de un usuario que tiene acceso a la base de datos de IAM. Si el tipo de base de datos de IAM es MySQL (MariaDB) y tiene las dos siguientes configuraciones: • gtid_mode=ON • gtid_purged=ON|AUTO asegúrese de que el usuario especificado tenga cualquiera de los siguientes privilegios en DBMS: • RELOAD • FLUSH_TABLES	
KLSRV_UNATT_DBMS_IAM_PASSWORD	Sí	La contraseña de un usuario que tiene acceso a la base de datos de IAM.	
KLSRV_UNATT_DBMS_IAM_SCHEMA	No	El esquema de DBMS personalizado. Si no especifica un esquema personalizado, IAM usará el esquema público. Solo puede especificar un esquema personalizado si se utiliza PostgreSQL o Postgres Pro como DBMS. De lo contrario, se ignora la variable. El nombre del esquema distingue entre mayúsculas y minúsculas: debe usar solo letras minúsculas. No especifique los nombres de esquema reservados de iam: client, iam, ksc, locker, pat, scope, voltron.	database_schema

KLSRV_UNATT_DB_IAM_NAME	Sí	El nombre de la base de datos de IAM. El nombre de la base de datos de IAM debe ser diferente del nombre de la base de datos que especificó en la variable KLSRV_UNATT_DB_NAME. Especifique una base de datos vacía creada manualmente.	iamdb
KLSRV_UNATT_KLADMINSGROUP	Sí	El nombre del grupo de seguridad para los servicios.	kladmins
KLSRV_UNATT_KLSRVUSER	Sí	El nombre de la cuenta para iniciar el servicio del Servidor de administración. La cuenta debe ser miembro del grupo de seguridad especificado en la variable KLSRV_UNATT_KLADMINSGROUP.	ksc
KLSRV_UNATT_KLSVCUSER	Sí	El nombre de la cuenta para iniciar otros servicios. La cuenta debe ser miembro del grupo de seguridad especificado en la variable KLSRV_UNATT_KLADMINSGROUP.	ksc
Si el Servidor de administración se despliega como un clúster de conmutación por error de Kaspersky Security Center Linux, el archivo de respuesta debe incluir las siguientes variables adicionales:			
KLFOC_UNATT_EXT_RESOURCE_MANAGEMENT	No	La configuración del clúster de conmutación por error. Si el parámetro se omite en el archivo de respuesta, se usa el valor predeterminado. Valores posibles: 0: Clúster de conmutación por error cuyos nodos se encuentran en un único centro de datos. 2: Clúster de conmutación por error distribuido geográficamente cuyos nodos se encuentran en diferentes centros de datos.	0 o 2
KLFOC_UNATT_NODE	Sí	El número de nodo (1 o 2).	1 o 2
KLFOC_UNATT_STATE_SHARE_MOUNT_PATH	Sí	El punto de montaje de la carpeta compartida de estados.	
KLFOC_UNATT_DATA_SHARE_MOUNT_PATH	Sí	El punto de montaje de la carpeta compartida de datos.	
KLFOC_UNATT_CONN_MODE	Sí	El modo de conectividad del clúster de conmutación por error.	VirtualAdapter o ExternalLoadBalancer
En caso de que la variable KLFOC_UNATT_CONN_MODE tenga el valor VirtualAdapter, el archivo de respuesta debe incluir las siguientes variables adicionales:			
KLFOC_UNATT_CONN_MODE_VA_NAME	Sí	El nombre del adaptador de red virtual.	
KLFOC_UNATT_CONN_MODE_VA_IPV4	Se requiere una de estas variables	La dirección IP del adaptador de red virtual.	Dirección IP
KLFOC_UNATT_CONN_MODE_VA_IPV6		La dirección IPv6 del adaptador de red virtual.	Dirección IPv6

Si el Servidor de administración no tiene acceso al repositorio de paquetes de distribución de aplicaciones para la instalación remota, descargue las dependencias necesarias para crear paquetes de instalación destinados a instalar aplicaciones en dispositivos Windows de la siguiente manera:

1. Cree el indicador RIUtilsArchiveDirUsed mediante el siguiente comando:

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

2. Ejecute el siguiente comando para reiniciar el servicio del Servidor de administración:

   `systemctl restart kladminserver_srv.service`

3. Descargue los módulos adicionales "Archivos para la instalación remota mediante Kaspersky Security Center" del sitio web de Kaspersky.

   Los archivos comprimidos descargados tienen los siguientes nombres:

   - ri_utils_win32.zip
   - ri_utils_arm64.zip

   No cambie el nombre de los archivos comprimidos.

4. Coloque los archivos comprimidos en el directorio /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives.

El Servidor de administración ahora tiene las dependencias necesarias.

Instalación de Kaspersky Security Center Linux en Astra Linux en el modo de entorno de software cerrado

En esta sección se describe cómo instalar Kaspersky Security Center Linux en el sistema operativo Astra Linux Special Edition.

Antes de la instalación:

- Instale un DBMS.
- Descargue la clave de la aplicación kaspersky_astra_pub_key.gpg.
- Descargue el archivo de instalación ksc64_[número_de_versión]_amd64.deb del sitio web de Kaspersky.

> En una cuenta con privilegios de raíz, ejecute los comandos proporcionados en esta instrucción con alta integridad y sin confidencialidad.

Para instalar Kaspersky Security Center Linux en un dispositivo con Astra Linux Special Edition (actualización 1.7.2), Astra Linux Special Edition (actualización 1.6) o Astra Linux Special Edition RUSB.10015-01 (actualización 1.8):

1. Abra el archivo `/etc/digsig/digsig_initramfs.conf` y luego especifique la siguiente configuración:

   ```
   DIGSIG_ELF_MODE=1
   ```

2. En la línea de comandos, ejecute el siguiente comando para instalar el paquete de compatibilidad:

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

3. Cree un directorio para la clave de la aplicación:

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

4. Coloque la clave de la aplicación en el directorio creado en el paso anterior:

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

5. Actualice la imagen inicial del sistema de archivos RAM para todos los kernel del sistema:

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

   Reinicie el sistema.

6. Cree un grupo 'kladmins' y cuentas sin privilegios 'ksc' y 'ksciam'. Las cuentas deben ser miembro del grupo 'kladmins'. Para hacer esto, ejecute secuencialmente los siguientes comandos:

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

7. Ejecute la instalación de Kaspersky Security Center Linux:

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

8. Realice la configuración de Kaspersky Security Center Linux:

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

9. Leer el Contrato de licencia de usuario final (EULA) y la Política de privacidad. El texto se muestra en la ventana de la línea de comandos. Presione la barra espaciadora para ver el siguiente segmento de texto. Luego, cuando se le solicite, ingrese los siguientes valores:

   a. Ingrese `y` si comprende y acepta los términos del EULA. Ingrese `n` si no acepta los términos del EULA. Para utilizar Kaspersky Security Center Linux, debe aceptar los términos del EULA.

   b. Ingrese `y` si comprende y acepta los términos de la Política de privacidad, y si acepta que sus datos se manejen y transmitan (incluso a terceros países) como se describe en la Política de privacidad. Ingrese `n` si no acepta los términos de la Política de privacidad. Para utilizar Kaspersky Security Center Linux, debe aceptar los términos de la Política de privacidad.

10. Cuando se le solicite, ingrese la siguiente configuración:

    a. Ingrese el FQDN o el nombre del DNS del Servidor de administración.

    b. Ingrese el número de puerto del Servidor de administración. El número de puerto predeterminado es 14000.

    c. Ingrese el número de puerto SSL del Servidor de administración. El número de puerto predeterminado es 13000.

    d. Evalúe el número aproximado de dispositivos que pretende administrar:

    - Si tiene de 1 a 100 dispositivos administrados, ingrese 1.
    - Si tiene de 101 a 1000 dispositivos administrados, ingrese 2.
    - Si tiene más de 1000 dispositivos administrados, ingrese 3.

Esta configuración se utiliza para el retardo aleatorio automático para el inicio de tareas a fin de optimizar la carga de la red. En la siguiente lista se muestra el intervalo dentro del cual se calcula el retardo:

- De 1 a 100 dispositivos administrados, valor 1. No se utiliza el retardo.
- De 101 a 1000 dispositivos administrados, valor 2. El retardo es de 5 minutos.
- Más de 1000 dispositivos administrados, valor 3. El retardo es de 10 minutos.

e. Ingrese el nombre del grupo de seguridad para los servicios. De forma predeterminada, se utiliza el grupo 'kladmins'.

f. Introduzca el nombre de la cuenta para iniciar el servicio del Servidor de administración. La cuenta debe ser miembro del grupo de seguridad ingresado. De manera predeterminada, se utiliza la cuenta ksc.

g. Introduzca el nombre de la cuenta para iniciar otros servicios. La cuenta debe ser miembro del grupo de seguridad ingresado. De manera predeterminada, se utiliza la cuenta ksc.

h. Seleccione el DBMS que haya instalado para trabajar con Kaspersky Security Center Linux:

- Si instaló MySQL o MariaDB, ingrese 1.
- Si instaló PostgreSQL o Postgres Pro SQL, ingrese 2.

i. Introduzca la dirección IP del dispositivo en el que está instalada la base de datos.

j. Introduzca el número de puerto de la base de datos. Este puerto se utiliza para comunicarse con el Servidor de administración. De forma predeterminada, se utilizan los siguientes puertos:

- Puerto 3306 para MySQL y MariaDB.
- Puerto 5432 para PostgreSQL y Postgres Pro.

k. Escriba el nombre de la base de datos.

l. Ingrese el nombre de usuario de la cuenta de administrador de la base de datos que utiliza para acceder a la base de datos.

m. Ingrese la contraseña de la cuenta de administrador de la base de datos que utiliza para acceder a la base de datos.

n. Ingrese el FQDN o el nombre del DNS del servidor de IAM.

Escriba el valor que especificó en el paso 10a.

o. Ingrese el nombre de la cuenta para iniciar el servicio kliam. La cuenta debe ser miembro del grupo de seguridad ingresado.

p. Seleccione el DBMS que haya instalado para trabajar con el servicio IAM:

- Si instaló MySQL o MariaDB, ingrese 1.
- Si instaló PostgreSQL o Postgres Pro SQL, ingrese 2.

q. Ingrese la dirección de DBMS que usará el servicio de IAM.

r. Introduzca el número de puerto de la base de datos. Este puerto se utiliza para comunicarse con el servicio IAM. De forma predeterminada, se utilizan los siguientes puertos:

- Puerto 3306 para MySQL y MariaDB.
- Puerto 5432 para PostgreSQL y Postgres Pro.

s. Ingrese el nombre de la base de datos que usará el servicio de IAM. El nombre de la base de datos utilizada por el servicio de IAM debe ser diferente de la base de datos utilizada por el Servidor de administración.

t. Ingrese el nombre de usuario de la cuenta root de la base de datos que utiliza para acceder a la base de datos de IAM.

u. Ingrese la contraseña de la cuenta root de la base de datos que utiliza para acceder a la base de datos de IAM.

Espere a que los servicios se agreguen e inicien automáticamente:

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

v. Cree una cuenta que actuará como administrador del Servidor de administración. Ingrese el nombre de usuario y la contraseña.

La contraseña debe cumplir con las siguientes reglas:

- La contraseña de usuario debe tener un mínimo de 8 caracteres y un máximo de 256.
- La contraseña debe incluir caracteres de al menos tres de los grupos enumerados a continuación:
  - Letras mayúsculas (A–Z)
  - Letras minúsculas (a-z)
  - Números (0–9)
  - Caracteres especiales (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

Se instala Kaspersky Security Center Linux y se agrega el usuario.

Para descargar las dependencias necesarias para crear paquetes de instalación de aplicaciones para dispositivos Windows:

1. Cree el indicador RIUtilsArchiveDirUsed mediante la ejecución del siguiente comando:

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

2. Ejecute el siguiente comando para reiniciar el servicio del Servidor de administración:

   ```
   systemctl restart kladminserver_srv.service
   ```

3. Descargue los módulos adicionales "Archivos para la instalación remota mediante Kaspersky Security Center" del sitio web de Kaspersky.

   Los archivos comprimidos descargados tienen los siguientes nombres:

   - ri_utils_win32.zip
   - ri_utils_arm64.zip

   No cambie el nombre de los archivos comprimidos.

4. Coloque los archivos comprimidos en el directorio /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives.

El Servidor de administración ahora tiene las dependencias necesarias.

Verificación del servicio

Use los siguientes comandos para verificar si un servicio se está ejecutando o no:

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

Instalación de Kaspersky Security Center Web Console

En esta sección, se describe cómo instalar el Servidor de Kaspersky Security Center Web Console (en lo sucesivo, también se usará la denominación "Kaspersky Security Center Web Console") en dispositivos con el sistema operativo Linux. Antes de la instalación, debe instalar un DBMS y el Servidor de administración de Kaspersky Security Center Linux.

> Si instala Kaspersky Security Center Web Console en Astra Linux en el modo de entorno de software cerrado, siga las instrucciones específicas para Astra Linux.

Utilice el archivo de instalación que corresponda a la distribución de Linux instalada en su dispositivo:

- Para Debian: ksc-web-console-<número_de_compilación>.x86_64.deb
- Para sistemas operativos basados en RPM: ksc-web-console-<número_de_compilación>.x86_64.rpm

El archivo de instalación debe descargarse del sitio web de Kaspersky.

Para instalar Kaspersky Security Center Web Console:

1. Asegúrese de que el dispositivo en el que desea instalar Kaspersky Security Center Web Console esté ejecutando una de las distribuciones de Linux compatibles.

2. Lea el Contrato de licencia de usuario final. Si el kit de distribución de Kaspersky Security Center Linux no contiene un archivo TXT con el texto del EULA, puede descargar dicho archivo del sitio web de Kaspersky. Si no acepta los términos del Contrato de licencia, no instale la aplicación.

3. Cree un archivo de respuesta que contenga parámetros para conectar Kaspersky Security Center Web Console al Servidor de administración: `/etc/ksc-web-console-setup.json`.

   Ejemplo de un archivo de respuesta que contiene el conjunto mínimo de parámetros

   El conjunto de parámetros del archivo de respuesta depende de la versión del Servidor de administración al que se conecta Kaspersky Security Center Web Console:

   - Versión 16 o posterior del Servidor de administración

     Ejemplo de un archivo de respuesta con el conjunto mínimo de parámetros para iniciar sesión en la versión 16 o posteriores del Servidor de administración:

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

   - Versión 15.4 o posterior del Servidor de administración

     Ejemplo de un archivo de respuesta con el conjunto mínimo de parámetros para iniciar sesión en la versión 15.4 o anteriores del Servidor de administración:

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

   Puede instalar Kaspersky Security Center Web Console en el mismo dispositivo donde está el Servidor de administración o en otro dispositivo. Si Kaspersky Security Center Web Console está instalado en otro dispositivo, la dirección de Kaspersky Security Center Web Console (especificada por `address`) y la dirección del Servidor de administración (especificada por `iamHost` o `kscHost`) son diferentes. Si Kaspersky Security Center Web Console está instalado en el mismo dispositivo que el Servidor de administración, estos parámetros tienen los mismos valores.

El valor `iamHost` debe coincidir con la dirección de IAM que especificó durante la instalación del Servidor de administración. Para obtener la dirección de IAM especificada, ejecute el siguiente comando en el dispositivo que tiene el Servidor de administración instalado:

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

Para obtener información detallada, consulte el artículo: Parámetros de instalación de Kaspersky Security Center Web Console.

Puede agregar varios Servidores de administración de diferentes versiones a la lista de servidores de confianza. En este caso, los servidores pueden utilizar diferentes métodos de autenticación.

Recomendamos que especifique números de puerto superiores a 1024. Si desea que Kaspersky Security Center Web Console funcione en puertos inferiores al 1024, después de la instalación debe asegurarse de tener la utilidad setcap y luego ejecutar el siguiente comando:

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

Si no tiene la utilidad setcap, puede instalarla. **Haga clic en este vínculo para ver los comandos.**

Para los sistemas operativos Debian y Ubuntu, ejecute uno de los siguientes comandos:

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

Para SUSE Linux Enterprise Server y Red Hat Enterprise Linux, ejecute el comando:

- `sudo zypper install libcap-progs`

Cuando instale Kaspersky Security Center Web Console en el sistema operativo ALT Linux, debe especificar un número de puerto distinto del 8080, debido a que el sistema operativo utiliza el puerto 8080.

Kaspersky Security Center Web Console no se puede actualizar utilizando el mismo archivo de instalación .rpm. Si desea cambiar los parámetros de un archivo de respuesta y utilizar ese archivo para reinstalar la aplicación, primero desinstale la aplicación y luego vuelva a instalarla utilizando el nuevo archivo de respuesta.

4. Con una cuenta con privilegios root, use la línea de comandos para ejecutar el archivo de instalación con la extensión .deb o .rpm, dependiendo de su distribución de Linux.

   - Para instalar o actualizar Kaspersky Security Center Web Console con un archivo .deb, ejecute el siguiente comando:

     ```
     sudo apt-get install ksc-web-console-<número de compilación>.x86_64.deb
     ```

   - Para instalar Kaspersky Security Center Web Console desde un archivo .rpm, ejecute uno de los siguientes comandos:

     ```
     sudo yum install ksc-web-console-<número de compilación>.x86_64.rpm
     ```

     o

     ```
     sudo alien -i ksc-web-console-<número de compilación>.x86_64.rpm
     ```

- Para actualizar Kaspersky Security Center Web Console a una versión más reciente, ejecute uno de estos comandos:

  - Para dispositivos que ejecutan un sistema operativo basado en RPM:
    `sudo yum install ksc-web-console-<número de compilación>.x86_64.rpm`

  - Para dispositivos que ejecutan un sistema operativo basado en Debian:
    `sudo apt-get install ksc-web-console-<número de compilación>.x86_64.deb`

  Se iniciará el proceso para desempaquetar el archivo de instalación. Espere a que se complete la instalación. Kaspersky Security Center Web Console se instalará en el directorio /var/opt/kaspersky/ksc-web-console.

5. Reinicie todos los servicios de Kaspersky Security Center Web Console con el siguiente comando:
   `sudo systemctl restart KSC*`

   Cuando finalice la instalación, podrá usar un navegador para abrir Kaspersky Security Center Web Console e iniciar sesión.

Si el certificado común del Servidor de administración se reemplaza con otro certificado de una copia de seguridad o se reemplaza mediante la utilidad klsetsrvcert, debe eliminarlo y luego volver a instalar Kaspersky Security Center Web Console. De lo contrario, se restringirá el inicio de sesión en Web Console.
Si después de la reinstalación no puede iniciar sesión en Web Console, compruebe la configuración del servidor de IAM.

Parámetros de instalación de Kaspersky Security Center Web Console

Para instalar el Servidor de Kaspersky Security Center Web Console en dispositivos con Linux, debe crear un "archivo de respuesta", el cual es un archivo .json con los parámetros necesarios para conectar Kaspersky Security Center Web Console al Servidor de administración. Debe nombrar este archivo como ksc-web-console-setup.json y colocarlo en el directorio /etc/ksc-web-console-setup.json.

El conjunto de parámetros del archivo de respuesta depende de la versión del Servidor de administración al que se conecta Kaspersky Security Center Web Console.

- Versión 16 o posterior del Servidor de administración

  La versión 16 y posteriores del Servidor de administración incluyen Identity and Access Manager (IAM), que proporciona autenticación de dominio con inicio de sesión único (SSO) en Kaspersky Security Center Web Console. Para que Kaspersky Security Center Web Console se conecte al Servidor de administración, el archivo de respuesta debe contener los parámetros para la interacción con el componente de IAM, incluso si no utiliza el inicio de sesión único (SSO).

  Ejemplo del archivo de respuesta para instalar Web Console que se conectará a la versión 16 del Servidor de administración o posteriores. En este ejemplo, Web Console y el Servidor de administración se instalan en diferentes dispositivos:

```
{
    "webConsoleAddress": "ksc-web-console.example.com",
    "port": 8080,
    "defaultLangId": 1049,
    "enableLog": true,
    "trusted":  {
        "Administration Server v16": {
    "iamHost": "ksc16.example.com",
    "iamOAuthPort": 4444,
    "iamProxyPort": 9050,
    "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
    "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
    "kscPort": 13299,
```

```
    "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "acceptEula": true,
    "certPath": "/root/server.crt",
    "keyPath": "/root/key-without-passphrase.pem",
    "internalCertsTTLDays": 1095,
    "webConsoleAccount": "Group1:User1",
    "managementServiceAccount": "Group1:User2",
    "serviceWebConsoleAccount": "Group1:User3",
    "pluginAccount": "Group1:User4",
    "natsMessageQueueAccount": "Group1:User6"
}
```

Ejemplo del archivo de respuesta para instalar Web Console que se conectará al Servidor de administración versión 15.4 o anteriores:

Los parámetros `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount`, `natsMessageQueueAccount`, `certPath` y `keyPath` son opcionales. Puede omitirlos en el archivo de respuesta.

Si desea utilizar un certificado personalizado, especifique los parámetros `certPath` y `keyPath`. Si no especifica los parámetros o especifica solo uno, el navegador web seguirá informándole que su conexión no es privada.

Por razones de seguridad, no recomendamos especificar los parámetros `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount` y `natsMessageQueueAccount`.
Si decide especificar estos parámetros, asegúrese de que las cuentas de usuario que está configurando pertenezcan al mismo grupo de seguridad. Cuando no se especifican estos parámetros, el instalador de Kaspersky Security Center Web Console creará un grupo de seguridad predeterminado y luego creará cuentas de usuario con nombres predeterminados en el grupo.
Los parámetros `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount` y `natsMessageQueueAccount` no deben utilizarse por separado: especifique los valores de todos estos parámetros o no especifique ninguno.

Puede instalar Kaspersky Security Center Web Console en el mismo dispositivo donde está el Servidor de administración o en otro dispositivo. Si Kaspersky Security Center Web Console está instalado en otro dispositivo, la dirección de Kaspersky Security Center Web Console (especificada por `webConsoleAddress`) y la dirección del Servidor de administración (especificada por `iamHost` o `kscHost`) son diferentes. Si Kaspersky Security Center Web Console está instalado en el mismo dispositivo que el Servidor de administración, estos parámetros tienen los mismos valores.

El valor `iamHost` debe coincidir con la dirección de IAM que se especificó durante la instalación del Servidor de administración. Para obtener la dirección de IAM especificada, ejecute el siguiente comando en el dispositivo que tiene el Servidor de administración instalado:

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

Recomendamos que especifique números de puerto superiores a 1024. Si desea que Kaspersky Security Center Web Console funcione en puertos inferiores al 1024, después de la instalación deberá ejecutar el siguiente comando:

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

Si no tiene la utilidad setcap, puede instalarla. **Haga clic en este vínculo para ver los comandos**.

Para los sistemas operativos Debian y Ubuntu, ejecute uno de los siguientes comandos:

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

Para SUSE Linux Enterprise Server y Red Hat Enterprise Linux, ejecute el comando:

- `sudo zypper install libcap-progs`

Cuando instale Kaspersky Security Center Web Console en el sistema operativo ALT Linux, debe especificar un número de puerto distinto del 8080, debido a que el sistema operativo utiliza el puerto 8080.

En la siguiente tabla se describen los parámetros que se pueden especificar en un archivo de respuesta.

Parámetros para instalar Kaspersky Security Center Web Console en dispositivos que ejecutan Linux

Configuración	Descripción	Valores disponibles
`webConsoleAddress`	Dirección del dispositivo (FQDN o nombre de host) donde se instaló Kaspersky Security Center Web Console (obligatoria). Si instala Kaspersky Security Center Web Console en el servidor de Kaspersky Security Center, use la dirección que especificó al instalar Kaspersky Security Center Linux. Si el instalador de Kaspersky Security Center Web Console se ejecuta en otro dispositivo, especifique la dirección (FQDN o nombre de host) del dispositivo que utilizará el navegador web para conectarse al servidor de Kaspersky Security Center Web Console.	Valor de cadena. Ejemplo: `"ksc.example.com"`
`port`	Puerto utilizado por Kaspersky Security Center Web Console para recibir conexiones desde navegadores web (obligatorio).	Valor numérico. El valor recomendado es 8080 (excepto p operativo ALT Linux).
`defaultLangId`	Idioma de la interfaz de usuario (por defecto, `1033`). De ser necesario, puede cambiar el idioma de la interfaz de Kaspersky Security Center Web Console.	Código numérico del idioma: • Alemán: `1031` • Inglés: `1033` • Español: `1034` • Español (México): `2058` • Francés: `1036` • Italiano: `1040` • Japonés: `1041` • Kazajo: `1087` • Polaco: `1045` • Portugués (Brasil): `1046` • Ruso: `1049` • Turco: `1055` • Chino simplificado: `2052` • Chino tradicional: `1028` Si no se especifica ningún valor, se usa el (en-US).
`enableLog`	Habilitar o no habilitar el registro de seguimiento de Kaspersky Security Center Web Console. Le recomendamos que cambie el valor predeterminado del parámetro solo si un especialista del Soporte técnico de Kaspersky lo solicita.	Valor booleano: • `true` —El registro está habilitado. • `false` —El registro está deshabilitad de manera predeterminada).

Configuración	Descripción	Valores disponibles
`trusted`	Lista de direcciones de los Servidores de administración de confianza a los que se puede conectar Kaspersky Security Center Web Console. Puede agregar varios Servidores de administración de diferentes versiones a la lista de servidores de confianza. Versión 16 o posteriores del Servidor de administración: • El nombre del Servidor de administración que se mostrará en la ventana del inicio de sesión. • `iamHost` es la dirección (FQDN o nombre de host) del Servidor de administración, que incluye el componente IAM (a partir de la versión 16 de Kaspersky Security Center Linux) y al que se conecta Kaspersky Security Center Web Console. El valor `iamHost` debe coincidir con la dirección de IAM que se especificó durante la instalación del Servidor de administración. Para obtener la dirección de IAM especificada, ejecute el siguiente comando en el dispositivo que tiene el Servidor de administración instalado: `grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml` • `iamOAuthPort` es el puerto que se utiliza para intercambiar tokens de autentificación a través del protocolo de autenticación OpenID Connect (valor predeterminado: 4444). Este puerto se utiliza tanto para la comunicación entre el Servidor de Kaspersky Security Center Web Console y el Servidor de administración, como entre el navegador (que se utiliza con Kaspersky Security Center Web Console) y el Servidor de administración. • `iamProxyPort` es el puerto que se utiliza para conectar el Servidor de Kaspersky Security Center Web Console al servidor de administración (valor predeterminado: 9050). • `iamCertPath` es la ruta al certificado de IAM. El certificado de IAM se crea automáticamente la primera vez que ejecuta el Servidor de administración. El certificado está en el dispositivo donde está instalado el Servidor de administración La ruta predeterminada de acceso al certificado: /var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem. El certificado de IAM autofirmado se rota automáticamente. • `iamPATPath` es la ruta al token utilizado para registrar Kaspersky Security Center Web Console como cliente OAuth en IAM. Este archivo se genera automáticamente la primera vez que se ejecuta el Servidor de administración. El token está en el dispositivo donde está instalado el Servidor de administración. La ruta predeterminada al token: /var/opt/kaspersky/klnagent_srv/iam/initial_token.txt. El token es válido indefinidamente y no requiere rotación. • `kscPort` es el puerto que se utiliza para conectar Kaspersky Security Center Web Console con el Servidor de administración a través de OpenAPI (valor predeterminado: 13299). • `kscCertPath` es la ruta al certificado del Servidor de administración. El certificado está en el dispositivo donde está instalado el Servidor de administración (ruta predeterminada al certificado: /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer).	Sección del archivo JSON con el siguient `"trusted": { "Administration Server v16": { "iamHost": "ksc-iam.example.com", "iamOAuthPort": 4444, "iamProxyPort": 9050, "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_c "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initia "kscPort": 13299, "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/ }, "Administration Server v15.4": { "kscHost": "ksc.example.com", "kscPort": 13299, "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/ } }` Puede especificar el nombre de cualquier administración en lugar de `Administrat v16` y `Administration Server v15.4`

Configuración	Descripción	Valores disponibles
	Versión 15.4 o posteriores del Servidor de administración: • El nombre del Servidor de administración que se mostrará en la ventana del inicio de sesión. • `kscHost` es la dirección (FQDN o nombre de host) del Servidor de administración al que se conecta Kaspersky Security Center Web Console. • `kscPort` es el puerto de OpenAPI que se utiliza para conectar el Servidor de Kaspersky Security Center Web Console con el Servidor de administración (valor predeterminado: 13299). • `kscCertPath` es la ruta al certificado del Servidor de administración. El certificado está en el dispositivo donde está instalado el Servidor de administración (ruta predeterminada al certificado: /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer). Al instalar Kaspersky Security Center Web Console en otro dispositivo que no sea el Servidor de administración, copie el archivo del certificado del Servidor de administración (especificado por `kscCertPath`), el archivo de certificado IAM (especificado por `iamCertPath`) y el archivo de token (especificado por `iamPATPath`) desde el dispositivo con el Servidor de administración instalado al dispositivo objetivo. Especifique la ruta local a estos archivos en el archivo de respuesta para el instalador de Web Console.	
`acceptEula`	Aceptar o no aceptar los términos y condiciones del Contrato de licencia de usuario final (EULA). El archivo que contiene los términos del CLUF se descarga junto con el archivo de instalación.	Valor booleano: • `true` —Confirmo que he leído comple entiendo y acepto los términos y las este Contrato de licencia de usuario • `false` —No acepto los términos del licencia (seleccionado por defecto). Si no especifica ningún valor, el instalador Security Center Web Console le mostrar de licencia y le preguntará si acepta o rec términos.
`certDomain`	Si desea generar un nuevo certificado autofirmado, use este parámetro para especificar el FQDN para conectar el navegador a Kaspersky Security Center Web Console.	Valor de cadena.
`certPath`	Use el parámetro para especificar la ruta al certificado personalizado de Kaspersky Security Center Web Console que es de confianza en su infraestructura y cumple con los requisitos para los certificados personalizados. Puede especificar solo una clave privada (`keyPath`) para un certificado o para una cadena de certificados.	Valor de cadena. Kaspersky Security Center Web Console compatible con los certificados cifrados. En el dispositivo donde se instalará Kaspe Center Web Console, especifique la ruta certificado en formato de codificación PE Ejemplo: `/root/server.crt`
`keyPath`	Utilice el parámetro para especificar la ruta a la clave privada asociada con el certificado personalizado de Kaspersky Security Center Web Console especificado en el parámetro `certPath`.	Valor de cadena. El archivo con la clave privada no debe es En el dispositivo donde se instalará Kaspe Center Web Console, especifique la ruta clave en formato de codificación PEM. Ejemplo: `/root/key-without-passphr`
`webConsoleAccount`	Nombre de la cuenta con la que se ejecuta el servicio Kaspersky Security Center Web Console.	Valor de cadena en el siguiente formato: `del grupo >:< nombre de usuario >"` Ejemplo: `"Group1:User1"`. Si no se especifica ningún valor, el instalad Kaspersky Security Center Web Console nueva cuenta con el nombre predetermin `user_management_%uid%`.

Configuración	Descripción	Valores disponibles
`managementServiceAccount`	Nombre de la cuenta con la que se ejecuta el Servicio de administración de Kaspersky Security Center Web Console.	Valor de cadena en el siguiente formato: `del grupo >:< nombre de usuario >"` Ejemplo: `"Group1:User2"`. Si no se especifica ningún valor, el instalac Kaspersky Security Center Web Console nueva cuenta con el nombre predetermin `user_nodejs_%uid%`.
`serviceWebConsoleAccount`	Nombre de la cuenta con la que se ejecuta el servicio Kaspersky Security Center Web Console.	Valor de cadena en el siguiente formato: `del grupo >:< nombre de usuario >"` Ejemplo: `"Group1:User3"`. Si no se especifica ningún valor, el instalac Kaspersky Security Center Web Console nueva cuenta con el nombre predetermin `user_svc_nodejs_%uid%`.
`pluginAccount`	Nombre de la cuenta con la que se ejecuta el servicio Kaspersky Security Center Product Plugins.	Valor de cadena en el siguiente formato: `del grupo >:< nombre de usuario >"` Ejemplo: `"Group1:User4"`. Si no se especifica ningún valor, el instalac Kaspersky Security Center Web Console nueva cuenta con el nombre predetermin `user_web_plugin_%uid%`.
`natsMessageQueueAccount`	Nombre de la cuenta con la que se ejecuta el servicio NATS de Kaspersky Security Center Web Console.	Valor de cadena en el siguiente formato: `del grupo >:< nombre de usuario >"` Ejemplo: `"Group1:User6"`. Si no se especifica ningún valor, el instalac Kaspersky Security Center Web Console nueva cuenta con el nombre predetermin `user_message_queue_%uid%`.
`internalCertsTTLDays`	Plazo de validez de los certificados internos de Kaspersky Security Center Web Console.	Configuración opcional. El valor predeterr

Instalación de Kaspersky Security Center Web Console en Astra Linux en el modo de entorno de software cerrado

En esta sección se describe cómo instalar el Servidor de Kaspersky Security Center Web Console (también denominada Kaspersky Security Center Web Console) en el sistema operativo Astra Linux Special Edition. Antes de la instalación, debe instalar un DBMS y el Servidor de administración de Kaspersky Security Center Linux.

Para instalar Kaspersky Security Center Web Console:

1. Asegúrese de que el dispositivo en el que desea instalar Kaspersky Security Center Web Console esté ejecutando una de las distribuciones de Linux compatibles.

2. Lea el Contrato de licencia de usuario final. Si el kit de distribución de Kaspersky Security Center Linux no contiene un archivo TXT con el texto del EULA, puede descargar dicho archivo del sitio web de Kaspersky. Si no acepta los términos del Contrato de licencia, no instale la aplicación.

3. Cree un archivo de respuesta que contenga parámetros para conectar Kaspersky Security Center Web Console al Servidor de administración: `/etc/ksc-web-console-setup.json`.

   Ejemplo de un archivo de respuesta que contiene el conjunto mínimo de parámetros

El conjunto de parámetros del archivo de respuesta depende de la versión del Servidor de administración al que se conecta Kaspersky Security Center Web Console:

- Versión 16 o posterior del Servidor de administración

  Ejemplo de un archivo de respuesta con el conjunto mínimo de parámetros para iniciar sesión en la versión 16 o posteriores del Servidor de administración:

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

- Versión 15.4 o posterior del Servidor de administración

  Ejemplo de un archivo de respuesta con el conjunto mínimo de parámetros para iniciar sesión en la versión 15.4 o anteriores del Servidor de administración:

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

Puede instalar Kaspersky Security Center Web Console en el mismo dispositivo donde está el Servidor de administración o en otro dispositivo. Si Kaspersky Security Center Web Console está instalado en otro dispositivo, la dirección de Kaspersky Security Center Web Console (especificada por `address`) y la dirección del Servidor de administración (especificada por `iamHost` o `kscHost`) son diferentes. Si Kaspersky Security Center Web Console está instalado en el mismo dispositivo que el Servidor de administración, estos parámetros tienen los mismos valores.

El valor `iamHost` debe coincidir con la dirección de IAM que especificó durante la instalación del Servidor de administración. Para obtener la dirección de IAM especificada, ejecute el siguiente comando en el dispositivo que tiene el Servidor de administración instalado:

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

Para obtener información detallada, consulte el artículo: Parámetros de instalación de Kaspersky Security Center Web Console.

Puede agregar varios Servidores de administración de diferentes versiones a la lista de servidores de confianza. En este caso, los servidores pueden utilizar diferentes métodos de autenticación.

4. Abra el archivo `/etc/digsig/digsig_initramfs.conf` y luego especifique la siguiente configuración:

```
DIGSIG_ELF_MODE=1
```

5. En la línea de comandos, ejecute el siguiente comando para instalar el paquete de compatibilidad:

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

6. Cree un directorio para la clave de la aplicación:

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

7. Coloque la clave de la aplicación `/opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg` en el directorio creado en el paso anterior:

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

Si el kit de distribución de Kaspersky Security Center Linux no incluye la clave de la aplicación kaspersky_astra_pub_key.gpg, puede descargarla haciendo clic en este enlace: https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

8. Actualice los discos RAM:

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

Reinicie el sistema.

9. Con una cuenta con privilegios de root, use la línea de comando para ejecutar el archivo de instalación. El archivo de instalación debe descargarse del sitio web de Kaspersky.

- Para instalar o actualizar Kaspersky Security Center Web Console, ejecute el siguiente comando:

```
sudo apt-get install ksc-web-console-<número_de_compilación>.x86_64.deb
```

- Para actualizar Kaspersky Security Center Web Console a una versión más reciente, ejecute el siguiente comando:

```
sudo apt-get install ksc-web-console-<número_de_compilación>.x86_64.deb
```

Se iniciará el proceso para desempaquetar el archivo de instalación. Espere a que se complete la instalación. Kaspersky Security Center Web Console se instala en el siguiente directorio: `/var/opt/kaspersky/ksc-web-console`.

10. Reinicie todos los servicios de Kaspersky Security Center Web Console con el siguiente comando:

```
sudo systemctl restart KSC*
```

Cuando finalice la instalación, podrá usar un navegador para abrir Kaspersky Security Center Web Console e iniciar sesión.

Instalación de Kaspersky Security Center Linux con un script

El script `ksc_fast_install.py` le permite implementar Kaspersky Security Center Linux y realizar la configuración inicial de sus componentes: Servidor de administración y Web Console, incluidos DBMS y los paquetes de soporte necesarios.

El script lee los parámetros del archivo de parámetros. Se utilizan los valores predeterminados de los parámetros. Si es necesario, puede cambiar los valores.

Cómo funciona el script

Durante la ejecución, el script:

- Comprueba si se cumplen las siguientes condiciones:
  - Cuenta con los derechos necesarios para ejecutar el script.
  - El script es compatible con el sistema operativo y el DBMS.
  - Se han aceptado los EULA y la Política de privacidad.

    Si no los acepta en el archivo de parámetros, se le pedirá que lo haga después de ejecutar el script.
  - Requisitos de hardware para el Servidor de administración y Web Console.

    Los requisitos se definen en la Guía de dimensionamiento.
- Instala el DBMS (si aún no está instalado) y configura sus parámetros
- Crea bases de datos de Kaspersky Security Center y configura las credenciales del sistema operativo
- Instala el Servidor de administración y Web Console
- Le proporciona el nombre de usuario y la contraseña para iniciar sesión en Web Console.

  Antes de cerrar el terminal de línea de comandos, guarde las credenciales de la forma que prefiera. Si pierde las credenciales, debe agregar una nueva cuenta de usuario ejecutando el comando:
  `` `/opt/kaspersky/ksc64/sbin/kladduser -n <usuario>` ``

Si no se cumplen una o varias condiciones, o si se produce un error, el script finaliza y se muestra la notificación correspondiente.

El script no incluye acciones para reforzar la seguridad del sistema. Para reducir el riesgo de que Kaspersky Security Center se vea comprometido, tenga en cuenta las recomendaciones de la Guía para reforzar la seguridad.
El método de instalación basado en scripts permite desplegar Kaspersky Security Center Linux versión 16.3 o posterior en un dispositivo que no tenga instalado Kaspersky Security Center Linux.
Se requiere Python 3.6 o posterior para ejecutar el script.

El despliegue solo es posible si el dispositivo actual no tiene instalado Kaspersky Security Center Linux.

No puede usar el script para actualizar Kaspersky Security Center Linux a una nueva versión ni si se ha desplegado un clúster de conmutación por error de Kaspersky Security Center Linux.

El script `ksc_fast_install.py` admite la instalación de Kaspersky Security Center Linux en las versiones de sistemas operativos con DBMS descritas en la tabla.

Versión del sistema operativo	DBMS
Ubuntu Server 26.04 LTS	PostgreSQL 18 MySQL 8.4 (compilación 8.4.10)
RED OS 8	PostgreSQL 16 MariaDB 10.11 (compilación 10.11.18)
Astra Linux Special Edition RUSB.10015-01 (actualización operativa 1.8.5)	PostgreSQL 15 MariaDB 10.11 (compilación 10.11.13)
CentOS Stream 10	PostgreSQL 18 MariaDB 10.11 (compilación 10.11.13)

El script no admite un esquema de base de datos personalizado.

Cómo realizar la implementación mediante el script

Requisitos previos

Antes de ejecutar el script, asegúrese de haber hecho lo siguiente:

- Actualice su sistema operativo ejecutando uno de los siguientes comandos: `dnf update` o `apt update`
- Obtenga los privilegios de superusuario ejecutando el comando: `sudo -i`
- Permita la ejecución del script ejecutando el comando: `chmod +x ./ksc_fast_install.py`
- Asegúrese de que el repositorio de su sistema operativo aloje el DBMS compatible ejecutando el comando: `sudo apt policy postgresql`

Para implementar Kaspersky Security Center Linux ejecutando el script:

1. Desde el sitio web de Kaspersky, descargue lo siguiente:
   - Paquetes de distribución .deb o .rpm para el Servidor de administración y Web Console.
   - El archivo «script de instalación de KSC».

   > Al usar el script, seleccione los paquetes de distribución del Servidor de administración y de Web Console que sean compatibles con el administrador de paquetes de su sistema operativo.

El archivo contiene los siguientes archivos:

- Archivo de script `ksc_fast_install.py`.
- Archivo de parámetros.

  El nombre de archivo predeterminado es `params.txt`. Si desea cambiar el nombre del archivo, asegúrese de haber especificado el nombre nuevo mediante el parámetro `--params` al ejecutar el script en el terminal de línea de comandos.
- Archivo con el EULA y la Política de privacidad del Servidor de administración.
- Archivo con el EULA de Kaspersky Security Center Web Console.
- Archivos con las sumas hash de los EULA.

2. Coloque todos los archivos descargados en el mismo directorio local.
3. Si es necesario, configure el archivo de parámetros.

Haga clic aquí para ver un ejemplo de archivo de parámetros con la descripción de sus parámetros

```
# Required parameters:

#klfi_server_eula_accepted=N

#klfi_nwc_eula_accepted=N

#klfi_pp_accepted=N

# Optional parameters:

#klfi_klserver_db=KAV

#klfi_klserver_dbuser=klserver

#klfi_klserver_address=

#klfi_kliam_db=KAV_IAM

#klfi_kliam_dbuser=kliam

#klfi_kliam_address=

#klfi_sys_group_kladmin=kladmins

#klfi_sys_user_klserver=klsrvuser

#klfi_sys_user_kliam=kliamuser

#klfi_sys_user_svc=klsvcuser

#klfi_nwc_port=8080

#klfi_display_name=
```

#klfi_netsize=M

Los parámetros klfi_server_eula_accepted=N, klfi_nwc_eula_accepted=N y klfi_pp_accepted=N son obligatorios y siempre están presentes en el archivo de parámetros. Los demás parámetros son opcionales.

Para los parámetros obligatorios:

- Si cambia el valor predeterminado sin descomentar una línea, se le solicitará que acepte el EULA y la Política de privacidad.
- Si especifica un valor distinto de Y o N, se le solicitará que acepte el EULA y la Política de privacidad, independientemente de si descomentó la línea.
- Si descomenta la línea sin cambiar el valor predeterminado N, el script no funcionará.
- Si descomenta la línea y establece el valor Y, el script no le mostrará ningún aviso.

Parámetro y su valor predeterminado	Descripción del parámetro y otros valores posibles (si los hubiera)
klfi_server_eula_accepted=N	Contrato de licencia de usuario final del Servidor de administración. Valores posibles: • Y–EULA aceptado. • N–EULA no aceptado.
klfi_nwc_eula_accepted=N	Contrato de licencia de usuario final de Kaspersky Security Center Web Console. Valores posibles: • Y–EULA aceptado. • N–EULA no aceptado.
klfi_pp_accepted=N	Política de privacidad. Valores posibles: • Y–Política de privacidad aceptada. • N–Política de privacidad no aceptada.
klfi_klserver_db=KAV	El nombre de la base de datos del Servidor de administración. El nombre debe ser diferente del nombre de la base de datos de IAM especificado en el parámetro klfi_kliam_db.
klfi_kliam_db=KAV_IAM	El nombre de la base de datos de IAM. El nombre debe ser diferente del nombre de la base de datos del Servidor de administración especificado en el parámetro klfi_klserver_db.
klfi_klserver_dbuser=klserver	Nombre del usuario de la base de datos del Servidor de administración.
klfi_kliam_dbuser=kliam	Nombre del usuario de la base de datos de IAM.
klfi_klserver_address=FQDN	El FQDN del Servidor de administración o el nombre actual del dispositivo. Si no se especifica el valor del parámetro, el script determina automáticamente el FQDN o el nombre del dispositivo en el que se ejecuta el script. Si el script no puede determinar los valores, la instalación finaliza con un error.
klfi_kliam_address=FQDN	El FQDN del servidor de IAM o el nombre actual del dispositivo. Si no se especifica el valor del parámetro, el script determina automáticamente el FQDN o el nombre del dispositivo en el que se ejecuta el script. Si el script no puede determinar los valores, la instalación finaliza con un error.
klfi_sys_group_kladmin=kladmins	El nombre del grupo de seguridad para los servicios.
klfi_sys_user_klserver=klsrvuser	El nombre de la cuenta para iniciar el servicio del Servidor de administración.
klfi_sys_user_kliam=kliamuser	El nombre de la cuenta para iniciar el servicio de IAM.
klfi_sys_user_svc=klsvcuser	El nombre de la cuenta para iniciar otros servicios.

`klfi_nwc_port=8080`	Puerto para la conexión a Kaspersky Security Center Web Console.
`klfi_display_name=FQDN`	El nombre del Servidor de administración que se mostrará en la ventana del inicio de sesión.
`klfi_netsize=M`	El número aproximado de dispositivos que desea administrar. Cada estimación tiene en cuenta los recursos necesarios para ejecutar las aplicaciones de Kaspersky. El cálculo contempla el funcionamiento simultáneo del Servidor de administración, el Agente de red, Kaspersky Security Center Web Console y Kaspersky Endpoint Security for Linux en un mismo dispositivo. El almacenamiento de las copias de seguridad del Servidor de administración no se incluye en estos cálculos. Use un recurso de archivos externo como punto de montaje para almacenar las copias de seguridad en otro dispositivo, o aumente el espacio disponible en disco para cubrir su almacenamiento. Recomendamos agregar entre 4 y 6 GB de RAM y 20 GB adicionales de espacio libre en disco para instalar el sistema operativo. Estimación de recursos de hardware según el tamaño de la red: • `S` – de 1 a 1000 dispositivos administrados. • CPU–8 núcleos • RAM–16 GB • Espacio disponible en disco para el directorio `/var` –70 GB, 300 IOPS o más • `M` – de 1001 a 10000 dispositivos administrados. • CPU–12 núcleos • RAM–24 GB • Espacio disponible en disco para el directorio `/var` –340 GB, 300 IOPS o más • `L` – de 10001 a 30000 dispositivos administrados. • CPU–20 núcleos • RAM–40 GB • Espacio disponible en disco para el directorio `/var` –490 GB, 300 IOPS o más • `XL` – de 30001 a 50000 dispositivos administrados. • CPU–28 núcleos • RAM–54 GB • Espacio disponible en disco para el directorio `/var` –640 GB, 300 IOPS o más

Las líneas del archivo de parámetros están comentadas. Si desea configurar los valores, elimine el símbolo # al principio de la línea que desea descomentar.

Los parámetros `klfi_server_eula_accepted`, `klfi_nwc_eula_accepted` y `klfi_pp_accepted` son obligatorios, y su valor predeterminado es `N`. Si ejecuta el script sin cambiar estos valores en el archivo de configuración, se le solicitará que acepte el Contrato de licencia de usuario final y la Política de privacidad.

4. Ejecute el script.

Después de ejecutar el script, se muestra una notificación sobre la implementación correcta de los componentes de Kaspersky Security Center Linux, así como el nombre de usuario y la contraseña para iniciar

sesión en Web Console.

Si no se cumplen las condiciones para la instalación basada en script, se especifican parámetros desconocidos en el archivo de parámetros o se repite un parámetro varias veces, el script devuelve un error y se muestra la notificación correspondiente.

Si el script detecta incorrectamente que la RAM es insuficiente durante la detección de recursos, deshabilite el uso de RAM dinámica durante la instalación.

Si se produce un error al instalar los componentes de Kaspersky Security Center Linux o el DBMS, el script revierte los cambios y, luego, finaliza.

Reversión de una instalación fallida

Si se produce un error al instalar los componentes de Kaspersky Security Center Linux o el DBMS, el script realiza la reversión automáticamente. Se elimina el componente o el DBMS que se instaló antes de que se produjera el error.

La actualización de los paquetes del sistema operativo y la instalación de paquetes de soporte no se revierten.

Si finaliza el script de forma manual, los pasos que se hayan completado correctamente no se revierten. La próxima vez que ejecute el script (mediante el comando `python3 ksc_fast_install.py`), la instalación se reanudará desde el paso en el que se interrumpió. Si no desea reanudar la instalación, ejecute el script con la opción `rollback`: `python3 ksc_fast_install.py rollback.`. Esto hace que el script revierta todas las acciones realizadas antes de que se detuviera.

Despliegue del clúster de conmutación por error de Kaspersky Security Center Linux

Un clúster de conmutación por error de Kaspersky Security Center Linux proporciona una alta disponibilidad de Kaspersky Security Center Linux y minimiza el tiempo de inactividad del Servidor de administración en caso de una falla. El clúster de conmutación por error se conforma de dos instancias idénticas de Kaspersky Security Center Linux, cada una instalada en un equipo diferente. Una de las instancias funciona como nodo activo y la otra como nodo pasivo. El nodo activo administra la protección de los dispositivos cliente, mientras que el pasivo está preparado para asumir todas las funciones del nodo activo en caso de que falle el nodo activo. Cuando ocurre una falla, el nodo pasivo se activa y el nodo activo se vuelve pasivo.

El clúster de conmutación por error de Kaspersky Security Center Linux admite dos configuraciones:

- Un clúster de conmutación por error cuyos nodos se encuentran en un único centro de datos.
- Un clúster de conmutación por error distribuido geográficamente cuyos nodos se encuentran en diferentes centros de datos.

En un clúster de conmutación por error de Kaspersky Security Center Linux, todos los servicios de Kaspersky Security Center Linux se administran de manera automática. No intente reiniciar los servicios manualmente.

Utilice la función syslog para solucionar problemas.

Condiciones para el cambio

El clúster de conmutación por error cambia la administración de protección de los dispositivos cliente del nodo activo al nodo pasivo si ocurre alguno de los siguientes eventos en el nodo activo:

- El nodo activo se rompe debido a una falla de software o hardware.
- El nodo activo se detiene temporalmente por actividades de mantenimiento.
- Al menos uno de los servicios (o procesos) de Kaspersky Security Center Linux se detuvo por error o a propósito. Los servicios de Kaspersky Security Center Linux son los siguientes: klnagent_klfoc, kladminserver_klfoc, klactprx_klfoc, klwebsrv_klfoc.
- La conexión de red entre el nodo activo y el almacenamiento en el servidor de archivos se interrumpió o terminó (solo para el clúster ubicado en un solo centro de datos).

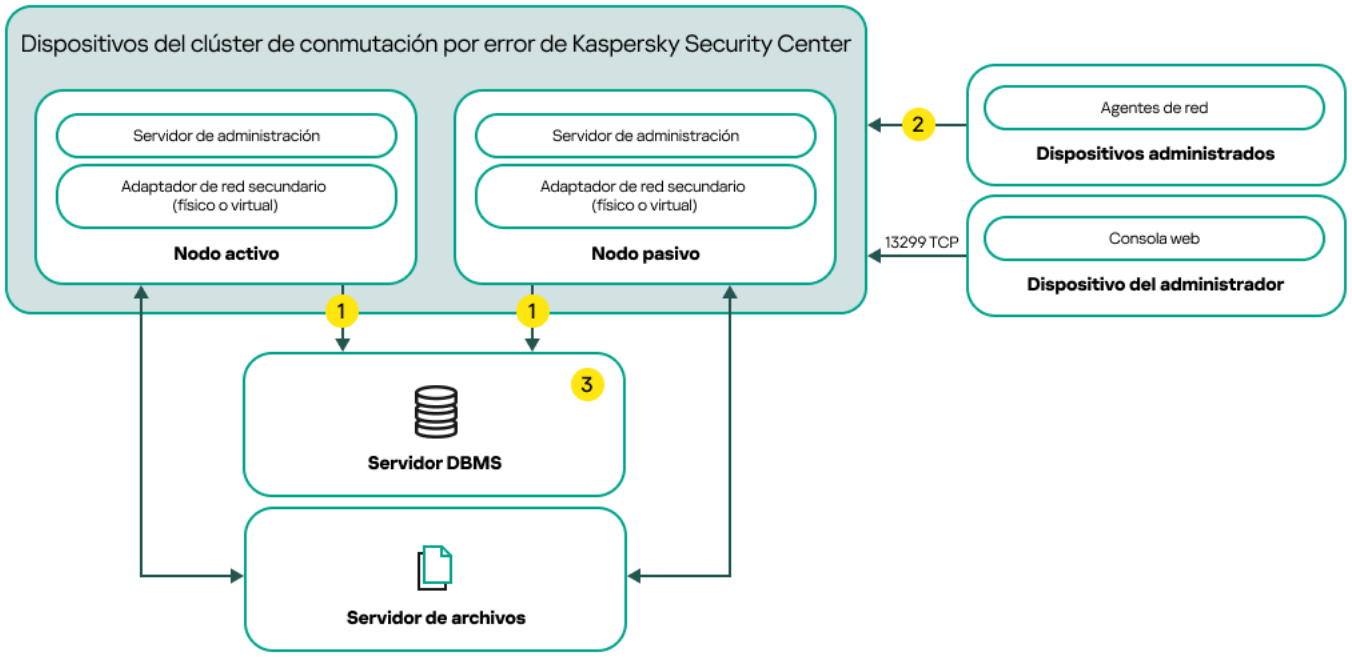
Clúster de conmutación por error de Kaspersky Security Center Linux. Esquemas de despliegue

Puede elegir uno de los siguientes esquemas para implementar el clúster de conmutación por error de Kaspersky Security Center Linux:

- Clúster de conmutación por error de Kaspersky Security Center Linux implementado en un único centro de datos:
  - Un esquema que utiliza un adaptador de red secundario y un DBMS instalado en un dispositivo dedicado.
  - Un esquema que usa un balanceador de carga de terceros y un DBMS instalado en un dispositivo dedicado.
- Clúster de conmutación por error de Kaspersky Security Center Linux distribuido geográficamente en varios centros de datos.

Clúster de conmutación por error de Kaspersky Security Center Linux

Un esquema que utiliza un adaptador de red secundario y un DBMS instalado en un dispositivo dedicado



Un esquema que utiliza un adaptador de red secundario y un DBMS instalado en un dispositivo dedicado

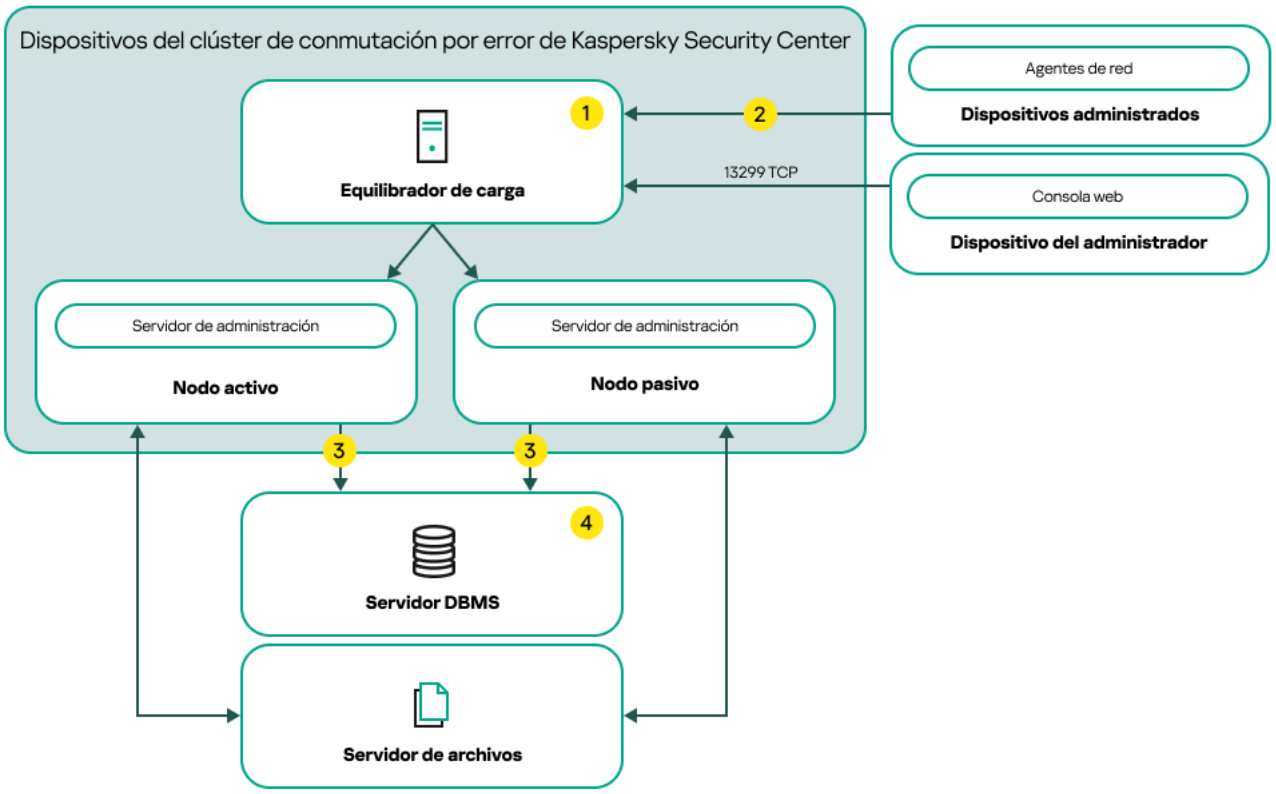
Leyenda del esquema:

1 El Servidor de administración envía información a la base de datos. Abra los puertos necesarios en el dispositivo donde se encuentra la base de datos, por ejemplo, el puerto 3306 para MySQL Server o el puerto 5432 para PostgreSQL o Postgres Pro. Consulte la documentación del DBMS para obtener la información necesaria.

2 Abra los siguientes puertos en los dispositivos con el Servidor de administración para conectarse a los dispositivos administrados: TCP 13000, UDP 13000 y TCP 17000.

3 Un dispositivo con sistema de administración de bases de datos (DBMS). Si usa MariaDB Galera Cluster como un DBMS, no se requiere un dispositivo dedicado para este propósito. Instale MariaDB Galera Cluster en cada uno de los nodos.

Un esquema que usa un balanceador de carga de terceros y un DBMS instalado en un dispositivo dedicado



Un esquema que usa un balanceador de carga de terceros y un DBMS instalado en un dispositivo dedicado

Leyenda del esquema:

1 En el dispositivo equilibrador de carga, abra todos los puertos del Servidor de administración: TCP 13000, UDP 13000, TCP 13299 y TCP 17000.

> Si desea usar la utilidad klakaut para la automatización, también debe abrir el puerto TCP 13291.

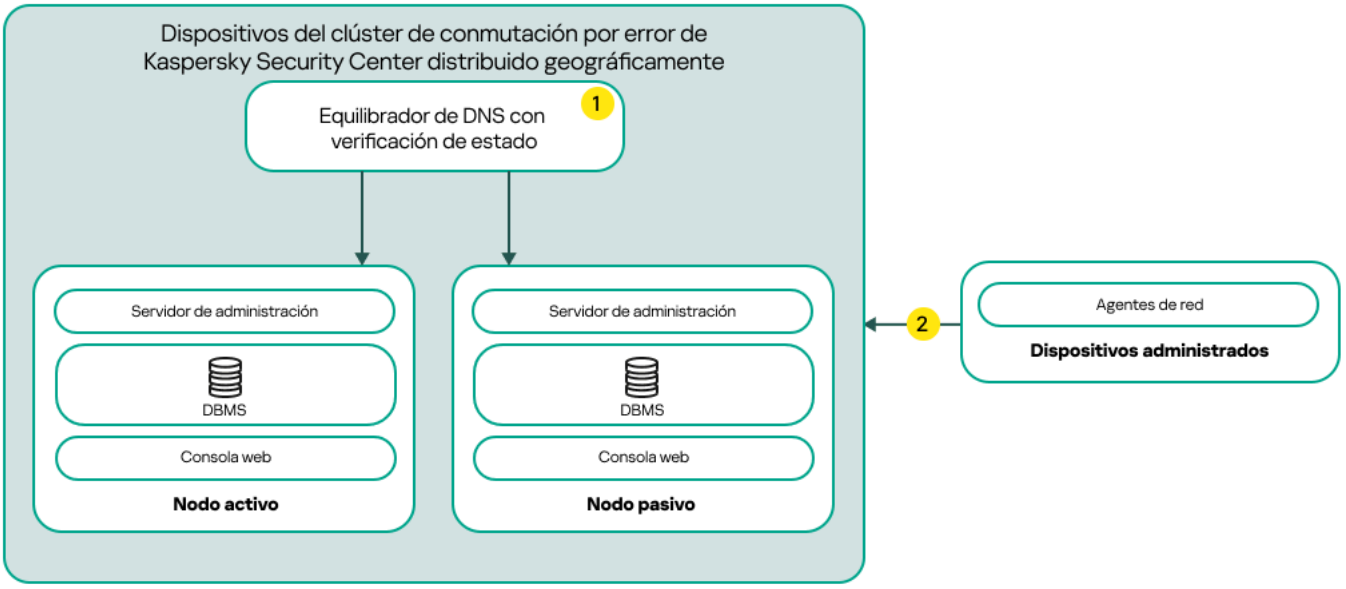
2 Abra los siguientes puertos en los dispositivos con el Servidor de administración para conectarse a los dispositivos administrados: TCP 13000, UDP 13000 y TCP 17000.

3 El Servidor de administración envía información a la base de datos. Abra los puertos necesarios en el dispositivo donde se encuentra la base de datos, por ejemplo, el puerto 3306 para MySQL Server o el puerto 5432 para PostgreSQL o Postgres Pro. Consulte la documentación del DBMS para obtener la información necesaria.

4 Un dispositivo con sistema de administración de bases de datos (DBMS). Si usa MariaDB Galera Cluster como un DBMS, no se requiere un dispositivo dedicado para este propósito. Instale MariaDB Galera Cluster en cada uno de los nodos.

Clúster de conmutación por error de Kaspersky Security Center Linux distribuido geográficamente

Este esquema de despliegue le permite proporcionar una alta disponibilidad de todos los componentes. En este esquema, el Servidor de administración, DBMS y Kaspersky Security Center Web Console se instalan en ambos nodos del clúster.



Esquema de despliegue del clúster de conmutación por error de Kaspersky Security Center Linux distribuido geográficamente

1 Equilibrador de DNS con verificación de estado que debe implementarse en su lado antes de la instalación del clúster de conmutación por error de Kaspersky Security Center Linux distribuido geográficamente.

El equilibrador de DNS comprueba periódicamente el estado de los nodos del clúster. Al acceder al clúster por su nombre de dominio, el equilibrador de DNS siempre devuelve la dirección IP del nodo activo.

2 Abra los siguientes puertos en los dispositivos con el Servidor de administración para conectarse a los dispositivos administrados: TCP 13000, UDP 13000 y TCP 17000.

Clúster de conmutación por error de Kaspersky Security Center Linux

Esta sección contiene información general sobre el clúster de conmutación por error de Kaspersky Security Center Linux implementado en un único centro de datos, así como instrucciones para preparar e implementar el clúster de conmutación por error de Kaspersky Security Center Linux en su red.

Procedimiento: Despliegue del clúster de conmutación por error de Kaspersky Security Center Linux

Un clúster de conmutación por error de Kaspersky Security Center Linux proporciona una alta disponibilidad de Kaspersky Security Center Linux y minimiza el tiempo de inactividad del Servidor de administración en caso de una falla. El clúster de conmutación por error se conforma de dos instancias idénticas de Kaspersky Security Center Linux, cada una instalada en un equipo diferente. Una de las instancias funciona como nodo activo y la otra como nodo pasivo. El nodo activo administra la protección de los dispositivos cliente, mientras que el pasivo está preparado para asumir todas las funciones del nodo activo en caso de que falle el nodo activo. Cuando ocurre una falla, el nodo pasivo se activa y el nodo activo se vuelve pasivo.

El despliegue de las aplicaciones de Kaspersky se divide en etapas:

Recomendamos seguir la secuencia de etapas que se describe en este escenario.

1. **Comprobar los requisitos de hardware**

   Asegúrese de tener el hardware que cumpla con los requisitos del clúster de conmutación por error.

2. **Elegir el esquema de despliegue**

   Elija el esquema de despliegue. Esto afectará las siguientes etapas del despliegue.

3. **Preparar las cuentas de usuario para los servicios de Kaspersky Security Center Linux**

   Realice los siguientes pasos en el nodo activo, el nodo pasivo y el servidor de archivos:

   1. Cree un grupo `kladmins`. Ejecute el siguiente comando:

      ```
      sudo groupadd kladmins
      ```

      ```
      sudo groupmod -g <new_GID> kladmins
      ```

      Asegúrese de que el grupo tenga el mismo GID en los tres dispositivos. Ejecute el siguiente comando:

      ```
      getent group kladmins
      ```

      Si los GID no coinciden, puede usar el siguiente comando para especificar el GID:

      ```
      sudo groupmod -g <new_GID> kladmins
      ```

   2. Cree una cuenta de usuario `ksc`. Asigne las cuentas de usuario al grupo `kladmins`. Ejecute el siguiente comando:

      ```
      sudo adduser ksc
      ```

      ```
      sudo usermod -u <new_UID> ksc
      ```

      ```
      sudo gpasswd -a ksc kladmins
      ```

      ```
      sudo usermod -g kladmins ksc
      ```

      Asegúrese de que la cuenta de usuario tenga el mismo UID en los tres dispositivos. Ejecute el siguiente comando:

      ```
      getent passwd ksc
      ```

      Si los UID no coinciden, puede usar el siguiente comando para especificar los UID:

      ```
      sudo usermod -u <new_UID> ksc
      ```

3. Cree una cuenta de usuario `rightless`. Asigne las cuentas de usuario al grupo `kladmins`. Ejecute el siguiente comando:

   ```
   sudo adduser rightless
   ```

   ```
   sudo usermod -u <new_UID> rightless
   ```

   ```
   sudo gpasswd -a rightless kladmins
   ```

   ```
   sudo usermod -g kladmins rightless
   ```

   Asegúrese de que la cuenta de usuario tenga el mismo UID en los tres dispositivos. Ejecute el siguiente comando:

   ```
   getent passwd rightless
   ```

   Si los UID no coinciden, puede usar el siguiente comando para especificar los UID:

   ```
   sudo usermod -u <new_UID> rightless
   ```

4. Cree una cuenta de usuario `ksciam`. Asigne las cuentas de usuario al grupo `kladmins`. Ejecute el siguiente comando:

   ```
   sudo adduser ksciam
   ```

   ```
   sudo usermod -u <new_UID> ksciam
   ```

   ```
   sudo gpasswd -a ksciam kladmins
   ```

   ```
   sudo usermod -g kladmins ksciam
   ```

   Asegúrese de que la cuenta de usuario tenga el mismo UID en los tres dispositivos. Ejecute el siguiente comando:

   ```
   getent passwd ksciam
   ```

   Si los UID no coinciden, puede usar el siguiente comando para especificar los UID:

   ```
   sudo usermod -u <new_UID> ksciam
   ```

5. Si es necesario, puede aumentar el límite predeterminado de los archivos que se pueden abrir (descriptores de archivo) en las cuentas utilizadas para el funcionamiento de los servicios de Kaspersky Security Center Linux. Para hacer esto, abra el archivo /etc/security/limits.conf y especifique los límites duros y blandos de los descriptores de archivos de la siguiente manera:

   ```
   ksc soft nofile <max_number_of_opened_files>
   ```

   ```
   ksc hard nofile <max_number_of_opened_files>
   ```

   De forma predeterminada, los límites de los descriptores de archivos se especifican durante la instalación. El límite suave de archivos es de 32 768, mientras que el límite duro es de 131 072.

4 Preparación del servidor de archivos

Prepare el servidor de archivos para que funcione como un componente del clúster de conmutación por error de Kaspersky Security Center Linux. Asegúrese de que el servidor de archivos cumpla con los requisitos de hardware y software; luego, cree dos carpetas compartidas para los datos de Kaspersky Security Center Linux y configure los permisos de acceso a esas carpetas.

Instrucciones: Preparación de un servidor de archivos para el clúster de conmutación por error de Kaspersky Security Center Linux

5 Instalación del DBMS

Instale el DBMS para Kaspersky Security Center Linux. Puede elegir uno de los DBMS compatibles. Para obtener información sobre cómo instalar el DBMS seleccionado, consulte su documentación.

Si su distribución del sistema operativo Linux no contiene un DBMS compatible, puede utilizar el repositorio de paquetes de un tercero para instalar el DBMS.

Después de instalar el DBMS, siga las instrucciones correspondientes:

- Configurar el servidor PostgreSQL o Postgres Pro para que funcione con Kaspersky Security Center Linux
- Configurar el servidor MariaDB x64 para trabajar con Kaspersky Security Center Linux

Cree manualmente una base de datos para IAM. El Servidor de administración no elimina la base de datos de IAM automáticamente al desinstalar o mover el servidor a otro dispositivo; debe eliminarla de forma manual.

- En el caso de PostgreSQL, ejecute el siguiente comando:

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

- En el caso de MariaDB, ejecute el siguiente comando:

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

En el dispositivo con el DBMS instalado, configure la conexión a los dispositivos que funcionarán como nodos activos y pasivos.

6. **Preparación de nodos activos y pasivos**

   Prepare dos dispositivos con hardware y software idénticos para que funcionen como un nodo activo y pasivo.

   Instrucciones: Preparación de nodos para el clúster de conmutación por error de Kaspersky Security Center Linux

7. **Instalación de Kaspersky Security Center Linux**

   Instale Kaspersky Security Center Linux en ambos nodos, en modo de clúster de conmutación por error.

   Realice la instalación de Kaspersky Security Center Linux primero en el dispositivo que desee que sea el nodo activo y luego en el pasivo.

   Instrucciones: instalación de Kaspersky Security Center Linux en los nodos del clúster de conmutación por error de Kaspersky Security Center Linux.

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

   Instale Kaspersky Security Center Web Console en un dispositivo independiente que no sea un nodo del clúster.

   El clúster de conmutación por error debe tener la dirección del Servidor de administración en el archivo de respuesta.

   El certificado del Servidor de administración se encuentra en la siguiente ruta: /mnt/KlFocDataShare_klfoc/1093/cert/klserver.cer

   Copie el archivo del certificado al dispositivo donde está instalando Kaspersky Security Center Web Console. En el archivo de respuesta, determine la ruta local al certificado.

9. **Prueba del clúster de conmutación por error**

   Compruebe que haya configurado correctamente el clúster de conmutación por error y que funcione correctamente. Por ejemplo, puede ejecutar el siguiente comando para iniciar el cambio al nodo pasivo:

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

   Use el siguiente comando para verificar que el servicio de administración de clústeres de conmutación por error aparezca como `Active: active (running)` en ambos nodos:

   `systemctl status klfocsvc_klfoc`

Use los siguientes comandos para verificar que los otros servicios de clúster de conmutación aparezcan como `Active: active (running)` en el nodo activo. En el nodo pasivo, estos servicios de clúster de conmutación por error deben aparecer como `Active: inactive (dead)` o `Active: failed (Result: signal)`.

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

El clúster de conmutación por error de Kaspersky Security Center Linux se encuentra desplegado.

Clúster de conmutación por error de Kaspersky Security Center Linux. Requisitos de hardware y software

Recomendamos que, después de instalar el Servidor de administración en un dispositivo, instale Kaspersky Endpoint Security for Linux en ese dispositivo.
Para la instalación simultánea, debe tener un mínimo de 300 IOPS, así como agregar 1,5 GB de RAM y un 15 % de CPU a los requisitos del Servidor de administración.
Para conocer los requisitos de hardware de Kaspersky Endpoint Security, consulte la Ayuda de Kaspersky Endpoint Security for Linux.

Para obtener información sobre la configuración de seguridad necesaria para trabajar con Kaspersky Security Center Linux, consulte la Ayuda de Kaspersky Endpoint Security for Linux.

Para implementar un clúster de conmutación por error de Kaspersky Security Center Linux, debe tener el siguiente hardware:

- Dos dispositivos con idéntico hardware y software. Estos dispositivos actuarán como nodos activos y pasivos.

  Configuración mínima para nodos activos y pasivos

Hardware	Valor
CPU	2 núcleos, 2500 MHz
RAM	6 GB
Espacio en disco	10 GB, 150 IOPS o más
Controlador de interfaz de red	1 Gbps

  El despliegue del clúster de conmutación por error falla cuando tiene instalados los paquetes arping e iputils-arping o solo el paquete arping. Antes de implementar un clúster de conmutación por error, asegúrese de tener solo el paquete iputils-arping instalado en ambos nodos.

  Puede consultar los requisitos de dimensionamiento de los nodos activos y pasivos según la cantidad de dispositivos administrados en el artículo Requisitos de hardware para el DBMS y el Servidor de administración.

- Un dispositivo en el que desea instalar Kaspersky Security Center Linux Web Console.

Configuración del dispositivo para un máximo de 10 administradores del sistema

Hardware	Valor
CPU	2 núcleos, 2500 MHz
RAM	4 GB
Espacio en disco	40 GB, 150 IOPS o más

Configuración del dispositivo para más de 10 administradores del sistema

Hardware	Valor
CPU	4 núcleos, 2500 MHz
RAM	8 GB
Espacio en disco	40 GB, 150 IOPS o más

- Un servidor de archivos compatible con el protocolo CIFS/SMB, versión 2.0 o posterior. Debe proporcionar un dispositivo dedicado que actuará como servidor de archivos.

  Configuración de un servidor de archivos

Hardware	Valor
CPU	4 núcleos, 2500 MHz
RAM	32 GB
Espacio en disco	500 GB, 500 IOPS o más
Controlador de interfaz de red	10 Gbps

  Asegúrese de haber proporcionado un ancho de banda de red elevado entre el servidor de archivos y los nodos activo y pasivo.

- Un dispositivo con sistema de administración de base de datos (DBMS). Si usa MariaDB Galera Cluster como un DBMS, no se requiere un dispositivo dedicado para este propósito.

- Un dispositivo equilibrador de carga. Se utiliza en un esquema de despliegue de un clúster de conmutación por error de Kaspersky Security Center Linux que implica el uso de un equilibrador de carga de terceros y el DBMS instalado en un dispositivo dedicado.

  Configuración del dispositivo para un equilibrador de carga Nginx

Hardware	Valor
CPU	2 núcleos, 2500 MHz
RAM	4 GB

Preparación de un servidor de archivos para un clúster de conmutación por error de Kaspersky Security Center Linux

Un servidor de archivos funciona como un componente necesario en un clúster de conmutación por error de Kaspersky Security Center Linux.

Para preparar un servidor de archivos, haga lo siguiente:

1. Asegúrese de que el servidor de archivos cumpla con los requisitos de hardware y software.

2. Instale y configure un servidor NFS:

   - El acceso al servidor de archivos debe estar habilitado para ambos nodos en la configuración del servidor NFS.
   - El protocolo NFS debe tener la versión 4.0 o 4.1.
   - Requisitos mínimos para el kernel de Linux:
     - 3.19.0-25, si usa NFS 4.0
     - 4.4.0-176, si usa NFS 4.1

   Dependiendo de su distribución de Linux, instale el paquete nfs-utils o el paquete nfs-kernel-server ejecutando el comando correspondiente:

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

3. En el servidor de archivos, cree dos carpetas y compártalas mediante NFS. Una de ellas se utiliza para almacenar información sobre el estado del clúster de conmutación por error. La otra se utiliza para almacenar los datos y la configuración de Kaspersky Security Center Linux. Deberá especificar las rutas a las carpetas compartidas cuando configure la instalación de Kaspersky Security Center Linux.

   Asegúrese de que no existan las siguientes carpetas:

   - `/mnt/KlFocStateShare`
   - `/mnt/KlFocDataShare_klfoc`

   Si alguna de estas carpetas existe, elimínela de forma recursiva.

   Ejecute el siguiente comando:

   ```
   sudo mkdir -p /mnt/KlFocStateShare
   sudo mkdir -p /mnt/KlFocDataShare_klfoc
   sudo chown ksc:kladmins /mnt/KlFocStateShare
   sudo chown ksc:kladmins /mnt/KlFocDataShare_klfoc
   sudo chmod -R 770 /mnt/KlFocStateShare /mnt/KlFocDataShare_klfoc
   sudo sh -c "echo /mnt/KlFocStateShare *\(rw,sync,no_subtree_check,no_root_squash\) >> /etc/exports"
   sudo sh -c "echo /mnt/KlFocDataShare_klfoc *\
   (rw,sync,no_subtree_check,no_root_squash\) >> /etc/exports"
   sudo exportfs -a
   sudo systemctl start rpcbind
   sudo systemctl start nfs-server
   ```

   Habilite el inicio automático mediante el siguiente comando:

   ```
   sudo systemctl enable rpcbind
   ```

Puede especificar carpetas personalizadas, pero recomendamos que use los nombres de carpetas sugeridos para mayor comodidad al consultar la Ayuda.

4. Reinicie el servidor de archivos.

El servidor de archivos está preparado. Para desplegar el clúster de conmutación por error de Kaspersky Security Center Linux, siga las instrucciones adicionales en este escenario.

Preparación de nodos para un clúster de conmutación por error de Kaspersky Security Center Linux

Antes de continuar, asegúrese de haber completado los pasos anteriores en el Procedimiento: Despliegue del clúster de conmutación por error de Kaspersky.

Prepare dos dispositivos para que funcionen como los nodos activo y pasivo del clúster de conmutación por error de Kaspersky Security Center Linux.

Configuración de carpetas comunes

Para configurar carpetas comunes:

1. Dependiendo de su distribución de Linux, instale el paquete nfs-utils o el paquete nfs-kernel-server en cada nodo ejecutando el comando correspondiente:

   `yum install nfs-utils`

   `apt install nfs-kernel-server`

2. Cree puntos de montaje mediante los siguientes comandos:

   `mkdir -p /mnt/KlFocStateShare`

   `mkdir -p /mnt/KlFocDataShare_klfoc`

3. Haga coincidir los puntos de montaje y las carpetas compartidas:

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

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

   Donde el `{servidor de archivos}` es el FQDN del servidor de archivos con carpetas compartidas.

4. Monte las carpetas compartidas ejecutando los siguientes comandos:

   `mount /mnt/KlFocStateShare`

   `mount /mnt/KlFocDataShare_klfoc`

5. Asegúrese de que los permisos para acceder a las carpetas compartidas pertenezcan a ksc:kladmins.

   Ejecute el siguiente comando:

   `ls -la /mnt/`

Configuración de adaptadores de red

Un adaptador de red secundario puede ser físico o virtual. Si elige un esquema de despliegue con un adaptador de red secundario, debe realizar el procedimiento correspondiente en ambos nodos:

- Use un adaptador de red secundario virtual basado en un adaptador de red físico (tecnología MACVLAN):

  1. Instale el paquete iputils-arping. Dependiendo de su distribución de Linux, ejecute uno de los siguientes comandos:

     - `yum install iputils`

     o

     - `apt install iputils-arping`

  2. Para asegurarse de que NetworkManager se use para administrar el adaptador de red físico, ejecute el siguiente comando:

     `nmcli device status`

     Si, como respuesta del comando, el adaptador de red físico no está siendo administrado, configure NetworkManager para administrarlo. Los pasos de configuración exactos dependerán de la distribución de Linux que utilice.

  3. Para identificar las interfaces, utilice el siguiente comando:

     `ip a`

  4. Para crear un perfil de configuración, ejecute el siguiente comando:

     `nmcli connection add type macvlan dev <interfaz física> mode bridge ifname <interfaz virtual> ipv4.addresses <máscara de dirección> ipv4.method manual autoconnect no`

- Utilice un adaptador de red secundario físico o cree un dispositivo TAP virtual con un hipervisor. En este procedimiento, debe deshabilitar el software NetworkManager.

  1. Conecte el adaptador de red secundario a un nodo.

  2. Instale el paquete iputils-arping. Dependiendo de su distribución de Linux, ejecute uno de los siguientes comandos:

     - `yum install iputils`

     o

     - `apt install iputils-arping`

  3. Para eliminar la conexión de NetworkManager para la interfaz de destino, ejecute el siguiente comando:

     `nmcli con del <connection name>`

     Para verificar las conexiones a la interfaz de destino, ejecute el siguiente comando:

     `nmcli con show`

  4. Modifique el archivo NetworkManager.conf. Localice la sección del archivo clave y asigne la interfaz de destino al parámetro `unmanaged-devices`:

     `[keyfile]`

`unmanaged-devices=interface-name:<nombre de la interfaz>`

5. Reinicie NetworkManager:

   `systemctl reload NetworkManager`

   Para asegurarse de que la interfaz de destino ya no esté administrada, ejecute el siguiente comando:

   `nmcli dev status`

Configuración del equilibrador de carga

Si eligió un esquema de implementación con un equilibrador de carga, siga las instrucciones a continuación para configurarlo.

Para configurar el equilibrador de carga:

1. Prepare un dispositivo específico basado en Linux con nginx u otro equilibrador de carga que tenga instalado.
2. Configure el equilibrio de carga. Configure el nodo activo como servidor principal y el nodo pasivo como servidor de respaldo.
3. En el servidor nginx, abra todos los puertos del Servidor de administración según lo que se detalla en el artículo Puertos utilizados por Kaspersky Security Center Linux.

Para desplegar el clúster de conmutación por error de Kaspersky Security Center Linux, siga las instrucciones adicionales del escenario.

> La disponibilidad de los nodos del clúster de conmutación por error se determina según la disponibilidad de los puertos de conexión principales con el Servidor de administración. El nodo pasivo no acepta ninguna conexión externa hasta que se produce un cambio.

Instalación de Kaspersky Security Center Linux en los nodos del clúster de conmutación por error de Kaspersky Security Center Linux

Antes de continuar, asegúrese de haber completado los pasos anteriores en el Procedimiento: Despliegue del clúster de conmutación por error de Kaspersky.

En este procedimiento, se describe cómo instalar Kaspersky Security Center Linux en los nodos del clúster de conmutación por error de Kaspersky Security Center Linux. Kaspersky Security Center Linux se instala por separado en ambos nodos del clúster de conmutación por error de Kaspersky Security Center Linux. Primero, debe instalar la aplicación en el nodo activo, luego en el pasivo. Durante la instalación, elija qué nodo estará activo y cuál será pasivo.

Dependiendo de la distribución de Linux instalada en su dispositivo, debe usar uno de los siguientes archivos de instalación:

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

El archivo de instalación debe descargarse del sitio web de Kaspersky.

Si usa RED OS versión 7.3.4 o una superior o MSVSPHERE versión 9.2 o una superior, debe instalar el paquete libxcrypt-compat en ambos nodos.

Instalación en el nodo activo

Para instalar Kaspersky Security Center Linux en el nodo activo:

1. Asegúrese de que el dispositivo en el que desee instalar Kaspersky Security Center Linux cuente con una de las distribuciones de Linux compatibles.

2. Si usa un adaptador de red secundario, ingrese el nombre cuando se le solicite. Puede ingresar el siguiente comando para mostrar todas las interfaces de red:

   ```
   ip addr
   ```

3. Realice la instalación de Kaspersky Security Center Linux. Dependiendo de su distribución de Linux, ejecute uno de los siguientes comandos:

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

4. Realice la configuración de Kaspersky Security Center Linux:

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

5. Leer el Contrato de licencia de usuario final (EULA) y la Política de privacidad. El texto se muestra en la ventana de la línea de comandos. Presione la barra espaciadora para ver el siguiente segmento de texto. Luego, cuando se le solicite, ingrese los siguientes valores:

   a. Ingrese `y` si comprende y acepta los términos del EULA. Ingrese `n` si no acepta los términos del EULA. Para utilizar Kaspersky Security Center Linux, debe aceptar los términos del EULA.

   b. Ingrese `y` si comprende y acepta los términos de la Política de privacidad, y si acepta que sus datos se manejen y transmitan (incluso a terceros países) como se describe en la Política de privacidad. Ingrese `n` si no acepta los términos de la Política de privacidad. Para utilizar Kaspersky Security Center Linux, debe aceptar los términos de la Política de privacidad.

6. Seleccione **Nodo de clúster principal** como un modo de instalación del Servidor de administración.

7. Cuando se le solicite, especifique la siguiente configuración:

   a. Ingrese la ruta local al punto de montaje del recurso compartido de estado: `/mnt/KlFocStateShare`

   b. Ingrese la ruta local al punto de montaje del recurso compartido de datos: `/mnt/KlFocDataShare_klfoc`

   c. Elija un modo de conectividad de clúster de conmutación por error: a través de un adaptador de red secundario o un equilibrador de carga externo.

   d. Si usa un adaptador de red secundario, ingrese el nombre.

   e. Ingrese el FQDN o el nombre del DNS del adaptador de red secundario o el FQDN o el nombre del DNS del equilibrador de carga externo.

   f. Ingrese el número de puerto SSL del Servidor de administración. El número de puerto predeterminado es 13000.

g. Evalúe el número aproximado de dispositivos que pretende administrar:

- Si tiene de 1 a 100 dispositivos administrados, ingrese 1.
- Si tiene de 101 a 1000 dispositivos administrados, ingrese 2.
- Si tiene más de 1000 dispositivos administrados, ingrese 3.

Esta configuración se utiliza para el retardo aleatorio automático para el inicio de tareas a fin de optimizar la carga de la red. En la siguiente lista se muestra el intervalo dentro del cual se calcula el retardo:

- De 1 a 100 dispositivos administrados, valor 1. No se utiliza el retardo.
- De 101 a 1000 dispositivos administrados, valor 2. El retardo es de 5 minutos.
- Más de 1000 dispositivos administrados, valor 3. El retardo es de 10 minutos.

h. Ingrese el nombre del grupo de seguridad para los servicios. De forma predeterminada, se utiliza el grupo 'kladmins'.

i. Introduzca el nombre de la cuenta para iniciar el servicio del Servidor de administración. La cuenta debe ser miembro del grupo de seguridad ingresado. De manera predeterminada, se utiliza la cuenta ksc.

j. Introduzca el nombre de la cuenta para iniciar otros servicios. La cuenta debe ser miembro del grupo de seguridad ingresado. De manera predeterminada, se utiliza la cuenta ksc.

k. Seleccione el DBMS que haya instalado para trabajar con Kaspersky Security Center Linux:

- Si instaló MySQL o MariaDB, ingrese 1.
- Si instaló PostgreSQL o Postgres Pro SQL, ingrese 2.

l. Introduzca el nombre DNS o la dirección IP del dispositivo en el que esté instalada la base de datos.

m. Introduzca el número de puerto de la base de datos. Este puerto se utiliza para comunicarse con el Servidor de administración. De forma predeterminada, se utilizan los siguientes puertos:

- Puerto 3306 para MySQL y MariaDB.
- Puerto 5432 para PostgreSQL y Postgres Pro.

n. Escriba el nombre de la base de datos.

o. Ingrese el nombre de usuario de la cuenta de administrador de la base de datos que utiliza para acceder a la base de datos.

p. Ingrese la contraseña de la cuenta de administrador de la base de datos que utiliza para acceder a la base de datos.

q. Ingrese el FQDN o el nombre del DNS del servidor IAM.

Ingrese el valor que especificó en el paso 7e.

r. Ingrese el nombre de la cuenta para iniciar el servicio IAM. La cuenta debe ser miembro del grupo de seguridad ingresado. De manera predeterminada, se utiliza la cuenta ksciam.

s. Seleccione el DBMS que haya instalado para trabajar con el servicio IAM:

- Si instaló MySQL o MariaDB, ingrese 1.
- Si instaló PostgreSQL o Postgres Pro SQL, ingrese 2.

t. Ingrese la dirección de DBMS de IAM que utilizará el servicio de IAM.

u. Ingrese el número de puerto de DBMS de IAM. Este puerto se utiliza para comunicarse con el servicio IAM. De forma predeterminada, se utilizan los siguientes puertos:

- Puerto 3306 para MySQL y MariaDB.
- Puerto 5432 para PostgreSQL y Postgres Pro.

v. Ingrese el nombre de la base de datos de IAM que utilizará el servicio de IAM. El nombre de la base de datos utilizada por el servicio de IAM debe ser diferente de la base de datos utilizada por el Servidor de administración.

w. Ingrese el nombre de usuario de la cuenta de la base de datos que utiliza para acceder a la base de datos de IAM.

x. Ingrese la contraseña de la cuenta de la base de datos que utiliza para acceder a la base de datos de IAM.

8. Espere a que los servicios se agreguen e inicien automáticamente:

- klfocsvc_klfoc
- kladminserver_klfoc
- klwebsrv_klfoc
- klactprx_klfoc
- klnagent_klfoc
- kliam_klfoc

9. Cree una cuenta que actuará como administrador del Servidor de administración. Ingrese el nombre de usuario y la contraseña. La contraseña de usuario no puede tener menos de 8 ni más de 256 caracteres.

   Si omite este paso, puede crear la cuenta más tarde; para ello, ejecute el siguiente comando:

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

Se agrega el usuario y se instala Kaspersky Security Center Linux en el nodo principal.

Instalación en el nodo secundario (pasivo)

Para instalar Kaspersky Security Center Linux en el nodo secundario:

1. Asegúrese de que el dispositivo en el que desee instalar Kaspersky Security Center Linux cuente con una de las distribuciones de Linux compatibles.

2. Realice la instalación de Kaspersky Security Center Linux. Dependiendo de su distribución de Linux, ejecute uno de los siguientes comandos:

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

3. Realice la configuración de Kaspersky Security Center Linux:

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

4. Leer el Contrato de licencia de usuario final (EULA) y la Política de privacidad. El texto se muestra en la ventana de la línea de comandos. Presione la barra espaciadora para ver el siguiente segmento de texto. Luego, cuando se le solicite, ingrese los siguientes valores:

   a. Ingrese `y` si comprende y acepta los términos del EULA. Ingrese `n` si no acepta los términos del EULA. Para utilizar Kaspersky Security Center Linux, debe aceptar los términos del EULA.

   b. Ingrese `y` si comprende y acepta los términos de la Política de privacidad, y si acepta que sus datos se manejen y transmitan (incluso a terceros países) como se describe en la Política de privacidad. Ingrese `n` si no acepta los términos de la Política de privacidad. Para utilizar Kaspersky Security Center Linux, debe aceptar los términos de la Política de privacidad.

5. Seleccione **Nodo de clúster secundario** como un modo de instalación del Servidor de administración.

6. Cuando se le solicite, ingrese la ruta local al punto de montaje del recurso compartido estatal:
   `/mnt/KlFocStateShare`

Kaspersky Security Center Linux queda instalado en el nodo secundario.

Verificación del servicio

Utilice el siguiente comando para verificar que el servicio de administración del clúster de conmutación por error esté en estado `Active: active (running)`:

```
systemctl status klfocsvc_klfoc
```

Utilice los siguientes comandos para verificar que otros servicios del clúster de conmutación por error estén en estado `Active: inactive (dead)`:

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

- `systemctl status klwebsrv_klfoc`
- `systemctl status kliam_klfoc`

Ahora, puede probar el clúster de conmutación por error de Kaspersky Security Center Linux para asegurarse de que lo configuró de forma correcta y de que funciona bien.

Iniciar y detener nodos del clúster manualmente

Es posible que deba detener todo el clúster de conmutación por error de Kaspersky Security Center Linux o desconectar de forma temporal uno de los nodos del clúster para realizar tareas de mantenimiento. Si este es el caso, siga las instrucciones de esta sección. No intente iniciar ni detener los servicios o procesos relacionados con el clúster de conmutación por error utilizando ningún otro medio. Esto puede provocar la pérdida de datos.

Iniciar y detener todo el clúster de conmutación por error para mantenimiento

Para iniciar o detener todo el clúster de conmutación por error, haga lo siguiente:

En el nodo activo, ejecute uno de los siguientes comandos:

- Para detener el clúster, ejecute: `/opt/kaspersky/ksc64/sbin/klfoc -stopcluster --stp klfoc`
- Para iniciar el clúster, ejecute: `/opt/kaspersky/ksc64/sbin/klfoc -startcluster --stp klfoc`

El clúster de conmutación por error se inicia o se detiene según el comando que ejecute.

Mantenimiento de uno de los nodos

Para mantener uno de los nodos, haga lo siguiente:

1. En el nodo activo, detenga el clúster de conmutación por error mediante el comando `klfoc -stopcluster --stp klfoc`.
2. En el nodo que desea mantener, vaya a /opt/kaspersky/ksc64/sbin.
3. Abra la línea de comandos y luego desconecte el nodo del clúster ejecutando el comando `detach_node.sh`.
4. En el nodo activo, inicie el clúster de conmutación por error mediante el comando `klfoc -startcluster --stp klfoc`.
5. Realizar actividades de mantenimiento.
6. En el nodo activo, detenga el clúster de conmutación por error mediante el comando `klfoc -stopcluster --stp klfoc`.
7. En el nodo que se mantuvo, vaya a /opt/kaspersky/ksc64/sbin.
8. Abra la línea de comandos y luego adjunte el nodo al clúster ejecutando el comando `attach_node.sh`.
9. En el nodo activo, inicie el clúster de conmutación por error mediante el comando `klfoc -startcluster --stp klfoc`.

10. Para asegurarse de que el nodo actual esté activo, ejecute los siguientes comandos a fin de verificar si los servicios se están ejecutando:

    `systemctl status klnagent_klfoc.service`

    `systemctl status kladminserver_klfoc.service`

    `systemctl status klactprx_klfoc.service`

    `systemctl status klwebsrv_klfoc.service`

    `systemctl status kliam_klfoc.service`

    Estos servicios se ejecutan en el nodo activo; no se ejecutan en el nodo pasivo.

El nodo se mantiene y se adjunta al clúster de conmutación por error.

Reinstalación de un nodo del clúster de conmutación por error

Para reinstalar un nodo del clúster de conmutación por error:

1. Cree una copia de seguridad del Servidor de administración.
2. Cambie el nodo activo al modo de mantenimiento.
3. De ser necesario para conservar el sistema operativo actual, realice los siguientes pasos.

   Si desea reemplazar el dispositivo o el sistema operativo, omita este paso.

   a. Para detener el clúster de conmutación por error, ejecute el siguiente comando:

   `klfoc -stopcluster --stp klfoc`

   b. Para detener forzosamente los servicios del clúster de conmutación por error, ejecute los siguientes comandos:

   `sudo systemctl stop klfocsvc_klfoc`

   `systemctl status kl*klfoc*`

   c. Para desinstalar los directorios del clúster de conmutación por error, ejecute los siguientes comandos:

   `sudo umount /mnt/KlFocDataShare_klfoc`

   `sudo umount /mnt/KlFocStateShare`

   d. Para desinstalar Kaspersky Security Center Linux, ejecute cualquiera de los siguientes comandos según su distribución de Linux:

   - `sudo dpkg --remove ksc64`

   o

   - `sudo yum remove ksc64`

e. En el caso del nodo pasivo, realice todos los pasos de las siguientes instrucciones:

1. Preparación de nodos para un clúster de conmutación por error de Kaspersky Security Center Linux.

2. Instalación de Kaspersky Security Center Linux en los nodos del clúster de conmutación por error de Kaspersky Security Center Linux.

4. Salga del modo de mantenimiento. Continúe desde el paso 6 (detenga el clúster de conmutación por error) de las instrucciones Iniciar y detener nodos del clúster manualmente.

Instalación de Kaspersky Security Center Web Console conectado al Servidor de administración instalado en nodos del clúster de conmutación por error de Kaspersky Security Center Linux

En esta sección, se describe cómo instalar el Servidor de Kaspersky Security Center Web Console (en adelante, también denominado Kaspersky Security Center Web Console), que se conecta al Servidor de administración instalado en los nodos del clúster de conmutación por error de Kaspersky Security Center Linux. Antes de instalar Kaspersky Security Center Web Console, instale un DBMS y el Servidor de administración de Kaspersky Security Center Linux en los nodos del clúster de conmutación por error de Kaspersky Security Center Linux.

Kaspersky Security Center Web Console no admite la instalación en nodos de clúster. Recomendamos que se instale Kaspersky Security Center Web Console en un servidor diferente.

Para instalar Kaspersky Security Center Web Console, que se conecta al Servidor de administración instalado en los nodos del clúster de conmutación por error de Kaspersky Security Center Linux, siga estos pasos:

1. Realice los pasos 1 y 2 del procedimiento de instalación de Kaspersky Security Center Web Console.

2. En el paso 3, en el archivo de respuesta, especifique el parámetro de instalación `trusted` para permitir que Kaspersky Security Center Web Console se conecte al Clúster de conmutación por error de Kaspersky Security Center de Linux.

   Componentes del **parámetro de instalación** `trusted`

   Si se conecta al clúster de conmutación por error de Kaspersky Security Center Linux mediante la autenticación de dominio con SSO, especifique el parámetro de instalación de confianza de la siguiente manera: si conecta Kaspersky Security Center Web Console a la versión 16 o posteriores del Servidor de administración, se utilizará la autenticación de dominio con inicio de sesión único (SSO) proporcionada por Identity and Access Manager (IAM). En este caso, especifique el parámetro de instalación `trusted` de la siguiente manera:

```
"trusted":  {
  "<Nombre del Servidor de administración>": {
    "iamHost": "ksc-iam.example.com",
    "iamOAuthPort": 4444,
    "iamProxyPort": 9050,
    "iamCertPath": "<carpeta de datos compartida>/iam/main_certificate.pem",
    "iamPATPath": "<carpeta de datos compartida>/iam/initial_token.txt",
    "kscPort": 13299,
    "kscCertPath": "<carpeta de datos compartida>/1093/cert/klserver.cer"
  }
}
```

donde:

- `< nombre del Servidor de administración >` es el nombre del clúster de conmutación por error de Kaspersky Security Center Linux que se mostrará en el ventana de inicio de sesión de Kaspersky Security Center Web Console.

- `iamHost` es la dirección del dispositivo donde se instalaron el Servidor de administración e IAM. Si creó un adaptador de red secundario al preparar los nodos del clúster, utilice el FQDN o el nombre de host del adaptador como dirección del clúster de conmutación por error de Kaspersky Security Center Linux. De lo contrario, deberá especificar el FQDN o el nombre de host del equilibrador de carga externo que utilice.

  El valor `iamHost` debe coincidir con la dirección de IAM que se especificó durante la instalación del Servidor de administración. Para obtener la dirección de IAM especificada, ejecute el siguiente comando en el dispositivo que tiene el Servidor de administración instalado:

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

- `iamOAuthPort` es el puerto que se utiliza para intercambiar tokens de autentificación a través del protocolo de autenticación OpenID Connect (valor predeterminado: 4444). Este puerto se utiliza tanto para la comunicación entre el Servidor de Kaspersky Security Center Web Console y el Servidor de administración, como entre el navegador (que se utiliza con Kaspersky Security Center Web Console) y el Servidor de administración.

- `iamProxyPort` es el puerto que se utiliza para conectar el Servidor de Kaspersky Security Center Web Console al servidor de administración (valor predeterminado: 9050).

- `iamCertPath` es la ruta al certificado de IAM. El certificado de IAM se crea automáticamente la primera vez que ejecuta el Servidor de administración. El certificado está en el dispositivo donde está instalado el Servidor de administración La ruta predeterminada al certificado es: `< carpeta de datos compartida >/iam/main_certificate.pem`. El certificado se encuentra en el almacenamiento de datos compartido del clúster de conmutación por error de Kaspersky Security Center Linux. El certificado de IAM autofirmado se rota automáticamente.

- `iamPATPath` es la ruta al token utilizado para registrar Kaspersky Security Center Web Console como cliente OAuth en IAM. Este archivo se genera automáticamente la primera vez que se ejecuta el Servidor de administración. El token está en el dispositivo donde está instalado el Servidor de administración. La ruta predeterminada al token es: <carpeta de datos compartida>/iam/initial_token.txt. El token se encuentra en el almacenamiento de datos compartido del clúster de conmutación por error de Kaspersky Security Center Linux. El token es válido indefinidamente y no requiere rotación.

- `kscPort` es el puerto OpenAPI que Kaspersky Security Center Web Console utiliza para conectarse al Servidor de administración (valor predeterminado: 13299).

- `kscCertPath` es el certificado del Servidor de administración que se encuentra en el almacenamiento de datos compartido del clúster de conmutación por error de Kaspersky Security Center Linux. La ruta predeterminada al archivo del certificado es `< carpeta de datos compartida >\1093\cert\klserver.cer`.

  Copie el archivo del certificado del Servidor de administración (especificado con `kscCertPath`), el archivo del certificado de IAM (especificado con `iamCertPath`) y el archivo de token (especificado con `iamPATPath`) desde el almacenamiento de datos compartido y péguelos en el dispositivo donde instale Kaspersky Security Center Web Console. Defina la ruta local al certificado del Servidor de administración.

Si conecta Kaspersky Security Center Web Console a la versión 15.4 o anteriores del Servidor de administración, se utilizará la autenticación especificando el nombre y la contraseña del usuario del dominio o del usuario interno. En este caso, especifique el parámetro de instalación de confianza de la siguiente manera:

```
"trusted":  {
  "<Nombre del Servidor de administración>": {
    "kscHost": "ksc.example.com",
    "kscPort": 13299,
    "kscCertPath": "<carpeta de datos compartida>/1093/cert/klserver.cer"
  }
}
```

donde:

- `<nombre del Servidor de administración>` es el nombre del clúster de conmutación por error de Kaspersky Security Center Linux que se mostrará en el ventana de inicio de sesión de Kaspersky Security Center Web Console.
- `kscHost` es la dirección del Servidor de administración (FQDN o nombre de host). Si creó un adaptador de red secundario al preparar los nodos del clúster, utilice la dirección del adaptador como dirección del clúster de conmutación por error de Kaspersky Security Center Linux. De lo contrario, ingrese la dirección del equilibrador de carga de terceros que esté utilizando.
- `kscPort` es el puerto de OpenAPI que Kaspersky Security Center Web Console utiliza para conectarse al Servidor de administración (valor predeterminado: 13299).
- `kscCertPath` es el certificado del Servidor de administración que se encuentra en el almacenamiento de datos compartido del clúster de conmutación por error de Kaspersky Security Center Linux. La ruta predeterminada al archivo del certificado es `<carpeta de datos compartida>\1093\cert\klserver.cer`. Copie el archivo del certificado de la carpeta compartida al dispositivo en el que se encuentre instalado Kaspersky Security Center Web Console. Defina la ruta local al certificado del Servidor de administración.

3. Lleve a cabo los demás pasos de instalación de Kaspersky Security Center Web Console, como si se tratara de una instalación estándar.

Cuando finalice la instalación, podrá usar un navegador para abrir Kaspersky Security Center Web Console e iniciar sesión.

Clúster de conmutación por error de Kaspersky Security Center Linux distribuido geográficamente

Esta sección contiene información general acerca del clúster de conmutación por error de Kaspersky Security Center Linux distribuido geográficamente, así como instrucciones para preparar y desplegar el clúster de conmutación por error distribuido geográficamente en su red para las siguientes configuraciones:

- Nodos del clúster que ejecutan Ubuntu con DBMS de PostgreSQL
- Nodos del clúster que ejecutan SberLinux con DBMS de Platform V Pangolin

Clúster distribuido geográficamente que ejecuta Ubuntu con DBMS de PostgreSQL

Siguiendo este escenario, puede preparar su infraestructura e implementar un clúster de conmutación por error de Kaspersky Security Center Linux distribuido geográficamente.

Requisitos previos

- Despliegue un equilibrador de DNS de alta disponibilidad con verificación de estado.
- Asegúrese de que los nodos del clúster activo y pasivo sean dos dispositivos con configuraciones de hardware y software idénticas.
  - Requisitos de hardware:
    - CPU: 16 núcleos, 2500 MHz
    - RAM: 32 GB
    - Espacio en disco: 500 GB con 300 IOPS o más
    - Controlador de interfaz de red: 1 Gbps
  - Requisitos de software:
    - Sistema operativo: Ubuntu Server 24.04 LTS (Noble Numbat) de 64 bits
    - DBMS: PostgreSQL 17 de 64 bits

Etapas

El clúster de conmutación por error de Kaspersky Security Center Linux desplegado dentro de un único centro de datos no se puede actualizar a un clúster de conmutación por error distribuido geográficamente.

El despliegue del clúster de conmutación por error de Kaspersky Security Center Linux distribuido geográficamente se realiza en etapas:

1. **Preparación de un sistema de archivos de nodos de clúster de conmutación por error**

   Prepare el sistema de archivos en ambos nodos del clúster. La preparación incluye la creación de volúmenes lógicos LVM y la configuración de directorios como puntos de montaje.

2. **Configuración de un sistema de archivos de clúster replicado**

   Instale las utilidades de DRBD y configure los recursos de DRBD para la replicación de datos entre los nodos del clúster de conmutación por error. Después de eso, cree un sistema de archivos replicado en el nodo del clúster activo.

3. **Instalación y configuración de Corosync y Pacemaker en los nodos del clúster de conmutación por error**

   Instale Corosync y Pacemaker para proporcionar comunicación de clúster y administración de recursos para alta disponibilidad.

4. **Instalación y configuración del DBMS de PostgreSQL**

   Instale y configure PostgreSQL en los nodos del clúster.

5. **Instalación de Kaspersky Security Center Linux en los nodos del clúster de conmutación por error**

   Instale Kaspersky Security Center Linux en los nodos del clúster y luego configure el cifrado entre los nodos del clúster.

6. **Instalación de Kaspersky Security Center Web Console en los nodos del clúster de conmutación por error**

   Instale Kaspersky Security Center Web Console en ambos nodos del clúster de conmutación por error para brindar alta disponibilidad.

Preparación de un sistema de archivos de nodos de clúster

Como primer paso en la preparación para el despliegue del clúster de conmutación por error de Kaspersky Security Center Linux distribuido geográficamente, debe configurar el sistema de archivos en ambos nodos del clúster. La preparación incluye la creación de volúmenes lógicos LVM y la configuración de directorios como puntos de montaje. Realice el siguiente procedimiento en ambos nodos del clúster.

Para preparar un sistema de archivos de nodos de clúster:

1. Cree un volumen lógico LVM para los datos y la base de datos del Servidor de administración:

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

   Cree un volumen lógico LVM separado para almacenar el archivo de respuesta:

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

   donde:

   - `volume group name` es el nombre del grupo de volúmenes utilizado por LVM.
   - `klfocdata` y `klfocstate` son nombres de volumen lógicos. Estos volúmenes lógicos se crean dentro del grupo de volúmenes

     Recomendamos usar estos nombres de volumen para mantener la coherencia, aunque puede especificar nombres personalizados si es necesario.
   - `volume size` un tamaño del volumen. Recomendamos asignar al menos 500 GB para los datos y la base de datos del Servidor de administración. El volumen para almacenar el archivo de respuesta requiere una pequeña cantidad de espacio.

2. Cree directorios que se utilizarán como puntos de montaje para los volúmenes lógicos.

   - Para los datos y la base de datos del Servidor de administración:

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

   - Para el archivo de respuesta:

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

Recomendamos utilizar los directorios `/mnt/KlFocDataShare_klfoc` y `/mnt/KlFocStateShare_klfoc` para mantener la coherencia, aunque puede especificar nombres personalizados si es necesario.

Se prepara el sistema de archivos de los nodos del clúster. Después de eso, debe configurar un sistema de archivos de clúster replicado.

Configuración de un sistema de archivos de clúster replicado

Instalación y configuración de DRBD

DRBD es un software de terceros que se utiliza para la replicación de datos (específicamente para los volúmenes de datos y los puntos de montaje preparados en el paso anterior).

Después de preparar el sistema de archivos de los nodos del clúster, debe instalar las utilidades de DRBD y configurar los recursos de DRBD para la replicación de datos entre los nodos del clúster. Realice el siguiente procedimiento en ambos nodos del clúster.

Para instalar y configurar DRBD en los nodos del clúster:

1. Instale las utilidades de DRBD:

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

   Recomendamos usar DRBD versión 9.2.6 o posterior, ya que proporciona cifrado de tráfico integrado.

   El tráfico DRBD también se puede cifrar mediante su propia solución VPN.

2. Cree archivos de configuración de recursos DRBD para cada volumen lógico creado durante la preparación del sistema de archivos (`klfocdata` y `klfocstate`).

   Todos los archivos de configuración deben colocarse en `/etc/drbd.d/`.

   - Recurso `klfocdata` (Datos y base de datos del Servidor de administración)

     Utilice la replicación asincrónica (protocolo A) para el recurso klfocdata. Configure todos los demás parámetros de acuerdo con su entorno.

     Ejemplo de archivo de configuración:

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

   - Recurso `klfocstate` (el archivo de respuesta)

     Utilice la replicación sincrónica (protocolo C) para crear el recurso klfocstate. Configure todos los demás parámetros de acuerdo con su entorno.

Ejemplo de archivo de configuración:

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

3. Inicialice los metadatos de DRBD para ambos recursos:

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

4. Inicie DRBD en todos los recursos configurados:

```
drbdadm up all
```

DRBD se instala y configura en ambos nodos del clúster.

Crear un sistema de archivos replicado en el nodo del clúster activo

Después de instalar y configurar DRBD en ambos nodos del clúster, cree un sistema de archivos replicado en el nodo del clúster activo. Realice el siguiente procedimiento en el nodo del clúster activo.

Para crear un sistema de archivos replicado en el nodo del clúster activo:

1. Promueva ambos recursos de DRBD al rol principal:

```
drbdadm primary --force klfocdata
drbdadm primary --force klfocstate
```

2. Formatee los dispositivos DRBD para preparar los volúmenes replicados para su uso en los nodos del clúster:

```
mkfs.ext4 /dev/drbd0
mkfs.ext4 /dev/drbd2
```

3. Configure los parámetros del sistema de archivos:

```
tune2fs -m 0 /dev/drbd0
tune2fs -m 0 /dev/drbd2
```

4. Monte los dispositivos DRBD en los directorios creados anteriormente:

```
mount -o noatime /dev/drbd0 /mnt/KlFocDataShare_klfoc
mount -o noatime /dev/drbd2 /mnt/KlFocStateShare_klfoc
```

   Si el servicio multipathd está instalado, debe configurarse para ignorar los dispositivos `/dev/drbd*` en ambos nodos del clúster.

5. Verifique el estado de la replicación:

```
drbdadm status
```

   El resultado de la configuración correcta del sistema de archivos:

```
klfocdata role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate

klfocstate role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate
```

Se configura un sistema de archivos replicado en el nodo del clúster activo. Después de eso, debe instalar y configurar Corosync y Pacemaker en los nodos del clúster.

Instalación y configuración de Corosync y Pacemaker en los nodos del clúster

Corosync y Pacemaker proporcionan comunicación de clúster y administración de recursos para una alta disponibilidad. Garantizan que los servicios se muevan automáticamente a un nodo en buen estado en caso de que ocurra un error, lo que minimiza el tiempo de inactividad.

Para instalar y configurar Corosync y Pacemaker en los nodos del clúster:

1. En ambos nodos del clúster, instale los paquetes necesarios:

```
sudo apt install pacemaker -y
sudo apt install crmsh -y
sudo apt install resource-agent-extra -y
```

2. Configure Corosync y Pacemaker en ambos nodos del clúster de acuerdo con la documentación oficial. Esto incluye habilitar el inicio automático, generar y distribuir la clave de autenticación y configurar los permisos de acceso para el archivo de clave de autenticación.

   Para asegurarse de que la configuración sea correcta, ejecute el siguiente comando en uno de los nodos del clúster:

```
crm status
```

   El resultado esperado debe mostrar el estado del clúster y enumerar todos los nodos activos, lo que confirma que Corosync es funcionando correctamente y los nodos se están comunicando.

3. En ambos nodos del clúster, configure los ajustes básicos del clúster de Pacemaker:

```
crm configure property stonith-enabled="false"
crm configure property symmetric-cluster="false"
crm configure rsc_defaults resource-stickiness="110"
crm configure rsc_defaults migration-threshold=3
crm configure property no-quorum-policy=ignore
```

4. En ambos nodos del clúster, desactive el inicio de los scripts que Corosync administrará:

```
systemctl disable drbd.service
```

5. En uno de los nodos del clúster, cree los recursos basados en DRBD en Pacemaker.

- Recurso DRBD para klfocdata

  a. Cree un recurso de clúster para el volumen DRBD `klfocdata`, lo que permite al clúster administrar y supervisar su estado automáticamente:

  ```
  crm configure primitive drbd_klfocdata ocf:linbit:drbd params drbd_resource="klfocdata" \
  op monitor interval="60s" op start interval="0" timeout="240s" op stop interval="0" \
  timeout="240s" op monitor role=Master interval="10s" op monitor role=Slave interval="30s"
  ```

  b. Cree un recurso administrado por clúster `ms_drbd_klfocdata` basado en el recurso creado `drbd_klfocdata`:

  ```
  crm configure ms ms_drbd_klfocdata drbd_klfocdata meta master-max="1" master-node-max="1" \
  clone-max="2" clone-node-max="1" notify="true"
  ```

  c. Cree un punto de montaje para el volumen de DRBD `fs_klfocdata`, y especifique el dispositivo, directorio de destino, tipo de sistema de archivos y opciones de montaje:

  ```
  crm configure primitive fs_klfocdata ocf:heartbeat:Filesystem params device="/dev/drbd0" \
  directory="/mnt/KlFocDataShare_klfoc" fstype="ext4" options="data=journal"
  ```

- Recurso DRBD para klfocstate

  a. Cree un recurso de clúster para el volumen DRBD `klfocstate`, lo que permite que el clúster administre y supervise su estado automáticamente:

  ```
  crm configure primitive drbd_klfocstate ocf:linbit:drbd params drbd_resource="klfocstate" \
  op monitor interval="60s" op start interval="0" timeout="240s" op stop interval="0" \
  timeout="240s" op monitor role=Master interval="10s" op monitor role=Slave interval="30s"
  ```

  b. Cree un recurso administrado por clúster ms_drbd_klfocstate basado en el recurso creado `drbd_klfocstate`:

  ```
  crm configure ms ms_drbd_klfocstate drbd_klfocstate meta master-max="1" master-node-max="1" \
  clone-max="2" clone-node-max="1" notify="true"
  ```

c. Cree un punto de montaje para el volumen DRBD `fs_klfocstate`, y especifique el dispositivo, el directorio de destino, el tipo de sistema de archivos y las opciones de montaje:

```
crm configure primitive fs_klfocstate ocf:heartbeat:Filesystem params device="/dev/drbd2" \
directory="/mnt/KlFocStateShare_klfoc" fstype="ext4" options="noatime"
```

6. Establezca el orden de montaje de los recursos cuyos DRBD se encuentran en estado Primario. Asigne a este recurso el nombre `cluster_resources`:

```
crm configure colocation cluster_resources inf: fs_klfocdata ms_drbd_klfocdata:Master ms_drbd_klfocstate:Master
```

7. Configure el grupo de recursos y servicios `group_klfoc`:

```
crm configure group group_klfoc fs_klfocdata fs_klfocstate
```

8. Configure el grupo de recursos `group_klfoc` para que se inicie después de los recursos DRBD correspondientes. Asigne a esta regla el nombre `all_after_drbd`:

```
crm configure order all_after_drbd inf: ms_drbd_klfocdata:promote group_klfoc:start
```

9. Establezca la preferencia para iniciar los recursos primarios y secundarios: prioridad 100 para `node1` y 50 para `node2`:

```
crm configure location loc_klfocdata_one ms_drbd_klfocdata 100: db1 # hostname of the first cluster node
crm configure location loc_klfocdata_two ms_drbd_klfocdata 50: db2 # hostname of the second cluster node
crm configure location loc_klfocstate_one ms_drbd_klfocstate 100: db1 # hostname of the first cluster node
crm configure location loc_klfocstate_two ms_drbd_klfocstate 50: db2 # hostname of the second cluster node
crm configure location loc_group_one group_klfoc 100: db1 # hostname of the first cluster node
crm configure location loc_group_two group_klfoc 50: db2 # hostname of the second cluster node
```

10. En ambos nodos del clúster, deshabilite el inicio automático del servicio DRBD:

```
systemctl disable drbd.service
```

Corosync y Pacemaker se instalan y configuran en los nodos del clúster. Después de eso, debe instalar el DBMS y crear la base de datos del Servidor de administración y la base de datos de IAM.

Instalación y configuración del DBMS de PostgreSQL

Después de instalar y configurar Corosync y Pacemaker en los nodos del clúster, debe instalar el DBMS en ambos nodos del clúster.

Para instalar y configurar del DBMS:

1. En ambos nodos del clúster, instale PostgreSQL 17 x64 o posterior.

   Para obtener información sobre cómo instalar PostgreSQL, consulte la documentación.

2. Asegúrese de que los nodos del clúster con el DBMS instalado no tengan cuentas de usuario de DBMS con los siguientes nombres:

   - client
   - iam

- ksc
- locker
- pat
- scope
- voltron

3. En ambos nodos del clúster, detenga el DBMS y luego deshabilite el inicio automático del servicio DBMS:

```
sudo systemctl stop postgresql
sudo systemctl disable postgresql
```

4. En el nodo del clúster activo, copie el directorio DBMS al directorio `/mnt/KlFocDataShare_klfoc/dbms`:

```
rsync -av /var/lib/postgresql/17/main/ /mnt/KlFocDataShare_klfoc/dbms
mv /var/lib/postgresql/17/main /var/lib/postgresql/17/main.bk
```

5. En el nodo del clúster activo, copie los archivos de configuración de PostgreSQL al directorio `/mnt/KlFocDataShare_klfoc/dbms`:

```
sudo cp /etc/postgresql/17/main/pg_hba.conf /mnt/KlFocDataShare_klfoc/dbms
sudo cp /etc/postgresql/17/main/pg_ident.conf /mnt/KlFocDataShare_klfoc/dbms
```

6. En ambos nodos del clúster, abra el archivo de configuración `/etc/postgresql/17/main/postgresql.conf` y luego establezca el directorio `/mnt/KlFocDataShare_klfoc/dbms` como el directorio de datos de la base de datos.

   También especifique las rutas a los archivos de configuración (`/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf` y `/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf`) y elimine el parámetro `include_dir`:

```
data_directory = '/mnt/KlFocDataShare_klfoc/dbms'
hba_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf'
ident_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf'
listen_addresses = '*'
```

7. En el archivo de configuración `/etc/postgresql/17/main/postgresql.conf`, ajuste la configuración de DBMS para cumplir con los requisitos de Kaspersky Security Center Linux.

8. Cree y configure cuentas para trabajar con PostgreSQL.

9. Cree el recurso de servicio de PostgreSQL:

```
crm configure primitive klfocsvc_dbms ocf:heartbeat:pgsql \
params pgctl="/usr/lib/postgresql/17/bin/pg_ctl" \
psql="/usr/bin/psql" \
pgdata="/mnt/KlFocDataShare_klfoc/dbms" \
config="/etc/postgresql/17/main/postgresql.conf" \
socketdir="/var/run/postgresql" \
op start timeout=60s \
op stop timeout=60s \
op monitor interval=30s timeout=60s
```

10. Agregue el recurso de PostgreSQL al grupo de clústeres `group_klfoc`:

```
crm configure edit group_klfoc
```

11. Agregue el nombre del recurso de `klfocsvc_dbms` PostgreSQL al final de la lista, por ejemplo:

```
group group_klfoc {
...
klfocsvc_dbms
}
```

12. En el nodo del clúster activo, en el servidor DBMS, cree una base de datos para IAM. El nombre de la base de datos debe ser diferente al de la base de datos que instaló para trabajar con Kaspersky Security Center Linux. El Servidor de administración no elimina la base de datos de IAM automáticamente cuando se desinstala o mueve el servidor a otro dispositivo; debe eliminarla de forma manual:

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

Se instala y configura el DBMS. Se crean la base de datos del Servidor de administración y la base de datos de IAM. Después de eso, debe instalar Kaspersky Security Center Linux en los nodos del clúster.

Instalación de Kaspersky Security Center Linux en los nodos del clúster de conmutación por error distribuidos geográficamente

Kaspersky Security Center Linux se instala en los nodos del clúster de conmutación por error distribuidos geográficamente mediante un archivo de respuesta en modo silencioso, es decir, sin la participación del usuario. El archivo de respuesta contiene un conjunto personalizado de parámetros de instalación: variables y sus respectivos valores.

Requisitos previos:

- Realice todos los pasos preparatorios:
  - Preparación de un sistema de archivos de nodos de clúster
  - Configuración de un sistema de archivos de clúster replicado
  - Instalación y configuración de Corosync y Pacemaker en los nodos del clúster
  - Instalación y configuración del DBMS de PostgreSQL
- Asegúrese de que los nodos del clúster ejecuten Ubuntu Server 24.04 LTS (Noble Numbat) x64.
- Descargue el archivo de instalación `ksc64_[version_number]_amd64.deb` del sitio web de Kaspersky.

Instalación en el nodo activo

Para instalar Kaspersky Security Center Linux en el nodo activo en modo silencioso:

1. Lea el Contrato de licencia de usuario final. Siga los pasos a continuación únicamente si comprende y acepta los términos del Contrato de licencia de usuario final.

2. Cree un grupo `kladmins` y las cuentas sin privilegios `ksc` y `ksciam` que deben ser miembros del grupo `kladmins`. Para hacerlo, ejecute secuencialmente los siguientes comandos en una cuenta con privilegios raíz:

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

3. En el directorio `/mnt/KlFocDataShare_klfoc/`, cree un directorio para los archivos de Kaspersky Security Center Linux:

```
mkdir /mnt/KlFocDataShare_klfoc/ksc/
```

4. Cree el archivo de respuesta (en formato TXT) y agregue una lista de variables en el formato VARIABLE_NAME=variable_value al archivo de respuesta. Agregue cada variable en una línea separada.

   En la lista de parámetros utilizados para la instalación de Kaspersky Security Center Linux en modo silencioso, especifique los siguientes parámetros necesarios para la implementación del clúster distribuido geográficamente:

   - `KLFOC_UNATT_EXT_RESOURCE_MANAGEMENT=2`

     Establezca el valor `2` para desplegar el clúster distribuido geográficamente.

   - `KLSRV_UNATT_SERVERADDRESS=<DNS balancer address>` y `KLSRV_UNATT_IAM_ADDRESS=<DNS balancer address>`

     El equilibrador de DNS con verificación de estado ya debe estar desplegado. Los valores de estos parámetros deben ser idénticos y configurarse con el FQDN del equilibrador de DNS.

5. Establezca el valor de la variable de entorno `KLAUTOANSWERS` en el entorno raíz que contiene el nombre completo del archivo de respuesta, incluida la ruta; por ejemplo, con el siguiente comando:

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

6. Inicie la instalación de Kaspersky Security Center Linux en modo silencioso ejecutando los siguientes comandos:

   - En el entorno raíz:

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

   - En el entorno del usuario:

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

7. Deshabilite el inicio automático del servicio klfocsvc_klfoc.service:

```
systemctl disable klfocsvc_klfoc.service
```

8. Después de instalar Kaspersky Security Center Linux, detenga el nodo del clúster activo.

9. Mueva todos los recursos del clúster al nodo pasivo.

   Puede usar el comando `crm node standby` (y recuperarlo con `crm node online`).

Instalación en el nodo pasivo

Para instalar Kaspersky Security Center Linux en el nodo pasivo:

1. Ejecute la instalación de Kaspersky Security Center Linux:

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

2. Realice la configuración de Kaspersky Security Center Linux:

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

3. Leer el Contrato de licencia de usuario final (EULA) y la Política de privacidad. El texto se muestra en la ventana de la línea de comandos. Presione la barra espaciadora para ver el siguiente segmento de texto. Luego, cuando se le solicite, ingrese los siguientes valores:

   - Ingrese `y` si comprende y acepta los términos del EULA. Ingrese `n` si no acepta los términos del EULA. Para utilizar Kaspersky Security Center Linux, debe aceptar los términos del EULA.

   - Ingrese `y` si comprende y acepta los términos de la Política de privacidad, y si acepta que sus datos se manejen y transmitan (incluso a terceros países) como se describe en la Política de privacidad. Ingrese n si no acepta los términos de la Política de privacidad. Para utilizar Kaspersky Security Center Linux, debe aceptar los términos de la Política de privacidad.

4. Seleccione el nodo de clúster pasivo como modo de instalación del Servidor de administración.

5. Cuando se le solicite, ingrese la ruta local al punto de montaje del recurso compartido de estado: `/mnt/KlFocStateShare_klfoc`.

6. Deshabilite el inicio automático del servicio klfocsvc_klfoc.service:

```
systemctl disable klfocsvc_klfoc.service
```

7. Cree el recurso del servicio `klfocsvc_klfoc`:

```
crm configure primitive klfocsvc_klfoc systemd:klfocsvc_klfoc \
op start timeout="900s" interval="0" \
op stop timeout="900s" interval="0" \
op monitor interval="30s" timeout="90s"
```

8. Agregue el recurso `klfocsvc_klfoc` al grupo `group_klfoc`:

```
crm configure edit group_klfoc
```

9. Agregue `klfocsvc_klfoc` al final de la línea del grupo, por ejemplo:

```
group group_klfoc {
...
klfocsvc_klfoc
}
```

10. Verifique que todos los recursos estén en el estado iniciado en el nodo activo.

```
crm status
```

Configuración del cifrado entre los nodos del clúster

Para configurar el cifrado entre los nodos del clúster:

Si instaló la versión 9.2.6 o posterior de DRBD durante la configuración de un sistema de archivos del clúster replicado, configure el cifrado entre los nodos del clúster de acuerdo con la documentación oficial de DRBD.

Como alternativa, puede cifrar el tráfico entre los nodos del clúster mediante su propia solución VPN.

Se instala el clúster de conmutación por error de Kaspersky Security Center Linux distribuido geográficamente. Después de eso, debe instalar Kaspersky Security Center Web Console en ambos nodos del clúster.

Clúster distribuido geográficamente que ejecuta SberLinux con DBMS de Platform V Pangolin

Siguiendo este escenario, puede preparar su infraestructura e implementar un clúster de conmutación por error de Kaspersky Security Center Linux distribuido geográficamente.

Requisitos previos

- Despliegue un equilibrador de DNS de alta disponibilidad con verificación de estado.
- Asegúrese de que los nodos del clúster activo y pasivo sean dos dispositivos con configuraciones de hardware y software idénticas.
  - Requisitos de hardware:
    - CPU: 16 núcleos, 2500 MHz
    - RAM: 32 GB
    - Espacio en disco: 500 GB con 300 IOPS o más
    - Controlador de interfaz de red: 1 Gbps

- Requisitos de software:
  - Sistema operativo: Platform V SberLinux OS Server (SLO) 9.5.1 de 64 bits
  - DBBMS: Platform V Pangolin 6.5.1 de 64 bits

Etapas

El clúster de conmutación por error de Kaspersky Security Center Linux desplegado dentro de un único centro de datos no se puede actualizar a un clúster de conmutación por error distribuido geográficamente.

El despliegue del clúster de conmutación por error de Kaspersky Security Center Linux distribuido geográficamente se realiza en etapas:

1. **Preparación de un sistema de archivos de nodos de clúster de conmutación por error**

   Prepare el sistema de archivos en ambos nodos del clúster. La preparación incluye la creación de volúmenes lógicos LVM y la configuración de directorios como puntos de montaje.

2. **Configuración de un sistema de archivos de clúster replicado**

   Instale las utilidades de DRBD y configure los recursos de DRBD para la replicación de datos entre los nodos del clúster de conmutación por error. Después de eso, cree un sistema de archivos replicado en el nodo del clúster activo.

3. **Instalación y configuración de Corosync y Pacemaker en los nodos del clúster de conmutación por error**

   Instale Corosync y Pacemaker para proporcionar comunicación de clúster y administración de recursos para alta disponibilidad.

4. **Instalación y configuración del DBMS de Platform V Pangolin**

   Instale y configure Platform V Pangolin en los nodos del clúster.

5. **Instalación de Kaspersky Security Center Linux en los nodos del clúster de conmutación por error**

   Instale Kaspersky Security Center Linux en los nodos del clúster y luego configure el cifrado entre los nodos del clúster.

6. **Instalación de Kaspersky Security Center Web Console en los nodos del clúster de conmutación por error**

   Instale Kaspersky Security Center Web Console en ambos nodos del clúster de conmutación por error para brindar alta disponibilidad.

Preparación de un sistema de archivos de nodos de clúster

Como primer paso en la preparación para el despliegue del clúster de conmutación por error de Kaspersky Security Center Linux distribuido geográficamente, debe configurar el sistema de archivos en ambos nodos del clúster. La preparación incluye la creación de volúmenes lógicos LVM y la configuración de directorios como puntos de montaje. Realice el siguiente procedimiento en ambos nodos del clúster.

Para preparar un sistema de archivos de nodos de clúster:

1. Cree un volumen lógico LVM para los datos y la base de datos del Servidor de administración:

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

Cree un volumen lógico LVM separado para almacenar el archivo de respuesta:

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

donde:

- `volume group name` es el nombre del grupo de volúmenes utilizado por LVM.
- `klfocdata` y `klfocstate` son nombres de volumen lógicos. Estos volúmenes lógicos se crean dentro del grupo de volúmenes

  Recomendamos usar estos nombres de volumen para mantener la coherencia, aunque puede especificar nombres personalizados si es necesario.
- `volume size` un tamaño del volumen. Recomendamos asignar al menos 500 GB para los datos y la base de datos del Servidor de administración. El volumen para almacenar el archivo de respuesta requiere una pequeña cantidad de espacio.

2. Cree directorios que se utilizarán como puntos de montaje para los volúmenes lógicos.

   - Para los datos y la base de datos del Servidor de administración:

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

   - Para el archivo de respuesta:

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

   Recomendamos utilizar los directorios `/mnt/KlFocDataShare_klfoc` y `/mnt/KlFocStateShare_klfoc` para mantener la coherencia, aunque puede especificar nombres personalizados si es necesario.

Se prepara el sistema de archivos de los nodos del clúster. Después de eso, debe configurar un sistema de archivos de clúster replicado.

Configuración de un sistema de archivos de clúster replicado

Instalación y configuración de DRBD

DRBD es un software de terceros que se utiliza para la replicación de datos (específicamente para los volúmenes de datos y los puntos de montaje preparados en el paso anterior).

Después de preparar el sistema de archivos de los nodos del clúster, debe instalar las utilidades de DRBD y configurar los recursos de DRBD para la replicación de datos entre los nodos del clúster. Realice el siguiente procedimiento en ambos nodos del clúster.

Para instalar y configurar DRBD en los nodos del clúster:

1. Instale las utilidades de DRBD de la siguiente manera:

   a. Habilite los repositorios EPEL y ELRepo en ambos nodos:

   ```
   dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
   dnf install https://www.elrepo.org/elrepo-release-9.el9.elrepo.noarch.rpm
   ```

b. Genere todas las versiones disponibles del paquete kmod-drbd9x y filtre la lista de paquetes creada para la plataforma el9_6 (por ejemplo, se usa Platform V SberLinux OS Server [SLO] 9.6):

```
dnf search --showduplicates kmod-drbd9x | grep el9_6
```

c. Instale la última versión disponible de la lista en ambos nodos. Ejemplo para Platform V SberLinux OS Server (SLO) 9.6:

```
dnf install kmod-drbd9x-9.2.14-1.el9_6.elrepo.x86_64
dnf install drbd drbd-utils drbd-udev drbd-pacemaker drbd-selinux
modprobe drbd
```

Si una versión más reciente aparece en el futuro, reemplace la cadena de la versión en consecuencia.

Recomendamos usar DRBD versión 9.2.6 o posterior, ya que proporciona cifrado de tráfico integrado.

El tráfico DRBD también se puede cifrar mediante su propia solución VPN.

2. Cree archivos de configuración de recursos DRBD para cada volumen lógico creado durante la preparación del sistema de archivos (`klfocdata` y `klfocstate`).

   Todos los archivos de configuración deben colocarse en `/etc/drbd.d/`.

   - Recurso `klfocdata` (Datos y base de datos del Servidor de administración)

     Utilice la replicación asincrónica (protocolo A) para el recurso klfocdata. Configure todos los demás parámetros de acuerdo con su entorno.

     Ejemplo de archivo de configuración:

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

   - Recurso `klfocstate` (el archivo de respuesta)

     Utilice la replicación sincrónica (protocolo C) para crear el recurso klfocstate. Configure todos los demás parámetros de acuerdo con su entorno.

     Ejemplo de archivo de configuración:

```
resource klfocstate {
    protocol C;
    net {
```

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

3. Inicialice los metadatos de DRBD para ambos recursos:

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

4. Inicie DRBD en todos los recursos configurados:

```
drbdadm up all
```

DRBD se instala y configura en ambos nodos del clúster.

Crear un sistema de archivos replicado en el nodo del clúster activo

Después de instalar y configurar DRBD en ambos nodos del clúster, cree un sistema de archivos replicado en el nodo del clúster activo. Realice el siguiente procedimiento en el nodo del clúster activo.

Para crear un sistema de archivos replicado en el nodo del clúster activo:

1. Promueva ambos recursos de DRBD al rol principal:

```
drbdadm primary --force klfocdata
drbdadm primary --force klfocstate
```

2. Formatee los dispositivos DRBD para preparar los volúmenes replicados para su uso en los nodos del clúster:

```
mkfs.ext4 /dev/drbd0
mkfs.ext4 /dev/drbd2
```

3. Configure los parámetros del sistema de archivos:

```
tune2fs -m 0 /dev/drbd0
tune2fs -m 0 /dev/drbd2
```

4. Monte los dispositivos DRBD en los directorios creados anteriormente:

```
mount -o noatime /dev/drbd0 /mnt/KlFocDataShare_klfoc
mount -o noatime /dev/drbd2 /mnt/KlFocStateShare_klfoc
```

   Si el servicio multipathd está instalado, debe configurarse para ignorar los dispositivos `/dev/drbd*` en ambos nodos del clúster.

5. Verifique el estado de la replicación:

```
drbdadm status
```

   El resultado de la configuración correcta del sistema de archivos:

```
klfocdata role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate

klfocstate role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate
```

Se configura un sistema de archivos replicado en el nodo del clúster activo. Después de eso, debe instalar y configurar Corosync y Pacemaker en los nodos del clúster.

Instalación y configuración de Corosync y Pacemaker en los nodos del clúster

Corosync y Pacemaker proporcionan comunicación de clúster y administración de recursos para una alta disponibilidad. Garantizan que los servicios se muevan automáticamente a un nodo en buen estado en caso de que ocurra un error, lo que minimiza el tiempo de inactividad.

Para instalar y configurar Corosync y Pacemaker en los nodos del clúster:

1. En ambos nodos del clúster, instale los paquetes necesarios:

```
dnf install pcs
dnf install drbd-pacemaker
```

2. Configure Corosync y Pacemaker en ambos nodos del clúster de acuerdo con la documentación oficial. Esto incluye habilitar el inicio automático, generar y distribuir la clave de autenticación y configurar los permisos de acceso para el archivo de clave de autenticación.

   Para asegurarse de que la configuración sea correcta, ejecute el siguiente comando en uno de los nodos del clúster:

```
pcs status
```

   El resultado esperado debe mostrar el estado del clúster y enumerar todos los nodos activos, lo que confirma que Corosync es funcionando correctamente y los nodos se están comunicando.

3. En ambos nodos del clúster, configure los ajustes básicos del clúster de Pacemaker:

```
pcs property set stonith-enabled=false
pcs property set symmetric-cluster=false
pcs resource defaults resource-stickiness=110
pcs resource defaults migration-threshold=3
pcs property set no-quorum-policy=ignore
```

4. En ambos nodos del clúster, desactive el inicio de los scripts que Corosync administrará:

```
systemctl disable drbd.service
```

5. En uno de los nodos del clúster, cree los recursos basados en DRBD en Pacemaker.

- Recurso DRBD para klfocdata

  a. Cree un recurso de clúster para el volumen DRBD `klfocdata`, lo que permite al clúster administrar y supervisar su estado automáticamente:

  ```
  pcs resource create drbd_klfocdata ocf:linbit:drbd \
  drbd_resource="klfocdata" \
  op monitor interval=60s \
  op start interval=0 timeout=240s \
  op stop interval=0 timeout=240s \
  op monitor role=Master interval=10s \
  op monitor role=Slave interval=30s \
  ```

  b. Cree un recurso administrado por clúster `ms_drbd_klfocdata` basado en el recurso creado `drbd_klfocdata`:

  ```
  pcs resource clone drbd_klfocdata promotable=true
  master-max=1
  clone-max=2
  clone-node-max=1 notify=true
  ```

  c. Cree un punto de montaje para el volumen de DRBD `fs_klfocdata`, y especifique el dispositivo, directorio de destino, tipo de sistema de archivos y opciones de montaje:

  ```
  pcs resource create fs_klfocdata ocf:heartbeat:Filesystem \
  device="/dev/drbd0" \
  directory="/mnt/KlFocDataShare_klfoc" \
  fstype="ext4" \
  options="data=journal"
  ```

- Recurso DRBD para klfocstate

  a. Cree un recurso de clúster para el volumen DRBD `klfocstate`, lo que permite que el clúster administre y supervise su estado automáticamente:

  ```
  pcs resource create drbd_klfocstate ocf:linbit:drbd \
  drbd_resource=klfocstate \
  op monitor interval=60s \
  op start interval=0 timeout=240s \
  op stop interval=0 timeout=240s \
  op monitor role=Promoted interval=10s \
  op monitor role=Unpromoted interval=30s \
  ```

b. Cree un recurso administrado por clúster ms_drbd_klfocstate basado en el recurso creado `drbd_klfocstate`:

```
pcs resource clone drbd_klfocstate promotable=true \
master-max=1 \
clone-max=2 \
clone-node-max=1 \
notify=true
```

c. Cree un punto de montaje para el volumen DRBD `fs_klfocstate`, y especifique el dispositivo, el directorio de destino, el tipo de sistema de archivos y las opciones de montaje:

```
pcs resource create fs_klfocstate ocf:heartbeat:Filesystem \
device="/dev/drbd2" \
directory="/mnt/KlFocStateShare_klfoc" \
fstype="ext4" \
options="noatime"
```

6. En ambos nodos del clúster, deshabilite el inicio automático del servicio DRBD:

```
systemctl disable drbd.service
```

Corosync y Pacemaker se instalan y configuran en los nodos del clúster. Después de eso, debe instalar el DBMS y crear la base de datos del Servidor de administración y la base de datos de IAM.

Instalación y configuración del DBMS de Platform V Pangolin

Después de instalar y configurar Corosync y Pacemaker en los nodos del clúster, debe instalar el DBMS en ambos nodos del clúster.

Para instalar y configurar del DBMS:

1. En ambos nodos del clúster, instale Platform V Pangolin 6.5.1 x64 o posterior.

   Para obtener información acerca de cómo instalar Platform V Pangolin, consulte su documentación.

2. Asegúrese de que los nodos del clúster con el DBMS instalado no tengan cuentas de usuario de DBMS con los siguientes nombres:

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

3. En el nodo del clúster activo, copie el directorio DBMS al directorio `/mnt/KlFocDataShare_klfoc/dbms`:

```
sudo rsync -av  /pgdata/06/data/ /mnt/KlFocDataShare_klfoc/dbms
sudo mv /pgdata/06/data/ /pgdata/06/data.bk/
```

4. En ambos nodos del clúster, abra el archivo de configuración `/mnt/KlFocDataShare_klfoc/dbms/postgresql.conf` y luego establezca el directorio `/mnt/KlFocDataShare_klfoc/dbms` como el directorio de datos de la base de datos.

   También especifique las rutas a los archivos de configuración (`/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf` y `/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf`) y elimine el parámetro `include_dir`:

   ```
   data_directory = '/mnt/KlFocDataShare_klfoc/dbms'
   hba_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf'
   ident_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf'
   listen_addresses = '*'
   ```

5. En el archivo de configuración `/mnt/KlFocDataShare_klfoc/dbms/postgresql.conf`, ajuste la configuración del DBMS para cumplir con los requisitos de Kaspersky Security Center Linux.

6. Cree y configure cuentas para trabajar con PostgreSQL.

7. Cree el recurso del servicio del DBMS:

   ```
   pcs resource create klfocsvc_dbms pgsql \
   pgctl="/usr/pangolin-6.5/bin/pg_ctl"  psql="/usr/bin/psql" pgdata="/mnt/KlFocDataShare_klfoc/dbms"
   config="/mnt/KlFocDataShare_klfoc/dbms/postgresql.conf" socketdir="/tmp" \
   op start timeout=60s interval=0s \
   op stop timeout=60s interval=0s \
   op monitor interval=30s timeout=60s \
   op promote timeout=120s interval=0s \
   op demote timeout=120s interval=0s \
   meta target-role=Started
   ```

8. En ambos nodos del clúster, deshabilite el inicio automático del servicio DBMS:

   ```
   sudo systemctl disable pangolin.service
   ```

9. Agregue el recurso DBMS `klfocsvc_dbms` al grupo de clústeres `group_klfoc`:

   ```
   pcs resource group add group_klfoc klfocsvc_dbms
   ```

10. Agregue el nombre del recurso DBMS `klfocsvc_dbms` al final de la lista, por ejemplo:

    ```
    group group_klfoc {
    ...
    klfocsvc_dbms
    }
    ```

11. En el nodo del clúster activo, en el servidor DBMS, cree una base de datos para IAM. El nombre de la base de datos debe ser diferente al de la base de datos que instaló para trabajar con Kaspersky Security Center Linux. El Servidor de administración no elimina la base de datos de IAM automáticamente cuando se desinstala o mueve el servidor a otro dispositivo; debe eliminarla de forma manual:

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

Se instala y configura el DBMS. Se crean la base de datos del Servidor de administración y la base de datos de IAM. Después de eso, debe instalar Kaspersky Security Center Linux en los nodos del clúster.

Instalación de Kaspersky Security Center Linux en los nodos del clúster de conmutación por error distribuidos geográficamente

Kaspersky Security Center Linux se instala en los nodos del clúster de conmutación por error distribuidos geográficamente mediante un archivo de respuesta en modo silencioso, es decir, sin la participación del usuario. El archivo de respuesta contiene un conjunto personalizado de parámetros de instalación: variables y sus respectivos valores.

Requisitos previos:

- Realice todos los pasos preparatorios:
  - Preparación de un sistema de archivos de nodos de clúster
  - Configuración de un sistema de archivos de clúster replicado
  - Instalación y configuración de Corosync y Pacemaker en los nodos del clúster
  - Instalación y configuración del DBMS de Platform V Pangolin
- Asegúrese de que los nodos del clúster ejecuten Platform V SberLinux OS Server (SLO) 9.5.1 x64.
- Descargue el archivo de instalación `ksc64_[version_number]_amd64.deb` del sitio web de Kaspersky.

Instalación en el nodo activo

Para instalar Kaspersky Security Center Linux en el nodo activo en modo silencioso:

1. Lea el Contrato de licencia de usuario final. Siga los pasos a continuación únicamente si comprende y acepta los términos del Contrato de licencia de usuario final.
2. Cree un grupo `kladmins` y las cuentas sin privilegios `ksc` y `ksciam` que deben ser miembros del grupo `kladmins`. Para hacerlo, ejecute secuencialmente los siguientes comandos en una cuenta con privilegios raíz:

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

3. En el directorio `/mnt/KlFocDataShare_klfoc/`, cree un directorio para los archivos de Kaspersky Security Center Linux:

   ```
   mkdir /mnt/KlFocDataShare_klfoc/ksc/
   ```

4. Cree el archivo de respuesta (en formato TXT) y agregue una lista de variables en el formato VARIABLE_NAME=variable_value al archivo de respuesta. Agregue cada variable en una línea separada.

En la lista de parámetros utilizados para la instalación de Kaspersky Security Center Linux en modo silencioso, especifique los siguientes parámetros necesarios para la implementación del clúster distribuido geográficamente:

- `KLFOC_UNATT_EXT_RESOURCE_MANAGEMENT=2`

  Establezca el valor `2` para desplegar el clúster distribuido geográficamente.

- `KLSRV_UNATT_SERVERADDRESS=<DNS balancer address>` y `KLSRV_UNATT_IAM_ADDRESS=<DNS balancer address>`

  El equilibrador de DNS con verificación de estado ya debe estar desplegado. Los valores de estos parámetros deben ser idénticos y configurarse con el FQDN del equilibrador de DNS.

5. Establezca el valor de la variable de entorno `KLAUTOANSWERS` en el entorno raíz que contiene el nombre completo del archivo de respuesta, incluida la ruta; por ejemplo, con el siguiente comando:

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

6. Inicie la instalación de Kaspersky Security Center Linux en modo silencioso ejecutando los siguientes comandos:

   - En el entorno raíz:

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

   - En el entorno del usuario:

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

7. Deshabilite el inicio automático del servicio klfocsvc_klfoc.service:

```
systemctl disable klfocsvc_klfoc.service
```

8. Después de instalar Kaspersky Security Center Linux, detenga el nodo del clúster activo.

9. Mueva todos los recursos del clúster al nodo pasivo.

   Puede usar el comando `pcs node standby` (y recuperarlo con `pcs node online`).

Instalación en el nodo pasivo

Para instalar Kaspersky Security Center Linux en el nodo pasivo:

1. Ejecute la instalación de Kaspersky Security Center Linux:

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

2. Realice la configuración de Kaspersky Security Center Linux:

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

3. Leer el Contrato de licencia de usuario final (EULA) y la Política de privacidad. El texto se muestra en la ventana de la línea de comandos. Presione la barra espaciadora para ver el siguiente segmento de texto. Luego, cuando se le solicite, ingrese los siguientes valores:

   - Ingrese `y` si comprende y acepta los términos del EULA. Ingrese `n` si no acepta los términos del EULA. Para utilizar Kaspersky Security Center Linux, debe aceptar los términos del EULA.

   - Ingrese `y` si comprende y acepta los términos de la Política de privacidad, y si acepta que sus datos se manejen y transmitan (incluso a terceros países) como se describe en la Política de privacidad. Ingrese n si no acepta los términos de la Política de privacidad. Para utilizar Kaspersky Security Center Linux, debe aceptar los términos de la Política de privacidad.

4. Seleccione el nodo de clúster pasivo como modo de instalación del Servidor de administración.

5. Cuando se le solicite, ingrese la ruta local al punto de montaje del recurso compartido de estado: `/mnt/KlFocStateShare_klfoc`.

6. Deshabilite el inicio automático del servicio klfocsvc_klfoc.service:

```
systemctl disable klfocsvc_klfoc.service
```

7. Cree el recurso del servicio `klfocsvc_klfoc`:

```
crm configure primitive klfocsvc_klfoc systemd:klfocsvc_klfoc \
op start timeout="900s" interval="0" \
op stop timeout="900s" interval="0" \
op monitor interval="30s" timeout="90s"
```

8. Agregue el recurso `klfocsvc_klfoc` al grupo `group_klfoc`:

```
pcs resource group add group_klfoc klfocsvc_klfoc
```

9. Agregue `klfocsvc_klfoc` al final de la línea del grupo, por ejemplo:

```
group group_klfoc {
...
klfocsvc_klfoc
}
```

10. Verifique que todos los recursos estén en el estado iniciado en el nodo activo.

```
pcs status
```

Configuración del cifrado entre los nodos del clúster

Para configurar el cifrado entre los nodos del clúster:

Si instaló la versión 9.2.6 o posterior de DRBD durante la configuración de un sistema de archivos del clúster replicado, configure el cifrado entre los nodos del clúster de acuerdo con la documentación oficial de DRBD.

Como alternativa, puede cifrar el tráfico entre los nodos del clúster mediante su propia solución VPN.

Se instala el clúster de conmutación por error de Kaspersky Security Center Linux distribuido geográficamente. Después de eso, debe instalar Kaspersky Security Center Web Console en ambos nodos del clúster.

Instalación de Kaspersky Security Center Web Console en nodos de clúster de conmutación por error distribuidos geográficamente

Para el despliegue de un clúster de conmutación por error de Kaspersky Security Center Linux distribuido geográficamente, se debe admitir la alta disponibilidad de Kaspersky Security Center Web Console. Para lograrlo, Kaspersky Security Center Web Console debe estar instalado en ambos nodos del clúster.

Para instalar Kaspersky Security Center Web Console:

1. En ambos nodos, cree un usuario para trabajar con Kaspersky Security Center Web Console. Para hacerlo, ejecute el siguiente comando bajo una cuenta con privilegios raíz:

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

   donde la contraseña debe contener al menos 8 caracteres.

2. En ambos nodos, lea el Contrato de licencia de usuario final (EULA). Si el kit de distribución de Kaspersky Security Center Linux no contiene un archivo TXT con el texto del EULA, puede descargar dicho archivo del sitio web de Kaspersky. Si no acepta los términos del Contrato de licencia, no instale la aplicación.

3. En ambos nodos, cree un archivo de respuesta que contenga parámetros para conectar Kaspersky Security Center Web Console al Servidor de administración: `/etc/ksc-web-console-setup.json`.

   Ejemplo de un archivo de respuesta que contiene el conjunto mínimo de parámetros

   El conjunto de parámetros del archivo de respuesta depende de la versión del Servidor de administración al que se conecta Kaspersky Security Center Web Console:

   - Versión 16 o posterior del Servidor de administración

     Ejemplo de un archivo de respuesta con el conjunto mínimo de parámetros para iniciar sesión en la versión 16 o posteriores del Servidor de administración:

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

- Versión 15.4 o posterior del Servidor de administración

  Ejemplo de un archivo de respuesta con el conjunto mínimo de parámetros para iniciar sesión en la versión 15.4 o anteriores del Servidor de administración:

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

Puede instalar Kaspersky Security Center Web Console en el mismo dispositivo donde está el Servidor de administración o en otro dispositivo. Si Kaspersky Security Center Web Console está instalado en otro dispositivo, la dirección de Kaspersky Security Center Web Console (especificada por `address`) y la dirección del Servidor de administración (especificada por `iamHost` o `kscHost`) son diferentes. Si Kaspersky Security Center Web Console está instalado en el mismo dispositivo que el Servidor de administración, estos parámetros tienen los mismos valores.

El valor `iamHost` debe coincidir con la dirección de IAM que especificó durante la instalación del Servidor de administración. Para obtener la dirección de IAM especificada, ejecute el siguiente comando en el dispositivo que tiene el Servidor de administración instalado:

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

Para obtener información detallada, consulte el artículo: Parámetros de instalación de Kaspersky Security Center Web Console.

Puede agregar varios Servidores de administración de diferentes versiones a la lista de servidores de confianza. En este caso, los servidores pueden utilizar diferentes métodos de autenticación.

Recomendamos que especifique números de puerto superiores a 1024. Si desea que Kaspersky Security Center Web Console funcione en puertos inferiores al 1024, después de la instalación debe asegurarse de tener la utilidad setcap y luego ejecutar el siguiente comando:

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

Si no tiene la utilidad setcap, puede instalarla. **Haga clic en este vínculo para ver los comandos.**

Para los sistemas operativos Debian y Ubuntu, ejecute uno de los siguientes comandos:

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

Para SUSE Linux Enterprise Server y Red Hat Enterprise Linux, ejecute el comando:

- `sudo zypper install libcap-progs`

4. En ambos nodos, ejecute el archivo de configuración con una cuenta con privilegios de cuenta root.

```
sudo apt-get install ksc-web-console-<build number>.x86_64.deb
```

Se iniciará el proceso para desempaquetar el archivo de instalación. Espere a que se complete la instalación. Kaspersky Security Center Web Console se instala en el siguiente directorio: `/var/opt/kaspersky/ksc-web-console`.

5. En uno de los nodos del clúster, cree un recurso de Pacemaker para el servicio KSCWebConsole para que KSCWebConsole sea un servicio administrado por Pacemaker:

```
crm configure primitive ksc_webconsole systemd:KSCWebConsole \
op monitor interval=30s timeout=60s \
op start timeout=120s \
op stop timeout=120s \
meta target-role=Stopped
```

6. En ambos nodos, detenga el servicio KSCWebConsole y deshabilite su inicio automático:

```
sudo systemctl stop KSCWebConsole
sudo systemctl disable KSCWebConsole
```

7. En uno de los nodos del clúster, agregue el recurso `ksc_webconsole` al grupo `group_klfoc`:

```
crm configure edit group_klfoc
```

8. Agregue `ksc_webconsole` al final de la línea de grupo, después de `klfocsvc_dbms`, por ejemplo:

```
group group_klfoc {
...
klfocsvc_dbms
ksc_webconsole
}
```

Cuando finalice la instalación, podrá usar un navegador para abrir Kaspersky Security Center Web Console e iniciar sesión.

Cuentas para trabajar con el DBMS

Para instalar y administrar el Servidor de administración e IAM, necesita cuentas internas de la base de datos. Estas cuentas le permiten acceder a la base de datos y requieren ciertos derechos.

El conjunto de derechos necesarios depende de los siguientes criterios:

- Tipo de DBMS:
  - MySQL o MariaDB
  - Basado en PostgreSQL

- Método de creación de la base de datos del Servidor de administración:
  - **Automático**. Durante la instalación del Servidor de administración, puede permitir que el programa de instalación del Servidor de administración (el instalador) cree automáticamente la base de datos del Servidor de administración (en adelante, también denominada la "base de datos del Servidor").
  - **Manual**. Puede crear una base de datos vacía utilizando un script o una aplicación de un tercero. Luego, durante la instalación del Servidor de administración, puede usar esa base de datos vacía como base de datos para el Servidor de administración.

La base de datos de IAM debe crearse manualmente, independientemente de cómo haya elegido crear la base de datos del Servidor de administración.

A la hora de asignar derechos y permisos a las cuentas, limítese a lo justo y necesario. Dicho de otro modo, no asigne más derechos que los que se necesiten para llevar a cabo las acciones necesarias. No utilice cuentas de superusuario estándar de su DBMS, como 'root' o 'postgres', como usuario de conexión al DBMS para Kaspersky Security Center Linux.

No realice ningún cambio manual en la base de datos del Servidor de administración y la base de datos de IAM, incluida la modificación de valores, la eliminación o la adición de esquemas, tablas e índices. Cualquier cambio en las bases de datos no realizado por el propio Servidor de administración interrumpe el funcionamiento correcto del Servidor de administración, ya sea inmediatamente o más tarde, por ejemplo, después de la actualización a la versión más reciente o durante la restauración a partir de una copia de seguridad, etc. La edición de bases de datos solo está permitida cuando haya recibido instrucciones explícitas del Servicio de soporte técnico de Kaspersky.
Al desinstalar o migrar el Servidor a otro dispositivo, debe eliminar manualmente las bases de datos del Servidor de administración y de IAM.

La siguiente información describe los derechos del DBMS que debe otorgar a las cuentas antes de instalar e iniciar el Servidor de administración.

MySQL y MariaDB

Si elige MySQL o MariaDB como DBMS, cree una cuenta interna en el DBMS que le permita acceder al DBMS. Luego, otorgue a esa cuenta los derechos necesarios. Tenga presente que el conjunto de derechos es siempre el mismo, independientemente del método utilizado para crear la base de datos. Los derechos necesarios se enumeran a continuación:

- Privilegios de esquema:
  - Base de datos del Servidor de administración: ALL (excepto GRANT OPTION)
  - Esquemas del sistema (mysql y sys): SELECT, SHOW VIEW
  - Procedimiento almacenado "sys.table_exists": EXECUTE (si su DBMS es MariaDB versión 10.5 o anterior, no necesita otorgar el privilegio EXECUTE)
- Privilegios globales para todos los esquemas: PROCESS, SUPER.

Para obtener más información sobre cómo configurar los derechos de las cuentas, consulte el artículo Creación de bases de datos y cuentas de usuario de MySQL y MariaDB.

Para obtener detalles sobre cómo mover datos de un espacio de tabla compartido a un espacio de tabla por archivo, consulte Mover datos de un espacio de tabla compartido a un espacio de tabla por archivo en los DBMS MySQL y MariaDB.

Configuración de privilegios para recuperar los datos del Servidor de administración

Los derechos asignados a la cuenta interna del DBMS bastan para restaurar los datos del Servidor de administración utilizando una copia de seguridad.

DBMS basado en PostgreSQL

En la siguiente tabla, se detallan los derechos que deberá asignar a este rol según el método elegido para crear la base de datos del Servidor. Para obtener más información sobre cómo configurar los derechos de los roles, consulte el artículo Creación de bases de datos y cuentas de usuario de MySQL y MariaDB.

Derechos del rol de Postgres

Base de datos creada automáticamente		Base de datos creada manualmente
Si utiliza el usuario *Postgres*, no necesita asignar privilegios adicionales.	Si crea un nuevo rol: privilegio CREATEDB.	Si crea un nuevo rol: • Privilegios para la base de datos del Servidor de administración: ALL. • Privilegios para todas las tablas del esquema public: ALL. • Privilegios para todas las secuencias del esquema public: ALL.

Configuración de privilegios para recuperar los datos del Servidor de administración

Para restaurar los datos del Servidor de administración desde la copia de seguridad, el rol de Postgres utilizado para acceder al DBMS debe tener derechos de propietario de la base de datos del Servidor de administración.

Mientras restaura los datos de una copia de seguridad, otorgue temporalmente privilegios de superusuario de Postgres a las cuentas estándar klserver y kliam que el Servidor de administración e IAM utilizan para conectarse al DBMS (en el ejemplo, `klserver` y `kliam`, respectivamente):

```
sudo -i -u postgres psql -c "ALTER ROLE klserver WITH SUPERUSER;"
```

```
sudo -i -u postgres psql -c "ALTER ROLE kliam WITH SUPERUSER;"
```

Después de recuperar correctamente los datos, restaure los derechos originales de las cuentas de usuario de Postgres.

```
sudo -i -u postgres psql -c "ALTER ROLE klserver WITH NOSUPERUSER;"
```

```
sudo -i -u postgres psql -c "ALTER ROLE kliam WITH NOSUPERUSER;"
```

Creación de bases de datos y cuentas de usuario de MySQL y MariaDB

Requisitos previos

Antes de crear bases de datos y asignar permisos a las cuentas de usuario del DBMS, instale y configure uno de los servidores conforme a los requisitos de optimización (si aún no lo ha hecho):

- MariaDB x64 para trabajar con Kaspersky Security Center Linux
- MySQL x64 para trabajar con Kaspersky Security Center Linux

No realice ningún cambio manual en la base de datos del Servidor de administración y la base de datos de IAM, incluida la modificación de valores, la eliminación o la adición de esquemas, tablas e índices. Cualquier cambio en las bases de datos no realizado por el propio Servidor de administración interrumpe el funcionamiento correcto del Servidor de administración, ya sea inmediatamente o más tarde, por ejemplo, después de la actualización a la versión más reciente o durante la restauración a partir de una copia de seguridad, etc. La edición de bases de datos solo está permitida cuando haya recibido instrucciones explícitas del Servicio de soporte técnico de Kaspersky.
Al desinstalar o migrar el Servidor a otro dispositivo, debe eliminar manualmente la base de datos.

Para configurar la cuenta del DBMS para la instalación del Servidor de administración:

1. Utilizando la cuenta root que creó al instalar el DBMS, ejecute un entorno para trabajar con MySQL o MariaDB:

   ```
   sudo mysql -u root -p
   ```

2. En el DBMS, cree cuentas de usuario internas con contraseñas. Los instaladores del Servidor de administración y de los servicios del Servidor de administración utilizan esta cuenta de usuario interna del DBMS para acceder a la base de datos.

   Cree una cuenta de usuario del Servidor de administración llamada `kscdbadmin` y especifique la contraseña en `<password>`:

   ```
   CREATE USER 'kscdbadmin' IDENTIFIED BY '< contraseña >';
   ```

3. Otorgue los siguientes privilegios a la nueva cuenta del DBMS:

   - Privilegios de esquema:
     - Base de datos del Servidor de administración: ALL (excepto GRANT OPTION)
     - Esquemas del sistema (mysql y sys): SELECT, SHOW VIEW
     - Procedimiento almacenado sys.table_exists: EXECUTE
   - Privilegios globales para todos los esquemas: PROCESS, SUPER.

   Para otorgar los privilegios necesarios a la cuenta creada en el DBMS, ejecute el siguiente script:

   ```
   GRANT USAGE ON *.* TO 'kscdbadmin';
   GRANT ALL ON kav.* TO 'kscdbadmin';
   ```

```
GRANT SELECT, SHOW VIEW ON mysql.* TO 'kscdbadmin';
GRANT SELECT, SHOW VIEW ON sys.* TO 'kscdbadmin';
GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'kscdbadmin';
GRANT PROCESS ON *.* TO 'kscdbadmin';
GRANT SUPER ON *.* TO 'kscdbadmin';
```

Si su DBMS es MariaDB versión 10.5 o anterior, no necesita otorgar el privilegio EXECUTE. En este caso, excluya el siguiente comando del script:

```
GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'kscdbadmin'.
```

4. Para ver la lista de privilegios otorgados a la cuenta del DBMS, ejecute el siguiente comando:

   ```
   SHOW grants for 'kscdbadmin';
   ```

5. Cree una cuenta del servidor IAM denominada `iamdbadmin` y especifique la contraseña en `<password>`:

   ```
   CREATE USER 'iamdbadmin' IDENTIFIED BY '<password>';
   ```

   Si su DBMS es MySQL 8.0 o una versión anterior, tenga en cuenta que su versión no es compatible con la autenticación SHA2 con caché. Cambie la autenticación predeterminada de "Almacenamiento en caché de la contraseña SHA2" a "Contraseña nativa de MySQL".

   - Para crear en el DBMS una cuenta que utilice la autenticación nativa con contraseña de MySQL, ejecute el siguiente comando:

     ```
     CREATE USER 'iamdbadmin'@'%' IDENTIFIED WITH mysql_native_password BY
     '< contraseña >';
     ```

   - Para cambiar el tipo de autenticación de una cuenta existente en el DBMS, ejecute el siguiente comando:

     ```
     ALTER USER 'iamdbadmin'@'%' IDENTIFIED WITH mysql_native_password BY
     '< contraseña >';
     ```

6. Otorgue los siguientes privilegios a la nueva cuenta del DBMS:

   - Privilegios de esquema:
     - Base de datos del Servidor de administración: ALL (excepto GRANT OPTION)
     - Esquemas del sistema (mysql y sys): SELECT, SHOW VIEW
     - Procedimiento almacenado sys.table_exists: EXECUTE
   - Privilegios globales para todos los esquemas: PROCESS, SUPER.

   Para otorgar los privilegios necesarios a la cuenta creada en el DBMS, ejecute el siguiente script:

   ```
   GRANT USAGE ON *.* TO 'iamdbadmin';
   GRANT ALL ON iam.* TO 'iamdbadmin';
   GRANT SELECT, SHOW VIEW ON mysql.* TO 'iamdbadmin';
   GRANT SELECT, SHOW VIEW ON sys.* TO 'iamdbadmin';
   GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'iamdbadmin';
   GRANT PROCESS ON *.* TO 'iamdbadmin';
   GRANT SUPER ON *.* TO 'iamdbadmin';
   ```

   Si su DBMS es MariaDB versión 10.5 o anterior, no necesita otorgar el privilegio EXECUTE. En este caso, excluya el siguiente comando del script: `GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'iamdbadmin'`.

7. Para ver la lista de privilegios otorgados a la cuenta del DBMS, ejecute el siguiente comando:

   ```
   SHOW grants for 'iamdbadmin';
   ```

8. Cree una base de datos del Servidor de administración (en este ejemplo, llamada *kav*) ejecutando el siguiente comando:

   ```
   CREATE DATABASE kav
   ```

   Use el mismo nombre de base de datos que especificó en el paso de creación de la cuenta de usuario del DBMS.

9. Cree una base de datos de IAM (en este ejemplo, el nombre de la base de datos de IAM es *iam*):

   ```
   CREATE DATABASE iam
   ```

Ejemplo de los comandos básicos de las instrucciones

```
administrator@ksclinux:~$ sudo mysql -u root -p

Enter password:

Welcome to the MySQL monitor&period; Commands end with ; or \g.

Your MySQL connection id is 8

Server version: 8.4.11-0ubuntu0.26.04.1 (Ubuntu)

Copyright (c) 2000, 2026, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its

affiliates&period; Other names may be trademarks of their respective

owners.

Type 'help;' or '\h' for help&period; Type '\c' to clear the current input statement.

mysql> CREATE USER 'kscdbadmin' IDENTIFIED BY 'Your_P@$$w0rd';

Query OK, 0 rows affected (0.02 sec)

mysql> GRANT USAGE ON *.* TO 'kscdbadmin';

ON mysql.* TO 'kscdbadmin';

GRANT SELECT, SHOW VIEW ON sys.* TO 'kscdbadmin';

GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'kscdbadmin';

GRANT PROCESS ON *.* TO 'kscdbadmin';

GRANT SUPER ON *.* TO 'kscdbadmQuery OK, 0 rows affected (0.00 sec)

mysql> GRANT ALL ON kav.* TO 'kscdbadmin';

Query OK, 0 rows affected (0.01 sec)
```

```
mysql> GRANT SELECT, SHOW VIEW ON mysql.* TO 'kscdbadmin';

Query OK, 0 rows affected (0.00 sec)

mysql> GRANT SELECT, SHOW VIEW ON sys.* TO 'kscdbadmin';

Query OK, 0 rows affected (0.01 sec)

mysql> GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'kscdbadmin';

in';

Query OK, 0 rows affected (0.00 sec)

mysql> GRANT PROCESS ON *.* TO 'kscdbadmin';

Query OK, 0 rows affected (0.01 sec)

mysql> GRANT SUPER ON *.* TO 'kscdbadmin';

Query OK, 0 rows affected, 1 warning (0.00 sec)

mysql> SHOW grants for 'kscdbadmin';

+-----------------------------------------------------------------------+

| Grants for kscdbadmin@% |

+-----------------------------------------------------------------------+

| GRANT PROCESS, SUPER ON *.* TO `kscdbadmin`@`%` |

| GRANT ALL PRIVILEGES ON `kav`.* TO `kscdbadmin`@`%` |

| GRANT SELECT, SHOW VIEW ON `mysql`.* TO `kscdbadmin`@`%` |

| GRANT SELECT, SHOW VIEW ON `sys`.* TO `kscdbadmin`@`%` |

| GRANT EXECUTE ON PROCEDURE `sys`.`table_exists` TO `kscdbadmin`@`%` |

+-----------------------------------------------------------------------+

5 rows in set (0.00 sec)

mysql> CREATE USER 'iamdbadmin' IDENTIFIED BY 'Your_P@$$w0rd';

Query OK, 0 rows affected (0.02 sec)

mysql> GRANT USAGE ON *.* TO 'iamdbadmin';

'iamdbadmin';

GRANT SELECT, SHOW VIEW ON sys.* TO 'iamdbadmin';
```

```
GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'iamdbadmin';

GRANT PROCESS ON *.* TO 'iamdbadmin';

GRANT SUPER ON *.* TO 'iamdbaQuery OK, 0 rows affected (0.01 sec)

mysql> GRANT ALL ON iam.* TO 'iamdbadmin';

Query OK, 0 rows affected (0.01 sec)

mysql> GRANT SELECT, SHOW VIEW ON mysql.* TO 'iamdbadmin';

dmin';

Query OK, 0 rows affected (0.01 sec)

mysql> GRANT SELECT, SHOW VIEW ON sys.* TO 'iamdbadmin';

Query OK, 0 rows affected (0.02 sec)

mysql> GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'iamdbadmin';

Query OK, 0 rows affected (0.01 sec)

mysql> GRANT PROCESS ON *.* TO 'iamdbadmin';

Query OK, 0 rows affected (0.00 sec)

mysql> GRANT SUPER ON *.* TO 'iamdbadmin';

Query OK, 0 rows affected, 1 warning (0.00 sec)

mysql> SHOW grants for 'iamdbadmin';

+-------------------------------------------------------------------+

| Grants for iamdbadmin@% |

+-------------------------------------------------------------------+

| GRANT PROCESS, SUPER ON *.* TO `iamdbadmin`@`%` |

| GRANT ALL PRIVILEGES ON `iam`.* TO `iamdbadmin`@`%` |

| GRANT SELECT, SHOW VIEW ON `mysql`.* TO `iamdbadmin`@`%` |

| GRANT SELECT, SHOW VIEW ON `sys`.* TO `iamdbadmin`@`%` |

| GRANT EXECUTE ON PROCEDURE `sys`.`table_exists` TO `iamdbadmin`@`%` |

+-------------------------------------------------------------------+

5 rows in set (0.00 sec)
```

```
mysql> CREATE DATABASE kav;

Query OK, 1 row affected (0.01 sec)

mysql> CREATE DATABASE iam;

Query OK, 1 row affected (0.01 sec)

mysql> exit

Bye

administrator@ksclinux:~$
```

Creación de bases de datos basadas en PostgreSQL y cuentas de usuario

Antes de otorgar permisos a la cuenta del DBMS, asegúrese de que el servidor del DBMS PostgreSQL esté configurado para funcionar con Kaspersky Security Center Linux.

No realice ningún cambio manual en la base de datos del Servidor de administración y la base de datos de IAM, incluida la modificación de valores, la eliminación o la adición de esquemas, tablas e índices. Cualquier cambio en las bases de datos no realizado por el propio Servidor de administración interrumpe el funcionamiento correcto del Servidor de administración, ya sea inmediatamente o más tarde, por ejemplo, después de la actualización a la versión más reciente o durante la restauración a partir de una copia de seguridad, etc. La edición de bases de datos solo está permitida cuando haya recibido instrucciones explícitas del Servicio de soporte técnico de Kaspersky.
Al desinstalar o migrar el servidor a otro dispositivo, debe eliminar manualmente las bases de datos del Servidor de administración y de IAM.

Para crear bases de datos y configurar las cuentas de usuario del DBMS para instalar Kaspersky Security Center Linux:

1. Inicie el entorno de administración del DBMS:
   `sudo -i -u postgres psql`
2. Inicie sesión con el usuario *Postgres* en la base de datos *Postgres*.
3. Cree el rol de Postgres para administrar la base de datos del Servidor de administración (en este ejemplo, el rol `kscdbadmin`):
   `CREATE USER "kscdbadmin" WITH PASSWORD '<password>';`
4. Cree una base de datos del Servidor de administración (en este ejemplo, el nombre de la base de datos del Servidor de administración es `kav`):
   `CREATE DATABASE "kav" ENCODING 'UTF8' OWNER "kscdbadmin";`
   Recomendamos especificar el rol de Postgres creado en el paso 3 de estas instrucciones como propietario de la base de datos del Servidor de administración (en este ejemplo, el rol es `kscdbadmin` y la contraseña es `<password>`).
   Especificar a otro usuario como propietario de la base de datos
   Si necesita especificar otro rol de Postgres, conéctese a la base de datos del Servidor de administración con ese rol de propietario (o con el rol de superusuario) y ejecute los siguientes comandos:

```
GRANT ALL PRIVILEGES ON DATABASE "kav" TO "kscdbadmin";
GRANT USAGE ON SCHEMA public TO "kscdbadmin";
GRANT CREATE ON SCHEMA public TO "kscdbadmin";
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "kscdbadmin";
GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "kscdbadmin";
```

Asegúrese de que el rol de propietario de la base de datos del Servidor de administración tenga los privilegios CONNECT y TEMPORARY.

Si aparece el error "La nueva codificación (UTF8) es incompatible con la codificación de la base de datos de plantilla", cree una base de datos mediante el comando:
`CREATE DATABASE "kav" ENCODING 'UTF8' OWNER "kscdbadmin" TEMPLATE template0;`
en lugar de:
`CREATE DATABASE "kav" ENCODING 'UTF8' OWNER "kscdbadmin";`

5. Cree un rol de Postgres para administrar la base de datos de IAM (en este ejemplo, el rol de Postgres es `iamdbadmin`):

```
CREATE USER "iamdbadmin" WITH PASSWORD '<password>';
```

6. Cree una base de datos de IAM (en este ejemplo, el nombre de la base de datos de IAM es `iam`):

```
CREATE DATABASE "iam" ENCODING 'UTF8' OWNER "iamdbadmin";
```

El nombre de la base de datos de IAM debe ser diferente del nombre de la base de datos que instaló para administrar la base de datos del Servidor de administración.

Recomendamos especificar el rol de Postgres creado en el paso 5 de estas instrucciones como propietario de la base de datos de IAM (en este ejemplo, el rol es `iamdbadmin` y la contraseña es `<password>`).

Especificación de otro usuario como propietario de la base de datos de IAM

Si necesita especificar otro rol de Postgres, conéctese a la base de datos de IAM con ese rol (o con el rol de superusuario) y ejecute los siguientes comandos:

```
GRANT ALL PRIVILEGES ON DATABASE "iam" TO "iamdbadmin";
GRANT USAGE ON SCHEMA public TO "iamdbadmin";
GRANT CREATE ON SCHEMA public TO "iamdbadmin";
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "iamdbadmin";
GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "iamdbadmin";
```

Asegúrese de que el rol de propietario de la base de datos de IAM tenga los privilegios CONNECT y TEMPORARY.

Si aparece el error "La nueva codificación (UTF8) es incompatible con la codificación de la base de datos de plantilla", cree una base de datos mediante el comando:
`CREATE DATABASE "iam" ENCODING 'UTF8' OWNER "iamdbadmin" TEMPLATE template0;`
en lugar de:
`CREATE DATABASE "iam" ENCODING 'UTF8' OWNER "iamdbadmin";`

Ejemplo de los comandos básicos de las instrucciones

```
administrator@ksclinux:~$ sudo -i -u postgres psql
psql (18.4 (Ubuntu 18.4-0ubuntu.0.26.04.1))
Type "help" to help.
postgres=# CREATE USER kscdbadmin WITH PASSWORD 'password';
CREATE ROLE
postgres=# CREATE DATABASE "kav" ENCODING 'UTF8' OWNER "kscdbadmin";
CREATE DATABASE
postgres=# CREATE USER iamdbadmin WITH PASSWORD 'password';
CREATE ROLE
postgres=# CREATE DATABASE "iam" ENCODING 'UTF8' OWNER "iamdbadmin";
CREATE DATABASE
postgres=# exit
administrator@ksclinux:~$
```

Mover datos desde un espacio de tabla compartido a un espacio de tabla por archivo en un DBMS MySQL o MariaDB

Para un DBMS MySQL y MariaDB, puede almacenar datos de las siguientes maneras:

- Como espacio de tabla compartido, cuando los datos de todas las bases de datos de usuario se almacenan en un solo archivo (normalmente, en el archivo `ibdata1`).
- Como espacio de tabla de archivo por tabla, cuando para cada tabla se crea un espacio de datos separado como un archivo separado.

El uso de un espacio de tabla compartido aumenta el riesgo de fragmentación del espacio de tabla. Dado que no es posible realizar una operación `SHRINK`, un archivo en un espacio de tabla compartido puede ocupar aproximadamente el 90 % del espacio en disco. Esto afecta negativamente al rendimiento del subsistema de disco. Por lo tanto, es útil optar por un espacio de tabla de archivo por tabla.

En este artículo se describe cómo mover datos de un espacio de tabla compartido a un espacio de tabla de archivo por tabla. Si otras aplicaciones también utilizan el DBMS MySQL o MariaDB, debe mover las bases de datos de estas aplicaciones al espacio de tabla de archivo por tabla.

Recomendamos realizar este procedimiento solo si utiliza MySQL o MariaDB como DBMS para el Servidor de administración.
Mover datos de un espacio de tabla compartido a un espacio de tabla de archivo por tabla puede aumentar la carga del subsistema de disco.

Requisitos previos

Antes de comenzar, asegúrese de lo siguiente:

- Creó una copia de seguridad de los datos del Servidor de administración ejecutando una tarea de copia de seguridad de datos o la utilidad klbackup.
- Creó una copia de seguridad de otras aplicaciones cuyas bases de datos están administradas con DBMS MySQL o MariaDB (si corresponde).
- En el dispositivo con el DBMS instalado, en la partición con la base de datos, hay espacio libre en disco.

El espacio en disco requerido es el 150 % del tamaño total actual de las bases de datos (el tamaño actual del archivo `ibdata1`).

Proceso

Para mover datos de un espacio de tabla compartido a un espacio de tabla de archivo por tabla:

1. Detenga el servicio del Servidor de administración de Kaspersky Security Center y otras aplicaciones que utilicen la instancia del DBMS para la que desea realizar este procedimiento.

2. Dependiendo de la versión del DBMS, inicie sesión en su DBMS como superusuario y luego, en cualquier aplicación conveniente, ejecute el script `fix_tablespace.sql`.

   Puede ver los `fix_tablespace.sql` scripts haciendo clic en estos vínculos:

   Ver el script de MySQL 5.7 y MariaDB 10.1 o superiores

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;
    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';' );
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;
        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

   Ver el script para MySQL 8.0 o superiores

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;
    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';' );
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` TABLESPACE =
```

```
innodb_file_per_table;' );
        PREPARE stmt2 FROM @`strSQL`;
        EXECUTE stmt2;
        DEALLOCATE PREPARE stmt2;
        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

No debe detener la ejecución del script.
Si no se produjeron errores en el DBMS, pero finalizó la ejecución del script, vuelva a ejecutar el script o deje de realizar los pasos de este procedimiento, reinicie el servicio del DBMS y restaure los datos del Servidor de administración desde la copia de seguridad.

3. En la sección `[mysqld]` del archivo my.cnf, establezca el parámetro `innodb_file_per_table` en `1`.
4. Reinicie el servicio MySQL o MariaDB.
5. Inicie el servicio del Servidor de administración de Kaspersky Security Center.

Los datos se mueven de un espacio de tabla compartido a un espacio de tabla de archivo por tabla.

Certificados para trabajar con Kaspersky Security Center Linux

En esta sección, se brinda información sobre los certificados de Kaspersky Security Center Linux, se ofrecen instrucciones para emitir y reemplazar certificados para Kaspersky Security Center Web Console y se explica cómo renovar un certificado para el Servidor de administración si el Servidor interactúa con Kaspersky Security Center Web Console.

Acerca de los certificados de Kaspersky Security Center

Los siguientes tipos de certificados permiten que los componentes de Kaspersky Security Center interactúen en forma segura:

- Certificado del Servidor de administración
- Certificado para dispositivos móviles
- Certificado del Servidor web
- Certificado de Kaspersky Security Center Web Console
- Certificado de Identity and Access Manager

De forma predeterminada, Kaspersky Security Center utiliza certificados autofirmados (es decir, certificados emitidos por el propio Kaspersky Security Center). Si es necesario, puede reemplazar los certificados autofirmados por certificados de usuario de acuerdo con las normas de seguridad de su organización. Cuando usa un certificado personalizado, el archivo de certificado debe incluir la cadena completa de claves públicas, incluidos todos los certificados intermedios hasta la Autoridad de certificación (CA) raíz. Los certificados personalizados asumen el mismo alcance funcional que los autofirmados una vez que el Servidor de administración ha verificado que cumplen con todos los requisitos. La única diferencia es que el Servidor de administración vuelve a emitir automáticamente el certificado autofirmado, mientras que, en el caso de un certificado de usuario, debe volver a emitirlo manualmente después de que caduque. Puede reemplazar los certificados por certificados de usuario mediante la utilidad klsetsrvcert o en la sección de propiedades del Servidor de administración de Kaspersky Security Center Web Console, según el tipo de certificado. Si decide usar la utilidad klsetsrvcert, utilice uno de los siguientes valores para indicar el tipo de certificado:

- C (certificado común para los puertos 13000 y 13291)
- CR (certificado común de reserva para los puertos 13000 y 13291)
- M (certificado para dispositivos móviles, para el puerto 13292)
- MR (certificado de reserva para dispositivos móviles, para el puerto 13292)
- MCA (entidad de certificación móvil para certificados de usuario autogenerados)

El período máximo de validez para cualquiera de los certificados del Servidor de administración debe ser de 397 días o menos.

Certificados del Servidor de administración

Se requiere un certificado del Servidor de administración para los siguientes propósitos:

- Autenticación del Servidor de administración cuando Kaspersky Security Center Web Console se conecta a él.
- Interacción segura entre el Servidor de administración y el Agente de red en los dispositivos administrados
- Autenticación cuando los Servidores de administración principales están conectados a los Servidores de administración secundarios.

El certificado del Servidor de administración se crea automáticamente durante la instalación del componente Servidor de administración y se almacena en el directorio /var/opt/kaspersky/klnagent_srv/1093/cert/. Usted especifica el certificado del Servidor de administración cuando crea un archivo de respuesta para instalar Kaspersky Security Center Web Console. El certificado del Servidor de administración se denomina certificado común ("C"). Después de instalar Kaspersky Security Center Web Console, el certificado que especificó se copia al directorio /var/opt/kaspersky/ksc-web-console/certificates/external.

El certificado del Servidor de administración es válido por 397 días. Kaspersky Security Center crea automáticamente un certificado común de reserva ("CR") 90 días antes de que caduque el certificado común. El certificado común de reserva se instala luego, de manera transparente, como nuevo certificado del Servidor de administración. Cuando el certificado común está próximo a caducar, el certificado de reserva se utiliza para mantener la conexión con las copias del Agente de red instaladas en los dispositivos administrados. Para tal fin, el certificado común de reserva se convierte en el nuevo certificado común 24 horas antes de que caduque el original.

El período máximo de validez para cualquiera de los certificados del Servidor de administración debe ser de 397 días o menos.

De ser necesario, puede asignarle un certificado personalizado al Servidor de administración. Por ejemplo, esto puede ser necesario para una mejor integración con la PKI existente de su empresa o para la configuración personalizada de los campos del certificado. Al reemplazar el certificado, todos los Agentes de red que estaban conectados anteriormente al Servidor de administración a través de SSL pierden su conexión y devuelven "Error de autenticación del Servidor de administración". Para eliminar este error, deberá restaurar la conexión después de la sustitución del certificado.

Si el certificado del Servidor de administración se pierde, para recuperarlo, debe reinstalar el componente Servidor de administración y, luego, restaurar los datos.

También puede hacer una copia de seguridad del certificado del Servidor de administración por separado de los demás ajustes del Servidor de administración para trasladar el Servidor de administración de un dispositivo a otro sin tener que volver a conectar los Agentes de red.

Si abre Kaspersky Security Center Web Console en diferentes navegadores y descarga el archivo del certificado del Servidor de administración desde la ventana de propiedades del Servidor de administración, los archivos descargados tendrán nombres diferentes.

Certificados para dispositivos móviles

El certificado para dispositivos móviles ("M") permite autenticar el Servidor de administración en los dispositivos móviles. El certificado móvil se especifica en las propiedades del Servidor de administración.

También existe un certificado de reserva para dispositivos móviles ("MR"). Se lo utiliza para reemplazar, de manera simple, el certificado para dispositivos móviles. Kaspersky Security Center lo genera en forma automática 90 días antes de que caduque el certificado para dispositivos móviles. Cuando el certificado para dispositivos móviles está próximo a caducar, el certificado MR se utiliza para mantener la conexión con las instancias del Agente de red instaladas en los dispositivos administrados. Para tal fin, el certificado de reserva para dispositivos móviles se convierte en el nuevo certificado para dispositivos móviles 24 horas antes de que caduque el original.

Si el procedimiento de conexión requiere el uso de un certificado cliente en dispositivos móviles (conexión con autenticación SSL bidireccional), puede generar esos certificados mediante la autoridad de certificación para certificados de usuario generados automáticamente ("MCA"). Además, en las propiedades del Servidor de administración, puede especificar certificados cliente personalizados emitidos por una autoridad de certificación, mientras que la integración con la Infraestructura de clave pública (PKI) del dominio de su organización le permite emitir certificados cliente mediante la autoridad de certificación de su dominio.

Además, para la autenticación del Servidor de administración en dispositivos móviles que operan con el sistema operativo iOS, se requiere un certificado de Servidor MDM de iOS. Para obtener más información, consulte Configurar un certificado de servidor MDM de iOS

https://support.kaspersky.com/help/KSMM/5.0/en-US/287007.htm
.

Certificado del Servidor web

El Servidor web, un componente del Servidor de administración de Kaspersky Security Center, utiliza un tipo especial de certificado. Este certificado es necesario para publicar paquetes de instalación del Agente de red que el usuario posteriormente descargará en dispositivos administrados, así como para los paquetes de instalación de Kaspersky Security para dispositivos móviles. El Servidor web puede usar distintos certificados para tal fin.

Si la compatibilidad con dispositivos móviles no está habilitada, el Servidor web usará uno de los siguientes certificados (en orden de prioridad):

1. certificado personalizado, elegido manualmente para el Servidor web a través de la Consola de administración
2. certificado común del Servidor de administración ("C")

Si la compatibilidad con dispositivos móviles está habilitada, el Servidor web usará uno de los siguientes certificados (en orden de prioridad):

1. certificado personalizado, elegido manualmente para el Servidor web a través de la Consola de administración
2. Certificado para dispositivos móviles personalizado
3. certificado para dispositivos móviles autofirmado ("M")
4. certificado común del Servidor de administración ("C")

Certificado de Kaspersky Security Center Web Console

El Servidor de Kaspersky Security Center Web Console (o también, en lo sucesivo, "Web Console") tiene su propio certificado. Cuando visita un sitio web, el navegador verifica si la conexión es fiable. El certificado de la consola web le permite autenticar la consola web y se utiliza para cifrar el tráfico entre el navegador y la consola web.

Cuando abre Web Console, el navegador le informa que la conexión a Web Console no es privada y que el certificado de Web Console no es válido. Esta advertencia se muestra porque el certificado de Kaspersky Security Center Web Console es autofirmado y Kaspersky Security Center lo genera automáticamente. Para deshacerse de esta advertencia, realice una de las siguientes acciones:

- Reemplace el certificado de Web Console con uno personalizado (opción recomendada). Cree un certificado que sea de confianza en su infraestructura y que cumpla con los requisitos para certificados personalizados.
- Agregue el certificado de Web Console a la lista de certificados que el navegador considera de confianza. Recomendamos que utilice esta opción solo si no puede crear un certificado personalizado.

De forma predeterminada, un certificado autofirmado tiene una validez de 30 días. Puede cambiar este valor en el archivo de configuración de Web Console, /var/opt/kaspersky/ksc-web-console/server/config.json. Para aplicar el valor especificado, debe reiniciar el proceso de Web Console.

Web Console vuelve a emitir automáticamente este certificado y comienza a utilizarlo antes de que caduque el certificado autofirmado.

Puede reemplazar el certificado autofirmado de Web Console por un certificado de usuario.

Certificado de Identity and Access Manager

Se requiere un certificado de Identity and Access Manager (certificado de IAM) para los siguientes propósitos:

- Autenticación del Servidor de administración cuando el navegador de un usuario se conecta a él a través del protocolo OAuth.
- Autenticación del Servidor de administración cuando Kaspersky Security Center Web Console se conecta a él.

El certificado de IAM se crea automáticamente la primera vez que ejecuta el Servidor de administración. El certificado se almacena en el dispositivo del Servidor de administración en el directorio: /var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem (para el clúster de conmutación por error de Kaspersky Security Center: <carpeta de datos compartida>/iam/main_certificate.pem). Debe especificar la ruta al certificado de IAM utilizando el parámetro `iamCertPath` cuando cree un archivo de respuesta para instalar Kaspersky Security Center Web Console.

El certificado de IAM es válido por 365 días. Kaspersky Security Center crea un certificado de IAM de reserva en forma automática 48 horas antes de que caduque el certificado actual. El certificado de reserva se utiliza más tarde para sustituir el certificado de IAM que caducó.

El período máximo de validez para cualquier certificado de IAM debe ser de 397 días o menos.

Si es necesario, puede asignar un certificado de IAM personalizado. Por ejemplo, esto puede ser necesario para una mejor integración con la PKI existente de su empresa o para la configuración personalizada de los campos del certificado.

Al iniciar sesión en Kaspersky Security Center Web Console, el navegador se redirige a la página de inicio de sesión del Servidor de administración (https://`<dirección del Servidor de administración>`:4444) para la autenticación. El tráfico entre el navegador y el Servidor de administración se cifra mediante el protocolo TLS y el certificado de IAM.

El navegador podría informarle que la conexión al Servidor de administración no es privada y que el certificado de IAM no es válido. La advertencia se muestra porque el certificado de IAM está autofirmado y es generado automáticamente por Kaspersky Security Center. Para deshacerse de esta advertencia, realice una de las siguientes acciones:

- Reemplace el certificado de IAM con uno personalizado (opción recomendada). Cree un certificado que sea de confianza en su infraestructura y que cumpla con los requisitos para certificados personalizados.
- Agregue el certificado de IAM a la lista de certificados que el navegador considera de confianza. Recomendamos que utilice esta opción solo si no puede crear un certificado personalizado.

Requisitos para los certificados personalizados utilizados en Kaspersky Security Center Linux

En la siguiente tabla, se enumeran los requisitos que deben reunir los certificados personalizados utilizados para los distintos componentes de Kaspersky Security Center Linux.

Requisitos que deben reunir los certificados de Kaspersky Security Center Linux

Tipo de certificado	Requisitos	Comentarios
Certificado común, certificado de reserva común ("C", "CR")	Longitud mínima de la clave: 2048. Restricciones básicas: • Restricción de longitud de ruta: ninguna Uso de claves: • Firma digital • Firma de certificados • Cifrado de claves • Firma de CRL Uso extendido de claves (opcional): autenticación de servidor, autenticación de cliente. El certificado debe incluir un Nombre alternativo del sujeto (SAN) válido que contenga la dirección de bucle invertido del Servidor de administración: • Para IPv4: 127.0.0.1 • Para IPv6: 0:0:0:0:0:0:0:1	El parámetro Extended Key Usage es opcional. El valor de la Restricción de longitud de ruta puede ser un número entero distinto de "Ninguna", pero no inferior a 1.
Certificado del Servidor web	Uso extendido de clave: autenticación de servidor. El contenedor PKCS #12 o PEM que se utilice para especificar el certificado debe incluir toda la cadena de claves públicas. El nombre alternativo del sujeto (SAN) del certificado está presente; es decir, el valor del campo `subjectAltName` es válido. El certificado debe ajustarse tanto a los requisitos que los navegadores exigen para los certificados de los servidores como a los requisitos básicos que ordena actualmente el CA/Browser Forum.	—
Certificado de Kaspersky Security Center Web Console	Uso extendido de claves (EKU): autenticación del servidor. El contenedor PEM que se utilice para especificar el certificado debe incluir toda la cadena de claves públicas. El nombre alternativo del sujeto (SAN) del certificado está presente; es decir, el valor del campo `subjectAltName` es válido. El valor debe coincidir con la dirección de IAM que se especificó durante la instalación del Servidor de administración. Para obtener la dirección de IAM especificada, ejecute el siguiente comando en el dispositivo que tiene el Servidor de administración instalado: `grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml` El certificado debe ajustarse tanto a los requisitos que los navegadores exigen para los certificados de los servidores como a los requisitos básicos que ordena actualmente el CA/Browser Forum.	Kaspersky Security Center Web Console no es compatible con los certificados cifrados.
Certificado de Identity and Access Manager (certificado de IAM)	Uso extendido de clave: autenticación de servidor. El contenedor PEM que se utilice para especificar el certificado debe incluir toda la cadena de claves públicas. El certificado debe ajustarse tanto a los requisitos que los navegadores exigen para los certificados de los servidores como a los requisitos básicos que ordena actualmente el CA/Browser Forum.	Kaspersky Security Center Web Console no es compatible con los certificados cifrados.

Reemisión de los certificados internos de Kaspersky Security Center Web Console

Kaspersky Security Center Web Console utiliza los siguientes certificados:

- Un certificado público (certificado TLS de Web Console) que Web Console presenta al navegador para establecer una conexión HTTPS.
- Un certificado interno que Web Console utiliza para las conexiones TLS.

Certificado público

La mayoría de los navegadores imponen un límite al plazo de validez de un certificado. Para ajustarse a este límite, el plazo de validez del certificado público de Kaspersky Security Center Web Console está limitado a 30 días. Puede reemplazar un certificado existente recibido de una autoridad de certificación (CA) emitiendo manualmente un nuevo certificado autofirmado.

Cuando abra Kaspersky Security Center Web Console, es posible que el navegador le advierta que la conexión a Kaspersky Security Center Web Console no es privada y que el certificado de Kaspersky Security Center Web Console no es válido. La advertencia se muestra porque Kaspersky Security Center Web Console utiliza un certificado autofirmado, generado automáticamente por Kaspersky Security Center. Para eliminar esta advertencia o prevenir su aparición, puede realizar una de las acciones siguientes:

- Reemplace el certificado público autofirmado de Web Console por un certificado de usuario (opción recomendada). Cree un certificado que sea de confianza en su infraestructura y que cumpla con los requisitos para certificados personalizados.
- Agregue el certificado de Kaspersky Security Center Web Console a la lista de certificados de confianza del navegador. Recomendamos que utilice esta opción solo si no puede crear un certificado personalizado.

Certificado interno

El certificado interno de Web Console se utiliza únicamente para la autenticación mutua interna de los componentes de Web Console y no se muestra al usuario.

De forma predeterminada, el plazo de validez del certificado interno de Kaspersky Security Center Web Console es de 3 años (1095 días).

14 días antes de que venza el plazo especificado, Web Console muestra una notificación para recordarle que debe volver a emitir el certificado interno.

Para volver a emitir el certificado interno vencido de Kaspersky Security Center Web Console:

Vuelva a instalar Kaspersky Security Center Web Console realizando una de las siguientes acciones:

- Si desea utilizar el mismo archivo de instalación de Kaspersky Security Center Web Console, desinstale Kaspersky Security Center Web Console y luego instale la misma versión de Kaspersky Security Center Web Console.
- Si desea utilizar un archivo de instalación de una versión actualizada, ejecutar el comando de actualización.

Se vuelve a emitir el certificado de Kaspersky Security Center Web Console.

Reemplazar el certificado de Kaspersky Security Center Web Console

De forma predeterminada, al instalar el Servidor de Kaspersky Security Center Web Console (también denominado Kaspersky Security Center Web Console), se emite automáticamente un certificado de navegador para la aplicación. Este certificado puede reemplazarse por uno personalizado.

Para asignar un certificado de usuario de Kaspersky Security Center Web Console:

1. Guarde el archivo del certificado y el archivo de la clave privada en el siguiente directorio:

   /var/opt/kaspersky/ksc-web-console/certificates/external/

   Formato de archivo admitido: PEM.
   Se requieren privilegios de root para leer y escribir en el directorio. El usuario con el que se ejecuta el servicio de la consola web interactiva solo tiene permiso de lectura.

2. Asigne los siguientes nombres a los archivos:

   - web-console.crt: archivo que contiene el certificado.
   - web-console.key: archivo que contiene la clave privada sin contraseña.

Se asignó un certificado principal personalizado y Web Console lo está utilizando.

Si desea reemplazar el certificado de usuario:

- Si desea reemplazar el certificado de usuario por otro certificado de usuario, siga las mismas instrucciones.
- Si desea reemplazar el certificado de usuario por un certificado autofirmado, elimine uno o ambos archivos del certificado de usuario.

Cuando caduca un certificado de usuario, Web Console muestra una notificación al respecto y continúa utilizando el certificado caducado.

Si el certificado principal de usuario que especificó no es válido, Web Console muestra una notificación al respecto, emite un certificado principal autofirmado y comienza a utilizarlo.

La notificación aparece por primera vez 14 días antes de que caduque el certificado.

Conversión de un certificado PFX al formato PEM

Si desea utilizar un certificado PFX en Kaspersky Security Center Web Console, primero debe convertirlo al formato PEM. Puede usar para ello cualquier utilidad multiplataforma basada en OpenSSL.

Para convertir un certificado PFX al formato PEM en el sistema operativo Linux:

1. En una utilidad multiplataforma basada en OpenSSL, ejecute los siguientes comandos:

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

   ```
   openssl pkcs12 -in <nombre de archivo.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > key.pem
   ```

2. Asegúrese de que el archivo del certificado y la clave privada se generen en el mismo directorio donde se almacena el archivo .pfx.

3. Kaspersky Security Center Web Console no permite usar certificados protegidos con una frase de contraseña. Por lo tanto, debe ejecutar el siguiente comando en una utilidad multiplataforma basada en OpenSSL para eliminar una frase de contraseña del archivo .pem:

```
openssl rsa -in key.pem -out key-without-passphrase.pem
```

> No utilice el mismo nombre para los archivos .pem de entrada y salida.

De este modo, se elimina el cifrado del nuevo archivo .pem. No debe introducir una frase de contraseña para usarlo.

Los archivos .crt y .pem pueden cargarse sin más en el instalador de Kaspersky Security Center Web Console.

Escenario: Especificación del certificado del Servidor de administración personalizado

Puede asignar el certificado del Servidor de administración personalizado, por ejemplo, para una mejor integración con la infraestructura de claves públicas (PKI) existente de su empresa o para la configuración personalizada de los campos del certificado. Es conveniente reemplazar el certificado inmediatamente después de la instalación del Servidor de administración y antes de que el asistente de inicio rápido termine con sus operaciones.

El período máximo de validez para cualquiera de los certificados del Servidor de administración debe ser de 397 días o menos.

Requisitos previos

Deben cumplirse las siguientes condiciones:

- El nuevo certificado debe crearse en formato PKCS#12 (por ejemplo, mediante la PKI de la organización).
- Para el nuevo certificado, se deben cumplir los requisitos que se enumeran en la siguiente tabla.

  En la siguiente tabla, tenga en cuenta el requisito "CA: true". Esto significa que el nuevo certificado debe ser emitido por una autoridad de certificación (CA) de confianza. El nuevo certificado con el requisito "CA: true" debe incluir toda la cadena de confianza y una clave privada, que debe almacenarse en un archivo con la extensión pfx o p12.

Tipo de certificado	Requisitos
Certificado común, certificado de reserva común ("C", "CR")	Longitud mínima de la clave: 2048. Restricciones básicas: • Restricción de longitud de ruta: ninguna El valor de la Restricción de longitud de ruta puede ser un número entero distinto de "Ninguna", pero no inferior a 1. Uso de claves: • Firma digital • Firma de certificados • Cifrado de claves • Firma de CRL Uso extendido de claves (EKU): autenticación del servidor y autenticación del cliente. El EKU es opcional, pero si su certificado lo contiene, los datos de autenticación del servidor y del cliente se deben especificar en el EKU. El certificado debe incluir un Nombre alternativo del sujeto (SAN) válido que contenga la dirección de bucle invertido del Servidor de administración: • Para IPv4: 127.0.0.1 • Para IPv6: 0:0:0:0:0:0:0:1
Certificado móvil, Certificado de reserva móvil ("M", "MR")	Longitud mínima de la clave: 2048. Restricciones básicas: • CA: cierto • Restricción de longitud de ruta: ninguna El valor de la restricción de longitud de ruta puede no ser "ninguna", pero en ese caso debe usarse un entero y el certificado común debe tener una restricción de longitud de ruta no inferior a 1. Uso de claves: • Firma digital • Firma de certificados • Cifrado de claves • Firma de CRL Uso extendido de clave: autenticación de servidor. El EKU es opcional, pero si su certificado lo contiene, los datos de autenticación del servidor se deben especificar en el EKU.
CA de certificado para certificados de usuario generados automáticamente ("MCA")	Longitud mínima de la clave: 2048. Restricciones básicas: • CA: cierto • Restricción de longitud de ruta: ninguna El valor de la restricción de longitud de ruta puede no ser "ninguna", pero en ese caso debe usarse un entero y el certificado común debe tener una restricción de longitud de ruta no inferior a 1. Uso de claves: • Firma digital • Firma de certificados • Cifrado de claves • Firma de CRL Uso extendido de claves (EKU): autenticación del cliente. El EKU es opcional, pero si su certificado lo contiene, los datos de autenticación del cliente se deben especificar en el EKU.

Los certificados emitidos por una CA pública no tienen el permiso de firma de certificado. Para utilizar dichos certificados, asegúrese de haber instalado la versión 13 o superior del Agente de red en los puntos de distribución o puertas de enlace de conexión de su red. De lo contrario, no podrá utilizar certificados sin el permiso de firma.

Etapas

La especificación del certificado del Servidor de administración se realiza por etapas:

1. **Reemplazo del certificado del Servidor de administración**

   Use la línea de comandos utilidad klsetsrvcert para este fin.

2. **Especificación de un nuevo certificado y restauración de la conexión de los Agentes de red al Servidor de administración**

   Al reemplazar el certificado, todos los Agentes de red que estaban conectados anteriormente al Servidor de administración a través de SSL pierden su conexión y devuelven "Error de autenticación del Servidor de administración". Para especificar el nuevo certificado y restaurar la conexión, use la línea de comandos utilidad klmover.

3. **Especificación de un nuevo certificado en el directorio de certificados de Kaspersky Security Center Web Console**

   Guarde el archivo con el certificado del Servidor de administración en el directorio: /var/opt/kaspersky/ksc-web-console/certificates/external/

   Asigne al archivo el nombre <address>-admin-server.crt, donde <address> es la dirección del Servidor de administración que especificó en el parámetro `iamHost` del archivo de respuestas del instalador de Web Console.

   Formato de archivo admitido: PEM.
   Se requieren privilegios de root para leer y escribir en el directorio. El usuario con el que se ejecuta el servicio de la consola web interactiva solo tiene permiso de lectura.

Resultados

Al concluir el escenario, los Agentes de red reemplazan el certificado del Servidor de administración y autentican el servidor en los dispositivos administrados.

Reemplazo del certificado del Servidor de administración mediante la utilidad klsetsrvcert

Para evitar perder el control de los dispositivos, consulte el Escenario: Especificación del certificado del Servidor de administración personalizado antes de continuar.

Para reemplazar el certificado del Servidor de administración:

Desde la línea de comandos, ejecute la siguiente utilidad:

```
/opt/kaspersky/ksc64/sbin/klsetsrvcert [-t <certificate type> {-i <path to new certificate> [-p <password>] [-o
<validation parameters>] | -g <dns name>}][-f <replacement time>][-r <root certificates>][-l <log file path>]
```

La descripción de los parámetros de la utilidad klsetsrvcert se presenta en la siguiente tabla.

Valores de los parámetros de la utilidad klsetsrvcert

Configuración	Valor
`-t < tipo de certificado >`	Tipo del certificado para reemplazar. Valores posibles del parámetro `< tipo de certificado >`: • `C`: reemplaza el certificado común para los puertos 13000 y 13291. • `CR`: reemplaza el certificado de reserva común para los puertos 13000 y 13291.
`-f < tiempo de reemplazo >`	Horario para cambiar el certificado, utilizando el formato "DD-MM-YYYY hh:mm" (para los puertos 13000 y 13291). Utilice este parámetro si desea reemplazar el certificado común con el certificado de reserva común antes de que caduque. Especifique la hora en que los dispositivos administrados deben sincronizarse con el Servidor de administración en un nuevo certificado.
`-i < ruta al nuevo certificado >`	Contenedor con el certificado y una clave privada en formato PKCS#12 (archivo con extensión .p12 o .pfx).
`-p < contraseña >`	Contraseña utilizada para la protección del contenedor p12. El certificado y la clave privada se almacenan en el contenedor, por lo tanto, se requiere la contraseña para descifrar el archivo con el contenedor.
`-o < parámetros de validación >`	Parámetros de validación del certificado (separados por punto y coma). Para utilizar un certificado personalizado sin permiso de firma, especifique `-o NoCA` en la utilidad klsetsrvcert. Esto es útil para los certificados emitidos por una CA pública. Para cambiar la longitud de la clave de cifrado para los tipos de certificado C o CR, especifique `-o RsaKeyLen: < longitud de la clave >` en la utilidad klsetsrvcert, donde el parámetro `< longitud de la clave >` es el valor de longitud de clave requerido. De lo contrario, se utiliza la longitud actual de la clave del certificado.
`-g < nombre del dns >`	Se creará un nuevo certificado para el nombre DNS especificado (Nombre común y Nombre alternativo del sujeto).
`-r < certificados raíz >`	Lista de autoridades de certificación raíz de confianza, formato PEM.
`-l < ruta del archivo de registro >`	Archivo de salida de resultados. De forma predeterminada, la salida se redirige en la corriente de la salida estándar.

Por ejemplo, para especificar el certificado del Servidor de administración personalizado, use el siguiente comando:

```
klsetsrvcert -t C -i <ruta al certificado nuevo> -p <contraseña> -o NoCA
```

Después de reemplazar el certificado, todos los Agentes de red conectados al Servidor de administración a través de SSL pierden su conexión. Para restaurarlo, use la línea de comando utilidad klmover.

Para que no se pierdan las conexiones de los agentes de red, use los siguientes comandos:

1. Para instalar el nuevo certificado,

   ```
   klsetsrvcert -t CR -i <ruta al certificado nuevo> -p <contraseña> -o NoCA
   ```

2. Para especificar la fecha en que se aplicará el nuevo certificado,

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

dónde "`DD-MM-YYYY hh:mm`" es la fecha 3-4 semanas posterior a la fecha actual. Al modificar el momento para cambiar el certificado por el nuevo, dará tiempo a que el nuevo certificado se distribuya a la totalidad de los agentes de red.

Preguntas y respuestas

¿Qué pasos adicionales se requieren después de reemplazar el certificado común del Servidor de administración?

1. Asegúrese de que **se cumplan los requisitos de los certificados personalizados**.

   Si utiliza un certificado personalizado en lugar del autofirmado, antes de actualizar Kaspersky Security Center Linux a la versión posterior, debe asegurarse de que el certificado incluya el Nombre alternativo del sujeto (SAN). Si no lo incluye, es importante reemplazar el certificado antes de actualizar Kaspersky Security Center Linux. De lo contrario, no podrá iniciar sesión en Web Console después de la actualización.

   Para asegurarse de que el certificado incluya SAN:

   1. En el dispositivo en el que se encuentra instalado el Servidor de administración, ejecute el siguiente comando:

      - Para un dispositivo Linux:

        ```
        sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
        ```

      - Para un dispositivo Windows:

        ```
        certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
        ```

   2. Asegúrese de que el Nombre alternativo del sujeto (SAN) esté presente en el resultado del comando y que contenga la dirección del dispositivo del Servidor de administración.

   3. Si no aparece el Nombre alternativo del sujeto, use la utilidad klsetsrvcert para reemplazar su certificado de usuario por uno que cumpla con los requisitos.

2. Asegúrese de que el archivo de configuración del servidor de IAM contenga la dirección del servidor de administración actual. De lo contrario, agregue la dirección al archivo de configuración.

3. Reinstale Web Console para evitar el siguiente error:

   El Servidor de administración utiliza un certificado que no es de confianza. Vuelva a configurar la aplicación especificando un certificado válido o comuníquese con el administrador principal.

Conexión de los Agentes de red al Servidor de administración mediante la utilidad klmover

Puede usar la utilidad klmover para restaurar la conexión desde dispositivos no controlados al Servidor de administración, por ejemplo, después de un error en el Servidor de administración, si no es posible restaurarla desde una copia de seguridad.

Para restaurar la conexión, ejecute la utilidad klmover desde la línea de comando:

- Para Linux:
  - Para sistemas de 32 bits: `/opt/kaspersky/klnagent/bin/klmover [-address <dirección del servidor>] [-pn <número de puerto>] [-ps <número de puerto SSL>] [-nossl] [-cert <ruta al archivo del certificado>]`
  - Para sistemas de 64 bits: `/opt/kaspersky/klnagent64/bin/klmover [-address <dirección del servidor>] [-pn <número de puerto>] [-ps <número de puerto SSL>] [-nossl] [-cert <ruta al archivo del certificado>]`
- Para Windows:
  - Para sistemas de 32 bits: `<ruta>\klmover.exe [-address <dirección del servidor>] [-pn <número de puerto>] [-ps <número de puerto SSL>] [-nossl] [-cert <ruta al archivo del certificado>]`
  - Para sistemas de 64 bits: `<ruta>\klmover.exe [-address <dirección del servidor>] [-pn <número de puerto>] [-ps <número de puerto SSL>] [-nossl] [-cert <ruta al archivo del certificado>]`
- For macOS:

  `/Library/Application Support/Kaspersky Lab/klnagent/Binaries/klmover [-address <dirección del servidor>] [-pn <número de puerto>] [-ps <número de puerto SSL>] [-nossl] [-cert <ruta al archivo del certificado>]`

  dónde `<ruta>` es la ruta de instalación predeterminada para el Agente de red o la ruta de instalación especificada por usted en la configuración del paquete de instalación del Agente de red.

Para evitar que los intrusos muevan los dispositivos fuera del control de su Servidor de administración, recomendamos que active la protección con contraseña para ejecutar la utilidad klmover. Para habilitar la protección con contraseña, seleccione la opción **Utilizar contraseña de desinstalación** en la configuración de la directiva del Agente de red.

Si pierde u olvida la contraseña del Agente de red protegido con contraseña, que está instalado en el dispositivo y que Kaspersky Security Center Linux ya no administra, no podrá eliminar el Agente de red mediante la utilidad klmover o la línea de comando. En este caso, deberá reinstalar el sistema operativo en el dispositivo que tiene instalado el Agente de red protegido con contraseña.

La utilidad klmover requiere derechos de administrador local.

Al activar la opción **Utilizar contraseña de desinstalación** en los dispositivos Windows, también se activa la protección con contraseña para la herramienta Cleaner (cleaner.exe).

No se puede utilizar la utilidad klmover para dispositivos cliente conectados al Servidor de administración mediante puertas de enlace de conexión. Para estos dispositivos, debe reconfigurar el Agente de red o reinstalar el Agente de red y especificar la puerta de enlace de conexión.

La descripción de los parámetros de la utilidad klmover se presenta en la siguiente tabla.

Valores de los parámetros de la utilidad klmover

Configuración	Valor
`-address < dirección del servidor >`	Dirección del Servidor de administración para la conexión. Puede especificar una dirección IP o el nombre de DNS.
`-pn < número de puerto >`	Número del puerto a través del cual se establece la conexión no cifrada con el Servidor de administración. El número de puerto predeterminado es 14000.
`-ps < número de puerto SSL >`	número del puerto SSL a través del cual se establece la conexión al Servidor de administración, utilizando SSL. El número de puerto predeterminado es 13000.
`-nossl`	usar conexión no cifrada al Servidor de administración. Si la clave no está en uso, el Agente de red se conecta al Servidor de administración mediante el protocolo cifrado SSL.
`-cert < ruta al archivo del certificado >`	usa el archivo de certificado especificado para la autenticación del acceso al Servidor de administración.
`-nauninstpwd < contraseña >`	Utilice este parámetro para especificar la contraseña de desinstalación del Agente de red. Configuración opcional.

Volver a emitir el certificado del Servidor web

El certificado del Servidor web que se utiliza en Kaspersky Security Center Linux se necesita para publicar los paquetes de instalación del Agente de red que luego se entregan a los dispositivos administrados, así como para publicar perfiles de MDM para iOS, apps de iOS y paquetes de instalación de Kaspersky Endpoint Security para dispositivos móviles. Dependiendo de la configuración vigente en la aplicación, son varios los certificados que pueden utilizarse como certificado del Servidor web (para obtener más detalles, consulte Acerca de los certificados de Kaspersky Security Center Linux).

Es posible que deba volver a emitir el certificado del Servidor web para cumplir con los requisitos de seguridad específicos de su organización o para mantener la conexión continua de sus dispositivos administrados antes de comenzar a actualizar la aplicación. Kaspersky Security Center ofrece dos formas de volver a emitir el certificado del Servidor web. La elección entre los dos métodos depende de si tiene dispositivos móviles conectados y administrados a través del protocolo móvil (es decir, mediante el certificado para dispositivos móviles).

Si nunca ha especificado su propio certificado personalizado como certificado del Servidor web en la sección **Servidor web** de la ventana de propiedades del Servidor de administración, el certificado para dispositivos móviles actúa como el certificado del Servidor Web. En este caso, para volver a emitir el certificado del Servidor web, se debe volver a emitir el protocolo móvil.

Para volver a emitir el certificado del Servidor web cuando tenga dispositivos móviles administrados a través del protocolo móvil, haga lo siguiente:

1. Genere un certificado personalizado y prepárelo para utilizarlo en Kaspersky Security Center Linux. Compruebe si su certificado personalizado cumple con los requisitos de Kaspersky Security Center Linux. Si es necesario, modifique el certificado.

2. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

3. En la pestaña **General**, vaya a la sección **Servidor web**.

4. En la subsección **Sobre HTTP**, seleccione la opción **Cargar el certificado desde un archivo** y haga clic en el botón **Cambiar certificado**.

5. En la ventana que se abre, en el campo **Formato del certificado** seleccione un tipo de certificado:

   - Si seleccionó **Contenedor PKCS #12**, haga clic en el botón **Examinar** ubicado junto al campo **Certificado** y busque el archivo del certificado en su disco duro. Si el archivo del certificado está protegido con contraseña, ingrese la contraseña en el campo **Contraseña**.

   - Si seleccionó **Certificado X.509**, haga clic en el botón **Examinar** ubicado junto al campo **Clave privada** y busque la clave privada en su disco duro. Si la clave privada está protegida con contraseña, ingrese la contraseña en el campo **Contraseña**.

6. Haga clic en el botón **Guardar** y, luego, en **Aceptar**.

   Se cierra la ventana.

7. Si es necesario, en el campo **Puerto HTTPS del Servidor web**, cambie el número del puerto HTTPS que usará el Servidor web y haga clic en el botón **Guardar**.

Se volverá a emitir el certificado del Servidor web.

Para volver a emitir el certificado del Servidor web cuando no tenga dispositivos móviles administrados a través del protocolo móvil, haga lo siguiente:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, elija la sección **Certificados**.

3. Si planea continuar usando el certificado emitido por Kaspersky Security Center, haga lo siguiente:

   a. Seleccione la opción **Certificado emitido usando mediante el Servidor de administración** y haga clic en el botón **Examinar**.

   b. En la ventana que se abre, en los grupos de opciones **Dirección de conexión** y **Plazo de activación**, seleccione las opciones relevantes y haga clic en **Aceptar**.

Como alternativa, si planea usar su propio certificado personalizado, haga lo siguiente:

a. Compruebe si su certificado personalizado cumple con los requisitos de Kaspersky Security Center Linux. Si es necesario, modifique el certificado.

b. Seleccione la opción **Otro certificado**, haga clic en el botón **Administrar certificado** y, en la ventana que se abre, haga clic en el botón **Examinar**.

c. En la ventana que se abre, en el campo **Formato del certificado** seleccione un tipo de certificado:

   - Si seleccionó **Contenedor PKCS #12**, haga clic en el botón **Examinar** ubicado junto al campo **Certificado** y busque el archivo del certificado en su disco duro. Si el archivo del certificado está protegido con contraseña, ingrese la contraseña en el campo **Contraseña**.

   - Si seleccionó **Certificado X.509**, haga clic en el botón **Examinar** ubicado junto al campo **Clave privada** y busque la clave privada en su disco duro. Si la clave privada está protegida con contraseña, ingrese la contraseña en el campo **Contraseña**.

d. Haga clic en el botón **Guardar** y, luego, en **Aceptar**.

El certificado para dispositivos móviles se vuelve a emitir para que se lo utilice como certificado del Servidor web.

Cambiar el certificado predeterminado de IAM a uno personalizado

Para asignar un certificado de usuario de IAM:

1. Genere un certificado personalizado y prepárelo para utilizarlo en Kaspersky Security Center Linux. Compruebe si su certificado personalizado cumple con los requisitos de Kaspersky Security Center Linux.
2. Asegúrese de que el grupo kladmins tenga acceso a los archivos de certificados de IAM.
3. Busque el archivo de configuración de IAM: `/var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml`

   En este archivo, agregue rutas a los archivos de certificado de IAM a la sección `server_iam`:

   - `certificates.main.cert`: ruta al archivo principal del certificado.
   - `certificates.main.key`: ruta a la clave privada del certificado principal. La clave privada no debe estar protegida con una contraseña.
4. Reinicie el servicio kliam con el siguiente comando:

   ```
   sudo service kliam_srv restart
   ```
5. Guarde el archivo del certificado de IAM en el siguiente directorio:

   /var/opt/kaspersky/ksc-web-console/certificates/external/

   > Formato de archivo admitido: PEM.
   > El usuario con el que se ejecuta el servicio Kaspersky Security Center Web Console debe tener privilegios suficientes para leer los archivos guardados en el directorio.
6. Asigne un nombre al archivo: <address>-iam-server.crt

   donde <address> es la dirección de IAM que especificó en el parámetro `iamHost` del archivo de respuestas del instalador de Web Console.

Se asignó un certificado de usuario de IAM y Web Console lo está utilizando.

Si necesita reemplazar el certificado de usuario de IAM, siga las mismas instrucciones.

Si el certificado de IAM no es válido y no se ha recibido uno nuevo válido, se muestra un error en Web Console.

De forma predeterminada, se muestra una notificación de advertencia 14 días antes de que venza el certificado actual. Se muestra una notificación crítica 2 días antes de que venza el certificado actual.

Si IAM cambió a un certificado de reserva después de que usted especificó manualmente un certificado de IAM (autofirmado o de usuario) para Web Console, Web Console obtiene automáticamente el certificado de reserva de IAM y continúa conectándose al Servidor de administración. El certificado de usuario que especificó permanece en el directorio /var/opt/kaspersky/ksc-web-console/certificates/external, pero no se utiliza.

Para cambiar el certificado de reserva de IAM:

1. Busque el archivo de configuración de IAM: `/var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml`

En este archivo, especifique las rutas a los archivos de certificados de IAM:

- `server_iam.certificates.reserve.cert`: ruta al archivo principal del certificado.
- `server_iam.certificates.reserve.key`: ruta a la clave privada del certificado principal. La clave privada no debe estar protegida con una contraseña.

2. Reinicie el servicio kliam con el siguiente comando:

   ```
   sudo systemctl restart kliam_srv.service
   ```

   Cuando caduque el archivo del certificado actual, se utilizará en su lugar el certificado de reserva de IAM.

Agregar la dirección del Servidor de administración a la configuración del Servidor de IAM

Después de cambiar el certificado del Servidor de administración común ("C") durante una actualización, reubicación o migración, debe especificar la dirección del Servidor de administración en el archivo de configuración del Servidor de IAM para garantizar la validación adecuada del certificado entre el Servidor de IAM y el Servidor de administración.

Para agregar la dirección del Servidor de administración a la configuración del Servidor de IAM:

1. Obtenga el valor del Nombre alternativo del sujeto (SAN) del certificado del Servidor de administración común ("C") mediante el siguiente comando:

   ```
   sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
   ```

2. Según el resultado del comando, realice una de las siguientes acciones:

   - Si el resultado indica que falta el valor o que solo contiene la dirección IP de la red, consulte los **requisitos del certificado de usuario**.

     Si utiliza un certificado personalizado en lugar del autofirmado, antes de actualizar Kaspersky Security Center Linux a la versión posterior, debe asegurarse de que el certificado incluya el Nombre alternativo del sujeto (SAN). Si no lo incluye, es importante reemplazar el certificado antes de actualizar Kaspersky Security Center Linux. De lo contrario, no podrá iniciar sesión en Web Console después de la actualización.

     Para asegurarse de que el certificado incluya SAN:

     1. En el dispositivo en el que se encuentra instalado el Servidor de administración, ejecute el siguiente comando:

        - Para un dispositivo Linux:

          ```
          sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
          ```

        - Para un dispositivo Windows:

          ```
          certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
          ```

2. Asegúrese de que el Nombre alternativo del sujeto (SAN) esté presente en el resultado del comando y que contenga la dirección del dispositivo del Servidor de administración.

3. Si no aparece el Nombre alternativo del sujeto, use la utilidad klsetsrvcert para reemplazar su certificado de usuario por uno que cumpla con los requisitos.

Si no cumple con los requisitos, reemplace el certificado común del Servidor de administración en el Servidor de administración anterior mediante la utilidad klsetsrvcert. Luego, repita el procedimiento de actualización, reubicación o migración.

- Si el valor coincide con el valor especificado durante la instalación de Kaspersky Security Center Linux (en el paso **Ingrese el nombre DNS del servidor de IAM** del asistente de instalación o, para una instalación silenciosa, en el parámetro `KLSRV_UNATT_IAM_ADDRESS`), no se requieren más acciones. El Servidor de IAM y el Servidor de administración interactuarán correctamente.

- Si el valor contiene nombres del DNS o direcciones de bucle invertido (127.0.0.1 o 0:0:0:0:0:0:0:1), use uno de ellos en el archivo de configuración. Se recomienda utilizar 127.0.0.1.

3. En la sección `server_iam` del archivo de configuración del Servidor de IAM, asegúrese de que el valor de `ksc_address: "<SAN_address>"` esté establecido en una de las direcciones SAN del certificado general del Servidor de administración.

   Puede utilizar un editor de texto para modificar el archivo de configuración del Servidor de IAM, por ejemplo, vi. El siguiente comando abre el archivo en el editor de texto vi:

   ```
   vi /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
   ```

   Ejemplo del bloque server_iam en el archivo de configuración del Servidor de IAM:

   ```
   server_iam:
       iam_address: "ksc.example.com"
       server_display_name: "ksc.example.com"
       ksc_address: "oldksc.example.internal"
       ksc_ca: "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
   ```

   Asegúrese de usar el mismo espacio que en el ejemplo.

4. Asegúrese de que el nombre de red en la configuración `ksc_address` se resuelva a la dirección de bucle invertido (127.0.0.1 o 0:0:0:0:0:0:0:1) del Servidor de administración. Para hacer esto, puede usar la utilidad Ping en el Servidor de administración.

   Si la dirección permitida es diferente o no se puede resolver la dirección, agregue una línea al archivo hosts del Servidor de administración.

5. Reinicie el servicio del Servidor de IAM para aplicar los cambios de configuración mediante el siguiente comando:

   ```
   sudo systemctl restart kliam_srv.service
   ```

La dirección del Servidor de administración se agrega al archivo de configuración del Servidor de IAM desde el certificado común del Servidor de administración.

Resolución de problemas

La presencia de varios Servidores de administración con el mismo nombre de red en la red, así como los problemas de configuración del Servidor de IAM, pueden provocar errores al iniciar sesión en Web Console. En la siguiente tabla se describen posibles errores y soluciones.

Error	Descripción	Solución
Su solicitud no se puede procesar en este momento. Espere y vuelva a intentarlo.	Además del proceso de inicialización de datos después de actualizar o restaurar Kaspersky Security Center Linux, este error puede ocurrir si falla la conexión al Servidor de administración mediante la dirección de red especificada.	Compruebe que la dirección especificada se resuelva en la dirección IP del Servidor de administración actual.
El Servidor de administración utiliza un certificado que no es de confianza. Vuelva a configurar la aplicación especificando un certificado válido o comuníquese con el administrador principal.	El error puede ocurrir si el valor de la dirección en el archivo de configuración del Servidor de IAM no coincide con el valor del atributo Nombre alternativo del sujeto (SAN) del certificado común del Servidor de administración.	Siga las instrucciones anteriores.
Nombre de usuario o contraseña incorrectos.	Además de las credenciales incorrectas, este error puede ocurrir si existe otro Servidor de administración con el mismo nombre en la red.	Compruebe que la dirección especificada se resuelva en la dirección IP del Servidor de administración actual.

Definición de una carpeta compartida

Después de la instalación del Servidor de administración, puede especificar la ubicación de la carpeta compartida en las propiedades del Servidor de administración. De forma predeterminada, la carpeta compartida se crea en el dispositivo con el Servidor de administración. Sin embargo, en algunos casos (como cuando hay carga alta o se debe acceder desde una red aislada, etc.), es útil localizar la carpeta compartida en un recurso de archivo dedicado.

La carpeta compartida se utiliza en ocasiones para realizar el despliegue del Agente de red.

Se debe desactivar la distinción entre mayúsculas y minúsculas para la carpeta compartida.

Iniciar y cerrar sesión en Kaspersky Security Center Web Console

Una vez que instale el Servidor de administración y el Servidor de Web Console, podrá iniciar sesión en Kaspersky Security Center Web Console. Debe conocer la dirección web del Servidor de administración y el número de puerto especificado durante la instalación (de manera predeterminada, el puerto es 8080). En su navegador, JavaScript debe estar habilitado.

Para iniciar sesión en Kaspersky Security Center Web Console, utilice los siguientes métodos:

- Mediante la autenticación de dominio (inicio de sesión único)

  Este método se utiliza para autenticar de forma segura la conexión de Kaspersky Security Center Web Console con el Servidor de administración, versión 16 y posteriores. Si desea utilizar la autenticación de dominio, debe especificar parámetros adicionales de la interacción con Identity and Access Manager (IAM) durante la instalación de Kaspersky Security Center Web Console.

- Mediante la especificación del nombre y la contraseña del usuario del dominio

  Antes de iniciar sesión con una cuenta de usuario de dominio, sondee el controlador de dominio para obtener la lista de usuarios del dominio. Luego, debe especificar el nombre de usuario del dominio y la contraseña para iniciar sesión en el Servidor de administración. Este método solo es compatible con la autenticación a través de Microsoft Active Directory.

- Mediante la especificación del nombre y la contraseña del usuario interno

La cuenta de usuario con la que desea iniciar sesión en Kaspersky Security Center Web Console debe tener un rol asignado. Antes de iniciar sesión, asegúrese de que se haya asignado un rol al dominio o la cuenta de usuario interno. De lo contrario, se producirá un error de inicio de sesión.

Inicio de sesión mediante la autenticación de dominio (inicio de sesión único)

Para iniciar sesión en Kaspersky Security Center Web Console con la autenticación de dominio:

1. En su navegador, vaya a https://`<dirección de Kaspersky Security Center Web Console>:<Número de puerto>`

   Se muestra la página de selección del Servidor de administración.

2. Si agregó varios servidores de confianza, en la lista Servidores de administración, seleccione el Servidor de administración al que desea conectarse.

   Si solo agregó un único Servidor de administración, no verá una lista de servidores de administración.

   El navegador redirige a https://`<dirección del Servidor de administración>`:4444.

3. Configuración de la autenticación de dominio Kerberos.

4. Realice una de las siguientes acciones:

   - Haga clic en el botón **Utilizar autenticación de dominio**.

   - Si el Servidor tiene uno o más Servidores de administración virtuales y desea iniciar sesión en uno de ellos usando la autenticación de dominio:

     a. Haga clic en **Mostrar opciones de Servidor virtual**.

     b. Escriba el nombre del Servidor de administración virtual que especificó cuando creó el servidor virtual.

     c. Haga clic en el botón **Utilizar autenticación de dominio**.

5. Especifique el código de seguridad de un solo uso generado por la app de autenticación en el dispositivo móvil.

   En el primer inicio de sesión, configure la autenticación en dos pasos para su cuenta. Si la configuración de autenticación de dos factores no está disponible para usted, comuníquese con un usuario que tenga el derecho Modificar ACL de objetos en el área funcional **Características generales**: **Permisos de usuario** y la autenticación de dos factores configurada para agregar su cuenta a la lista de permitidos para autenticación de dos factores.

Después de iniciar sesión, se muestra la página de inicio de Kaspersky Security Center Web Console, con la última configuración de idioma y tema. Puede navegar por Kaspersky Security Center Web Console y usarla para trabajar con Kaspersky Security Center Linux.

Inicio de sesión con el nombre y la contraseña del usuario interno o el usuario del dominio

Para iniciar sesión en Kaspersky Security Center Web Console especificando el nombre y la contraseña de usuario:

1. En su navegador, vaya a https://`<dirección de Kaspersky Security Center Web Console>`:`<Número de puerto>`

   Se muestra la página de selección del Servidor de administración.

2. Si agregó varios servidores de confianza, en la lista Servidores de administración, seleccione el Servidor de administración al que desea conectarse.

   Si solo agregó un único Servidor de administración, no verá una lista de servidores de administración.

   El navegador redirige a https://`<dirección del Servidor de administración>`:4444.

3. Realice una de las siguientes acciones:

   - Para iniciar sesión en el Servidor de administración con una cuenta de usuario de dominio, ingrese el nombre de usuario y la contraseña del usuario del dominio.

     Puede ingresar el nombre del usuario del dominio en uno de los siguientes formatos:

     - `Nombre de usuario@dns.domain`
     - `NTDOMAIN\Nombre de usuario`

     > Antes de iniciar sesión con una cuenta de usuario de dominio, sondee el controlador de dominio para obtener la lista de usuarios del dominio.

   - Para iniciar sesión en el Servidor de administración al especificar el nombre de usuario y la contraseña del administrador, ingrese el nombre de usuario y la contraseña del usuario interno.
   - Si el Servidor tiene uno o más servidores virtuales y desea iniciar sesión en uno de ellos, haga lo siguiente:

     a. Haga clic en **Mostrar opciones de Servidor virtual**.

     b. Escriba el nombre del Servidor de administración virtual que especificó cuando creó el servidor virtual.

     c. Ingrese el nombre de usuario y la contraseña del administrador que tiene derechos en el Servidor de administración virtual.

4. Haga clic en el botón **Entrar**.

5. Especifique el código de seguridad de un solo uso generado por la app de autenticación en el dispositivo móvil.

   En el primer inicio de sesión, configure la autenticación en dos pasos para su cuenta. Si la configuración de autenticación de dos factores no está disponible para usted, comuníquese con un usuario que tenga el derecho Modificar ACL de objetos en el área funcional **Características generales**: **Permisos de usuario** y la autenticación de dos factores configurada para agregar su cuenta a la lista de permitidos para autenticación de dos factores.

6. Si el cambio de contraseña forzado está habilitado en su cuenta o su contraseña ha caducado, aparecerá la ventana de cambio de contraseña. Establezca una nueva contraseña para iniciar sesión en Kaspersky Security Center Web Console.

Después de iniciar sesión, se muestra la página de inicio de Kaspersky Security Center Web Console, con la última configuración de idioma y tema. Puede navegar por Kaspersky Security Center Web Console y usarla para trabajar con Kaspersky Security Center Linux.

Cerrar sesión

Para cerrar sesión en Kaspersky Security Center Web Console,

En el panel superior, vaya al menú de su cuenta haciendo clic en el nombre de su cuenta y luego seleccione **Salir**.

Kaspersky Security Center Web Console se cierra y se muestra la página de inicio de sesión.

Interfaz de Kaspersky Security Center Web Console

Kaspersky Security Center Linux se administra a través de la interfaz de Kaspersky Security Center Web Console.

La ventana de Kaspersky Security Center Web Console contiene los siguientes elementos:

- un menú principal, en la parte izquierda de la ventana
- Un panel superior en la parte superior de la ventana
- un área de trabajo, en la parte derecha de la ventana

Menú principal

El menú principal contiene estas secciones:

- **Servidor de administración**. Muestra el nombre del Servidor de administración al que se está conectado. Puede hacer clic en el nombre del Servidor de administración para abrir las propiedades del Servidor de administración.
- **Navegación por la consola**. Muestra el mapa del menú principal. La mayoría de las secciones que se muestran pueden agregarse a los marcadores o establecerse como página de inicio. De forma predeterminada, los **Navegación por la consola** están configurados como página de inicio. Puede cambiar esta configuración.

- **Supervisión**. Brinda una visión general de la infraestructura, los estados de protección e información estadística.
- **Administración de activos**. Contiene herramientas para la administración de dispositivos y hardware, y directivas de aplicaciones de Kaspersky.
- **Tareas**. Contiene herramientas para crear y ejecutar tareas.
- **Usuarios y roles**. Permite administrar los usuarios y sus roles, configurar derechos de usuario mediante la asignación de roles a los usuarios y asociar perfiles de directivas con roles.
- **Repositorios**. Proporciona acceso a los repositorios de aplicaciones.
- **Administración de software**. Permite administrar aplicaciones de Kaspersky y de terceros, así como paquetes de instalación y parches.
- **Operaciones**. Contiene una variedad de operaciones, como la administración de licencias de aplicaciones y la visualización y administración de unidades cifradas y eventos de cifrado.
- **Descubrimiento y despliegue**. Permite sondear la red para detectar dispositivos cliente y organizar los dispositivos en grupos de administración de forma manual o automática. Esta sección también contiene el asistente de inicio rápido y el asistente de despliegue de la protección.
- **Marketplace**. Contiene información sobre toda la gama de soluciones empresariales de Kaspersky; permite seleccionar las que se necesitan y comprarlas en el sitio web de Kaspersky.
- **Configuración**. Permite crear una copia de seguridad del estado de un complemento web para que sea posible restaurar el estado guardado en otro momento. Contiene también los ajustes personales del usuario vinculados al aspecto de la interfaz, como el idioma o el tema.

Si es necesario, para minimizar el menú principal y ver los íconos, puede hacer clic en el corchete angular (<<) en la parte inferior de la pantalla.

Panel superior

El panel superior siempre se muestra en todas las secciones de la consola y no se puede ocultar.

El lado izquierdo del panel contiene el nombre y el logotipo de la aplicación. Si hace clic en el nombre o el logotipo de la aplicación, se abre la página de inicio de Kaspersky Security Center Web Console.

En el lado derecho del panel, se muestran las siguientes configuraciones:

- Ícono de notificación (). Si hace clic en el ícono, se abre un panel con notificaciones.
- El menú de la cuenta. Contiene un vínculo a la Ayuda de Kaspersky Security Center Linux. También le permite cerrar sesión en Kaspersky Security Center Linux, cambiar la contraseña de su cuenta y ver la versión de Kaspersky Security Center Web Console y la lista de complementos web de administración que están instalados.

Área de trabajo

El área de trabajo muestra la información que elige ver en las secciones de la ventana de la interfaz de Kaspersky Security Center Web Console. También contiene elementos de control que puede usar para configurar cómo se muestra la información.

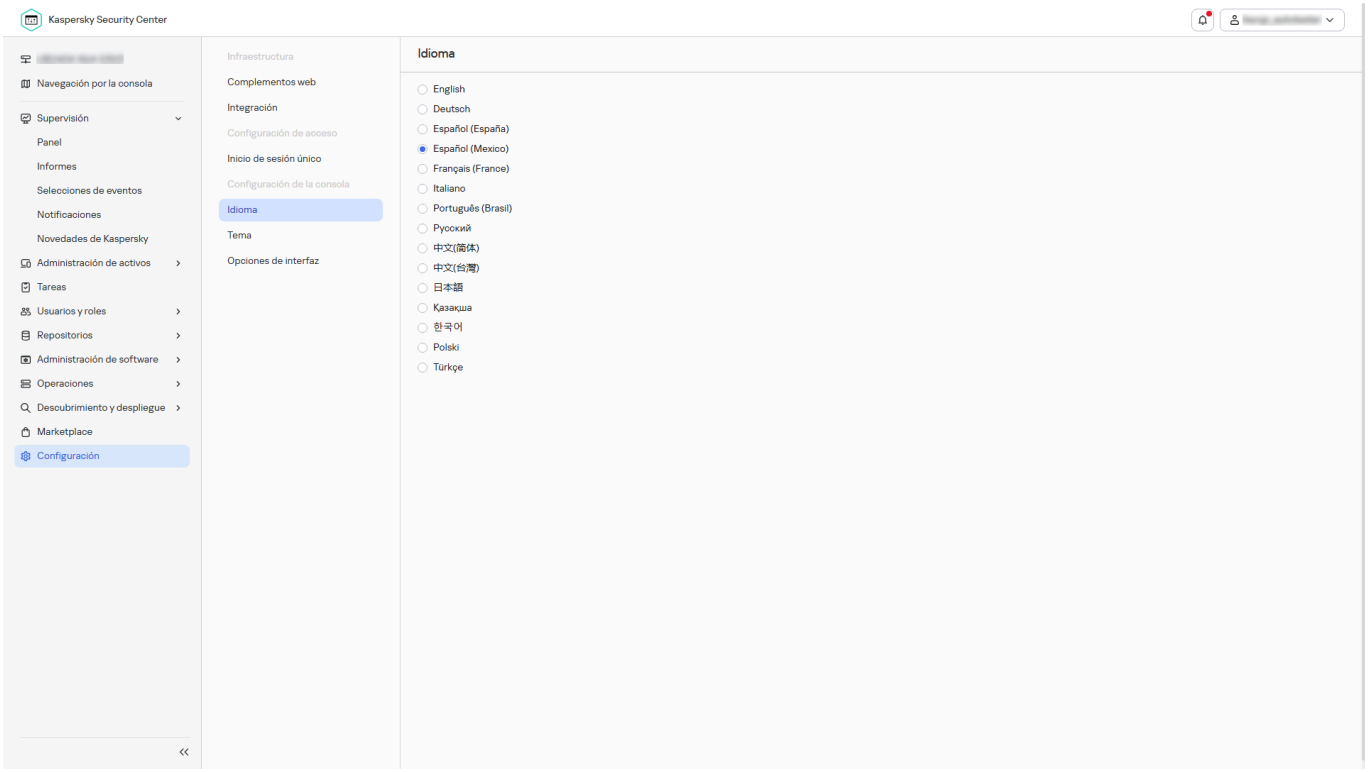
Recomendamos utilizar una sola pestaña del navegador para trabajar con Kaspersky Security Center Web Console.

Cambiar el idioma de la interfaz de Kaspersky Security Center Web Console

Puede seleccionar el idioma de la interfaz de Kaspersky Security Center Web Console.

Para cambiar el idioma de la interfaz, haga lo siguiente:

1. En el menú principal, vaya a **Configuración** → **Idioma**.
2. Seleccione uno de los idiomas de localización admitidos.



Cambiar el idioma de la interfaz de Kaspersky Security Center Web Console

Cambiar la página de inicio de Kaspersky Security Center Web Console

La página de inicio se muestra después de iniciar sesión en Kaspersky Security Center Web Console.

De forma predeterminada, la sección **Navegación por la consola** está configurada como página de inicio. Si es necesario, puede cambiar la página de inicio.

Para cambiar la página de inicio:

1. En la sección **Navegación por la consola**, pase el cursor del mouse sobre el elemento que desea establecer como página de inicio.
2. Cuando aparezca el icono de inicio (), haga clic en él.

   Se cambia la página de inicio. Se muestra un mensaje correspondiente en la pantalla. El elemento seleccionado como página de inicio se marca con el icono de la casa ().

Las secciones **Marketplace** y **Configuración** no se pueden establecer como página de inicio.

Añadir y eliminar marcadores

Puede agregar secciones de uso frecuente de Kaspersky Security Center Web Console a los marcadores para acceder a ellas rápidamente desde la sección **Marcadores** del menú principal.

Si no ha agregado ninguna sección a los marcadores, la sección **Marcadores** no aparece en el menú principal.

Puede añadir a marcadores sólo las secciones que muestran páginas. Por ejemplo, si va a **Administración de activos → Dispositivos administrados**, se abre una página con la tabla de dispositivos, lo que significa que puede agregar esta sección a los marcadores. Si se muestra una ventana o no se muestra ningún elemento después de seleccionar la sección en el menú principal, no puede añadir dicha sección a los marcadores.

Para añadir una sección a los marcadores:

1. En el menú principal, coloque el cursor del mouse sobre la sección que desee anclar.
2. Después del marcador () se muestra el ícono, haga clic en el ícono.

   Esta sección aparece en la sección **Marcadores**.

Para eliminar una sección de los marcadores:

1. En el menú principal, vaya a la sección **Marcadores**.
2. Pase el cursor del ratón sobre la sección que desea desanclar y haga clic en el ícono de desanclar ().

   La sección se elimina de los marcadores.

También puede agregar y eliminar secciones de los marcadores de la sección **Navegación por la consola** situando el cursor del ratón sobre ellas y haciendo clic en el icono del marcador (). El elemento seleccionado se marcará con el icono de marcador ( ) y aparecerá en la sección **Marcadores** del menú principal. Si desea eliminar el elemento de los marcadores, haga clic en el ícono ().

La sección **Marcadores** se muestra solo en el menú principal. Nunca aparece en la página de **Navegación por la consola**.

Eliminación de Kaspersky Security Center Web Console

Es posible que deba eliminar Kaspersky Security Center Web Console Server (también conocido como Kaspersky Security Center Web Console) en los siguientes casos:

- Restauración de datos a partir de una copia de seguridad con otro certificado común.
- Reemisión del certificado común del Servidor de administración.
- Reemplazo del certificado de Web Console con un certificado personalizado.
- Kaspersky Security Center Web Console ya no se usa en un dispositivo.

Para eliminar Kaspersky Security Center Web Console:

1. Dependiendo de su distribución de Linux, ejecute uno de los siguientes comandos:
   - `sudo dnf remove ksc-web-console`
   - `sudo apt remove ksc-web-console`
2. Verifique el resultado mediante el siguiente comando:

   `sudo systemctl status KSC*`

   Kaspersky Security Center Web Console debe estar ausente en el resultado del comando.

Si desea restaurar Kaspersky Security Center Web Console, instálelo en el dispositivo como se describe en el artículo: Instalación de Kaspersky Security Center Web Console.

Asistente de inicio rápido

Kaspersky Security Center Linux le permite ajustar una selección mínima de parámetros de configuración para crear un sistema centralizado de administración para proteger su red contra amenazas de seguridad. La configuración de estos ajustes se realiza a través del asistente de inicio rápido. Cuando el asistente se está ejecutando, le permite hacer los siguientes cambios en la aplicación:

- Agregar archivos de clave o introducir códigos de activación que puedan distribuirse automáticamente a los dispositivos de los grupos de administración.
- Configure el envío por correo electrónico de notificaciones de eventos que ocurren durante el funcionamiento del Servidor de administración y las aplicaciones administradas.
- Crear una directiva de protección para estaciones de trabajo y servidores, además de tareas de análisis antimalware, tareas de descarga de actualizaciones y tareas de copia de seguridad de datos, para el nivel superior de la jerarquía de dispositivos administrados.

  El asistente de inicio rápido únicamente crea directivas para aquellas aplicaciones que no tienen una directiva en su carpeta **Dispositivos administrados**. El asistente de inicio rápido no crea tareas si detecta tareas con el mismo nombre creadas para el nivel más alto de la jerarquía de dispositivos administrados.

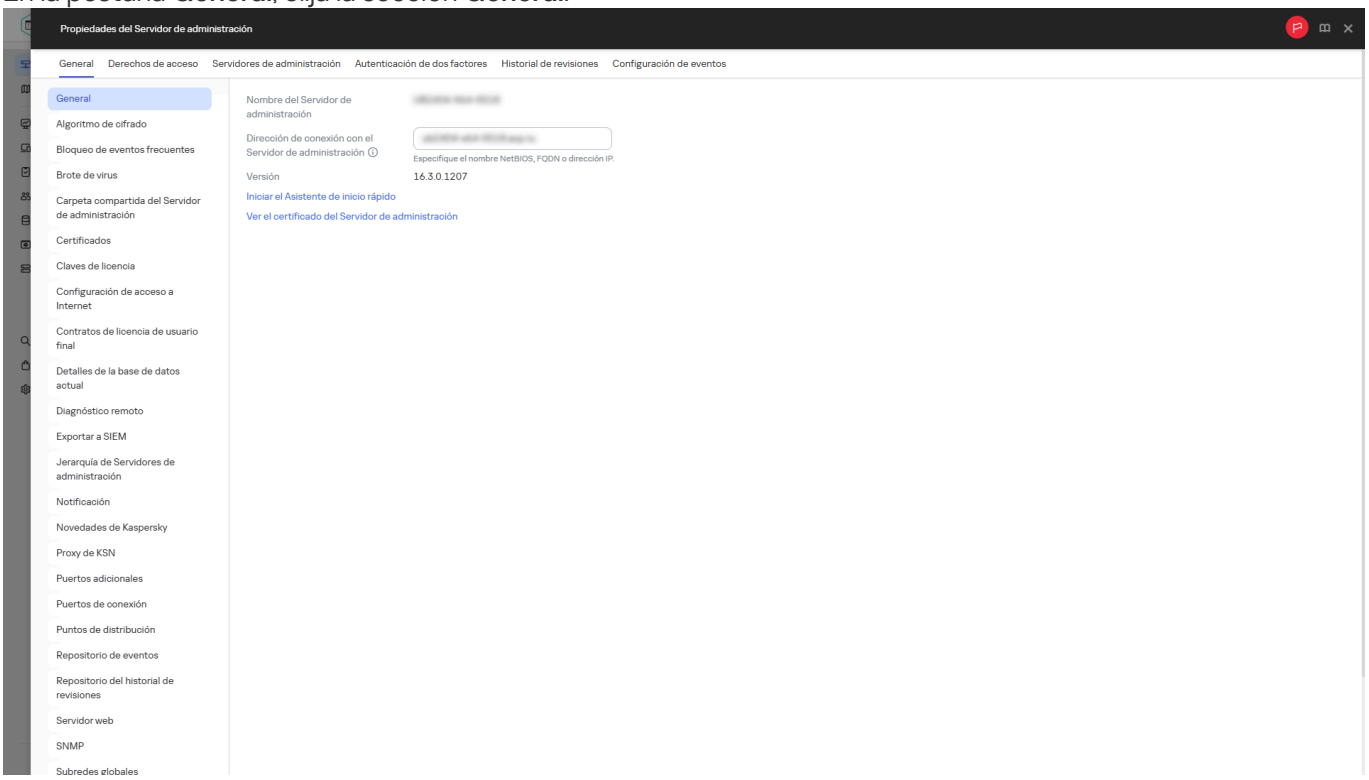
La aplicación le preguntará si desea abrir el asistente de inicio rápido cuando termine con la instalación del Servidor de administración y se conecte a este por primera vez. El asistente de inicio rápido también se puede ejecutar manualmente en cualquier momento.

Para iniciar el asistente de inicio rápido manualmente:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, elija la sección **General**.



Ventana de propiedades del Servidor de administración

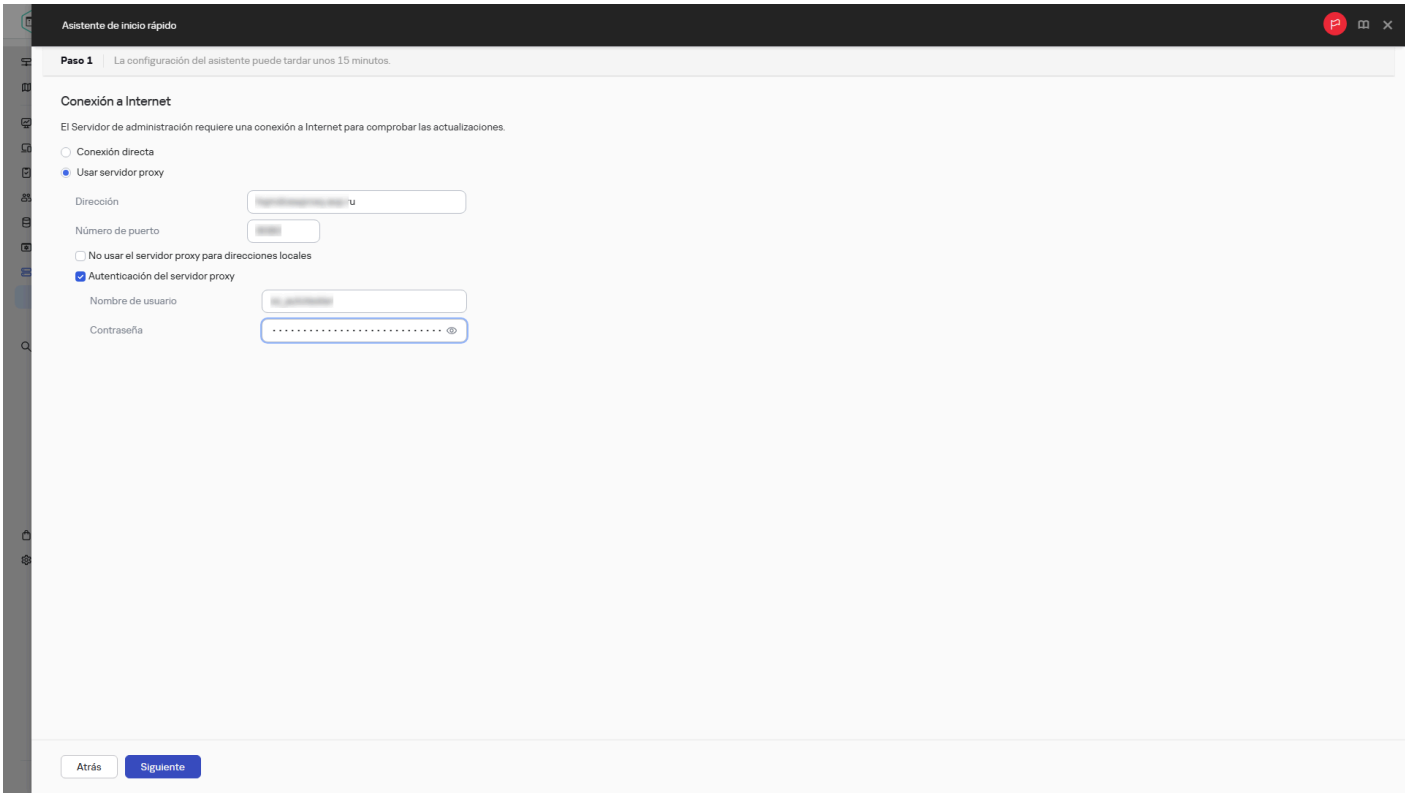
3. Haga clic en **Iniciar el Asistente de inicio rápido**.

   El asistente le ofrecerá realizar la configuración inicial del Servidor de administración. Siga los pasos del asistente. Avance por el asistente utilizando el botón **Siguiente**.

Paso 1. Especificar la configuración de la conexión a Internet

Especifique la configuración de acceso a Internet para el Servidor de administración. Debe configurar el acceso a Internet para usar Kaspersky Security Network y descargar actualizaciones y bases de datos antivirus para Kaspersky Security Center Linux y las aplicaciones de Kaspersky administradas.

Active la opción **Usar servidor proxy** si quiere usar un servidor proxy al conectarse a Internet. Si activa esta opción, los campos estarán disponibles para ingresar ajustes. Deberá introducir los siguientes valores de conexión del servidor proxy:



Configuración de la conexión a Internet

- **Dirección**

  Dirección del servidor proxy usado para conectar Kaspersky Security Center Linux a Internet.

- **Número de puerto**

  Número del puerto a través del cual se establecerá la conexión proxy de Kaspersky Security Center Linux.

- **No usar el servidor proxy para direcciones locales**

  Ningún servidor proxy se usará para conectarse a los dispositivos en la red local.

- **Autenticación del servidor proxy**

  Si se selecciona esta casilla, en los campos de entrada se podrán especificar las credenciales para la autenticación del servidor proxy.

  Este campo de entrada está disponible cuando la casilla **Usar servidor proxy** está desmarcada.

- **Nombre de usuario**

  Cuenta de usuario con la que se establece la conexión al servidor proxy (este campo está disponible si se selecciona la casilla **Autenticación del servidor proxy**).

- **Contraseña**

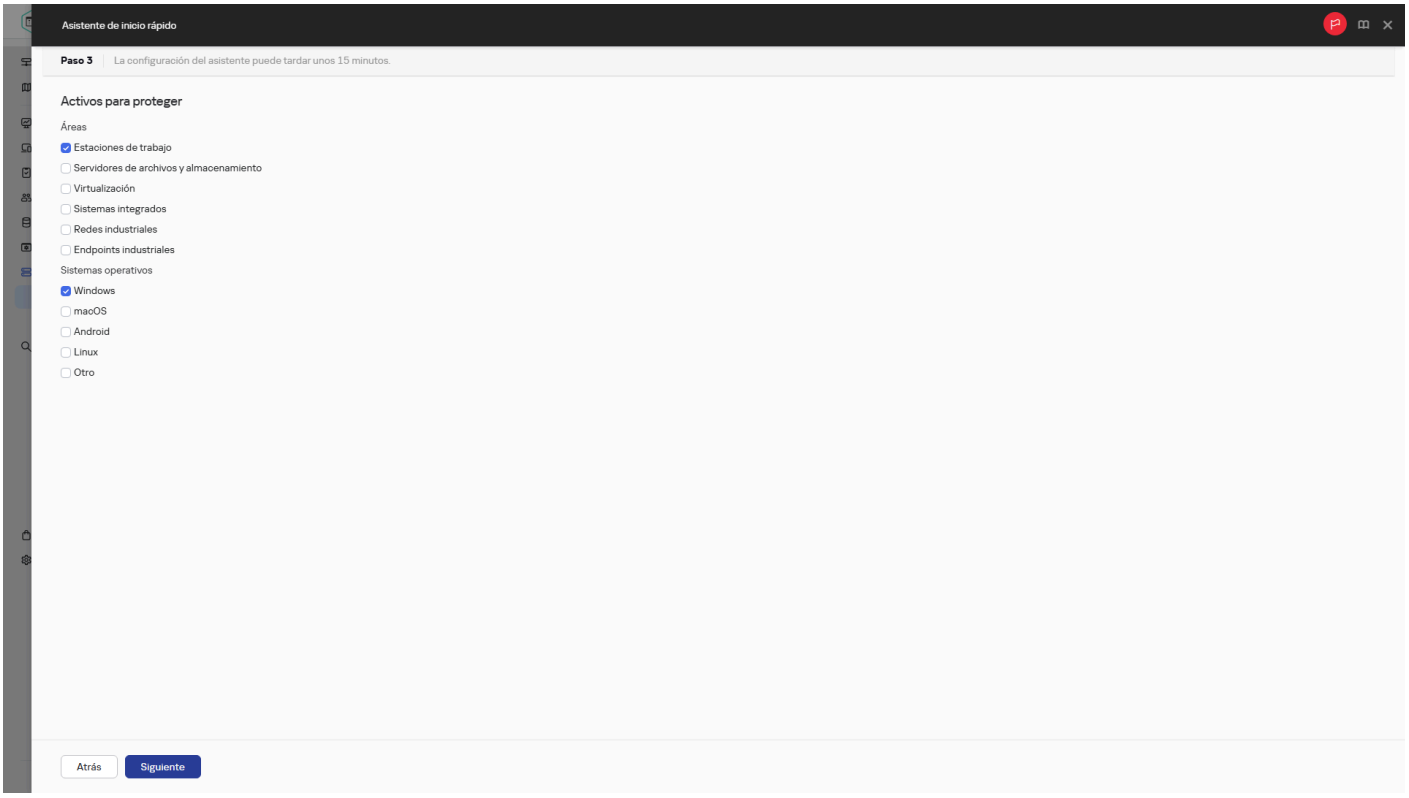
  Contraseña que especifica el usuario con cuya cuenta se establece la conexión al servidor proxy (este campo está disponible si se selecciona la casilla **Autenticación del servidor proxy**).

  Para ver la contraseña indicada, mantenga presionado el botón **Mostrar** durante la cantidad de tiempo que sea necesario.

Puede configurar el acceso a Internet más tarde, sin usar el asistente de inicio rápido.

Paso 2. Descargando actualizaciones requeridas

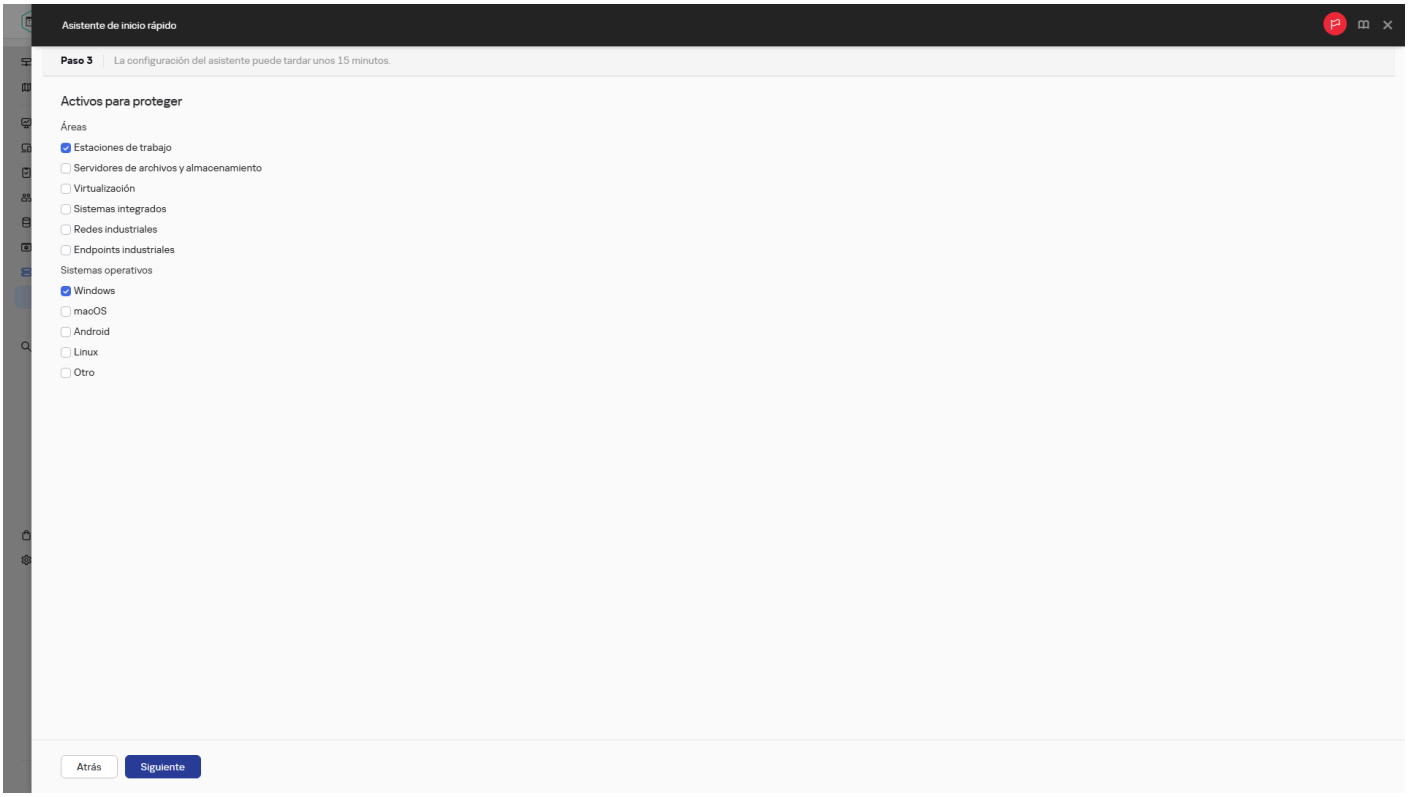
Las actualizaciones necesarias se descargan de los servidores de Kaspersky automáticamente.



Descargando actualizaciones requeridas

Paso 3. Selección de los activos para asegurar

Seleccione las áreas que desee proteger y los sistemas operativos que estén presentes en su red. Cuando selecciona estas opciones, especifica los filtros para los complementos de administración de aplicaciones y los paquetes de distribución en los servidores de Kaspersky que puede descargar para instalar en los dispositivos cliente en su red.



Selección de los activos para asegurar

Seleccione las opciones:

- **Áreas**

  Puede seleccionar las siguientes clases de entornos:

  - **Estaciones de trabajo**
  - **Servidores de archivos y almacenamiento**
  - **Virtualización**
  - **Sistemas integrados**
  - **Redes industriales**
  - **Endpoints industriales**

- **Sistemas operativos**

  Puede seleccionar las siguientes plataformas:

  - Microsoft Windows
  - macOS
  - Android
  - Linux
  - Otro

  Para obtener información sobre los sistemas operativos compatibles, consulte la sección Requisitos de hardware y software para Kaspersky Security Center Web Console.

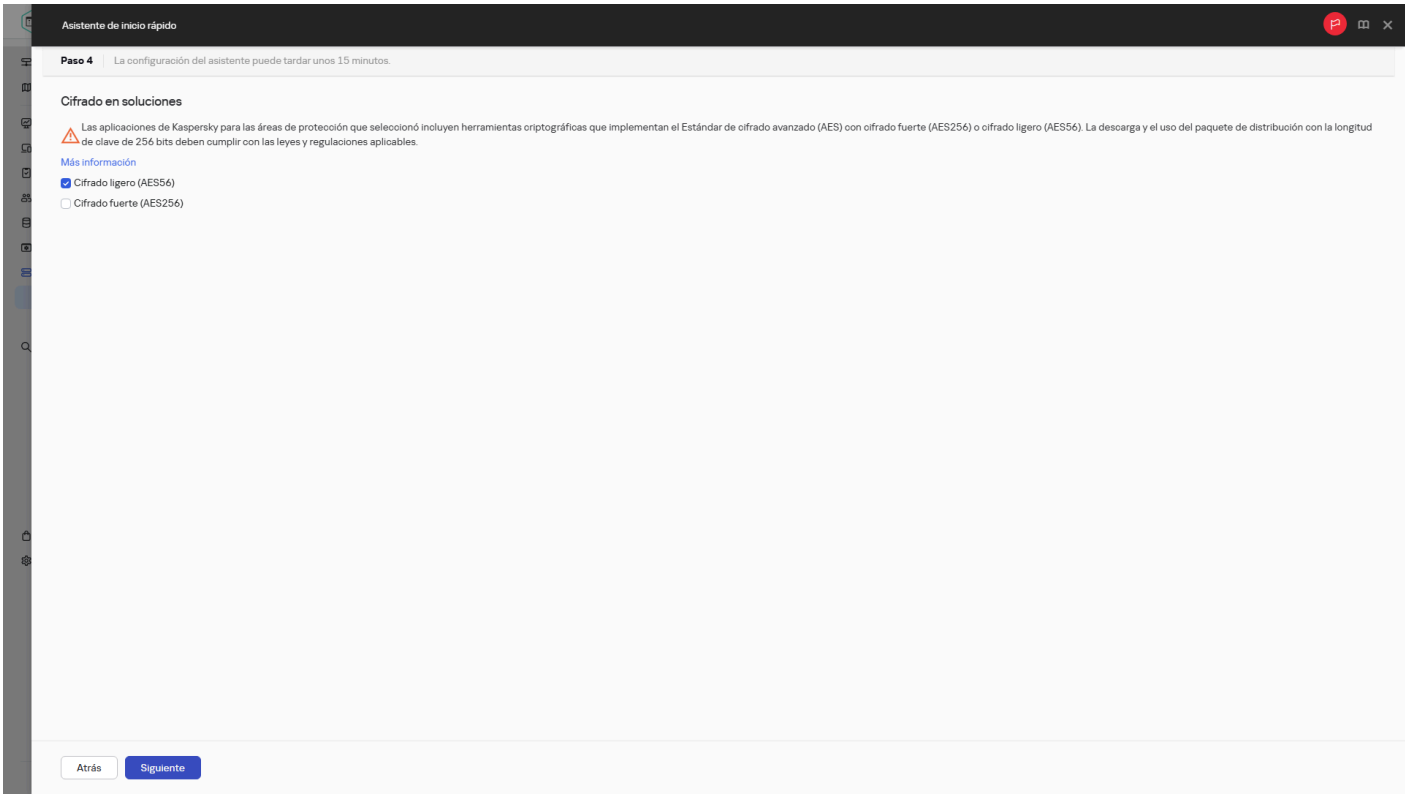
Puede seleccionar los paquetes de aplicaciones de Kaspersky de la lista de paquetes disponibles más adelante, sin usar el asistente de inicio rápido. Para ayudarse a encontrar los paquetes necesarios, puede filtrar la lista de paquetes disponibles utilizando una serie de criterios.

Paso 4. Seleccionar el cifrado en las soluciones

La ventana **Cifrado en soluciones** aparecerá únicamente si ha seleccionado **Estaciones de trabajo** como área de protección.

Kaspersky Endpoint Security para Windows incluye herramientas para cifrar la información almacenada en dispositivos cliente con Windows. Estas herramientas implementan el estándar de cifrado avanzado AES, con una longitud de clave de 256 o 56 bits.

El paquete de distribución con una longitud de clave de 256 bits solo puede descargarse y utilizarse si lo permiten las leyes y normativas en vigor. Para descargar un paquete de distribución de Kaspersky Endpoint Security para Windows que se adecue a las necesidades de su organización, consulte la legislación del país en el que se encuentren los dispositivos cliente de su organización.



Seleccionar el cifrado en las soluciones

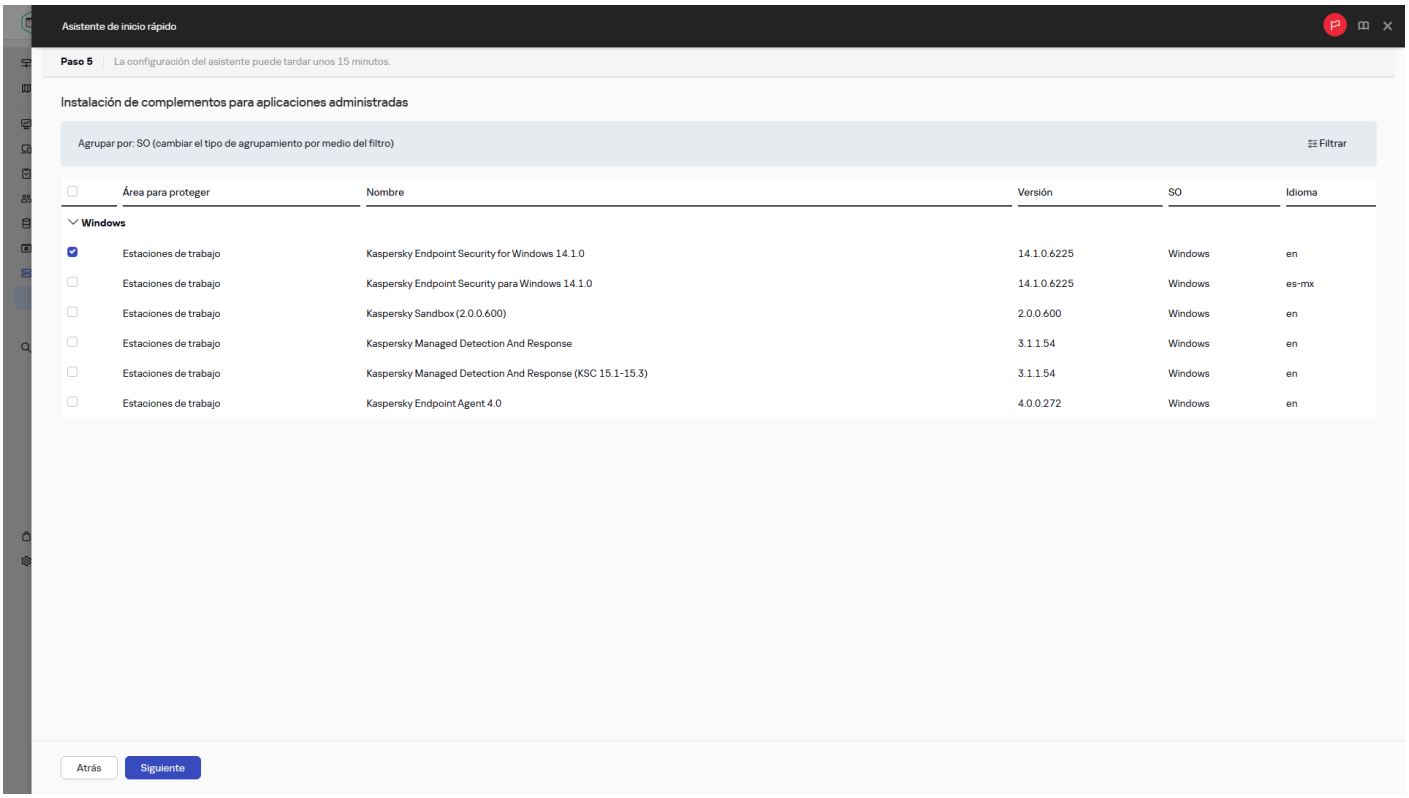
En la ventana **Cifrado en soluciones**, seleccione uno de los siguientes tipos de cifrado:

- Cifrado ligero. Este tipo de cifrado utiliza una longitud de clave de 56 bits.
- Cifrado fuerte. Este tipo de cifrado utiliza una longitud de clave de 256 bits.

Puede seleccionar el paquete de distribución de Kaspersky Endpoint Security para Windows que corresponda al tipo de cifrado requerido más adelante, por fuera del asistente de inicio rápido.

Paso 5. Configurar la instalación de los complementos para las aplicaciones administradas

Seleccione los complementos para aplicaciones administradas que se instalarán. Se muestra una lista de complementos ubicados en los servidores de Kaspersky. La lista tendrá aplicado un filtro basado en las opciones seleccionadas en el paso anterior del asistente. Por defecto, una lista completa incluye complementos de todos los idiomas. Para mostrar solo el complemento de un idioma específico, utilice el filtro.



Instalación de complementos para aplicaciones administradas

La lista de complementos incluye las siguientes columnas:

- **Área para proteger**

  Las áreas seleccionadas para protección se muestran en esta columna.

- **Tipo**

  Los tipos de complementos se muestran en esta columna.

- **Nombre**

  Estarán seleccionados los complementos que dependan de los componentes y las plataformas que haya seleccionado en el paso anterior.

- **Versión**

  La lista incluye complementos de todas las versiones colocadas en los servidores de Kaspersky. De forma predeterminada, se seleccionan los complementos de las últimas versiones.

- **Versión más reciente**

  Esta columna indica si la versión del complemento es la más reciente. Si se muestra el valor **true**, el complemento correspondiente tiene la versión más reciente instalada. Si se muestra el valor **false**, el complemento correspondiente tiene una versión posterior.

- **SO**

  Esta columna muestra los sistemas operativos de los complementos.

- **Idioma**

  De forma predeterminada, el idioma de localización de un complemento se define basándose en el idioma de Kaspersky Security Center Linux seleccionado durante la instalación. Puede especificar otros idiomas en la lista desplegable **Mostrar el idioma de localización de la Consola de administración o**.

Una vez seleccionados los complementos, haga clic en **Siguiente** para iniciar la instalación.

Puede instalar complementos de administración para aplicaciones Kaspersky manualmente, por separado del asistente de inicio rápido.

El asistente de inicio rápido instala automáticamente los complementos seleccionados. Para instalar algunos complementos, debe aceptar los términos del EULA. Lea el texto de EULA que se muestra, seleccione la casilla de verificación **Acepto participar en Kaspersky Security Network** y haga clic en el botón **Instalar**. Si no acepta los términos del EULA, el complemento no se instala.

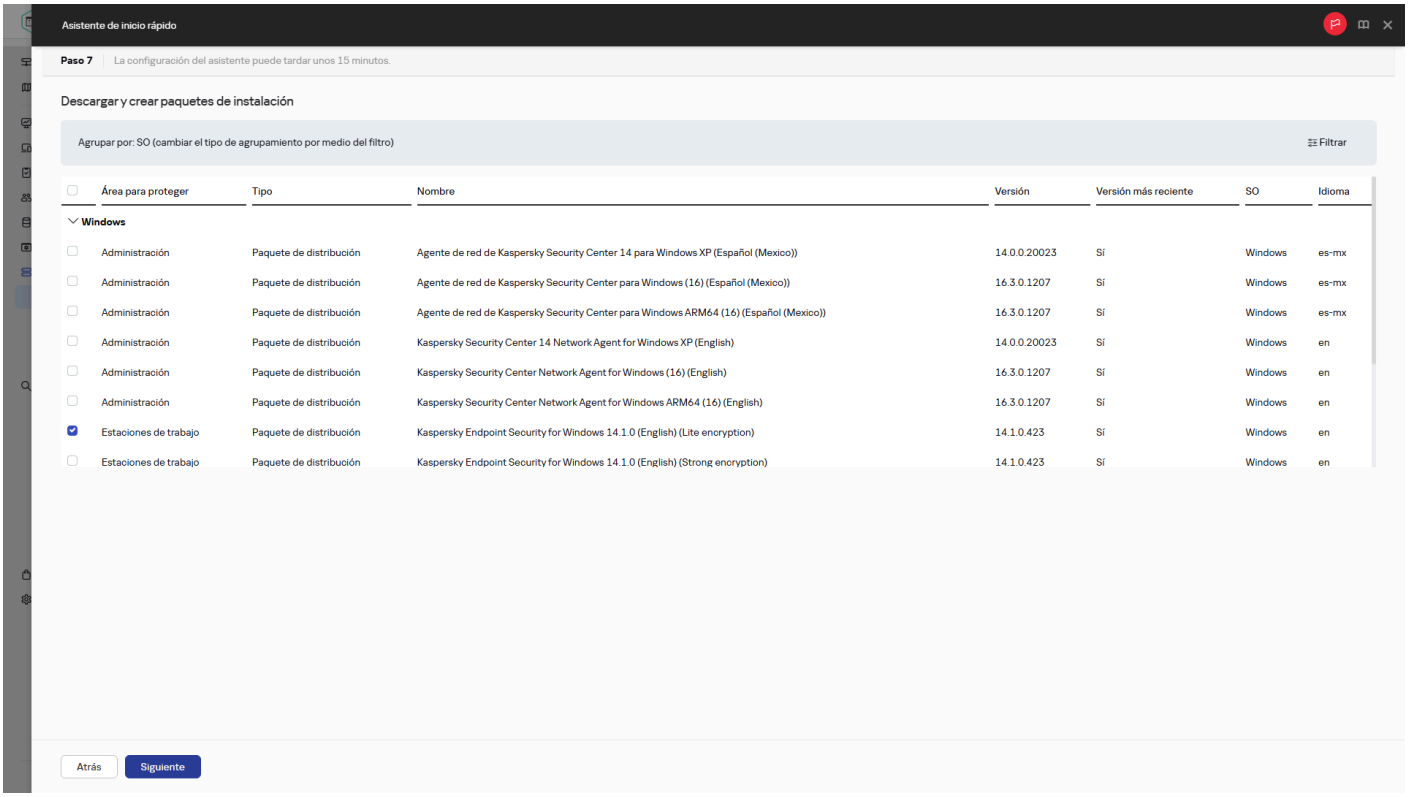
Cuando todos los complementos seleccionados se hayan instalado, el asistente de inicio rápido avanzará automáticamente al paso siguiente.

Paso 6. Descarga de paquetes de distribución y creación de paquetes de instalación

Seleccione los paquetes de distribución que desea descargar.

Los paquetes de distribución de las aplicaciones administradas pueden requerir que la versión de Kaspersky Security Center Linux instalada no sea anterior a una versión en particular.

Después de seleccionar un tipo de cifrado para Kaspersky Endpoint Security para Windows, se muestra una lista de paquetes de distribución de ambos tipos de cifrado. El paquete de distribución que corresponda al tipo de cifrado elegido estará seleccionado en dicha lista. Puede seleccionar los paquetes de distribución de cualquier tipo de cifrado. El idioma del paquete de distribución se corresponde con el idioma de Kaspersky Security Center Linux. Cuando no existe un paquete de distribución en el idioma de Kaspersky Security Center Linux, se selecciona el paquete de distribución en inglés.



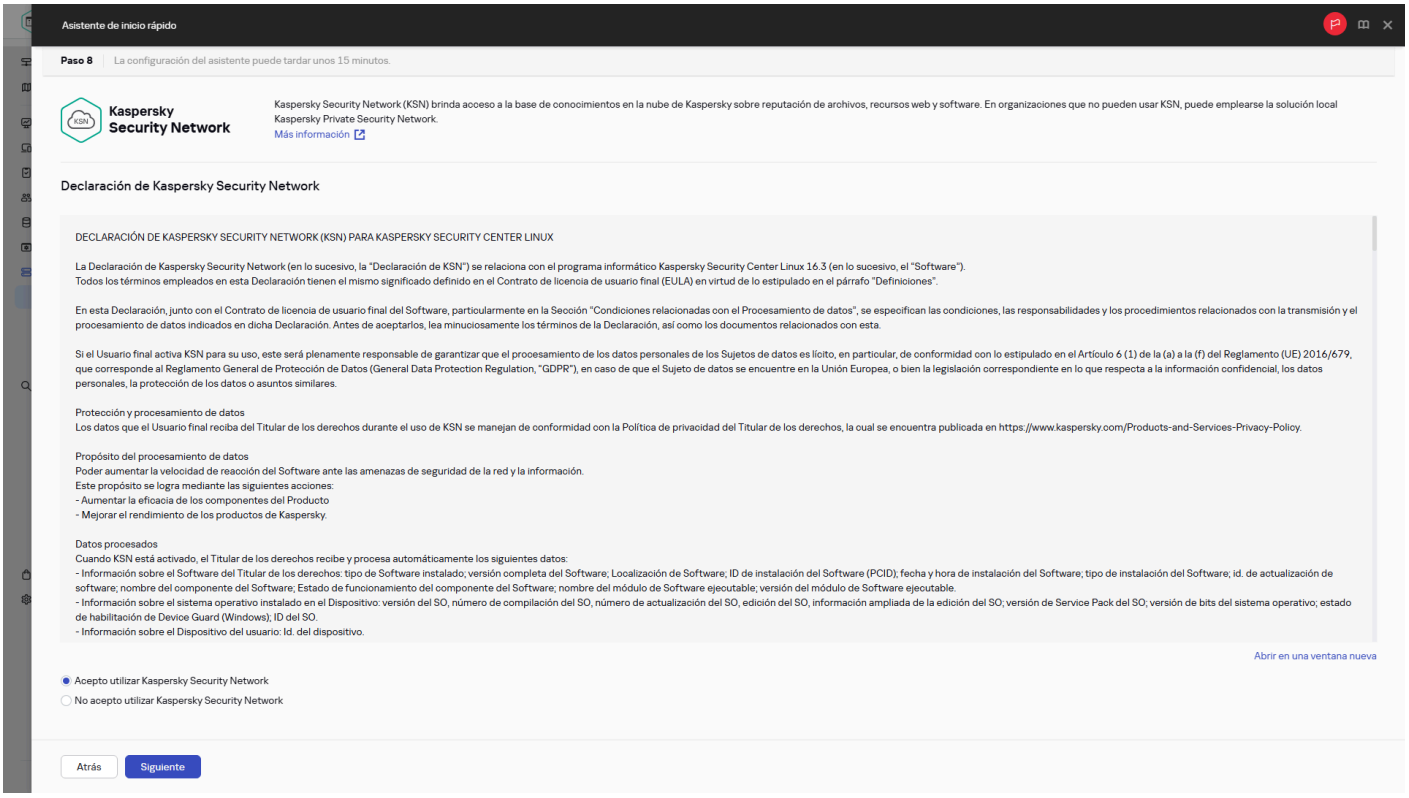
Descarga de paquetes de distribución y creación de paquetes de instalación

Para finalizar la descarga de algunos paquetes de distribución, debe aceptar el EULA. Cuando hace clic en el botón **Aceptar**, se muestra el texto de EULA. Para avanzar al siguiente paso del asistente, debe aceptar los términos y condiciones del EULA y los términos y condiciones de la Política de privacidad de Kaspersky. Si no acepta los términos y condiciones, se cancela la descarga del paquete.

Después de haber aceptado los términos y condiciones del EULA y los términos y condiciones de la Política de privacidad de Kaspersky, la descarga de los paquetes de distribución continúa. Más tarde, podrá usar paquetes de instalación para desplegar las aplicaciones de Kaspersky a los dispositivos cliente.

Paso 7. Configurar Kaspersky Security Network

Configure la transmisión de información sobre las operaciones de Kaspersky Security Center Linux a la base de conocimientos Kaspersky Security Network.



Configurar Kaspersky Security Network

Seleccione una de las siguientes opciones:

- **Acepto participar en Kaspersky Security Network**

  Kaspersky Security Center Linux y las aplicaciones administradas instaladas en los dispositivos cliente transferirán automáticamente sus detalles operativos a Kaspersky Security Network. Participar en Kaspersky Security Network permite que las bases de datos con información sobre virus y otros riesgos se actualicen más rápidamente, lo cual se traduce en una mayor velocidad de respuesta ante amenazas a la seguridad emergentes.

- **No acepto participar en Kaspersky Security Network**

  Kaspersky Security Center Linux y las aplicaciones administradas no proporcionarán información a Kaspersky Security Network.

  Si selecciona esta opción, se deshabilitará el uso de Kaspersky Security Network.

Puede configurar el acceso a Kaspersky Security Network (KSN) más tarde, por separado del asistente de inicio rápido.

Paso 8. Selección del método de activación de la aplicación

Seleccione una de las siguientes opciones de activación de Kaspersky Security Center Linux:

- **Introducir su código de activación**

  Un *código de activación* es una secuencia única de veinte letras latinas y números. Se ingresa un código de activación para agregar una clave que activa Kaspersky Security Center Linux. Recibe el código de activación en la dirección de correo electrónico que especificó después de comprar Kaspersky Security Center.

  Para activar la aplicación mediante un código de activación, necesita acceso a Internet para conectarse con los servidores de activación de Kaspersky.

  Si seleccionó esta opción de activación, puede habilitar la opción **Distribuir clave de licencia automáticamente a los dispositivos administrados**.

  Si esta opción está habilitada, la clave de licencia se distribuirá automáticamente a los dispositivos administrados.

  Si esta opción está deshabilitada, puede implementar la clave de licencia en los dispositivos administrados más adelante en la sección **Operaciones** → **Licencias** → **Licencias** del menú principal.

- **Especificando un archivo de clave**

  El *archivo de clave* es un archivo con la extensión .key que le proporciona Kaspersky. Los archivos de clave se usan para agregar una clave que activa la aplicación.

  Recibe el archivo de clave en la dirección de correo electrónico que especificó después de comprar Kaspersky Security Center.

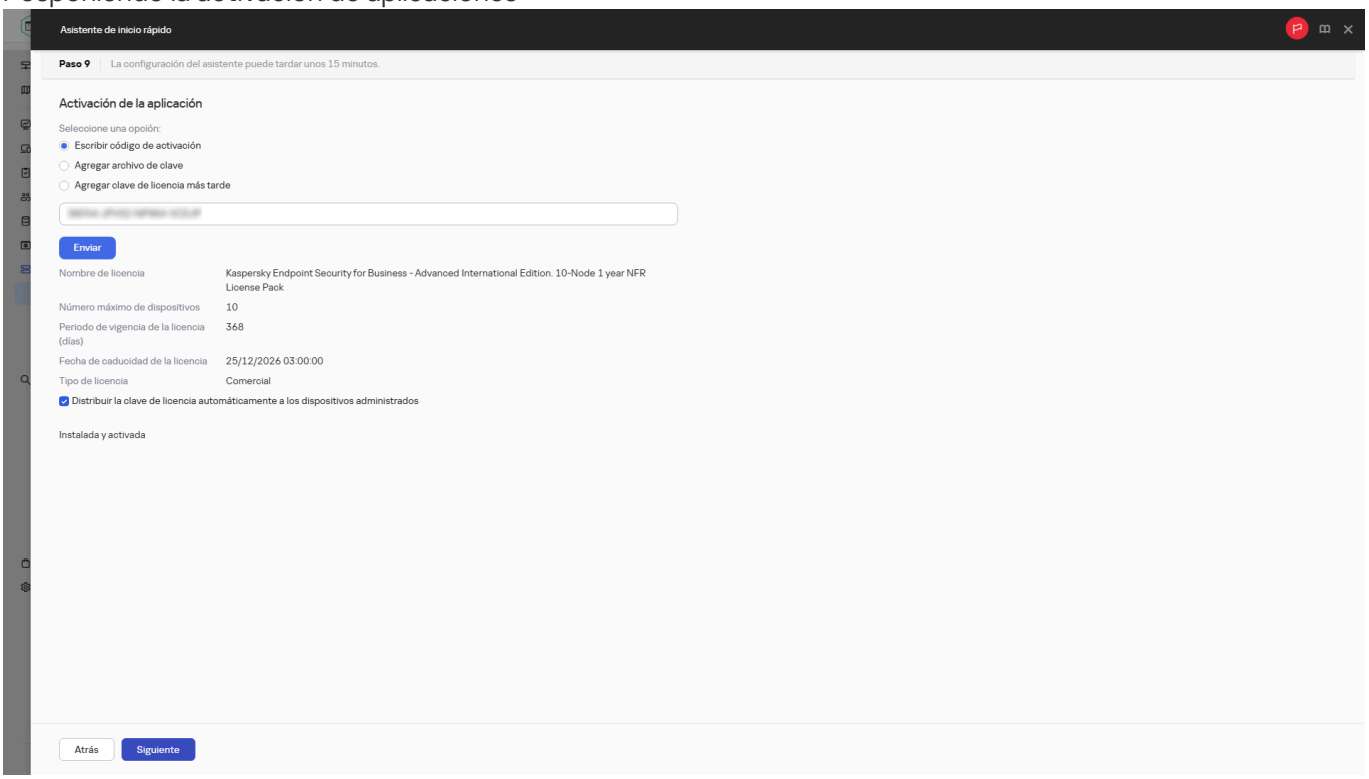
  No es necesario conectarse a los servidores de activación de Kaspersky para activar la aplicación con un archivo de clave.

  Si seleccionó esta opción de activación, puede habilitar la opción **Distribuir clave de licencia automáticamente a los dispositivos administrados**.

  Si esta opción está habilitada, la clave de licencia se distribuirá automáticamente a los dispositivos administrados.

  Si esta opción está deshabilitada, puede implementar la clave de licencia en los dispositivos administrados más adelante en la sección **Operaciones** → **Licencias** → **Licencias** del menú principal.

- Posponiendo la activación de aplicaciones



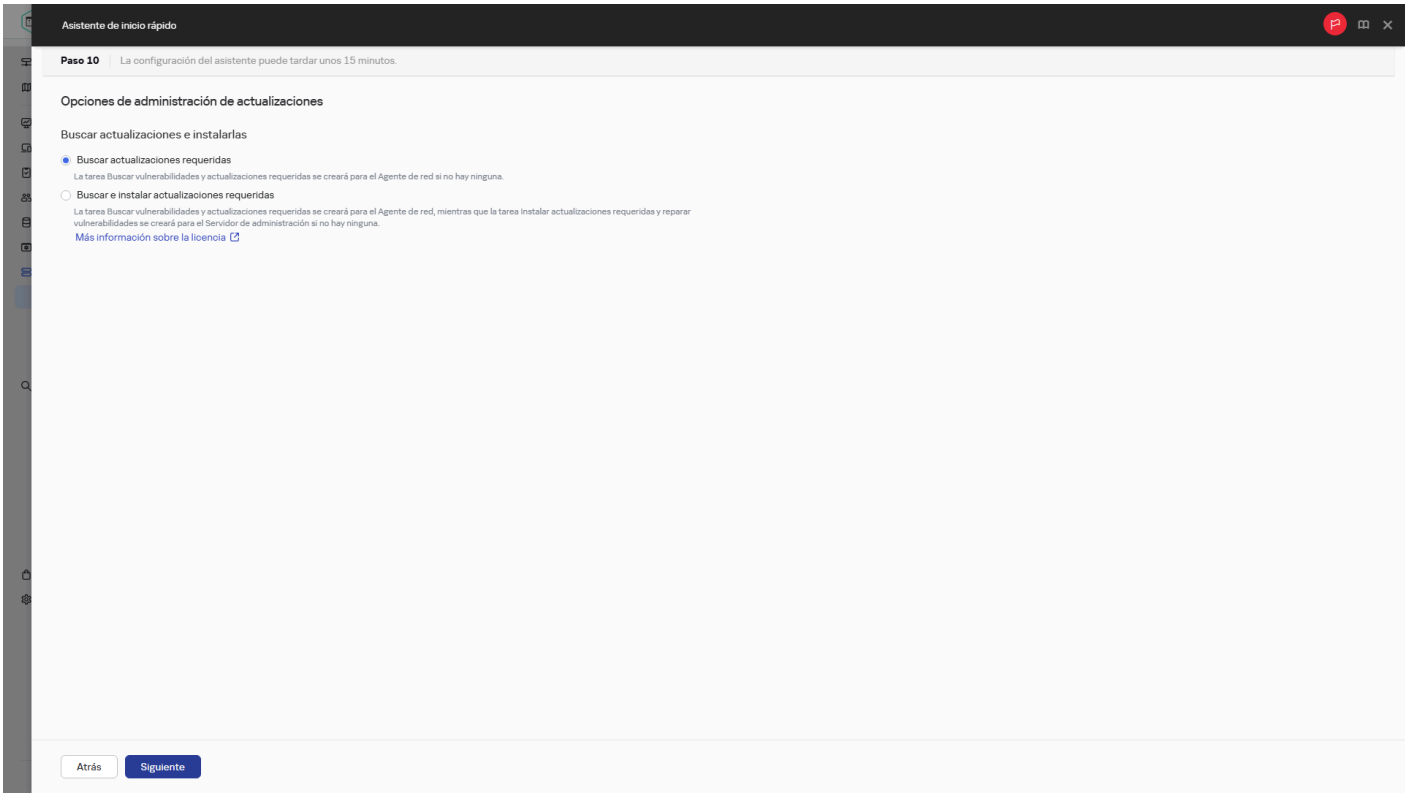
Selección del método de activación de la aplicación

Si decide posponer la activación de la aplicación, puede agregar una clave de licencia más adelante en cualquier momento **Operaciones** → **Licencias**.

Cuando trabaje con Kaspersky Security Center desplegado desde una AMI paga o para un SKU que se factura mensualmente según el uso, no puede especificar un archivo de clave o ingresar un código.

Paso 9. Especificar la configuración de administración de las actualizaciones de terceros

El paso **Opciones de administración de actualizaciones** del asistente de inicio rápido no se muestra si no se cuenta con una licencia de Administración de vulnerabilidades y parches y la tarea *Buscar vulnerabilidades y actualizaciones requeridas* ya existe.



Configuración de administración de las actualizaciones de terceros

Para las actualizaciones de software de terceros, seleccione una de las siguientes opciones:

- **Buscar actualizaciones requeridas**

  La tarea *Buscar vulnerabilidades y actualizaciones requeridas* se creará automáticamente si no existe.

  Esta opción está seleccionada de forma predeterminada.

- **Buscar e instalar actualizaciones requeridas**

  Las tareas *Buscar vulnerabilidades y actualizaciones requeridas* e *Instalar actualizaciones requeridas y reparar vulnerabilidades* se crearán automáticamente si no existen.

  Esta opción solo está disponible si se cuenta con una licencia de Administración de vulnerabilidades y parches.

En el caso de las actualizaciones de Windows Update, seleccione la opción **Usar los orígenes de actualizaciones definidos en la directiva del dominio.**

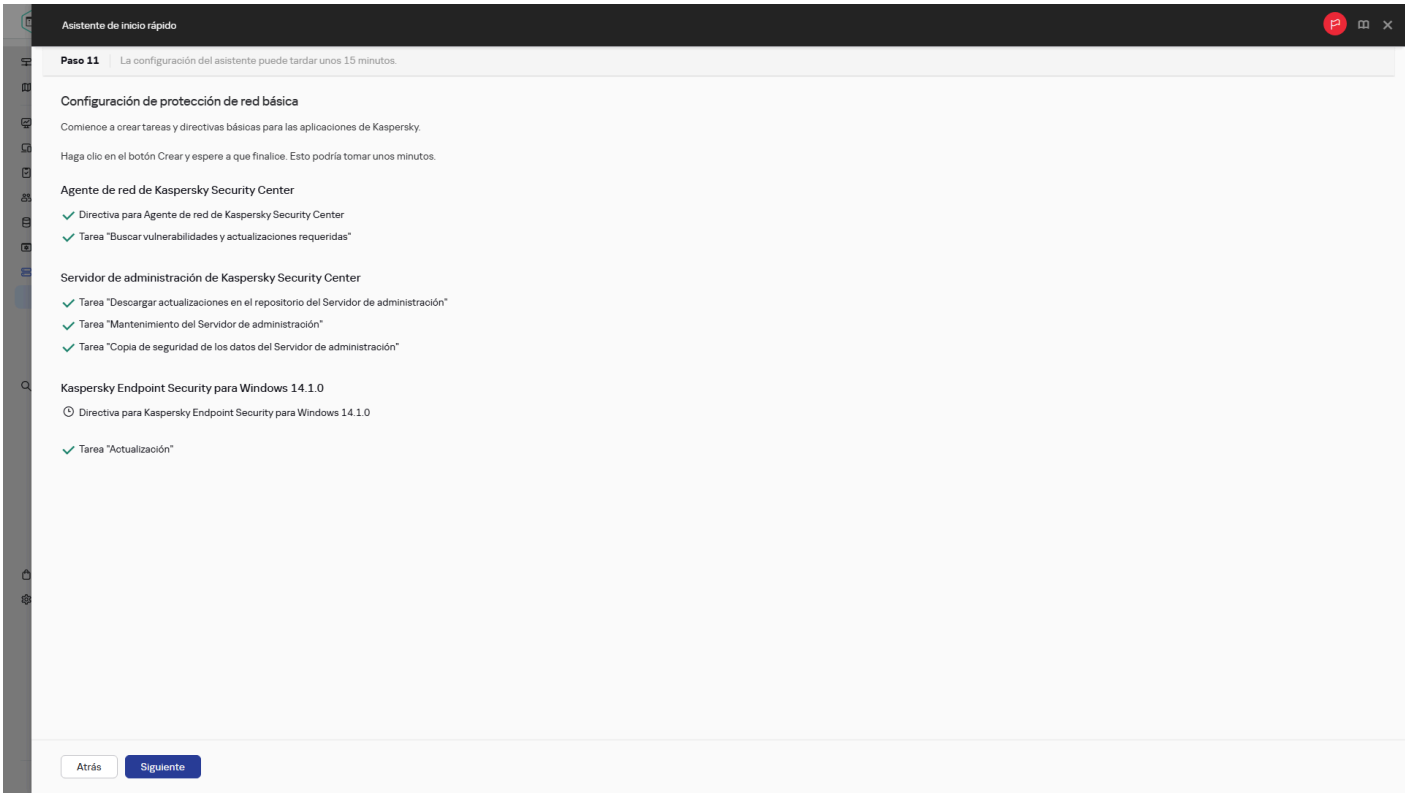
Los dispositivos cliente descargarán las actualizaciones de Windows Update de conformidad con la configuración de la directiva de su dominio. La directiva del Agente de red se creará automáticamente en caso de que no exista.

Puede crear las tareas *Buscar vulnerabilidades y actualizaciones requeridas* e *Instalar actualizaciones requeridas y reparar vulnerabilidades* por separado desde el asistente de inicio rápido.

Paso 10. Creación de una configuración básica de protección de la red

Puede ver la lista de directivas y tareas creadas.

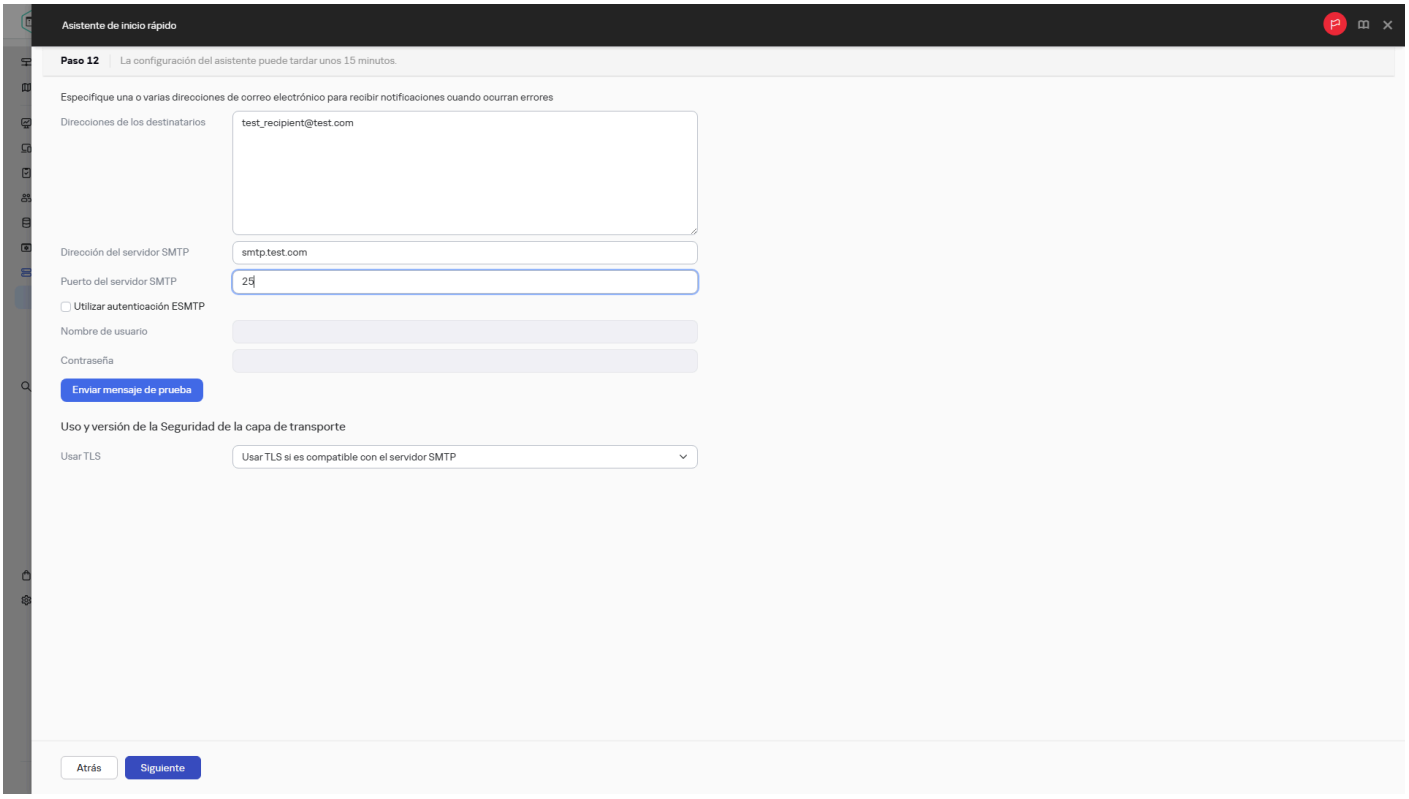
Espere a que terminen de crearse las tareas y directivas antes de avanzar al siguiente paso del asistente.



Creación de una configuración básica de protección de la red

Paso 11. Configuración de notificaciones por correo electrónico

Configure la entrega de notificaciones sobre eventos registrados durante el funcionamiento de aplicaciones Kaspersky en los dispositivos cliente. Estos parámetros servirán de configuración predeterminada de las directivas de la aplicación.



Configuración de notificaciones por correo electrónico

Para configurar la entrega de notificaciones sobre eventos que ocurren en Aplicaciones de Kaspersky, use la configuración siguiente:

- **Direcciones de los destinatarios**

  Las direcciones de correo electrónico de usuarios a quien la aplicación enviará notificaciones. Puede especificar una o más direcciones. Si ingresa más de una dirección, sepárelas con un punto y coma.

- **Dirección del servidor SMTP**

  La dirección o direcciones de los servidores de correo de su organización.

  Si ingresa más de una dirección, sepárelas con un punto y coma. Puede utilizar los siguientes parámetros:

  - Dirección IPv4 o IPv6
  - Nombre DNS del servidor SMTP

- **Puerto del servidor SMTP**

  Número del puerto de comunicación del servidor SMTP. Si utiliza varios servidores SMTP, la conexión con ellos se establecerá a través del puerto de comunicación especificado. El número de puerto predeterminado es 25.

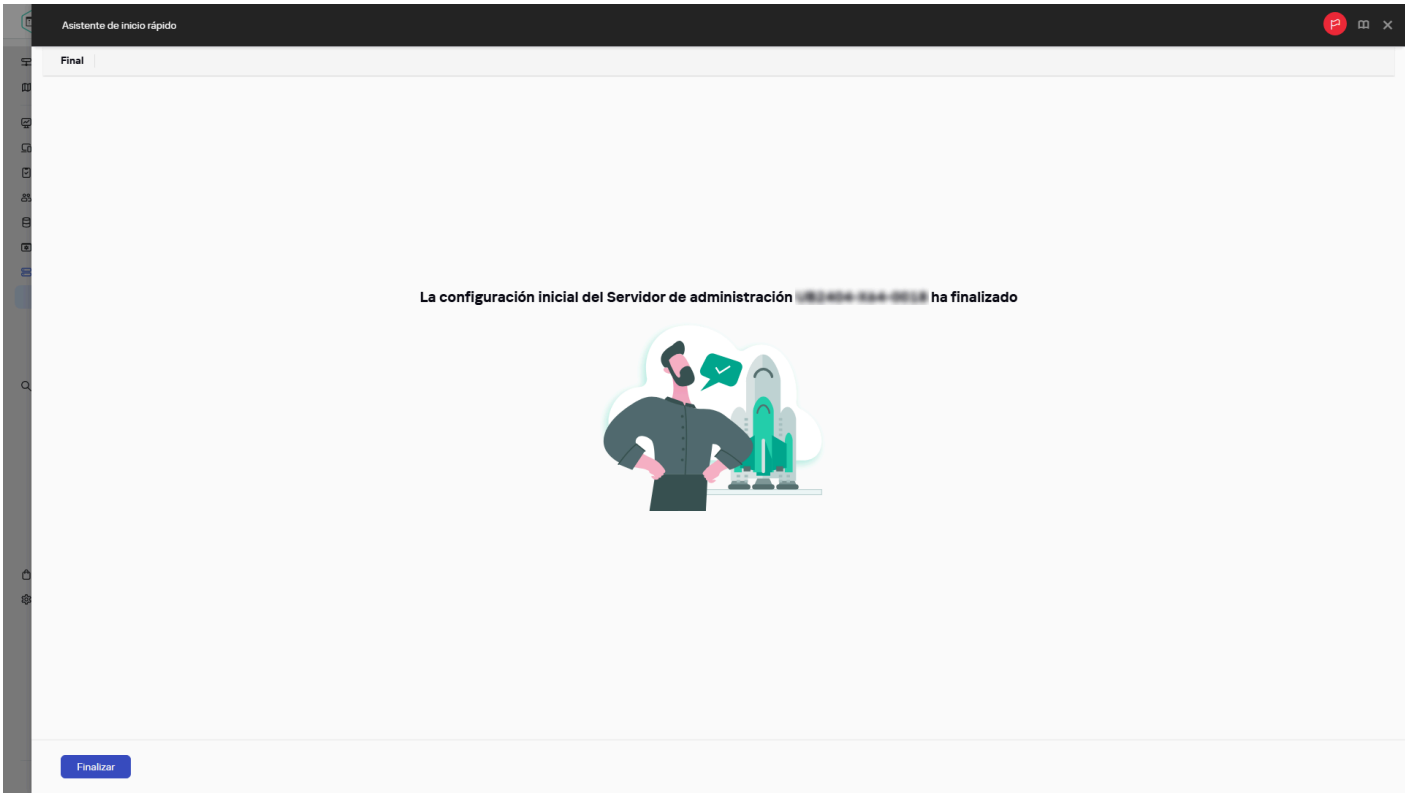
- **Utilizar autenticación ESMTP**

  Habilita la compatibilidad con la autenticación ESMTP. Cuando la casilla está seleccionada, en los campos **Nombre de usuario** y **Contraseña**, puede especificar la configuración de la autorización de ESMTP. Esta casilla está desactivada por defecto.

Puede probar la configuración de la notificación por correo electrónico nueva haciendo clic en el botón **Enviar mensaje de prueba**.

Paso 12. Cierre del asistente de inicio rápido

Para cerrar el asistente, haga clic en el botón **Finalizar**.



Paso final del Asistente de inicio rápido

Una vez que termine con el asistente de inicio rápido, puede ejecutar el Asistente de despliegue de la protección para instalar automáticamente las aplicaciones antivirus o el Agente de red en los dispositivos de la red.

Asistente de despliegue de la protección

Puede usar el Asistente de despliegue de la protección para instalar aplicaciones de Kaspersky. El Asistente de despliegue de la protección permite la instalación remota de aplicaciones mediante paquetes de instalación creados previamente o directamente desde un paquete de distribución.

El Asistente de despliegue de la protección realiza las siguientes acciones:

- Descarga un paquete de instalación para instalar la aplicación deseada (si el paquete no se creó de antemano). El paquete de instalación se encuentra en **Administración de software** → **Paquetes de instalación**. El paquete puede usarse para instalar la aplicación en otro momento.

- Crea y ejecuta una tarea de instalación remota para dispositivos específicos o para un grupo de administración. La nueva tarea de instalación remota se agrega a la sección **Tareas**. Podrá iniciar la tarea manualmente cuando lo desee. El tipo de tarea es **Instalar aplicación de forma remota**.

Si desea instalar el Agente de red en dispositivos con el sistema operativo SUSE Linux Enterprise Server 15, primero, instale el paquete insserv-compat para configurar el Agente de red.

Paso 1. Iniciar el Asistente de despliegue de la protección

El Asistente de despliegue de la protección puede ejecutarse manualmente en cualquier momento.

Para iniciar manualmente el Asistente de despliegue de la protección,

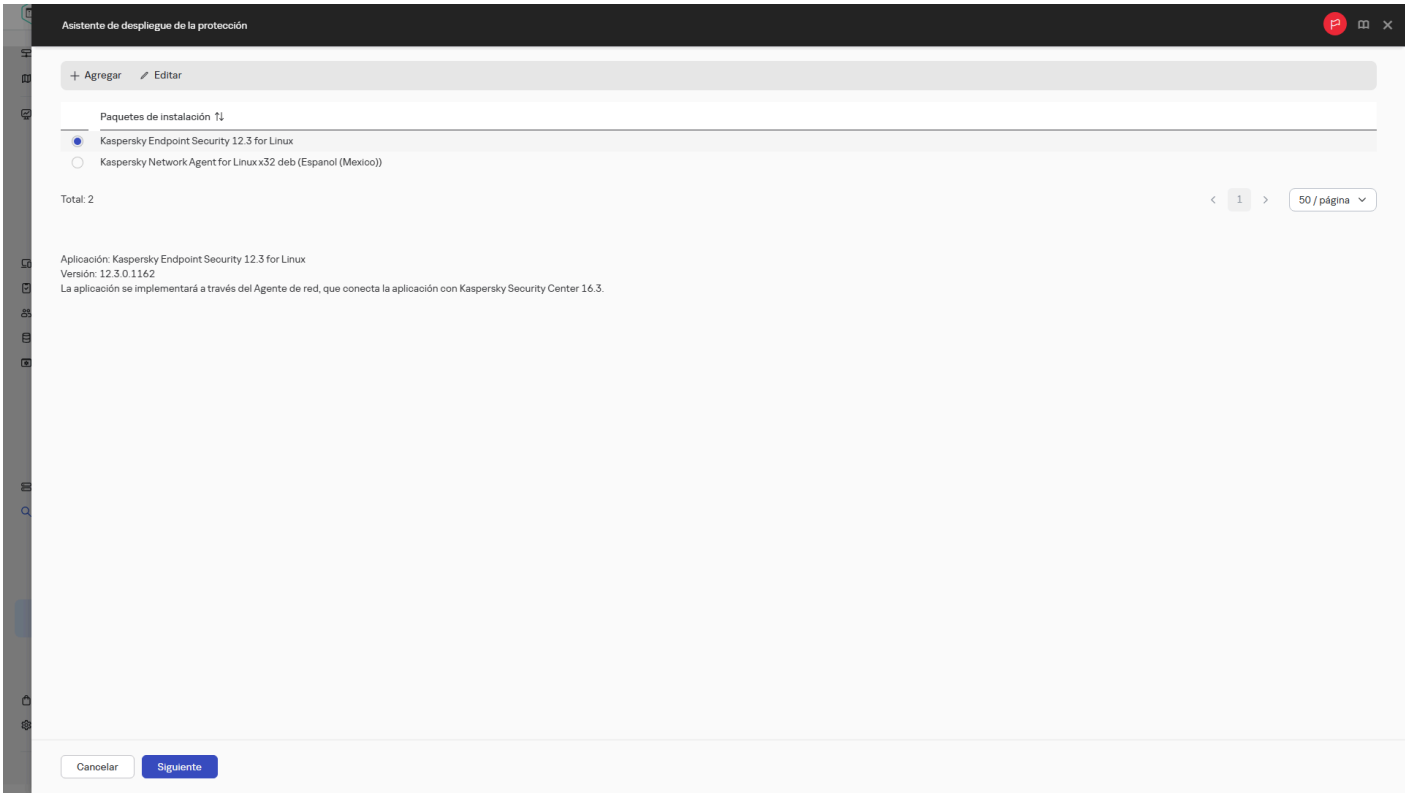
En el menú principal, vaya a **Descubrimiento y despliegue** → **Despliegue y asignación** → **Asistente de despliegue de la protección**.

Se abre el Asistente de despliegue de la protección. Avance por el asistente utilizando el botón **Siguiente**.

Paso 2. Seleccionar el paquete de instalación

Seleccione el paquete de instalación de la aplicación que desee instalar.

Si el paquete de instalación de la aplicación requerida no está en la lista, haga clic en el botón **Agregar** y luego seleccione la aplicación en la lista.



Seleccionar el paquete de instalación

Paso 3. Selección de un método para la distribución del archivo de clave o código de activación

Seleccione un método para la distribución del archivo de clave o el código de activación:

- **No agregar una clave de licencia al paquete de instalación**

  La clave se distribuirá automáticamente a todos los dispositivos con los que sea compatible si se cumplen las siguientes condiciones:

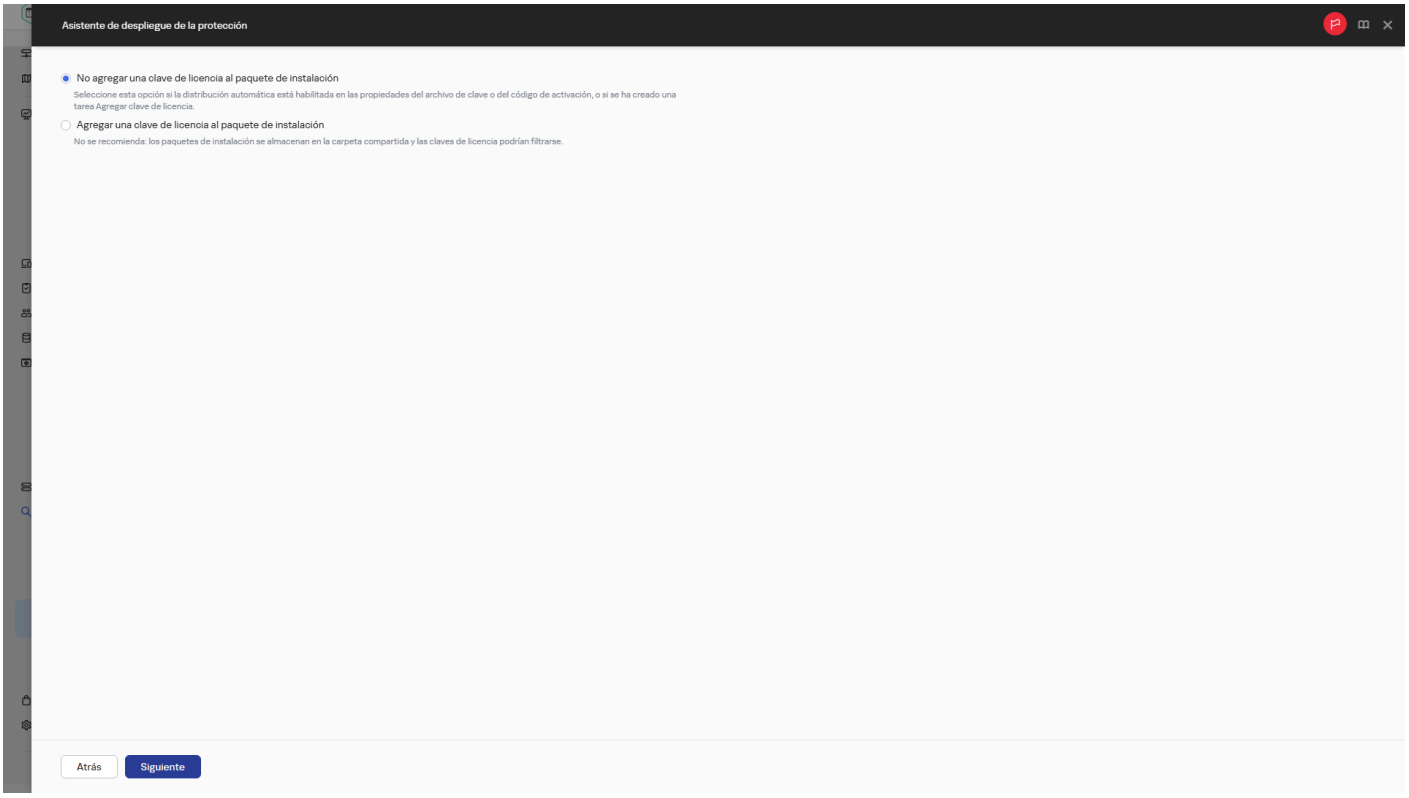
  - Si la distribución automática está habilitada en las propiedades de la clave.
  - Si se creó la tarea **Agregar clave**.

- **Agregar una clave de licencia al paquete de instalación**

  La clave se distribuirá a los dispositivos con el paquete de instalación.

  No le recomendamos distribuir la clave con este método, ya que los derechos Acceso de lectura compartidos están activados para el repositorio de paquetes de instalación.

Si el paquete de instalación ya contiene un archivo de clave o un código de activación, la ventana solo mostrará los información de la clave de licencia.

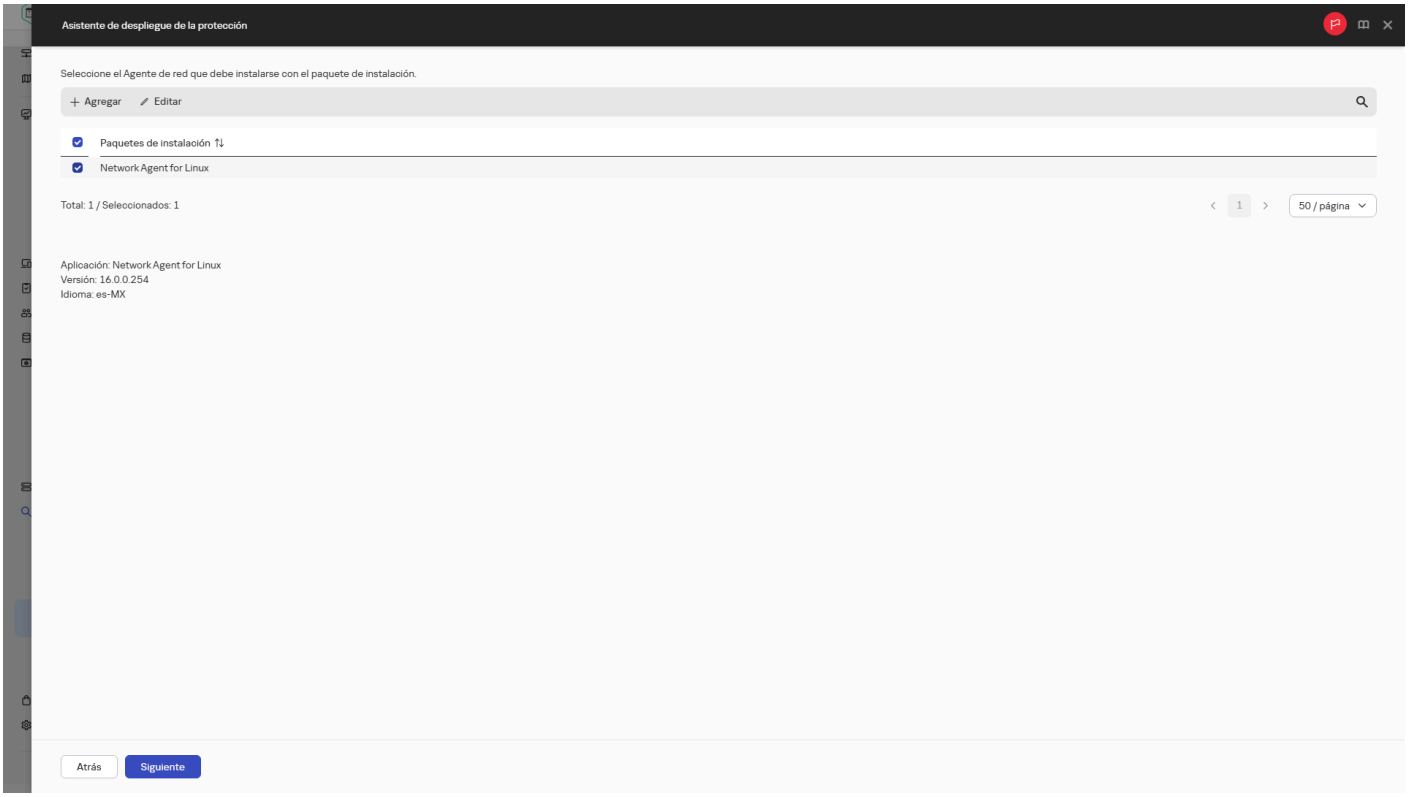


Selección de un método para la distribución del archivo de clave o código de activación

Paso 4. Seleccionar la versión del Agente de red

Si el paquete de instalación que seleccionó no fue el del Agente de red, también deberá instalar el Agente de red, que conecta la aplicación con el Servidor de administración.

Seleccione la última versión del Agente de red.



Seleccionar la versión del Agente de red

Paso 5. Seleccionar los dispositivos

Especifique una lista de dispositivos en los que se instalará la aplicación:

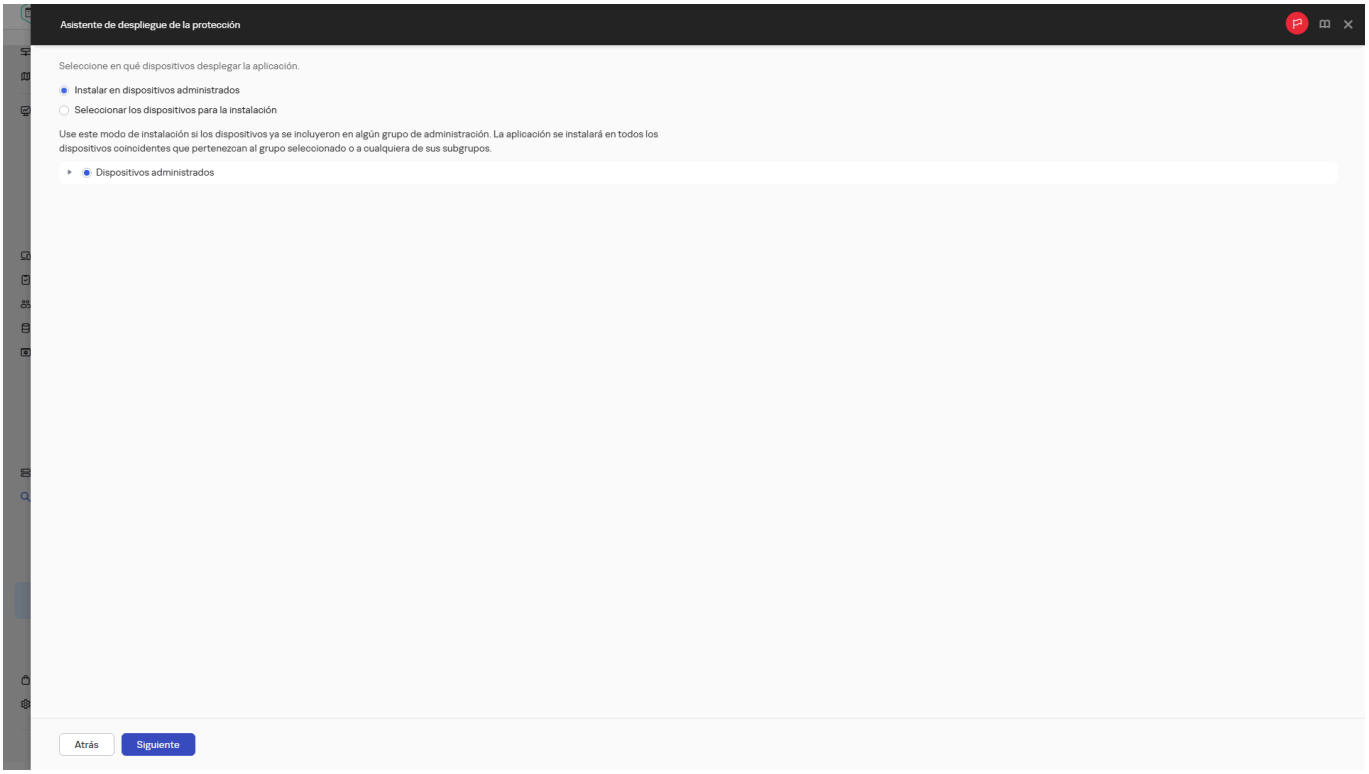
- **Instalar en dispositivos administrados**

  Si selecciona esta opción, la tarea de instalación remota se creará para un grupo de dispositivos.

- **Seleccionar los dispositivos para la instalación**

  La tarea se asignará a los dispositivos incluidos en una selección de dispositivos. Puede elegir una selección existente.

Esta opción puede ser útil para, por ejemplo, ejecutar una tarea en los dispositivos que tengan una versión específica de un sistema operativo.



Especificar la lista de dispositivos en los que se instalará la aplicación

Paso 6. Configurar la tarea de instalación remota

En la página **Configuración de la tarea de instalación remota**, especifique la configuración para la instalación remota de la aplicación.

En el grupo de configuraciones **Forzar la descarga del paquete de instalación**, puede especificar cómo se distribuyen a los dispositivos cliente los archivos que se requieren para la instalación de una aplicación:

- **Con el Agente de red**

  Si habilita esta opción, los paquetes de instalación se transferirán a los dispositivos cliente a través del Agente de red instalado en esos dispositivos.

  Si no habilita esta opción, los paquetes de instalación se distribuirán utilizando las herramientas provistas por el sistema operativo de los dispositivos cliente.

  Recomendamos habilitar esta opción si la tarea está asignada a dispositivos que tienen instalado el Agente de red.

  Esta opción está habilitada de manera predeterminada.

- **Con los recursos del sistema operativo a través de los puntos de distribución**

  Si se selecciona la casilla, los paquetes de instalación se distribuirán a los dispositivos cliente mediante los mecanismos del sistema operativo a través de un punto de distribución. Puede seleccionar esta opción si existe al menos un punto de distribución en la red.

  Si habilitó la opción **Con el Agente de red**, las herramientas del sistema operativo se utilizarán para transferir los archivos solo si las herramientas del Agente de red no están disponibles.

Está opción se habilita de manera predeterminada para las tareas de instalación remota creadas en servidores de administración virtuales.

La única forma de instalar una aplicación para Windows (incluido el Agente de red para Windows) en un dispositivo que no tiene instalado el Agente de red es a través de un punto de distribución basado en Windows. Por lo tanto, cuando instale una aplicación para Windows, haga lo siguiente:

- Seleccione esta opción.
- Asegúrese de que los dispositivos cliente de destino tengan asignado un punto de distribución.
- Asegúrese de que el punto de distribución utilice Windows.

- **Con los recursos del sistema operativo a través del Servidor de administración**

  Si se habilita esta opción, los archivos se transmitirán a los dispositivos cliente a través del Servidor de administración utilizando las herramientas provistas por el sistema operativo de los dispositivos cliente. Puede habilitar esta opción si no hay ningún Agente de red instalado en el dispositivo cliente, pero el dispositivo cliente está en la misma red que el Servidor de administración.

  Esta opción está activada de forma predeterminada.

Defina la configuración adicional:

- **No reinstalar la aplicación si ya está instalada**

  Si habilita esta opción y se detecta que la aplicación ya está instalada en el dispositivo cliente, no se la reinstalará.

  Si no habilita esta opción, la aplicación se instalará en todos los casos.

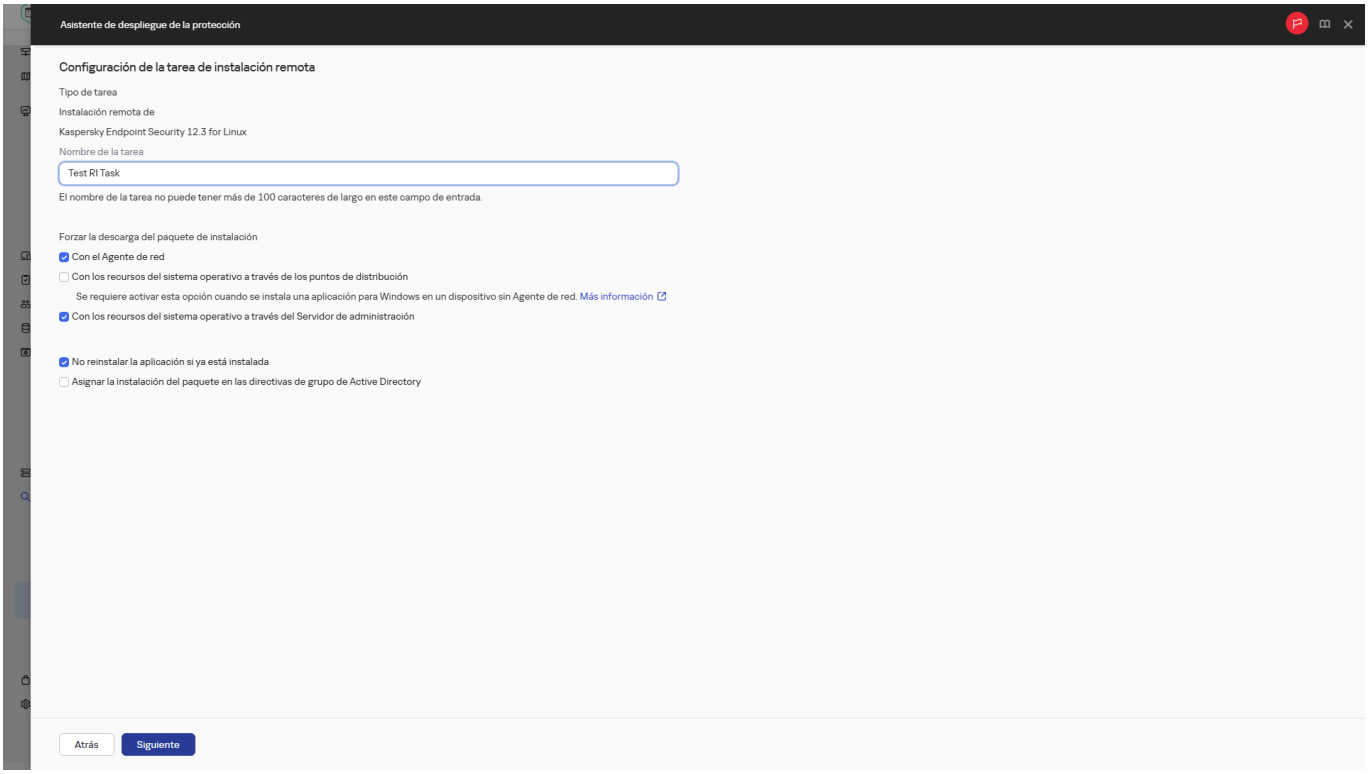
  Esta opción está activada de forma predeterminada.

- **Asignar la instalación del paquete en las directivas de grupo de Active Directory**

  Si se habilita esta opción, se instala un paquete de instalación mediante las directivas de grupo de Active Directory.

  Esta opción se encuentra disponible si se selecciona el paquete de instalación del Agente de red.

Esta opción está deshabilitada de forma predeterminada.



Configurar la tarea de instalación remota

Paso 7. Opciones de reinicio

Indique qué acción se llevará a cabo si se necesita reiniciar el sistema operativo al instalar la aplicación:

- **No reiniciar el dispositivo**

  Cuando termine la operación, los dispositivos cliente no se reiniciarán automáticamente. Para que la operación se complete, deberá reiniciar los dispositivos en forma manual o mediante, por ejemplo, una tarea de administración de dispositivos. Los resultados de la tarea y el estado de cada dispositivo darán cuenta de que hay un reinicio pendiente. Esta opción es útil cuando la tarea va a ejecutarse en servidores y dispositivos que deben operar continuamente.

- **Reiniciar el dispositivo**

  Los dispositivos cliente se reiniciarán automáticamente siempre que resulte necesario para completar la operación. Esta opción es útil cuando la tarea se realiza en dispositivos que admiten una breve interrupción para apagarse o reiniciarse.

- **Solicitar al usuario una acción**

  A través de un recordatorio en pantalla, se le pedirá a cada usuario que reinicie su dispositivo manualmente. Puede configurar algunos ajustes avanzados para esta opción: el texto del mensaje que se le muestra al usuario, la frecuencia con la que se muestra este mensaje y el tiempo que se espera antes de reiniciar el dispositivo por la fuerza (sin que el usuario confirme el reinicio). Esta opción es la más adecuada para estaciones de trabajo en las que los usuarios deben poder seleccionar el momento más conveniente para reiniciar.

Esta opción está seleccionada de forma predeterminada.

- **Repetir solicitud cada (min)**

  Si habilita esta opción, la aplicación le solicitará al usuario que reinicie su sistema operativo con la frecuencia especificada.

  Esta opción está activada de forma predeterminada. El intervalo por defecto es de 5 minutos. Los valores disponibles van de 1 a 1440 minutos.

  Si no habilita esta opción, la solicitud se mostrará una sola vez.

- **Reiniciar después de (min)**

  Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

  Esta opción está activada de forma predeterminada. El tiempo de espera por defecto es de 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

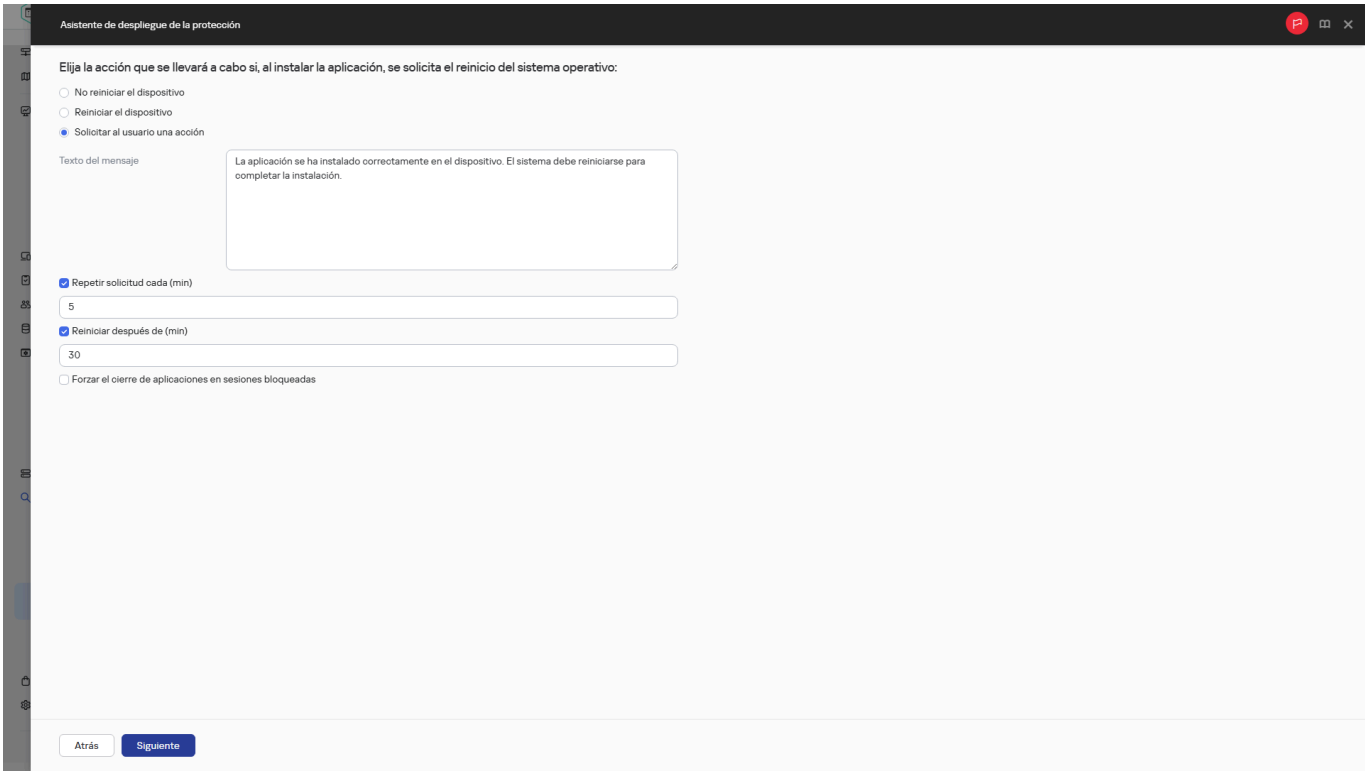
- **Forzar el cierre de aplicaciones en sesiones bloqueadas**

  Las aplicaciones abiertas en el dispositivo cliente podrían impedir que se lo reinicie. Si el usuario está editando un documento en un procesador de textos, por ejemplo, y no ha guardado el archivo, el procesador de textos no permitirá que el dispositivo se reinicie.

  Si habilita esta opción, las aplicaciones que se estén ejecutando en un dispositivo bloqueado se cerrarán por la fuerza y, tras ello, el dispositivo se reiniciará. Los usuarios podrían perder los cambios que no hayan guardado.

  Si no habilita esta opción, los dispositivos bloqueados no se reiniciarán. El estado de la tarea en tales dispositivos indicará que hay un reinicio pendiente. Los usuarios tendrán que cerrar manualmente todas las aplicaciones abiertas para luego reiniciar sus dispositivos.

  Esta opción está deshabilitada de forma predeterminada.



Seleccionar la opción de reinicio del sistema operativo

Paso 8. Eliminar aplicaciones incompatibles antes de la instalación

Verá este paso únicamente si se tiene constancia de que la aplicación que se va a desplegar es incompatible con otras aplicaciones.

Seleccione la opción si desea que Kaspersky Security Center Linux elimine automáticamente aplicaciones que sean incompatibles con la aplicación que despliegue.

También se muestra la lista de aplicaciones incompatibles.

Si no selecciona la opción, la aplicación se instalará únicamente en aquellos dispositivos que no tengan aplicaciones incompatibles.

Paso 9. Mover los dispositivos a Dispositivos administrados

Indique si los dispositivos deberán moverse a un grupo de administración después de la instalación del Agente de red.

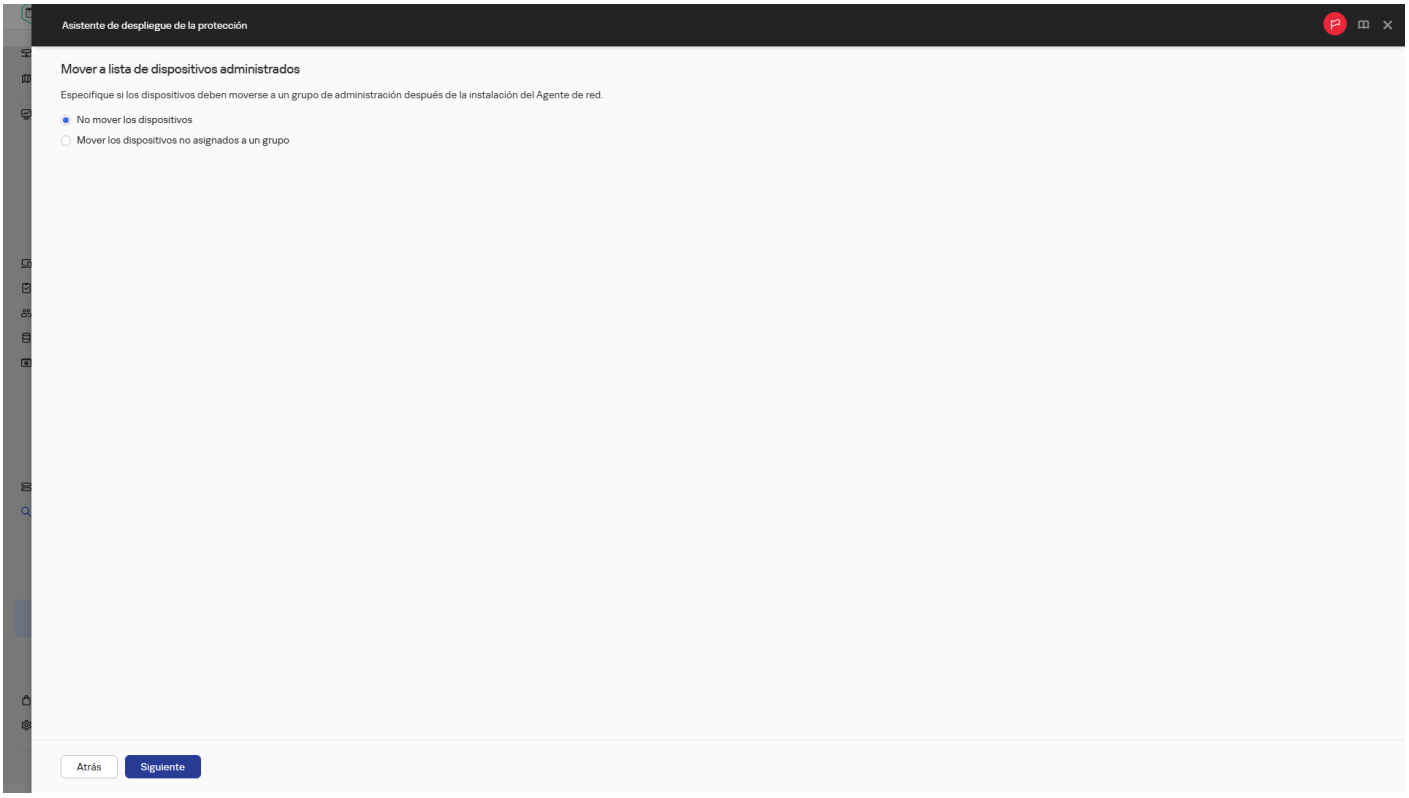
- **No mover los dispositivos**

  Los dispositivos se mantendrán en los grupos en los que se encuentren. Los dispositivos que no pertenezcan a ningún grupo quedarán sin asignar.

- **Mover los dispositivos no asignados a un grupo**

  Los dispositivos se moverán al grupo de administración que seleccione.

La opción **No mover los dispositivos** está seleccionada de manera predeterminada. Es posible que quiera mover los dispositivos manualmente por seguridad.



Seleccionar una opción para mover dispositivos a un grupo de administración

Paso 10. Seleccionar cuentas con acceso a los dispositivos

De ser necesario, agregue las cuentas que se utilizarán para iniciar la tarea de instalación remota:

- **No se necesita una cuenta (el Agente de red está instalado)**

  Si selecciona esta opción, no necesitará especificar la cuenta con la que se ejecutará el instalador de la aplicación. Para ejecutar la tarea, se usará la cuenta con la que se haya iniciado el servicio del Servidor de administración.

  Esta opción no está disponible si el Agente de red no se ha instalado en los dispositivos cliente.

- **Se necesita una cuenta (no se utiliza el Agente de red)**

  Seleccione esta opción si el Agente de red no está instalado en los dispositivos a los que asigna la tarea de instalación remota. En este caso, puede especificar una cuenta de usuario o un certificado SSH para instalar la aplicación.

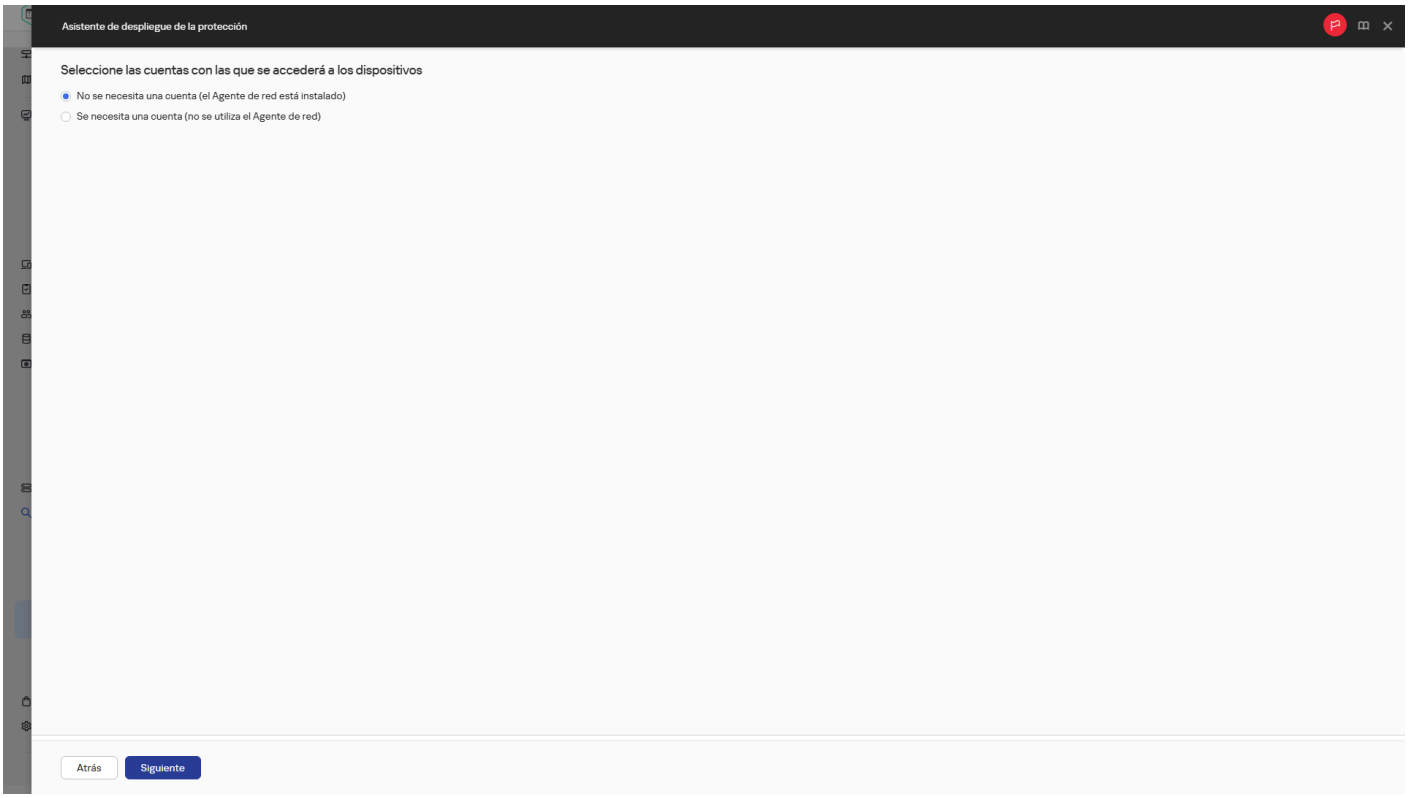
  - **Cuenta local o de dominio**. Si se selecciona esta opción, especifique la cuenta bajo la que se ejecutará el instalador de aplicación. Haga clic en el botón **Agregar**, seleccione **Cuenta local o de dominio** y, a continuación, especifique las credenciales de la cuenta de usuario.

    Puede especificar varias cuentas de usuario si, por ejemplo, ninguna de ellas tiene todos los derechos requeridos en todos los dispositivos a los que asigne esta tarea. En este caso, todas las cuentas añadidas se utilizan para ejecutar la tarea, en orden consecutivo de arriba abajo.

  - **Certificado de SSH**. Si desea instalar una aplicación en un dispositivo cliente basado en Linux, puede especificar un certificado SSH en lugar de una cuenta de usuario. Haga clic en el botón **Agregar**, seleccione **Certificado de SSH** y, a continuación, especifique las claves pública y privada del certificado.

Para generar una clave privada, puede utilizar la utilidad ssh-keygen. Tenga en cuenta que Kaspersky Security Center Linux espera que la clave privada esté en formato PEM, pero, de manera predeterminada, la utilidad ssh-keygen genera claves SSH en formato OPENSSH. Kaspersky Security Center Linux no admite el formato OPENSSH. Para crear una clave privada en el formato PEM admitido, agregue la opción -m PEM en el comando ssh-keygen. Por ejemplo:

```
ssh-keygen -m PEM -t rsa -b 4096 -C "<correo electrónico del usuario>"
```



Seleccionar cuentas con acceso a los dispositivos

Paso 11. Inicio de la instalación

Esta página es el último paso del asistente. En este paso, la tarea **Tarea de instalación remota** está correctamente creada y configurada.

De manera predeterminada, la opción **Ejecutar la tarea al finalizar el asistente** no está seleccionada. Si selecciona esta opción, la tarea **Tarea de instalación remota** comenzará inmediatamente después de que complete el asistente. Si no selecciona esta opción, la tarea **Tarea de instalación remota** no comenzará. Podrá iniciar la tarea manualmente cuando lo desee.

Haga clic en **Aceptar** para completar el paso final del Asistente de despliegue de la protección.

Actualización de Kaspersky Security Center Linux

Puede instalar la versión 17 del Servidor de administración en un dispositivo que tenga instalada una versión anterior del Servidor de administración (a partir de la versión 13). Al actualizar a la versión 17, se conservan todos los datos y configuraciones de la versión anterior del Servidor de administración.

Requisitos previos

- Crear una copia de seguridad de los datos del Servidor de administración antes de comenzar con la actualización.
- Al actualizar el Servidor de administración de la versión 16 o anterior a la versión 16.1 o posterior, se habilita la autenticación de dos factores. Para obtener más información, consulte Acerca de la autenticación de dos factores para una cuenta.

  Para asegurarse de que los usuarios puedan iniciar sesión en Web Console con sus cuentas existentes mediante el uso de claves secretas de autenticación de dos factores configuradas, y que los scripts de automatización de OpenAPI continúen funcionando después de la actualización, debe realizar los siguientes pasos:

  - Habilitación de la autenticación de dos factores para todos los usuarios
  - Los administradores deben configurar la autenticación de dos factores para sus propias cuentas
  - Excluir cuentas de la autenticación de dos factores

    Si es necesario, agregue las cuentas de integridad utilizadas para ejecutar scripts a través de OpenAPI a la lista de exclusión.
- Asegúrese de utilizar las versiones del sistema operativo y del DBMS que sean compatibles con la versión 17 del Servidor de administración. De ser necesario, puede trasladar el Servidor de administración a otro dispositivo, que cuente con un sistema operativo y un DBMS más recientes.
- Cuando actualice el Servidor de administración de la versión 15.4 o anterior a la versión 16 o posterior, cree una base de datos para IAM en el servidor DBMS. El nombre de la base de datos debe ser diferente al de la base de datos que instaló para trabajar con Kaspersky Security Center Linux.
  - En el caso de PostgreSQL, ejecute el siguiente comando:

    ```
    sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
    ```
  - En el caso de MariaDB, ejecute el siguiente comando:

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

- Al actualizar el Servidor de administración de la versión 15.4 o anterior a la versión 16 o posterior, prepare el archivo de respuesta con nuevos parámetros para IAM. Para ver la lista de parámetros requeridos, consulte el artículo Instalación de Kaspersky Security Center Linux en modo silencioso. Agregue la variable de entorno `KLAUTOANSWERS`. Establezca el valor de la variable en la ruta al archivo de respuestas.

- El puerto utilizado por el proceso de kliam para la autenticación del protocolo OpenID Connect debe estar disponible. El valor predeterminado es 4444. Consulte la descripción del parámetro `trusted` en el siguiente artículo: Parámetros de instalación de Kaspersky Security Center Web Console.

Etapas

1 Actualización de un Servidor de administración

Puede actualizar una versión del Servidor de administración a través de uno de los siguientes métodos:

- Utilizando el archivo de instalación de Kaspersky Security Center Linux
- Al crear la Copia de seguridad de datos del Servidor de administración, instalar una nueva versión del Servidor de administración y restaurar los datos del Servidor de administración desde la copia de seguridad

> Durante la actualización, es fundamental que el DBMS no sea utilizado simultáneamente por el Servidor de administración y por otras aplicaciones.

Si su red incluye varios Servidores de administración, debe actualizar cada Servidor manualmente. Kaspersky Security Center Linux no admite la actualización centralizada.

2 Ejecución del script postinstall.pl (paso opcional)

Si el archivo de respuesta no incluye parámetros de IAM o no se encuentra el archivo de respuesta, verá un mensaje en el terminal durante la actualización para que ejecute el script postinstall.pl.

En esta etapa del escenario, puede hacer lo siguiente:

1. En el sistema operativo del Servidor de administración, cree una cuenta de usuario sin privilegios "ksciam" que sea miembro del grupo "kladmins":

   ```
   adduser ksciam
   gpasswd -a ksciam kladmins
   usermod -g kladmins ksciam
   ```

2. En una cuenta con privilegios root, ejecute el script /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl para configurar el Servidor de administración después de la actualización. Cuando se le solicite, ingrese la siguiente configuración:

   1. Ingrese el nombre DNS del servidor de FQDN. Debe usar el nombre del DNS del Servidor de administración que se especificó cuando se instaló Kaspersky Security Center Linux.

   2. Ingrese el nombre de la cuenta para iniciar el servicio IAM. La cuenta debe ser miembro del grupo de seguridad ingresado. De manera predeterminada, se utiliza la cuenta ksciam.

3. Seleccione el DBMS que haya instalado para trabajar con el servicio IAM:
    - Si instaló MySQL o MariaDB, ingrese 1.
    - Si instaló PostgreSQL o Postgres Pro SQL, ingrese 2.
4. Ingrese la dirección de DBMS de IAM que utilizará el servicio de IAM.
5. Ingrese el número de puerto de DBMS de IAM. Este puerto se utiliza para comunicarse con el servicio IAM. De forma predeterminada, se utilizan los siguientes puertos:
    - Puerto 3306 para MySQL y MariaDB.
    - Puerto 5432 para PostgreSQL y Postgres Pro.
6. Ingrese el nombre de la base de datos de IAM que utilizará el servicio de IAM. El nombre de la base de datos utilizada por el servicio de IAM debe ser diferente de la base de datos utilizada por el Servidor de administración.

3. Actualización de Kaspersky Security Center Web Console
4. **(Opcional) Actualización del Agente de red en los dispositivos a una nueva versión.**
5. **Asegurarse de que la lista de permitidos para autenticación de dos factores contenga solo las cuentas de usuario que deben tener acceso al Servidor de administración.**

    Revise la lista de permitidos para autenticación de dos factores y elimine cualquier otra cuenta de ella.

Tenga en cuenta que, si actualiza el Servidor de administración a la versión 17, no podrá crear nuevos paquetes de instalación del Agente de red versión 15 ni versiones anteriores. Sin embargo, los paquetes de instalación creados anteriormente estarán disponibles.

Cuando se instala una versión actualizada de Kaspersky Security Center Linux, se conservan los complementos instalados para las aplicaciones de Kaspersky compatibles. El complemento del Servidor de administración y el del Agente de red se actualizan automáticamente.

Actualizar Kaspersky Security Center Linux versión 16 o posterior

En esta sección se describen las siguientes opciones para actualizar Kaspersky Security Center Linux de la versión 16 o posterior a la versión más reciente:

- Actualización mediante el archivo de instalación
- Actualización mediante una copia de seguridad
- Actualización en los nodos del clúster de conmutación por error de Kaspersky Security Center Linux

Actualización de Kaspersky Security Center Linux de la versión 16 o posterior mediante el archivo de instalación

Si desea actualizar el Servidor de administración de la versión 16 o posterior a la versión más reciente, puede instalar la versión nueva sobre la antigua mediante el archivo de instalación de Kaspersky Security Center Linux.

Para actualizar Kaspersky Security Center Linux de la versión 16 o posterior a la versión más reciente mediante el instalador, siga estos pasos:

1. Descargue el archivo de instalación de Kaspersky Security Center Linux con un paquete completo para la versión 17 desde el sitio web de Kaspersky:

   - Para dispositivos que ejecutan un sistema operativo basado en RPM—`ksc64-<version number>.x86_64.rpm`
   - Para dispositivos que ejecutan un sistema operativo basado en Debian—`ksc64_<version number>_amd64.deb`

2. Comience a actualizar Kaspersky Security Center Linux. Ejecute uno de los siguientes comandos en la terminal de línea de comandos:

   - Para dispositivos que ejecutan un sistema operativo basado en RPM:

     ```
     sudo yum install ./ksc64-<version number>.x86_64.rpm
     ```

   - Para dispositivos que ejecutan un sistema operativo basado en Debian:

     ```
     sudo apt-get install ./ksc64_<version number>_amd64.deb
     ```

   Una vez que el comando se ejecuta correctamente, se crea el script `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl`. El mensaje sobre eso se muestra en la terminal.

3. Ejecute el script `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` para configurar el Servidor de administración actualizado:

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

4. Lea el Contrato de licencia y la Política de privacidad, que aparecen en la terminal de la línea de comandos. Si está de acuerdo con todos los términos del Contrato de licencia y la Política de privacidad:

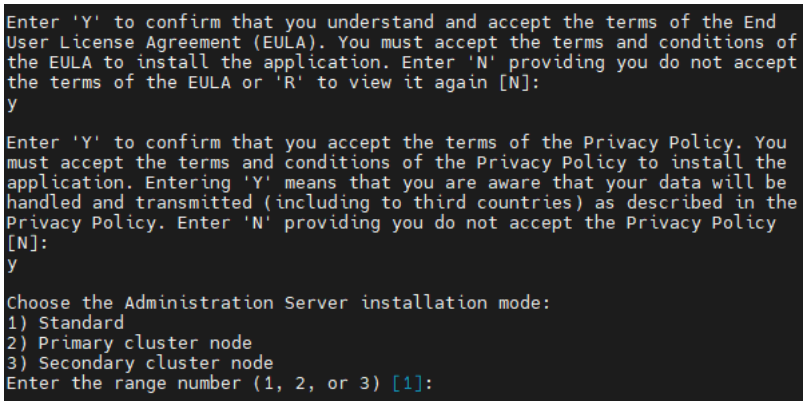
   a. Ingrese `Y` para confirmar que leyó, comprende y acepta completamente los términos y condiciones del EULA.

   b. Ingrese `Y` nuevamente para confirmar que leyó, comprende y acepta la Política de privacidad, en la que se describe el manejo de datos.

   La instalación de la aplicación en su dispositivo continuará después de que ingrese `Y` dos veces.

5. Ingrese `1` para seleccionar el modo de instalación estándar del Servidor de administración.

La siguiente imagen muestra los dos últimos pasos.



Aceptación de los términos del EULA y la Política de privacidad, y selección del modo de instalación estándar para el Servidor de administración en la terminal de línea de comandos

Luego, el script configurará y completará la actualización del Servidor de administración. Durante la actualización, no es posible modificar los ajustes del Servidor de administración configurados antes de la actualización.

6. Actualice Kaspersky Security Center Web Console a una nueva versión.

7. Para dispositivos que tienen instalada una versión anterior del Agente de red, cree y ejecute la tarea de instalación remota para la nueva versión del Agente de red.

   Le recomendamos que actualice el Agente de red para Linux a la misma versión que Kaspersky Security Center Linux.

   La versión actualizada del Agente de red se instalará una vez que se complete la tarea de instalación remota.

   Ejecute los siguientes comandos en activos basados en Linux para eliminar las dependencias que ya no son necesarias:

   - Para activos basados en Debian, ejecute cualquiera de los siguientes comandos:

     ```
     sudo apt-get -y autoremove
     ```

     ```
     sudo apt -y autoremove
     ```

   - Para activos basados en RPM, ejecute cualquiera de los siguientes comandos:

     ```
     sudo dnf autoremove
     ```

     ```
     sudo yum autoremove
     ```

Actualización de Kaspersky Security Center Linux de la versión 16 o posterior mediante una copia de seguridad

Para actualizar el Servidor de administración de la versión 16 o posterior, puede crear una copia de seguridad de los datos del Servidor de administración y restaurarlos después de instalar la nueva versión de Kaspersky Security Center Linux. Si ocurre un problema durante la instalación, se puede restaurar la versión anterior del Servidor de administración mediante la copia de seguridad de los datos del Servidor de administración creada antes de la actualización.

Para actualizar Kaspersky Security Center Linux de la versión16 o posterior a la versión más reciente mediante una copia de seguridad, siga estos pasos:

1. Antes de la actualización, hacer una copia de seguridad de los datos del Servidor de administración con una versión anterior de la aplicación.

2. Desinstale la versión anterior de Kaspersky Security Center Linux.

3. Instale la versión 17 de Kaspersky Security Center Linux en el dispositivo donde se instaló el Servidor de administración.

   Si el esquema de la base de datos de la copia de seguridad difiere del que utiliza actualmente el Servidor de administración o IAM, los datos se restaurarán al esquema actual.

   Si se usa el esquema public en la copia de seguridad, se deben cumplir las siguientes condiciones:

   - El esquema public de la base de datos existe en la base de datos.
   - Puede modificar el esquema public de la base de datos desde la cuenta del DBMS que usa el Servidor de administración o IAM para acceder a la base de datos.

   De lo contrario, la restauración de datos finaliza con un error.

4. Restaurar los datos del Servidor de administración de la copia de seguridad creada antes de la actualización.

5. Instale Kaspersky Security Center Web Console.

   Si se ha instalado anteriormente Kaspersky Security Center Web Console, vuelva a instalarlo con el mismo archivo de respuesta.

   Iniciar sesión en Kaspersky Security Center Web Console con la cuenta de usuario interna del administrador.

   Después de restaurar los datos del Servidor de administración, el proceso de inicialización puede durar hasta 15 minutos, aunque el tiempo exacto dependerá del rendimiento del hardware y del tamaño de los datos. Durante este tiempo, es posible que Kaspersky Security Center Web Console no se conecte y muestre errores.

6. Para dispositivos que tienen instalada una versión anterior del Agente de red, cree y ejecute la tarea de instalación remota para la nueva versión del Agente de red.

   > Le recomendamos que actualice el Agente de red para Linux a la misma versión que Kaspersky Security Center Linux.

   La versión actualizada del Agente de red se instalará una vez que se complete la tarea de instalación remota.

Ejecute los siguientes comandos en activos basados en Linux para eliminar las dependencias que ya no son necesarias:

- Para activos basados en Debian, ejecute cualquiera de los siguientes comandos:

```
sudo apt-get -y autoremove
```

```
sudo apt -y autoremove
```

- Para activos basados en RPM, ejecute cualquiera de los siguientes comandos:

```
sudo dnf autoremove
```

```
sudo yum autoremove
```

Actualización de Kaspersky Security Center Linux de la versión 16 o posterior en los nodos del clúster de conmutación por error de Kaspersky Security Center Linux

Puede instalar la versión más reciente del Servidor de administración en cada nodo del clúster de conmutación por error de Kaspersky Security Center Linux donde esté instalada la versión 16 o posterior del Servidor de administración. Al actualizar a la versión más reciente, se conservan todos los datos y configuraciones de la versión anterior del Servidor de administración.

Si realizó la instalación de Kaspersky Security Center Linux de manera local en los dispositivos, para actualizar Kaspersky Security Center Linux en esos dispositivos, puede también utilizar el archivo de instalación o una copia de seguridad.

No se admite la actualización de Kaspersky Security Center Linux a la versión 17 en los nodos del clúster de conmutación por error mediante un archivo de instalación. Para actualizar de una versión anterior a la versión 17, cree una copia de seguridad de los datos del Servidor de administración, instale la nueva versión del clúster de conmutación por error de Kaspersky Security Center Linux y, luego, restaure los datos del Servidor de administración desde la copia de seguridad. Esta limitación también se aplica a un clúster distribuido geográficamente.

Para actualizar Kaspersky Security Center Linux de la versión 16 o posterior en los nodos del clúster de conmutación por error de Kaspersky Security Center Linux, haga lo siguiente:

1. Descargue el archivo de instalación de Kaspersky Security Center Linux con un paquete completo para la versión 17 desde el sitio web de Kaspersky:

   - Para dispositivos que ejecutan un sistema operativo basado en RPM: `ksc64-<version number>-<build number>.x86_64.rpm`
   - Para dispositivos que ejecutan un sistema operativo basado en Debian: `ksc64_<version number>-<build number>_amd64.deb`

2. Detenga el clúster.

3. En el nodo activo del clúster, ejecute el siguiente comando en la terminal de línea de comandos para ejecutar la actualización:

   - Para dispositivos que ejecutan un sistema operativo basado en RPM:

     ```
     sudo yum install ./ksc64-<version number>-<build number>.x86_64.rpm
     ```

   - Para dispositivos que ejecutan un sistema operativo basado en Debian:

     ```
     sudo apt-get install ./ksc64_<version number>-<build number>_amd64.deb
     ```

   Una vez que el comando se ejecuta correctamente, se crea el script `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl`. El mensaje sobre eso se muestra en la terminal.

   Si se produce algún error, consulte la solución descrita en la Base de conocimientos.

4. Ejecute el script `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` para configurar el Servidor de administración actualizado:

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

5. Lea el Contrato de licencia y la Política de privacidad, que aparecen en la terminal de la línea de comandos. Si está de acuerdo con todos los términos del Contrato de licencia y la Política de privacidad:

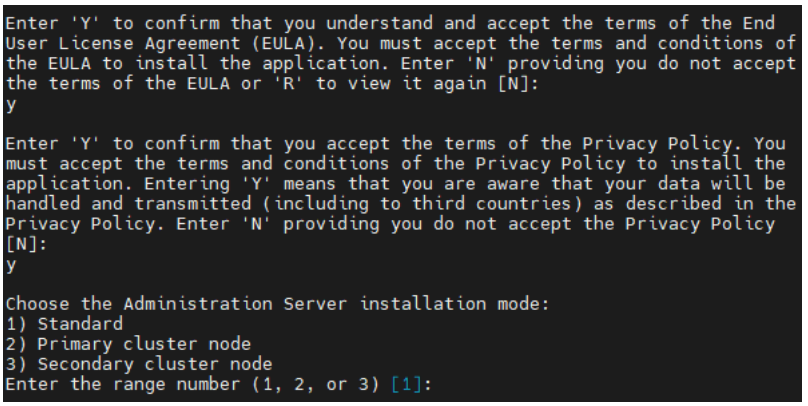
   a. Ingrese `Y` para confirmar que leyó, comprende y acepta completamente los términos y condiciones del EULA.

   b. Ingrese `Y` nuevamente para confirmar que leyó, comprende y acepta la Política de privacidad, en la que se describe el manejo de datos.

   La instalación de la aplicación en su dispositivo continuará después de que ingrese `Y` dos veces.

6. Ingrese `2` para seleccionar el nodo que esté actualizando.

   La siguiente imagen muestra los dos últimos pasos.



Aceptación de los términos del EULA y de la Política de privacidad, y selección del modo de instalación estándar en la terminal de línea de comandos

Luego, el script configurará y completará la actualización del Servidor de administración. Durante la actualización, no es posible modificar los ajustes del Servidor de administración configurados antes de la actualización.

7. Realice los pasos 3 a 5 en el nodo pasivo.

   En el paso 6, ingrese `3` para seleccionar el nodo.

8. Inicie el clúster.

   > Puede iniciar el clúster en cualquier nodo. Si inicia el clúster en el nodo pasivo, ese nodo se convertirá en el nodo activo.

9. Para dispositivos que tienen instalada una versión anterior del Agente de red, cree y ejecute la tarea de instalación remota para la nueva versión del Agente de red.

   > Le recomendamos que actualice el Agente de red para Linux a la misma versión que Kaspersky Security Center Linux.

   La versión actualizada del Agente de red se instalará una vez que se complete la tarea de instalación remota.

   Ejecute los siguientes comandos en activos basados en Linux para eliminar las dependencias que ya no son necesarias:

   - Para activos basados en Debian, ejecute cualquiera de los siguientes comandos:

     ```
     sudo apt-get -y autoremove
     ```

     ```
     sudo apt -y autoremove
     ```

   - Para activos basados en RPM, ejecute cualquiera de los siguientes comandos:

     ```
     sudo dnf autoremove
     ```

     ```
     sudo yum autoremove
     ```

   Como resultado, instaló la versión más reciente del Servidor de administración en los nodos del clúster de conmutación por error de Kaspersky Security Center Linux.

Actualizar Kaspersky Security Center Linux versión 15.4 o anterior

En esta sección, se describen las siguientes opciones para actualizar Kaspersky Security Center Linux de la versión 15.4 o anterior a la versión 16 o posterior:

- Actualización mediante el archivo de instalación
- Actualización mediante una copia de seguridad
- Actualización en los nodos del clúster de conmutación por error de Kaspersky Security Center Linux

Cada opción de actualización de Kaspersky Security Center Linux de la versión 15.4 o anterior a la versión 16 o posterior incluye pasos para crear y configurar una base de datos de IAM en un servidor DBMS, crear una cuenta 'ksciam' sin privilegios para ejecutar el servicio de IAM y agregar esta cuenta al grupo de seguridad 'kladmins'.

Actualización de Kaspersky Security Center Linux de la versión 15.4 o anterior mediante el archivo de instalación

Para actualizar el Servidor de administración de la versión 13 a 15.4 a la versión 16 o posterior, puede instalar una nueva versión sobre una anterior mediante el archivo de instalación de Kaspersky Security Center Linux.

Antes de empezar, verifique los requisitos de un certificado personalizado.

Si utiliza un certificado personalizado en lugar del autofirmado, antes de actualizar Kaspersky Security Center Linux a la versión posterior, debe asegurarse de que el certificado incluya el Nombre alternativo del sujeto (SAN). Si no lo incluye, es importante reemplazar el certificado antes de actualizar Kaspersky Security Center Linux. De lo contrario, no podrá iniciar sesión en Web Console después de la actualización.

Para asegurarse de que el certificado incluya SAN:

1. En el dispositivo en el que se encuentra instalado el Servidor de administración, ejecute el siguiente comando:

   - Para un dispositivo Linux:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout
     -ext subjectAltName
     ```

   - Para un dispositivo Windows:

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. Asegúrese de que el Nombre alternativo del sujeto (SAN) esté presente en el resultado del comando y que contenga la dirección del dispositivo del Servidor de administración.

3. Si no aparece el Nombre alternativo del sujeto, use la utilidad klsetsrvcert para reemplazar su certificado de usuario por uno que cumpla con los requisitos.

Para actualizar Kaspersky Security Center Linux de la versión 15.4 o anterior a la versión más reciente usando el archivo de instalación, haga lo siguiente:

1. Descargue el archivo de instalación de Kaspersky Security Center Linux con un paquete completo para la versión 17 desde el sitio web de Kaspersky:

   - Para dispositivos que ejecutan un sistema operativo basado en RPM—`ksc64-<version number>.x86_64.rpm`

   - Para dispositivos que ejecutan un sistema operativo basado en Debian—`ksc64_<version number>_amd64.deb`

2. En el servidor de DBMS, cree una base de datos para IAM. El nombre de la base de datos de IAM debe ser diferente al de la base de datos que instaló para trabajar con Kaspersky Security Center Linux.

   - En el caso de PostgreSQL, ejecute el siguiente comando:

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

- En el caso de MariaDB, ejecute el siguiente comando:

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

3. Cree una cuenta sin privilegios 'ksciam', agréguela al grupo de seguridad 'kladmins' y luego establezca el grupo 'kladmins' como el grupo principal para la cuenta 'ksciam'. Para hacer esto, ejecute secuencialmente los siguientes comandos:

```
sudo adduser ksciam
sudo gpasswd -a ksciam kladmins
sudo usermod -g kladmins ksciam
```

4. Comience a actualizar Kaspersky Security Center Linux. Ejecute uno de los siguientes comandos en la terminal de línea de comandos:

   - Para dispositivos que ejecutan un sistema operativo basado en RPM:

   ```
   sudo yum install ./ksc64-<número de versión>.x86_64.rpm
   ```

   - Para dispositivos que ejecutan un sistema operativo basado en Debian:

   ```
   sudo apt-get install ./ksc64_<número de versión>_amd64.deb
   ```

   Una vez que el comando se ejecuta correctamente, se crea el script `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl`. El mensaje sobre eso se muestra en la terminal.

5. Ejecute el script `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` para configurar el Servidor de administración actualizado:

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

6. Lea el Contrato de licencia y la Política de privacidad, que aparecen en la terminal de la línea de comandos. Si está de acuerdo con todos los términos del Contrato de licencia y la Política de privacidad:

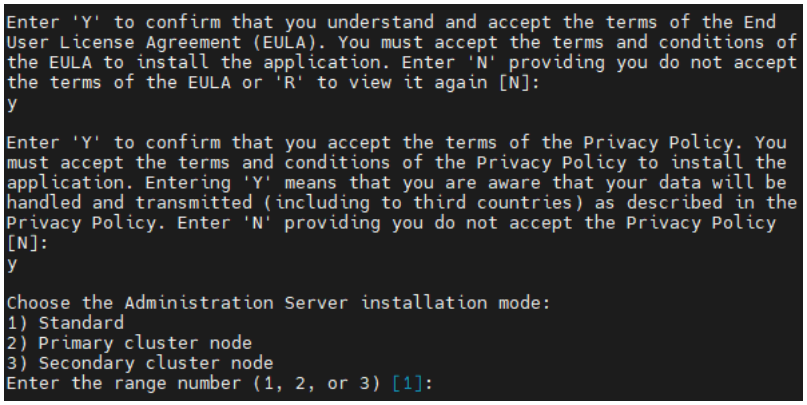
   a. Ingrese `Y` para confirmar que leyó, comprende y acepta completamente los términos y condiciones del EULA.

   b. Ingrese `Y` nuevamente para confirmar que leyó, comprende y acepta la Política de privacidad, en la que se describe el manejo de datos.

   La instalación de la aplicación en su dispositivo continuará después de que ingrese `Y` dos veces.

7. Ingrese `1` para seleccionar el modo de instalación estándar del Servidor de administración.

La siguiente imagen muestra los dos últimos pasos.



Aceptación de los términos del EULA y la Política de privacidad, y selección del modo de instalación estándar para el Servidor de administración en la terminal de línea de comandos

8. Luego, el script configurará y completará la actualización del Servidor de administración. Durante la actualización, no es posible modificar los ajustes del Servidor de administración configurados antes de la actualización. Cuando se le solicite, ingrese la siguiente configuración:

   a. Ingrese el nombre DNS del servidor de FQDN.

      Debe usar el nombre del DNS del Servidor de administración que se especificó cuando se instaló Kaspersky Security Center Linux.

   b. Ingrese el nombre de la cuenta para iniciar el servicio IAM. La cuenta debe ser miembro del grupo de seguridad ingresado. De manera predeterminada, se utiliza la cuenta ksciam.

   c. Seleccione el DBMS que haya instalado para trabajar con el servicio IAM:

      - Si instaló MySQL o MariaDB, ingrese `1`.
      - Si instaló PostgreSQL o Postgres Pro SQL, ingrese `2`.

   d. Ingrese la dirección de DBMS de IAM que utilizará el servicio de IAM.

   e. Ingrese el número de puerto de DBMS de IAM. Este puerto se utiliza para comunicarse con el servicio IAM. De forma predeterminada, se utilizan los siguientes puertos:

      - Puerto 3306 para MySQL y MariaDB.
      - Puerto 5432 para PostgreSQL y Postgres Pro.

   f. Ingrese el nombre de la base de datos de IAM que utilizará el servicio de IAM. El nombre de la base de datos utilizada por el servicio de IAM debe ser diferente de la base de datos utilizada por el Servidor de administración.

   g. Ingrese el nombre de usuario y la contraseña de DBMS que usará el servicio de IAM.

   h. Si instaló PostgreSQL o Postgres Pro, puede especificar el esquema de base de datos que usará IAM. Para hacerlo, especifique el nombre del esquema.

      Si no desea usar un esquema personalizado, presione `ENTER` y se utilizará un esquema predeterminado.

El nombre del esquema distingue entre mayúsculas y minúsculas: debe usar solo letras minúsculas. No especifique los nombres de esquema reservados de iam: `client, iam, ksc, locker, pat, scope, voltron`.

9. Actualice Kaspersky Security Center Web Console a una nueva versión.
10. Para dispositivos que tienen instalada una versión anterior del Agente de red, cree y ejecute la tarea de instalación remota para la nueva versión del Agente de red.

    Le recomendamos que actualice el Agente de red para Linux a la misma versión que Kaspersky Security Center Linux.

    La versión actualizada del Agente de red se instalará una vez que se complete la tarea de instalación remota.

    Ejecute los siguientes comandos en activos basados en Linux para eliminar las dependencias que ya no son necesarias:

    - Para activos basados en Debian, ejecute cualquiera de los siguientes comandos:

      ```
      sudo apt-get -y autoremove
      ```

      ```
      sudo apt -y autoremove
      ```

    - Para activos basados en RPM, ejecute cualquiera de los siguientes comandos:

      ```
      sudo dnf autoremove
      ```

      ```
      sudo yum autoremove
      ```

Actualización de Kaspersky Security Center Linux de la versión 15.4 o anterior mediante una copia de seguridad

Para actualizar el Servidor de administración de la versión 14.2–15.4 a la versión 16 o posterior, puede crear una copia de seguridad de los datos del Servidor de administración y restaurarla después de instalar una nueva versión de Kaspersky Security Center Linux. Si ocurre un problema durante la instalación, se puede restaurar la versión anterior del Servidor de administración mediante la copia de seguridad de los datos del Servidor de administración creada antes de la actualización.

Requisitos previos

1. **Verifique los requisitos de un certificado personalizado.**

   Si utiliza un certificado personalizado en lugar del autofirmado, antes de actualizar Kaspersky Security Center Linux a la versión posterior, debe asegurarse de que el certificado incluya el Nombre alternativo del sujeto (SAN). Si no lo incluye, es importante reemplazar el certificado antes de actualizar Kaspersky Security Center Linux. De lo contrario, no podrá iniciar sesión en Web Console después de la actualización.

   Para asegurarse de que el certificado incluya SAN:

   1. En el dispositivo en el que se encuentra instalado el Servidor de administración, ejecute el siguiente comando:

      - Para un dispositivo Linux:

        ```
        sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
        ```

      - Para un dispositivo Windows:

        ```
        certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
        ```

   2. Asegúrese de que el Nombre alternativo del sujeto (SAN) esté presente en el resultado del comando y que contenga la dirección del dispositivo del Servidor de administración.

   3. Si no aparece el Nombre alternativo del sujeto, use la utilidad klsetsrvcert para reemplazar su certificado de usuario por uno que cumpla con los requisitos.

2. Cree una copia de seguridad de los datos del Servidor de administración con una versión anterior de la aplicación.

El procedimiento de actualización

Para actualizar Kaspersky Security Center Linux de la versión 15.4 o anterior a la versión más reciente mediante una copia de seguridad:

1. Desinstale la versión anterior de Kaspersky Security Center Linux.

2. En el servidor de DBMS, cree una base de datos para IAM. El nombre de la base de datos de IAM debe ser diferente al de la base de datos que instaló para trabajar con Kaspersky Security Center Linux.

   - En el caso de PostgreSQL, ejecute el siguiente comando:

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

   - En el caso de MariaDB, ejecute el siguiente comando:

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

3. Cree una cuenta sin privilegios 'ksciam', agréguela al grupo de seguridad 'kladmins' y luego establezca el grupo 'kladmins' como el grupo principal para la cuenta 'ksciam'. Para hacer esto, ejecute secuencialmente los siguientes comandos:

```
sudo adduser ksciam
sudo gpasswd -a ksciam kladmins
sudo usermod -g kladmins ksciam
```

4. Instale la versión 17 de Kaspersky Security Center Linux en el dispositivo donde se instaló el Servidor de administración.

   Si el esquema de la base de datos de la copia de seguridad difiere del que utiliza actualmente el Servidor de administración o IAM, los datos se restaurarán al esquema actual.

   Si se usa el esquema public en la copia de seguridad, se deben cumplir las siguientes condiciones:

   - El esquema public de la base de datos existe en la base de datos.
   - Puede modificar el esquema public de la base de datos desde la cuenta del DBMS que usa el Servidor de administración o IAM para acceder a la base de datos.

   De lo contrario, la restauración de datos finaliza con un error.

5. Restaurar los datos del Servidor de administración de la copia de seguridad creada antes de la actualización.

6. Configure la verificación de certificados del Servidor de administración y del Servidor de IAM.

7. Instale Kaspersky Security Center Web Console.

   Si se ha instalado anteriormente Kaspersky Security Center Web Console, vuelva a instalarlo con el mismo archivo de respuesta.

   Iniciar sesión en Kaspersky Security Center Web Console con la cuenta de usuario interna del administrador.

   Después de restaurar los datos del Servidor de administración, el proceso de inicialización puede durar hasta 15 minutos, aunque el tiempo exacto dependerá del rendimiento del hardware y del tamaño de los datos. Durante este tiempo, es posible que Kaspersky Security Center Web Console no se conecte y muestre errores.

8. Para dispositivos que tienen instalada una versión anterior del Agente de red, cree y ejecute la tarea de instalación remota para la nueva versión del Agente de red.

   > Le recomendamos que actualice el Agente de red para Linux a la misma versión que Kaspersky Security Center Linux.

   La versión actualizada del Agente de red se instalará una vez que se complete la tarea de instalación remota.

   Ejecute los siguientes comandos en activos basados en Linux para eliminar las dependencias que ya no son necesarias:

   - Para activos basados en Debian, ejecute cualquiera de los siguientes comandos:

     ```
     sudo apt-get -y autoremove
     ```

     ```
     sudo apt -y autoremove
     ```

- Para activos basados en RPM, ejecute cualquiera de los siguientes comandos:

```
sudo dnf autoremove
```

```
sudo yum autoremove
```

Actualización de Kaspersky Security Center Linux de la versión 15.4 o anterior en los nodos del clúster de conmutación por error de Kaspersky Security Center Linux

Puede instalar la versión 16 o posterior del Servidor de administración en cada nodo del clúster de conmutación por error de Kaspersky Security Center Linux donde esté instalada la versión 14-15.4 del Servidor de administración. Cuando actualiza, se conservan todos los datos y configuraciones de la versión anterior del Servidor de administración.

Antes de empezar, verifique los requisitos de un certificado personalizado.

Si utiliza un certificado personalizado en lugar del autofirmado, antes de actualizar Kaspersky Security Center Linux a la versión posterior, debe asegurarse de que el certificado incluya el Nombre alternativo del sujeto (SAN). Si no lo incluye, es importante reemplazar el certificado antes de actualizar Kaspersky Security Center Linux. De lo contrario, no podrá iniciar sesión en Web Console después de la actualización.

Para asegurarse de que el certificado incluya SAN:

1. En el dispositivo en el que se encuentra instalado el Servidor de administración, ejecute el siguiente comando:

   - Para un dispositivo Linux:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
     ```

   - Para un dispositivo Windows:

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. Asegúrese de que el Nombre alternativo del sujeto (SAN) esté presente en el resultado del comando y que contenga la dirección del dispositivo del Servidor de administración.

3. Si no aparece el Nombre alternativo del sujeto, use la utilidad klsetsrvcert para reemplazar su certificado de usuario por uno que cumpla con los requisitos.

Si realizó la instalación de Kaspersky Security Center Linux de manera local en los dispositivos, para actualizar Kaspersky Security Center Linux en esos dispositivos, puede también utilizar el archivo de instalación o una copia de seguridad.

Para actualizar Kaspersky Security Center Linux de la versión 15.4 o anterior en los nodos del clúster de conmutación por error de Kaspersky Security Center Linux, haga lo siguiente:

1. Descargue el archivo de instalación de Kaspersky Security Center Linux con un paquete completo para la versión 17 desde el sitio web de Kaspersky:

   - Para dispositivos que ejecutan un sistema operativo basado en RPM: `ksc64-<version number>-<build number>.x86_64.rpm`
   - Para dispositivos que ejecutan un sistema operativo basado en Debian: `ksc64_<version number>-<build number>_amd64.deb`

2. Detenga el clúster.

3. En el servidor de DBMS, cree una base de datos para IAM. El nombre de la base de datos de IAM debe ser diferente del nombre de la base de datos que instaló para trabajar con Kaspersky Security Center Linux.

   - En el caso de PostgreSQL, ejecute el siguiente comando:

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

   - En el caso de MariaDB, ejecute el siguiente comando:

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

4. Cree una cuenta sin privilegios 'ksciam', agréguela al grupo de seguridad 'kladmins' y luego establezca el grupo 'kladmins' como el grupo principal para la cuenta 'ksciam'. Para hacer esto, ejecute secuencialmente los siguientes comandos:

   ```
   sudo adduser ksciam
   sudo gpasswd -a ksciam kladmins
   sudo usermod -g kladmins ksciam
   ```

5. En el nodo activo del clúster, ejecute uno de los siguientes comandos en la línea de comando para iniciar la actualización:

   - Para dispositivos que ejecutan un sistema operativo basado en RPM:

     ```
     sudo yum install ./ksc64-<número de versión>-<número de compilación>.x86_64.rpm
     ```

   - Para dispositivos que ejecutan un sistema operativo basado en Debian:

     ```
     sudo apt-get install ./ksc64_<número de versión>-<número de compilación>_amd64.deb
     ```

   Una vez que el comando se ejecuta correctamente, se crea el script `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl`. El mensaje sobre eso se muestra en la terminal.

6. Ejecute el script `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` para configurar el Servidor de administración actualizado:

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

7. Lea el Contrato de licencia y la Política de privacidad, que aparecen en la terminal de la línea de comandos. Si está de acuerdo con todos los términos del Contrato de licencia y la Política de privacidad:

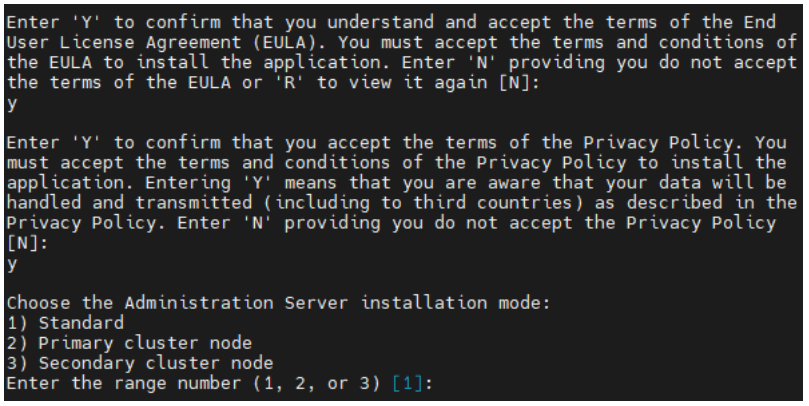
   a. Ingrese `Y` para confirmar que leyó, comprende y acepta completamente los términos y condiciones del EULA.

   b. Ingrese `Y` nuevamente para confirmar que leyó, comprende y acepta la Política de privacidad, en la que se describe el manejo de datos.

   La instalación de la aplicación en su dispositivo continuará después de que ingrese `Y` dos veces.

8. Ingrese `2` para seleccionar el nodo que esté actualizando.

   La siguiente imagen muestra los dos últimos pasos.



Aceptación de los términos del EULA y de la Política de privacidad, y selección del modo de instalación estándar en la terminal de línea de comandos

9. Luego, el script configurará y completará la actualización del Servidor de administración. Durante la actualización, no es posible modificar los ajustes del Servidor de administración configurados antes de la actualización. Cuando se le solicite, ingrese la siguiente configuración:

   a. Ingrese el nombre DNS del servidor de FQDN.

      Debe usar el nombre del DNS del Servidor de administración que se especificó cuando se instaló Kaspersky Security Center Linux.

   b. Ingrese el nombre de la cuenta para iniciar el servicio IAM. La cuenta debe ser miembro del grupo de seguridad ingresado. De manera predeterminada, se utiliza la cuenta ksciam.

   c. Seleccione el DBMS que haya instalado para trabajar con el servicio IAM:

      - Si instaló MySQL o MariaDB, ingrese `1`.
      - Si instaló PostgreSQL o Postgres Pro SQL, ingrese `2`.

   d. Ingrese la dirección de DBMS de IAM que utilizará el servicio de IAM.

e. Ingrese el número de puerto de DBMS de IAM. Este puerto se utiliza para comunicarse con el servicio IAM. De forma predeterminada, se utilizan los siguientes puertos:

- Puerto 3306 para MySQL y MariaDB.
- Puerto 5432 para PostgreSQL y Postgres Pro.

f. Ingrese el nombre de la base de datos de IAM que utilizará el servicio de IAM. El nombre de la base de datos utilizada por el servicio de IAM debe ser diferente de la base de datos utilizada por el Servidor de administración.

g. Ingrese el nombre de usuario y la contraseña de DBMS que usará el servicio de IAM.

10. Realice el paso 5 en el nodo pasivo.

    En el paso 6, ingrese `3` para seleccionar el nodo.

11. Inicie el clúster.

    Puede iniciar el clúster en cualquier nodo. Si inicia el clúster en el nodo pasivo, ese nodo se convertirá en el nodo activo.

12. Para dispositivos que tienen instalada una versión anterior del Agente de red, cree y ejecute la tarea de instalación remota para la nueva versión del Agente de red.

    Le recomendamos que actualice el Agente de red para Linux a la misma versión que Kaspersky Security Center Linux.

    La versión actualizada del Agente de red se instalará una vez que se complete la tarea de instalación remota.

    Ejecute los siguientes comandos en activos basados en Linux para eliminar las dependencias que ya no son necesarias:

    - Para activos basados en Debian, ejecute cualquiera de los siguientes comandos:

      ```
      sudo apt-get -y autoremove
      ```

      ```
      sudo apt -y autoremove
      ```

    - Para activos basados en RPM, ejecute cualquiera de los siguientes comandos:

      ```
      sudo dnf autoremove
      ```

      ```
      sudo yum autoremove
      ```

    Como resultado, instaló la versión más reciente del Servidor de administración en los nodos del clúster de conmutación por error de Kaspersky Security Center Linux.

Actualización de Kaspersky Security Center Web Console

En este artículo, se describe cómo actualizar el Servidor de Kaspersky Security Center Web Console (también llamado Kaspersky Security Center Web Console) en dispositivos con sistema operativo Linux.

Si necesita actualizar Kaspersky Security Center Web Console en Astra Linux en el modo de entorno de software cerrado, siga las instrucciones específicas para Astra Linux.

Utilice el archivo de instalación que corresponda a la distribución de Linux instalada en su dispositivo:

- Para sistemas operativos basados en Debian: ksc-web-console-<número_de_compilación>.x86_64.deb
- Para sistemas operativos basados en RPM: ksc-web-console-<número_de_compilación>.x86_64.rpm

El archivo de instalación debe descargarse del sitio web de Kaspersky.

Para actualizar Kaspersky Security Center Web Console:

1. Asegúrese de que el dispositivo en el que desee actualizar Kaspersky Security Center Web Console cuente con una de las distribuciones de Linux compatibles.
2. Lea y acepte el Contrato de licencia de usuario final (EULA, por las siglas del término en inglés). Si el kit de distribución de Kaspersky Security Center Linux no contiene un archivo TXT con el texto del EULA, puede descargar dicho archivo del sitio web de Kaspersky. Si no está de acuerdo con los términos del Contrato de licencia, no utilice el archivo de instalación para actualizar Kaspersky Security Center Web Console.
3. Utilice el mismo archivo de respuesta que haya preparado antes de instalar Kaspersky Security Center Web Console. El nombre del archivo de respuesta es ksc-web-console-setup.json. La localización del archivo es /etc/ksc-web-console-setup.json.

   Si al instalar Kaspersky Security Center Web Console especificó los valores de los parámetros `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount` y `natsMessageQueueAccount`, asegúrese de que todos estos parámetros estén especificados en el archivo de respuesta.

   Si el archivo de respuesta no existe, cree un nuevo archivo de respuesta que contenga los parámetros para conectar Kaspersky Security Center Web Console al Servidor de administración. Dé a este archivo el nombre ksc-web-console-setup.json y colóquelo en el directorio /etc.

   Ejemplo de un archivo de respuesta que contiene el conjunto mínimo de parámetros

El conjunto de parámetros del archivo de respuesta depende de la versión del Servidor de administración al que se conecta Kaspersky Security Center Web Console:

- Versión 16 o posterior del Servidor de administración

  Ejemplo de un archivo de respuesta con el conjunto mínimo de parámetros para iniciar sesión en la versión 16 o posteriores del Servidor de administración:

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

- Versión 15.4 o posterior del Servidor de administración

  Ejemplo de un archivo de respuesta con el conjunto mínimo de parámetros para iniciar sesión en la versión 15.4 o anteriores del Servidor de administración:

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

Puede instalar Kaspersky Security Center Web Console en el mismo dispositivo donde está el Servidor de administración o en otro dispositivo. Si Kaspersky Security Center Web Console está instalado en otro dispositivo, la dirección de Kaspersky Security Center Web Console (especificada por `address`) y la dirección del Servidor de administración (especificada por `iamHost` o `kscHost`) son diferentes. Si Kaspersky Security Center Web Console está instalado en el mismo dispositivo que el Servidor de administración, estos parámetros tienen los mismos valores.

El valor `iamHost` debe coincidir con la dirección de IAM que especificó durante la instalación del Servidor de administración. Para obtener la dirección de IAM especificada, ejecute el siguiente comando en el dispositivo que tiene el Servidor de administración instalado:

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

Para obtener información detallada, consulte el artículo: Parámetros de instalación de Kaspersky Security Center Web Console.

Puede agregar varios Servidores de administración de diferentes versiones a la lista de servidores de confianza. En este caso, los servidores pueden utilizar diferentes métodos de autenticación.

Si desea actualizar una copia de Kaspersky Security Center Web Console que esté conectada a un Servidor de administración instalado en los nodos de un clúster de conmutación por error de Kaspersky Security Center Linux, en el archivo de respuesta, defina el parámetro de instalación "trusted" para permitir que el clúster de conmutación por error de Kaspersky Security Center Linux se conecte a Kaspersky Security Center Web Console.

Componentes del **parámetro de instalación** `trusted`

Si se conecta al clúster de conmutación por error de Kaspersky Security Center Linux mediante la autenticación de dominio con SSO, especifique el parámetro de instalación de confianza de la siguiente manera: si conecta Kaspersky Security Center Web Console a la versión 16 o posteriores del Servidor de administración, se utilizará la autenticación de dominio con inicio de sesión único (SSO) proporcionada por Identity and Access Manager (IAM). En este caso, especifique el parámetro de instalación `trusted` de la siguiente manera:

```
"trusted":  {
  "<Nombre del Servidor de administración>": {
    "iamHost": "ksc-iam.example.com",
    "iamOAuthPort": 4444,
    "iamProxyPort": 9050,
    "iamCertPath": "<carpeta de datos compartida>/iam/main_certificate.pem",
    "iamPATPath": "<carpeta de datos compartida>/iam/initial_token.txt",
    "kscPort": 13299,
    "kscCertPath": "<carpeta de datos compartida>/1093/cert/klserver.cer"
  }
}
```

donde:

- `<nombre del Servidor de administración>` es el nombre del clúster de conmutación por error de Kaspersky Security Center Linux que se mostrará en el ventana de inicio de sesión de Kaspersky Security Center Web Console.

- `iamHost` es la dirección del dispositivo donde se instalaron el Servidor de administración e IAM. Si creó un adaptador de red secundario al preparar los nodos del clúster, utilice el FQDN o el nombre de host del adaptador como dirección del clúster de conmutación por error de Kaspersky Security Center Linux. De lo contrario, deberá especificar el FQDN o el nombre de host del equilibrador de carga externo que utilice.

  El valor `iamHost` debe coincidir con la dirección de IAM que se especificó durante la instalación del Servidor de administración. Para obtener la dirección de IAM especificada, ejecute el siguiente comando en el dispositivo que tiene el Servidor de administración instalado:

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

- `iamOAuthPort` es el puerto que se utiliza para intercambiar tokens de autentificación a través del protocolo de autenticación OpenID Connect (valor predeterminado: 4444). Este puerto se utiliza tanto para la comunicación entre el Servidor de Kaspersky Security Center Web Console y el Servidor de administración, como entre el navegador (que se utiliza con Kaspersky Security Center Web Console) y el Servidor de administración.

- `iamProxyPort` es el puerto que se utiliza para conectar el Servidor de Kaspersky Security Center Web Console al servidor de administración (valor predeterminado: 9050).

- `iamCertPath` es la ruta al certificado de IAM. El certificado de IAM se crea automáticamente la primera vez que ejecuta el Servidor de administración. El certificado está en el dispositivo donde está instalado el Servidor de administración La ruta predeterminada al certificado es: `<carpeta de datos compartida>/iam/main_certificate.pem`. El certificado se encuentra en el almacenamiento de datos compartido del clúster de conmutación por error de Kaspersky Security Center Linux. El certificado de IAM autofirmado se rota automáticamente.

- `iamPATPath` es la ruta al token utilizado para registrar Kaspersky Security Center Web Console como cliente OAuth en IAM. Este archivo se genera automáticamente la primera vez que se ejecuta el Servidor de administración. El token está en el dispositivo donde está instalado el Servidor de administración. La ruta predeterminada al token es: <carpeta de datos compartida>/iam/initial_token.txt. El token se encuentra en el almacenamiento de datos compartido del clúster de conmutación por error de Kaspersky Security Center Linux. El token es válido indefinidamente y no requiere rotación.

- `kscPort` es el puerto OpenAPI que Kaspersky Security Center Web Console utiliza para conectarse al Servidor de administración (valor predeterminado: 13299).

- `kscCertPath` es el certificado del Servidor de administración que se encuentra en el almacenamiento de datos compartido del clúster de conmutación por error de Kaspersky Security Center Linux. La ruta predeterminada al archivo del certificado es `< carpeta de datos compartida >\1093\cert\klserver.cer`.

  Copie el archivo del certificado del Servidor de administración (especificado con `kscCertPath`), el archivo del certificado de IAM (especificado con `iamCertPath`) y el archivo de token (especificado con `iamPATPath`) desde el almacenamiento de datos compartido y péguelos en el dispositivo donde instale Kaspersky Security Center Web Console. Defina la ruta local al certificado del Servidor de administración.

Si conecta Kaspersky Security Center Web Console a la versión 15.4 o anteriores del Servidor de administración, se utilizará la autenticación especificando el nombre y la contraseña del usuario del dominio o del usuario interno. En este caso, especifique el parámetro de instalación de confianza de la siguiente manera:

```
"trusted":  {
  "<Nombre del Servidor de administración>": {
    "kscHost": "ksc.example.com",
    "kscPort": 13299,
    "kscCertPath": "<carpeta de datos compartida>/1093/cert/klserver.cer"
  }
}
```

donde:

- `< nombre del Servidor de administración >` es el nombre del clúster de conmutación por error de Kaspersky Security Center Linux que se mostrará en el ventana de inicio de sesión de Kaspersky Security Center Web Console.

- `kscHost` es la dirección del Servidor de administración (FQDN o nombre de host). Si creó un adaptador de red secundario al preparar los nodos del clúster, utilice la dirección del adaptador como dirección del clúster de conmutación por error de Kaspersky Security Center Linux. De lo contrario, ingrese la dirección del equilibrador de carga de terceros que esté utilizando.

- `kscPort` es el puerto de OpenAPI que Kaspersky Security Center Web Console utiliza para conectarse al Servidor de administración (valor predeterminado: 13299).

- `kscCertPath` es el certificado del Servidor de administración que se encuentra en el almacenamiento de datos compartido del clúster de conmutación por error de Kaspersky Security Center Linux. La ruta predeterminada al archivo del certificado es `< carpeta de datos compartida >\1093\cert\klserver.cer`. Copie el archivo del certificado de la carpeta compartida al dispositivo en el que se encuentre instalado Kaspersky Security Center Web Console. Defina la ruta local al certificado del Servidor de administración.

Kaspersky Security Center Web Console no se puede actualizar utilizando el mismo archivo de instalación. Si desea cambiar los parámetros de un archivo de respuesta y utilizar ese archivo para reinstalar la aplicación, primero desinstale la aplicación y luego vuelva a instalarla utilizando el nuevo archivo de respuesta.

4. Con una cuenta con privilegios root, use la línea de comandos para ejecutar el archivo de instalación de extensión .deb o .rpm, dependiendo de su distribución de Linux.

   Para actualizar Kaspersky Security Center Web Console a una versión más reciente, ejecute uno de estos comandos:

   - Para dispositivos que ejecutan un sistema operativo basado en RPM:
     `sudo yum install ksc-web-console-<número_de_compilación>.x86_64.rpm`
   - Para dispositivos que ejecutan un sistema operativo basado en Debian:
     `sudo apt-get install ksc-web-console-<número_de_compilación>.x86_64.deb`

   Se iniciará el proceso para desempaquetar el archivo de instalación. Espere a que se complete la instalación.

5. Reinicie todos los servicios de Kaspersky Security Center Web Console con el siguiente comando:
   `sudo systemctl restart KSC*`

Cuando finalice la actualización, puede usar un navegador para abrir Kaspersky Security Center Web Console e iniciar sesión.

Actualización de Kaspersky Security Center Web Console en Astra Linux en el modo de entorno de software cerrado

En esta sección, se explica cómo actualizar el Servidor de Kaspersky Security Center Web Console (también denominado Kaspersky Security Center Web Console) en el sistema operativo Astra Linux Special Edition.

Para actualizar Kaspersky Security Center Web Console:

1. Asegúrese de que el dispositivo en el que desee actualizar Kaspersky Security Center Web Console cuente con una de las distribuciones de Linux compatibles.

2. Lea y acepte el Contrato de licencia de usuario final (EULA, por las siglas del término en inglés). Si el kit de distribución de Kaspersky Security Center Linux no contiene un archivo TXT con el texto del EULA, puede descargar dicho archivo del sitio web de Kaspersky. Si no está de acuerdo con los términos del Contrato de licencia, no utilice el archivo de instalación para actualizar Kaspersky Security Center Web Console.

3. Utilice el mismo archivo de respuesta que haya preparado antes de instalar Kaspersky Security Center Web Console. El nombre del archivo de respuesta es ksc-web-console-setup.json. La localización del archivo es /etc/ksc-web-console-setup.json.

   Si el archivo de respuesta no existe, cree un nuevo archivo de respuesta que contenga los parámetros para conectar Kaspersky Security Center Web Console al Servidor de administración. Dé a este archivo el nombre ksc-web-console-setup.json y colóquelo en el directorio /etc.

   Ejemplo de un archivo de respuesta que contiene el conjunto mínimo de parámetros

El conjunto de parámetros del archivo de respuesta depende de la versión del Servidor de administración al que se conecta Kaspersky Security Center Web Console:

- Versión 16 o posterior del Servidor de administración

  Ejemplo de un archivo de respuesta con el conjunto mínimo de parámetros para iniciar sesión en la versión 16 o posteriores del Servidor de administración:

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

- Versión 15.4 o posterior del Servidor de administración

  Ejemplo de un archivo de respuesta con el conjunto mínimo de parámetros para iniciar sesión en la versión 15.4 o anteriores del Servidor de administración:

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

Puede instalar Kaspersky Security Center Web Console en el mismo dispositivo donde está el Servidor de administración o en otro dispositivo. Si Kaspersky Security Center Web Console está instalado en otro dispositivo, la dirección de Kaspersky Security Center Web Console (especificada por `address`) y la dirección del Servidor de administración (especificada por `iamHost` o `kscHost`) son diferentes. Si Kaspersky Security Center Web Console está instalado en el mismo dispositivo que el Servidor de administración, estos parámetros tienen los mismos valores.

El valor `iamHost` debe coincidir con la dirección de IAM que especificó durante la instalación del Servidor de administración. Para obtener la dirección de IAM especificada, ejecute el siguiente comando en el dispositivo que tiene el Servidor de administración instalado:

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

Para obtener información detallada, consulte el artículo: Parámetros de instalación de Kaspersky Security Center Web Console.

Puede agregar varios Servidores de administración de diferentes versiones a la lista de servidores de confianza. En este caso, los servidores pueden utilizar diferentes métodos de autenticación.

4. Asegúrese de que, en el archivo `/etc/digsig/digsig_initramfs.conf`, el parámetro `DIGSIG_ELF_MODE` aparezca de la siguiente manera:

   ```
   DIGSIG_ELF_MODE=1
   ```

5. Verifique que el paquete de compatibilidad `astra-digsig-oldkeys` esté instalado.

   Si el paquete no está instalado, ejecute el siguiente comando:

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

6. Si no existe, cree un directorio para la clave de la aplicación:

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

7. Coloque la clave de la aplicación, /opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg, en el directorio creado en el paso anterior:

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

   > Si el kit de distribución de Kaspersky Security Center Linux no incluye la clave de la aplicación kaspersky_astra_pub_key.gpg, puede descargarla haciendo clic en este enlace: https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

8. Actualice los discos RAM:

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

   Reinicie el sistema.

9. Con una cuenta con privilegios de root, use la línea de comando para ejecutar el archivo de instalación. El archivo de instalación debe descargarse del sitio web de Kaspersky.

   Para actualizar Kaspersky Security Center Web Console a una versión más reciente, ejecute el siguiente comando:

   ```
   sudo apt-get install ksc-web-console-<número_de_compilación>.x86_64.deb
   ```

   Se iniciará el proceso para desempaquetar el archivo de instalación. Espere a que se complete la instalación.

10. Reinicie todos los servicios de Kaspersky Security Center Web Console con el siguiente comando:

    ```
    sudo systemctl restart KSC*
    ```

Cuando finalice la actualización, puede usar un navegador para abrir Kaspersky Security Center Web Console e iniciar sesión.

Migración a Kaspersky Security Center Linux

Utilice el **Escenario de migración a Kaspersky Security Center** si se cumplen todas las condiciones:

- No necesita instalar el Servidor de administración y el DBMS en dispositivos separados.
- El sistema operativo del Servidor de administración es Ubuntu, Astra Linux, CentOS o RED OS.
- PostgreSQL es adecuado para el nuevo Servidor de administración.
- El Servidor de administración anterior utilizaba PostgreSQL o Microsoft SQL Server como DBMS.

Seleccione **Guía general para migrar a un nuevo servidor de Kaspersky Security Center Linux** si se cumple al menos una de las condiciones:

- Necesita instalar el Servidor de administración y el DBMS en dispositivos separados.
- El nuevo Servidor de administración debe utilizar un DBMS distinto de PostgreSQL.
- El sistema operativo del Servidor de administración no es Ubuntu, Astra Linux, CentOS ni RED OS.

Seleccione **Migración a Kaspersky Security Center mediante el Asistente de migración** si:

- El tipo de DBMS del Servidor de administración de Kaspersky Security Center anterior es distinto del del nuevo servidor y no se utiliza Microsoft SQL Server.
- Tiene experiencia en trasladar dispositivos administrados al nuevo Servidor de administración mediante tareas y utilidades de Kaspersky Security Center.

Consulte los manuales para obtener información detallada sobre las consideraciones especiales y las limitaciones.

Guía general para migrar a un nuevo servidor de Kaspersky Security Center Linux

Puede usar una copia de seguridad de los datos para migrarlos de un Servidor de administración de Kaspersky Security Center Windows o de Kaspersky Security Center Linux a un nuevo servidor de Kaspersky Security Center Linux al migrar la solución o reemplazar el hardware.

Antes de migrar datos de Kaspersky Security Center Windows, asegúrese de que Kaspersky Security Center Linux admita las funciones necesarias de Kaspersky Security Center Windows.

La guía general de migración contempla un escenario en el que el nuevo Servidor de administración recibe un nuevo nombre del DNS. Para restaurar la conexión de los dispositivos administrados, debe cambiar el registro DNS del servidor anterior. Si tiene suficiente experiencia en la configuración de las soluciones, puede diseñar su propio procedimiento para asignar la dirección anterior al nuevo servidor durante la instalación. La presencia del Servidor de administración anterior en la red puede causar fallas en la administración de dispositivos e interferir con el inicio de sesión en Web Console del nuevo Servidor de administración. También puede hacer que la tarea de instalación del Agente de red se conecte al servidor anterior.

Limitaciones

- La migración se puede realizar entre los siguientes DBMS:
  - Microsoft SQL Server → MySQL, MariaDB
  - Microsoft SQL Server → PostgreSQL, Postgres Pro
  - MySQL → MySQL, MariaDB
  - MariaDB → MySQL, MariaDB
  - PostgreSQL → PostgreSQL
  - Postgres Pro → Postgres Pro
- Debe especificar el tipo de DBMS de destino en la utilidad de copia de seguridad al migrar desde Microsoft SQL Server. En los demás casos, la compatibilidad de las bases de datos se determina según el párrafo anterior.
- La versión del DBMS del nuevo Servidor de administración no debe ser anterior a la versión del DBMS utilizado en el Servidor de administración anterior.
- Kaspersky Security Center Windows debe actualizarse a la versión más reciente antes de crear una copia de seguridad para la migración de datos.
- Si utiliza MySQL o MariaDB como DBMS para Kaspersky Security Center Windows y Kaspersky Security Center Linux, el parámetro `lower_case_table_names` debe ser el mismo en el DBMS actual y el nuevo.

1 Preparación para crear una copia de seguridad

Este paso contiene instrucciones para preparar un Servidor de administración configurado previamente para su posterior migración al nuevo Servidor de administración de Kaspersky Security Center Linux. Los pasos preliminares son los siguientes:

1. Compruebe la versión del Servidor de administración para crear una copia de seguridad compatible con Kaspersky Security Center Linux.

   Todas las versiones actuales de **Kaspersky Security Center Linux** admiten la migración de datos al actualizar la aplicación a una versión más reciente. Las copias de seguridad solo se pueden crear y restaurar dentro de un mismo tipo de DBMS.

   Para **Kaspersky Security Center Windows**, consulte la versión del Servidor de administración en **Propiedades** → **General** → **Versión**. Si la versión es anterior a 15.1.0.22239, actualice Kaspersky Security Center Windows a la versión más reciente.

   Actualización de Kaspersky Security Center Windows a la versión más reciente

   1. Desde el sitio web de Kaspersky, descargue el paquete de distribución correspondiente al idioma de localización del Servidor de administración instalado: `Version 15.1.0.22239 | Windows | Full distributive`.

      El archivo ejecutable se guarda en la carpeta **Descargas** con el siguiente nombre: `ksc_15.1_<build number>_full_<language>.exe`.

2. Copie el paquete de distribución en el Servidor de administración.

3. Ejecute el archivo ejecutable `ksc_15.1_<build number>_full_<language>.exe` como administrador.

4. En la ventana que se abre, haga clic en el enlace **Instalar Kaspersky Security Center**.

   Se inicia el asistente de instalación del Servidor de administración.

5. Lea el Contrato de licencia y la Política de privacidad. Si está de acuerdo con todos los términos y condiciones del Contrato de licencia de usuario final y la Política de privacidad, seleccione las siguientes casillas en **Confirmo que he leído y que comprendo y acepto en su totalidad los términos y las condiciones de lo siguiente**:

   - **Los términos y las condiciones de este EULA**.
   - **la Política de privacidad que describe el manejo de los datos**.

6. Seleccione **Actualizar el Servidor de administración y la consola web (recomendado)** y vaya al siguiente paso.

7. Cree una copia de seguridad seleccionando **Quiero crear una copia de seguridad de los datos** y complete el asistente de copia de seguridad.

8. Haga clic en **Actualizar**.

9. Durante la actualización, confirme todos los pasos del asistente de instalación de Web Console para actualizar la versión.

   El proceso de actualización puede tardar algún tiempo. Una vez finalizado el asistente de instalación, es posible que la Consola de administración no acepte conexiones hasta que se inicialice la base de datos.

10. Espere a que finalice la actualización.

2. Verifique que el certificado del Servidor de administración cumpla con los requisitos.

   Antes de crear una copia de seguridad, asegúrese de que el certificado contenga el nombre alternativo del sujeto (SAN). Si el certificado no lo incluye, es importante reemplazarlo; de lo contrario, no podrá iniciar sesión en Web Console después de restaurar una copia de seguridad.

   Para verificar que el certificado incluya un nombre alternativo del sujeto:

   - Para un dispositivo Windows:

     a. En la Consola de administración, seleccione el Servidor de administración que desea verificar.

     b. En el menú contextual, seleccione **Propiedades → General → Ver certificado del Servidor de administración**.

     c. En la ventana que aparece, compruebe el valor de **nombre alternativo del sujeto**.

   - Para un dispositivo Linux, ejecute el siguiente comando:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
     ```

   Asegúrese de que el nombre alternativo del sujeto contenga el nombre de dominio (DNS) del host del Servidor de administración.

Si el valor contiene solo una dirección IP o no aparece ningún valor, reemplace manualmente el certificado por uno que cumpla los requisitos para trabajar con Kaspersky Security Center Linux. Reemplace el certificado general del Servidor de administración mediante la utilidad klsetsrvcert.

Reemplazo del certificado general del Servidor de administración mediante la utilidad klsetsrvcert

1. Cree un certificado nuevo con una fecha de inicio de uso diferida en los dispositivos mediante el siguiente comando:

   - Para Kaspersky Security Center Windows:

     ```
     "%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -t CR -g "
     <oldksc.example.internal>" -o "RsaKeyLen:2048"
     ```

   - Para Kaspersky Security Center Linux:

     ```
     /opt/kaspersky/ksc64/sbin/klsetsrvcert -t CR -g "<oldksc.example.internal>" -o "RsaKeyLen:2048"
     ```

   donde `"<oldksc.example.internal>"` es el FQDN de la conexión al Servidor de administración.

   > No utilice una dirección IP para este valor.

2. Establezca la fecha de inicio del nuevo certificado en todos los hosts mediante el siguiente comando:

   - Para Kaspersky Security Center Windows:

     ```
     "%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -f "DD-MM-YYYY hh:mm"
     ```

   - Para Kaspersky Security Center Linux:

     ```
     /opt/kaspersky/ksc64/sbin/klsetsrvcert -f "DD-MM-YYYY hh:mm"
     ```

   donde la fecha `"DD-MM-YYYY hh:mm"` es al menos 30 días posterior a la fecha actual. De forma predeterminada, el período de distribución de un certificado nuevo (`CR`) es de 90 días.

   > Cuando llegue la fecha configurada, deberá reinstalar Web Console para restaurar el acceso y actualizar su certificado.

3. Si es necesario, después de migrar a un nuevo Servidor de administración, ejecute la utilidad klmover para restaurar la conexión de los hosts con el Servidor de administración. Es posible que deba ejecutar la utilidad si el host estuvo apagado durante todo el período de distribución del certificado o si no se conectó al Servidor de administración.

2 Creación de una copia de seguridad de la instalación anterior del Servidor de administración

Creación de una copia de seguridad de Kaspersky Security Center Windows

1. Desde el menú **Inicio** → **Kaspersky Security Center** → **Utilidad de copia de seguridad de Kaspersky**, ejecute la utilidad `klbackup.exe` desde la carpeta de instalación de Kaspersky Security Center Linux.

   Se inicia el asistente de instalación. En Microsoft Windows en modo Server Core, use la versión de consola de la utilidad klbackup.

2. En el primer paso, seleccione **Realizar copia de seguridad de los datos del Servidor de administración**.

3. En el paso **Configuración de la copia de seguridad**:

   a. Haga clic en el botón **Examinar** y cree una nueva carpeta para guardar la copia de seguridad fuera del directorio predeterminado, por ejemplo, `C:\kscbackups`.

   b. Si utiliza Microsoft SQL Server, seleccione la opción **Migración de la base de datos** → **Migrar al formato de Postgres** para usarla con el script de instalación rápida. Con el método habitual de implementación de Kaspersky Security Center Linux, también puede migrar los datos a una base de datos MySQL/MariaDB.

   c. Establezca una contraseña para la copia de seguridad a fin de proteger los datos contra el acceso no autorizado.

4. Espere a que se cree la copia de seguridad y cierre la utilidad.

Se crea un nuevo directorio en el directorio con la marca de tiempo de la copia de seguridad.

Crear una copia de seguridad de Kaspersky Security Center Linux

1. En el dispositivo del Servidor de administración, introduzca el siguiente comando en la línea de comando:

```
sudo /opt/kaspersky/ksc64/sbin/klbackup -path /root/kscbackups -use_ts
```

2. Espere a que se cree la copia de seguridad.

En el directorio especificado en `-path`, se crea un nuevo directorio con la marca de tiempo de la copia de seguridad.

Después de crear una copia de seguridad del Servidor de administración anterior, retire de servicio el dispositivo que lo aloja.

Retirar de servicio el dispositivo del Servidor de administración

1. Copie la copia de seguridad resultante a la estación de trabajo del administrador para transferir los datos.

2. Apague el sistema operativo del Servidor de administración.

3. Desconecte el adaptador de red de la red corporativa.

4. Libere la dirección IP del dispositivo si desea usarla para la nueva instalación de Kaspersky Security Center Linux.

5. Asegúrese de que el dispositivo esté completamente desconectado.

La presencia del Servidor de administración anterior en la red puede causar fallas en la administración de dispositivos e interferir con el inicio de sesión en Web Console del nuevo Servidor de administración. También puede hacer que la tarea de instalación del Agente de red se conecte al servidor anterior.

3 Instalación inicial de Kaspersky Security Center Linux

- **Preparativos para el despliegue**

  Antes de continuar con la instalación, prepare lo siguiente:

  - La imagen de disco de instalación del sistema operativo y el repositorio de paquetes de la aplicación.
  - Una app de autenticación para la autenticación de dos factores (2FA) al iniciar sesión en Web Console.
  - Un nuevo FQDN (por ejemplo, *ksclinux.example.com*). Si tiene suficiente experiencia en la configuración de las soluciones, puede diseñar su propio procedimiento para asignar el FQDN anterior al nuevo servidor durante la instalación. En este caso, en el paso 5, "Configuración de la aplicación después de restaurarla a partir de una copia de seguridad", omita el paso 4. "Restablecimiento de la conexión de los dispositivos administrados al FQDN del Servidor de administración anterior".
  - La estación de trabajo del administrador con un navegador que permita acceder a Internet para descargar paquetes de distribución y administrar Web Console.
  - Asegúrese de que el servidor DNS y el servidor de hora (NTP) estén disponibles para los componentes de la aplicación.
  - Según el procedimiento, libere la dirección IP anterior si se utilizó una dirección IP para conectar los dispositivos administrados.
  - Configure el equipo de red y el servidor proxy de acuerdo con los requisitos:
    - Puertos para la comunicación de los componentes de la aplicación.
    - Acceso a los servidores de Kaspersky.
    - Guía para reforzar la seguridad.

- **Elección de una configuración, configuración e instalación**

  a. Prepare el equipo para el Servidor de administración, el DBMS y Web Console de acuerdo con los requisitos de hardware y software y los recursos de hardware calculados, a fin de poder administrar la cantidad requerida de dispositivos con la carga prevista.

  Para mejorar la seguridad de los componentes de la solución, incluya la aplicación Kaspersky Endpoint Security for Linux en los cálculos de dimensionamiento e instálela en los nodos de Kaspersky Security Center Linux.

  b. Instale y configure el sistema operativo y los componentes de la solución Kaspersky Security Center de acuerdo con las instrucciones para el despliegue inicial de la solución.

- **Primer inicio de sesión en Web Console**

  1. En el navegador, abra la dirección para conectarse a Web Console: `https://<FQDN>:8080`

  donde `<FQDN>` es la dirección del Servidor de administración especificada en la configuración de instalación del script; por ejemplo, *https://ksclinux.example.com:8080*.

  2. Para iniciar sesión en Web Console, use el nombre de usuario y la contraseña que aparecen en la salida del script.

  3. Configure la app de autenticación:

  a. Copie la clave secreta para obtener códigos de un solo uso en la app o escanee el código QR desde el asistente de configuración de la autenticación de Web Console.

  b. Ingrese el código generado para autenticarse e iniciar sesión en Web Console.

  4. Revise y confirme que ha leído la Guía para reforzar la seguridad.

  5. Configure el Servidor de administración mediante el asistente de inicio rápido si no tiene previsto restaurar los datos del Servidor de administración desde una copia de seguridad.

4 Restauración a partir de una copia de seguridad del Servidor de administración

La restauración a partir de una copia de seguridad del Servidor de administración consta de los siguientes pasos:

1. Transferencia de la copia de seguridad al Servidor de administración

Transfiera la copia de seguridad del Servidor de administración anterior al dispositivo del nuevo Servidor de administración mediante un medio extraíble o a través de la red.

Para transferir la copia de seguridad al Servidor de administración a través de la red:

La posibilidad de usar la utilidad scp para copiar los datos depende de si el servicio SSH está instalado y en ejecución en el sistema operativo del dispositivo del Servidor de administración, así como de la directiva de seguridad de su organización.

1. En la línea de comando del dispositivo, use el comando *cd* para cambiar al directorio que contiene los archivos de la copia de seguridad del Servidor de administración anterior; por ejemplo:

   Windows

   ```
   cd C:\kscbackups
   ```

   Linux

   ```
   cd /root/kscbackups
   ```

2. Copie el directorio que contiene los archivos de la copia de seguridad mediante la utilidad scp:

   ```
   scp -r <klbackup202x-xx-xx> <administrator>@<ksclinux.example.com>:
   ```

   donde:

   `<klbackup202x-xx-xx>` es el directorio que contiene los archivos de la copia de seguridad.

   `<administrator>` es el usuario con privilegios del nuevo Servidor de administración que tiene derechos de conexión SSH.

   `<ksclinux.example.com>` es el FQDN del nuevo Servidor de administración.

   El directorio que contiene la copia de seguridad se copia al directorio de inicio del usuario especificado.

2. Procedimiento para restaurar a partir de una copia de seguridad

1. En el dispositivo del nuevo Servidor de administración, abra la línea de comando.

2. Mientras restaura los datos a partir de una copia de seguridad, otorgue temporalmente derechos de superusuario de PostgreSQL a las cuentas estándar klserver y kliam que el Servidor de administración usa para conectarse al DBMS:

   ```
   sudo -i -u postgres psql -c "ALTER ROLE klserver WITH SUPERUSER;"
   ```

   ```
   sudo -i -u postgres psql -c "ALTER ROLE kliam WITH SUPERUSER;"
   ```

3. Use la utilidad klbackup para iniciar la restauración de los datos a partir de la copia de seguridad del Servidor de administración anterior:

   ```
   sudo /opt/kaspersky/ksc64/sbin/klbackup -path </home/administrator/klbackup202x-xx-xx> -restore
   ```

   donde `</home/administrator/klbackup202x-xx-xx>` es la ruta completa al directorio que contiene los archivos de la copia de seguridad.

4. Si no se estableció una contraseña para la copia de seguridad, cuando se le solicite, presione **Intro** sin escribir ninguna contraseña.

5. Espere a que finalice la utilidad.

   Las instalaciones grandes pueden tardar mucho tiempo.

6. Restaure los derechos originales de las cuentas de PostgreSQL que el Servidor de administración usa para conectarse al DBMS.

```
sudo -i -u postgres psql -c "ALTER ROLE klserver WITH NOSUPERUSER;"
```

```
sudo -i -u postgres psql -c "ALTER ROLE kliam WITH NOSUPERUSER;"
```

5 Configuración de la aplicación después de restaurarla a partir de una copia de seguridad

Omita este paso si no restauró los datos a partir de una copia de seguridad.

El procedimiento para configurar la aplicación después de restaurarla a partir de una copia de seguridad consta de los siguientes pasos:

1. Restauración de Web Console

1. Obtenga la dirección del servidor anterior del archivo de configuración de IAM Server:

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

Ejemplo

```
ksc_address: "oldksc.example.internal"
```

2. Compruebe que la dirección FQDN del Servidor de administración anterior se convierta correctamente en la dirección IP de bucle invertido del nuevo Servidor de administración. Para hacerlo, realice los siguientes pasos:

   a. Ejecute el comando `ping` con la dirección del Servidor de administración anterior.

   Ejemplo de obtención correcta de una dirección IP de bucle invertido

```
administrator@ksclinux:~$ ping oldksc.example.internal
ping oldksc.example.internal
PING ksclinux (127.0.1.1) 56(84) bytes of data.
64 bytes from ksclinux (127.0.1.1): icmp_seq=1 ttl=64 time=0.037 ms
```

   b. Agregue la dirección del Servidor de administración anterior al archivo `[[/etc/hosts]]` del sistema operativo del nuevo Servidor de administración si no se obtuvo la dirección o si se obtuvo una dirección IP externa. Para hacerlo, realice los siguientes pasos:

   - Abra /etc/hosts para editarlo:

```
sudo nano /etc/hosts
```

- Ingrese el nombre del servidor anterior como alias adicional para la dirección del dispositivo del Servidor de administración.

  Ejemplo

  ```
  127.0.0.1       localhost
  127.0.1.1       ksclinux.example.com ksclinux oldksc.example.internal
  <...>
  ```

3. Reinstale Web Console.

   a. Elimine el Servidor de Web Console local:

   Según su distribución de Kaspersky Security Center Linux, ejecute uno de los siguientes comandos:

   - Para un dispositivo que ejecuta un sistema operativo basado en Debian:

     ```
     sudo apt remove ksc-web-console -y
     ```

   - Para un dispositivo que ejecuta un sistema operativo basado en Red Hat Enterprise Linux:

     ```
     sudo dnf remove ksc-web-console -y
     ```

   b. Inicie la instalación del paquete de Web Console desde el directorio que contiene los paquetes de distribución:

   - En un dispositivo que ejecuta un sistema operativo basado en Debian:

     ```
     sudo apt install ~/kscdistr/ksc-web-console-16.3.12907.x86_64.deb -y
     ```

   - Para un dispositivo que ejecuta un sistema operativo basado en Red Hat Enterprise Linux:

     ```
     sudo dnf install ~/kscdistr/ksc-web-console-16.3.12907.x86_64.rpm -y
     ```

2. Restauración del acceso del usuario kscadmin para la migración desde Kaspersky Security Center Windows

La base de datos de usuarios se ha sobrescrito; cree el usuario kscadmin y configure la autenticación de dos factores desde cero.

1. Abra la línea de comando en el sistema operativo del dispositivo del Servidor de administración y ejecute el siguiente comando para crear un usuario:

   ```
   sudo /opt/kaspersky/ksc64/sbin/kladduser -n kscadmin
   ```

   Después de presionar **Intro**, establezca una contraseña y vuelva a ingresarla.

2. En su navegador, abra la dirección para conectarse a Web Console:

```
https://<FQDN>:8080
```

donde `<FQDN>` es la dirección del Servidor de administración especificada en la configuración de instalación del script; por ejemplo, *https://ksclinux.example.com:8080*.

3. Utilice el nombre de usuario y la contraseña generados para iniciar sesión en Web Console.

4. Configure una app de autenticación. Para hacerlo, realice los siguientes pasos:

   a. Elimine el perfil anterior de la cuenta de usuario kscadmin que configuró en su app de autenticación antes de comenzar a restaurar la copia de seguridad del Servidor de administración.

   b. Copie la clave secreta para obtener códigos de un solo uso en la app o escanee el código QR desde el asistente de configuración de la autenticación de Web Console.

   c. Ingrese el código generado para autenticarse e iniciar sesión en Web Console.

3. Prueba del Servidor de administración

1. Pruebe la interfaz de Web Console con el usuario kscadmin y con otros usuarios.

2. Ejecute las siguientes tareas en secuencia:

   - Descargar actualizaciones en el repositorio del Servidor de administración
   - Mantenimiento del Servidor de administración
   - Copia de seguridad de los datos del Servidor de administración

   Reemplace las rutas de Windows en la configuración de las tareas por las rutas de Linux del nuevo Servidor de administración, o elimine las tareas y configure otras nuevas desde cero.

3. Revise los resultados de las tareas y, si es necesario, modifique la configuración de las tareas, las directivas de administración y la configuración del Servidor de administración.

4. Restablecimiento de la conexión de los dispositivos administrados al FQDN del Servidor de administración anterior

Si asignó un nuevo FQDN al nuevo Servidor de administración (por ejemplo, ksclinux.example.com), agregue uno de los siguientes tipos de registros DNS:

- Un registro CNAME que asigne el nombre anterior del Servidor de administración al nuevo nombre del Servidor de administración.

  Para obtener más información sobre cómo configurar los registros requeridos, consulte la documentación de su Servidor DNS.

- Un registro A y un registro AAAA para la dirección anterior del Servidor de administración que apunten a la nueva dirección IP del Servidor de administración.

  Para un servicio DNS basado en Windows Server, ejecute los comandos con los valores correspondientes a su infraestructura.

Para agregar un registro A de DNS para un servicio DNS basado en Windows Server, ejecute los comandos con los valores correspondientes a su infraestructura:

1. Conéctese al Servidor DNS.
2. Abra PowerShell y obtenga la dirección IP del registro A existente mediante el siguiente comando:

```
Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
```

3. Cambie la dirección IP del registro A mediante los siguientes comandos:

```
$OldKSC = Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
```

```
$NewKSC = $OldKSC.Clone()
```

```
$NewKSC.RecordData.IPv4Address = [System.Net.IPAddress]::parse('<IP-address of the administration server>')
```

```
Set-DnsServerResourceRecord -OldInputObject $OldKSC -NewInputObject $NewKSC -ZoneName "<zone name>"
```

4. Compruebe que la dirección IP del registro A se haya actualizado mediante el siguiente comando:

```
Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
```

La salida del comando muestra la dirección IP del Servidor de administración de Kaspersky Security Center Linux. Los dispositivos administrados restaurarán sus conexiones después de actualizar la caché DNS local.

6 Configuración de la protección antivirus del Servidor de administración

Para implementar las recomendaciones de protección antivirus de la Guía para reforzar la seguridad en el Servidor de administración, instale las aplicaciones de Kaspersky en el Servidor de administración y configure las directivas de administración de las aplicaciones instaladas.

La instalación y la configuración constan de los siguientes pasos:

1. Creación de un grupo de administración independiente

1. En la ventana principal de Web Console, seleccione **Administración de activos → Jerarquía de grupos**.
2. Seleccione la casilla junto al grupo **Dispositivos administrados**.
3. Haga clic en **Agregar**.
4. En la ventana que aparece, escriba un nombre para el nuevo grupo (por ejemplo, *kscserver*) y confirme su creación haciendo clic en el botón **Agregar**.

2. Creación de una directiva para el Agente de red sin heredar la configuración

1. En la ventana principal de Web Console, vaya a la sección **Administración de activos → Directivas**.
2. Luego, haga clic en el botón **Agregar**.
3. En el Asistente de nueva directiva, seleccione la aplicación **Agente de red de Kaspersky Security Center Linux** y haga clic en **Siguiente**.
4. Desactive la opción **Heredar configuración de la directiva principal** y haga clic en **Guardar**.

3. Instalación del complemento de administración de Kaspersky Endpoint Security for Linux desde Kaspersky Security Center Linux o de forma manual

Puede instalar el complemento de administración de Kaspersky Endpoint Security for Linux de las siguientes maneras:

- Desde la lista de paquetes de distribución disponibles en Web Console
- Manualmente desde un archivo

Para instalar el complemento de administración de Kaspersky Endpoint Security desde la lista de paquetes de distribución disponibles en Web Console:

1. En la ventana principal de Web Console, seleccione **Configuración → Complementos web**.

   Se abre la lista de complementos web instalados.

2. Luego, haga clic en el botón **Agregar**.

   Se muestra la lista de complementos de administración disponibles. Esta lista se actualiza automáticamente cada vez que se publica una nueva versión de un complemento web.

3. En la lista de complementos disponibles, seleccione la versión más reciente del complemento web de Kaspersky Endpoint Security for Linux.
4. En la ventana de descripción del complemento web, haga clic en el botón **Instalar complemento**.
5. Espere a que finalice la instalación y haga clic en el botón **Aceptar** de la ventana de información.

El nuevo complemento se agrega a la lista de complementos web instalados.

Video: instalación del complemento web mediante el asistente



Para instalar manualmente el complemento de administración de Kaspersky Endpoint Security desde un archivo:

1. Descargue el archivo que contiene el complemento web desde la página de descarga de la aplicación, en la sección Kaspersky Endpoint Security for Linux: **Complemento de Control de aplicaciones → Complemento de la consola web**.

2. Descomprima el archivo descargado en el equipo local.

3. En la ventana principal de Web Console, seleccione **Configuración → Complementos web**.

   Se abre la lista de complementos web instalados.

4. Haga clic en el botón **Agregar desde archivo**.

5. En la ventana que se abre, ingrese la ruta del archivo plugin.zip y la ruta del archivo signature.txt.

   Estos archivos se encuentran en la carpeta en la que descomprimió el archivo que contiene el complemento web.

6. Luego, haga clic en el botón **Agregar**.

7. Espere a que finalice la instalación y haga clic en el botón **Aceptar** de la ventana de información.

El nuevo complemento aparece en la lista de complementos web instalados (**Configuración → Complementos web**).

Video: instalación del complemento web de administración en redes aisladas



4. Creación de una directiva para Kaspersky Endpoint Security for Linux sin heredar la configuración

Al usar Kaspersky Endpoint Security for Linux junto con Kaspersky Security Center Linux, debe configurar la directiva de acuerdo con las recomendaciones de los expertos de Kaspersky.

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Seleccione un grupo de administración para el Servidor de administración.
3. Haga clic en **Agregar**.

   El Asistente de nueva directiva se inicia.
4. En la ventana que se abre, seleccione la aplicación Kaspersky Endpoint Security for Linux de la lista.
5. Especifique el **Modo estándar o modo de Endpoint Detection and Response Agent** para Kaspersky Endpoint Security for Linux.
6. Decida si desea utilizar Kaspersky Security Network.
7. Revise las recomendaciones de optimización para los dispositivos administrados.
8. En el nombre de la directiva, indique que la directiva pertenece al Servidor de administración.
9. Desactive la opción **Heredar la configuración de la directiva principal**.
10. Guarde sus cambios.

Video: creación de una directiva



5. Creación de una tarea de grupo de actualización para Kaspersky Endpoint Security for Linux

1. En la ventana principal de Web Console, seleccione la sección **Tareas**.
2. Seleccione un grupo de administración para el Servidor de administración.
3. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea.
4. En la ventana que se abre, seleccione la aplicación Kaspersky Endpoint Security for Linux de la lista.
5. Especifique el tipo de tarea *Actualización* y avance por los siguientes pasos sin cambiar ninguna configuración.

   Se abre la ventana de propiedades de la tarea.
6. En la sección **Configuración de la aplicación → Orígenes de actualizaciones**, habilite la fuente de Kaspersky Security Center y aumente su prioridad.

En una red aislada, use Kaspersky Update Utility para crear un repositorio para las tareas de actualización.

Video: configuración de las actualizaciones centralizadas de las bases de datos



6. Adición de una clave de licencia al repositorio del Servidor de administración con distribución automática

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione la sección **Licencias**.
2. Haga clic en **Agregar**.
3. Seleccione la opción **Código de activación** y haga clic en **Enviar**.

   En una red aislada, use un archivo de clave que puede solicitar mediante el servicio disponible en https://keyfile.kaspersky.com/en.
4. En la lista de licencias, haga clic en el nombre de la licencia.
5. Seleccione la casilla **Distribuir la clave de licencia automáticamente a los dispositivos administrados**.
6. Guarde sus cambios.

Video: activación de la aplicación con un código de activación



Video: activación de la aplicación con un archivo de clave



7. Creación de paquetes de instalación para el Agente de red y Kaspersky Endpoint Security for Linux

1. En la ventana principal de Web Console, seleccione **Administración de software → Paquetes de instalación**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente de nuevo paquete.

3. Seleccione **Crear un paquete de instalación para una aplicación de Kaspersky**.
4. En la lista de aplicaciones, busque la versión más reciente de Kaspersky Endpoint Security for Linux y haga clic en su nombre.
5. En la barra lateral, haga clic en el botón **Descargar y crear paquete de instalación** para iniciar la descarga.

   Revise y acepte los contratos de licencia para comenzar a usar las aplicaciones.
6. Vuelva a la lista de aplicaciones y descargue la versión más reciente del Agente de red de Kaspersky para Linux.

   Revise y acepte los contratos de licencia para comenzar a usar las aplicaciones.
7. En la ventana principal de Web Console, haga clic en los nombres de las aplicaciones de la lista de aplicaciones descargadas.

En una red aislada, descargue los paquetes de distribución del sitio web de Kaspersky y, en el Asistente de nuevo paquete, seleccione la opción **Crear un paquete de instalación a partir de un archivo**.

Video: creación automática de un paquete de instalación en Kaspersky Security Center



Video: creación manual de un paquete de instalación a partir de un archivo en Kaspersky Security Center



8. Instalar el Agente de red para Linux

1. En la ventana principal de Web Console, seleccione **Administración de software → Paquetes de instalación**.
2. Seleccione la casilla junto al paquete **Agente de red de Kaspersky para Linux**.
3. Haga clic en **Desplegar**.

   Se abre el Asistente de despliegue de la protección.
4. Seleccione la opción **Uso de un paquete independiente**.
5. En el paso **Mover dispositivos a la carpeta Dispositivos administrados**, omita la configuración de las reglas para mover dispositivos a un grupo de administración. Esta opción no se aplica al dispositivo del Servidor de administración.
6. En el paso **Resultado de la creación del paquete de instalación independiente**, seleccione y copie la ruta completa al script de instalación de la aplicación.
7. Abra la línea de comando del sistema operativo del Servidor de administración.
8. Inicie la instalación del paquete independiente:

   ```
   sudo bash "</var/opt/.../stand-alone_package_sh>"
   ```

   donde `</var/opt/.../stand-alone_package_sh>` es la ruta completa al archivo de script del paquete de instalación independiente que copió anteriormente.

   Si la instalación se realiza correctamente, se muestra una notificación que lo confirma.
9. Mueva el dispositivo del Servidor de administración (por ejemplo, *ksclinux*) del grupo **Dispositivos administrados** al grupo de administración preparado anteriormente (por ejemplo, *kscserver*).

9. Instalar Kaspersky Endpoint Security for Linux

1. En la ventana principal de Web Console, seleccione **Administración de software → Paquetes de instalación**.
2. Seleccione la casilla del paquete de Kaspersky Endpoint Security for Linux.
3. Haga clic en **Desplegar**.

   Se abre el Asistente de despliegue de la protección.
4. Seleccione la opción **Uso de un paquete independiente**.
5. En el paso **Resultado de la creación del paquete de instalación independiente**, seleccione y copie la ruta completa al script de instalación de la aplicación.
6. Abra la línea de comando del sistema operativo del Servidor de administración.
7. Inicie la instalación del paquete independiente:

   ```
   sudo bash "</var/opt/.../stand-alone_package_sh>"
   ```

   donde `</var/opt/.../stand-alone_package_sh>` es la ruta completa al archivo de script del paquete de instalación independiente que copió anteriormente.

   Si la instalación se realiza correctamente, se muestra una notificación que lo confirma.

8. En la ventana principal de Web Console, en la sección **Tareas**, seleccione el nodo raíz de la lista de grupos de administración que lleva el nombre del Servidor de administración.

9. En la lista de tareas del Servidor de administración, inicie las siguientes tareas en este orden:

   - "Descargar actualizaciones en el repositorio del Servidor de administración"
   - Actualización (Kaspersky Endpoint Security for Linux)

10. En la ventana principal de Web Console, seleccione **Administración de activos** → **Dispositivos administrados**.

11. Haga clic en el nombre del objeto de dispositivo del Servidor de administración.

12. Revise los valores de los principales indicadores del estado del dispositivo:

    - Última actualización de las bases de datos de antivirus (actualizadas)
    - Conectado al Servidor de administración (actualizado)
    - Estado de la protección (En ejecución)
    - Evento *Clave agregada correctamente* (presente)

Siga el escenario de despliegue de Kaspersky Endpoint Security for Linux para desplegar la aplicación en los dispositivos de su red.

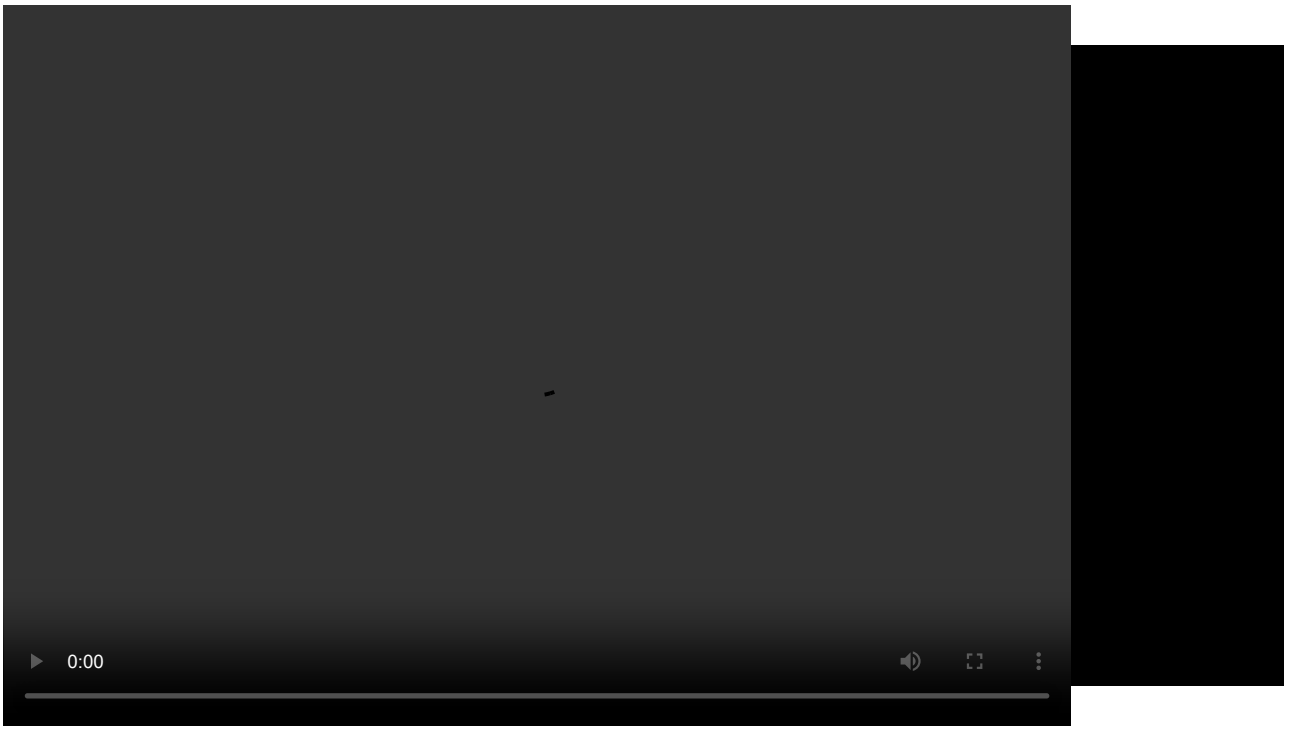
Video tutorial: Migrar a Kaspersky Security Center Linux con un respaldo de los datos del Servidor de administración

Vea el video para aprender a migrar los datos del Servidor de administración de Kaspersky Security Center Windows a Kaspersky Security Center Linux utilizando el respaldo de los datos del Servidor de administración (con la utilidad klbackup).

Para admitir la migración de datos a PostgreSQL o Postgres Pro, debe enviar una solicitud al Soporte técnico de Kaspersky e instalar uno de los siguientes parches:

- Para Kaspersky Secure Mobility Management basado en Kaspersky Security Center 14.2 Windows: 14.2.0.48079-pf5
- Para Kaspersky Security Center 15.1 Windows: 15.1.0.20748-pf2

La migración de datos a PostgreSQL o Postgres Pro también está disponible después de actualizar Kaspersky Security Center Windows a la versión 15.1.0.22239.



Migrar a Kaspersky Security Center Linux con un respaldo de los datos del Servidor de administración Video

Migración a Kaspersky Security Center a través del Asistente de migración

En este escenario, puede transferir la estructura del grupo de administración, incluidos los dispositivos administrados y otros objetos de grupo (directivas, tareas, tareas globales, etiquetas y selecciones de dispositivos) desde Kaspersky Security Center Windows bajo la administración de Kaspersky Security Center Linux.

La migración de datos a Kaspersky Security Center es posible con la versión 15.1.0.22239 o posterior de Kaspersky Security Center Windows.

Características del método de migración

- Migración parcial de los datos del Servidor de administración
- La selección de objetos para la migración está disponible
- El grupo o subgrupo de administración que se va a migrar no puede contener más de 10 000 dispositivos
- Se utiliza para transferir parcialmente los datos del Servidor de administración, incluidos solo los objetos de grupo dentro del alcance de la migración. Los objetos de grupo fuera del alcance de la migración deben restaurarse manualmente

Alcance de la migración

- Estructura de grupos de administración
- Dispositivos administrados incluidos en los grupos de administración (no más de 10 000 dispositivos)
- Etiquetas asignadas a los dispositivos de migración

- Tareas globales del Agente de red y aplicaciones administradas (no para el Servidor de administración)
- Tareas de grupo del Agente de red y aplicaciones administradas
- Directivas de aplicaciones administradas
- Plantillas de informes
- Rol de usuario
- Usuarios y grupos de seguridad internos
- Categorías de aplicaciones personalizadas con contenido agregado manualmente
- Selecciones de dispositivos personalizados

Limitaciones

- La migración solo es posible desde Kaspersky Security Center Windows (versión 15.1 o posterior) a Kaspersky Security Center Linux (versión 15 o posterior).
- Solo puede realizar este escenario mediante el uso de Kaspersky Security Center Web Console.
- Los siguientes ámbitos no se pueden migrar:
  - Tareas globales del Servidor de administración
  - Eventos guardados en el Servidor de administración
  - Repositorio de paquetes de distribución de aplicaciones para instalación remota
  - Certificado del Servidor de administración
  - Claves de licencia utilizadas por el Servidor de administración y las aplicaciones administradas
  - Servidores de administración virtuales
  - Ajustes de la directiva del Agente de red
  - Reglas de movimiento de dispositivos
  - Reglas para etiquetar dispositivos de forma automática
  - Puntos de distribución
  - Configuración de la aplicación de Kaspersky guardada en el Servidor de administración

Antes de comenzar, obtenga más información sobre las características y las limitaciones de Kaspersky Security Center Linux:

- Diferencias funcionales entre Kaspersky Security Center Windows y Kaspersky Security Center Linux
- Lista de aplicaciones de Kaspersky compatibles con Kaspersky Security Center Linux

Etapas

El escenario de migración se desarrolla en etapas:

1 Pasos preliminares

Este paso contiene instrucciones para preparar un Servidor de administración configurado previamente para su posterior migración al nuevo Servidor de administración de Kaspersky Security Center Linux. Los pasos preliminares son los siguientes:

1. Compruebe la versión del Servidor de administración para crear una copia de seguridad compatible con Kaspersky Security Center Linux.

   Todas las versiones actuales de **Kaspersky Security Center Linux** admiten la migración de datos al actualizar la aplicación a una versión más reciente. Las copias de seguridad solo se pueden crear y restaurar dentro de un mismo tipo de DBMS.

   En **Kaspersky Security Center Windows**, compruebe la versión del Servidor de administración en **Propiedades** → **General** → **Versión**. Si la versión es anterior a 15.1.0.22239, actualice Kaspersky Security Center Windows a la versión más reciente.

   Actualización de Kaspersky Security Center Windows a la versión más reciente

   1. Desde el sitio web de Kaspersky, descargue el paquete de distribución correspondiente al idioma de localización del Servidor de administración instalado: `Version 15.1.0.22239 | Windows | Full distributive`.

      El archivo ejecutable se guarda en la carpeta **Descargas** con el siguiente nombre: `ksc_15.1_<build number>_full_<language>.exe`.

   2. Copie el paquete de distribución en el Servidor de administración.

   3. Ejecute el archivo ejecutable `ksc_15.1_<build number>_full_<language>.exe` como administrador.

   4. En la ventana que se abre, haga clic en el enlace **Instalar Kaspersky Security Center**.

      Se inicia el asistente de instalación del Servidor de administración.

   5. Lea el Contrato de licencia y la Política de privacidad. Si está de acuerdo con todos los términos y condiciones del Contrato de licencia de usuario final y la Política de privacidad, seleccione las siguientes casillas en **Confirmo que he leído y que comprendo y acepto en su totalidad los términos y las condiciones de lo siguiente**:

      - **Los términos y las condiciones de este EULA**.
      - **la Política de privacidad que describe el manejo de los datos**.

   6. Seleccione **Actualizar el Servidor de administración y la consola web (recomendado)** y vaya al siguiente paso.

   7. Cree una copia de seguridad seleccionando **Quiero crear una copia de seguridad de los datos** y complete el asistente de copia de seguridad.

   8. Haga clic en **Actualizar**.

9. Durante la actualización, confirme todos los pasos del asistente de instalación de Web Console para actualizar la versión.

   El proceso de actualización puede tardar algún tiempo. Una vez finalizado el asistente de instalación, es posible que la Consola de administración no acepte conexiones hasta que se inicialice la base de datos.

10. Espere a que finalice la actualización.

2. Verifique que el certificado del Servidor de administración cumpla con los requisitos.

   Antes de crear una copia de seguridad, asegúrese de que el certificado contenga el nombre alternativo del sujeto (SAN). Si el certificado no lo incluye, es importante reemplazarlo; de lo contrario, no podrá iniciar sesión en Web Console después de restaurar una copia de seguridad.

   Para verificar que el certificado incluya un nombre alternativo del sujeto:

   - Para un dispositivo Windows:

     a. En la Consola de administración, seleccione el Servidor de administración que desea verificar.

     b. En el menú contextual, seleccione **Propiedades → General → Ver certificado del Servidor de administración**.

     c. En la ventana que aparece, compruebe el valor de **nombre alternativo del sujeto**.

   - Para un dispositivo Linux, ejecute el siguiente comando:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
     ```

   Asegúrese de que el nombre alternativo del sujeto contenga el nombre de dominio (DNS) del host del Servidor de administración.

   Si el valor contiene únicamente una dirección IP externa sin un nombre de dominio (DNS), o si no aparece ningún valor, reemplace manualmente el certificado por uno que cumpla con los requisitos para trabajar con Kaspersky Security Center Linux. Reemplace el certificado general del Servidor de administración mediante la utilidad klsetsrvcert.

   Reemplazo del certificado general del Servidor de administración mediante la utilidad klsetsrvcert

   1. Cree un certificado nuevo con una fecha de inicio de uso diferida en los dispositivos mediante el siguiente comando:

      - Para Kaspersky Security Center Windows:

        ```
        "%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -t CR -g "
        <oldksc.example.internal>" -o "RsaKeyLen:2048"
        ```

      - Para Kaspersky Security Center Linux:

        ```
        /opt/kaspersky/ksc64/sbin/klsetsrvcert -t CR -g "<oldksc.example.internal>" -o "RsaKeyLen:2048"
        ```

      donde `"<oldksc.example.internal>"` es el FQDN de la conexión al Servidor de administración.

      No utilice una dirección IP para este valor.

2. Establezca la fecha de inicio del nuevo certificado en todos los hosts mediante el siguiente comando:

   - Para Kaspersky Security Center Windows:

     ```
     "%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -f "DD-MM-YYYY hh:mm"
     ```

   - Para Kaspersky Security Center Linux:

     ```
     /opt/kaspersky/ksc64/sbin/klsetsrvcert -f "DD-MM-YYYY hh:mm"
     ```

   donde la fecha `"DD-MM-YYYY hh:mm"` es al menos 30 días posterior a la fecha actual. De forma predeterminada, el período de distribución de un certificado nuevo (`CR`) es de 90 días.

   > Cuando llegue la fecha configurada, deberá reinstalar Web Console para restaurar el acceso y actualizar su certificado.

3. Si es necesario, después de migrar a un nuevo Servidor de administración, ejecute la utilidad klmover para restaurar la conexión de los hosts con el Servidor de administración. Es posible que deba ejecutar la utilidad si el host estuvo apagado durante todo el período de distribución del certificado o si no se conectó al Servidor de administración.

2 Elija un método de migración

Debe realizar la migración a Kaspersky Security Center Linux a través del Asistente de migración. Los pasos del Asistente de migración dependen de si los Servidores de administración de Kaspersky Security Center Windows y Kaspersky Security Center Linux están organizados en una jerarquía:

- Migración con una jerarquía de Servidores de administración

  Elija esta opción si el Servidor de administración de Kaspersky Security Center Windows actúa como Servidor secundario del Servidor de administración de Kaspersky Security Center Linux. Usted podrá encargarse del proceso de migración y cambiar de un Servidor a otro utilizando una sola instancia de Kaspersky Security Center Web Console. Si prefiere esta opción, puede organizar los Servidores de administración en una jerarquía para simplificar el procedimiento de migración. Para hacerlo, cree la jerarquía antes de iniciar la migración.

- Migración con un archivo de exportación (archivo ZIP)

  Elija esta opción si los Servidores de administración de Kaspersky Security Center Windows y Kaspersky Security Center Linux no están organizados en una jerarquía. Para llevar a cabo la migración, puede utilizar dos instancias de Kaspersky Security Center Web Console: una para Kaspersky Security Center Windows y otra para Kaspersky Security Center Linux. En este caso, utilizará el archivo de exportación que creó y descargó durante la exportación desde Kaspersky Security Center Windows e importará este archivo a Kaspersky Security Center Linux.

3 Cree una copia de seguridad del certificado y la clave privada del Servidor de administración de Kaspersky Security Center Windows (paso opcional)

Es posible que desee poner los dispositivos administrados bajo la administración del Servidor de administración de Kaspersky Security Center Linux mediante la restauración del certificado y la clave privada del Servidor de administración a partir de una copia de seguridad. En este caso, haga una copia de seguridad del certificado y la clave privada del Servidor de administración de Kaspersky Security Center Windows. A continuación, en la etapa 7, debe restaurar el certificado y la clave privada.

4 Exportación de datos desde Kaspersky Security Center Windows

Abra Kaspersky Security Center Windows y, luego, ejecute el Asistente de migración.

5 Importe datos a Kaspersky Security Center Linux

Continúe con el Asistente de migración para importar los datos exportados a Kaspersky Security Center Linux. Si los servidores están organizados en una jerarquía, la importación se inicia de forma automática después de una exportación exitosa dentro del mismo asistente. Si los servidores no están organizados en una jerarquía, continúe con el Asistente de migración después de cambiar a Kaspersky Security Center Linux.

6 Realice acciones adicionales para transferir objetos y configuraciones de Kaspersky Security Center Windows a Kaspersky Security Center Linux de forma manual (paso opcional)

También es posible transferir los objetos y las configuraciones que no se pueden transferir a través del Asistente de migración. Por ejemplo, también puede hacer lo siguiente:

- Transferir las claves de licencia que utilizó el Servidor de administración y las aplicaciones administradas
- Configurar tareas globales del Servidor de administración
- Configurar los ajustes de la directiva del Agente de red
- Crear paquetes de instalación de aplicaciones
- Crear Servidores virtuales
- Configurar reglas de movimiento de dispositivos
- Configurar reglas para etiquetar dispositivos de forma automática
- Crear categorías de aplicaciones

- Asignar y configurar puntos de distribución

  Si mueve un dispositivo que actúa como punto de distribución a otro Servidor de administración, los dispositivos incluidos en el alcance del punto de distribución no se mueven automáticamente. Tiene que mover cada dispositivo individualmente. Si un punto de distribución actúa como puerta de enlace, debe ejecutar el script `# /opt/kaspersky/klnagent64/bin/setup/postinstall.pl` para que el punto de distribución ya no funcione como puerta de enlace.

7 Mueva los dispositivos administrados importados bajo la administración de Kaspersky Security Center Linux:

Para completar la migración, mueva los dispositivos administrados importados bajo la administración de Kaspersky Security Center Linux. Puede hacerlo usando uno de los siguientes métodos:

- Mediante la utilidad klmover

  Use la utilidad klmover y especifique la configuración de conexión para el nuevo Servidor de administración.

- Mediante la tarea *Cambiar Servidor de administración*

  Cree una tarea *Cambiar Servidor de administración*, especifique los dispositivos administrados importados, el nuevo Servidor de administración y otras configuraciones de la tarea. Luego, ejecute la tarea para poner los dispositivos administrados bajo la administración del Servidor de administración de Kaspersky Security Center Linux.

- Mediante la eliminación (si ya está instalado) y la instalación posterior del Agente de red en los dispositivos administrados

  Cree un nuevo paquete de instalación del Agente de red y especifique la configuración de conexión para el nuevo Servidor de administración en las propiedades del paquete de instalación. Elimine el Agente de red en los dispositivos administrados importados y, luego, use el paquete de instalación para instalar el Agente de red en los dispositivos administrados importados a través de una tarea de instalación remota. También puede crear y utilizar un paquete de instalación independiente para instalar el Agente de red de manera local. Para obtener más información, consulte Cambio de dispositivos administrados bajo la administración de Kaspersky Security Center Linux.

- A través de la restauración del certificado y la clave privada del Servidor de administración desde una copia de seguridad (solo para la migración a Kaspersky Security Center Linux 15.1 o versiones posteriores)

  Asigne al dispositivo que aloja el Servidor de administración de Kaspersky Security Center Linux la misma dirección IP asignada al Servidor de administración de Kaspersky Security Center Windows. Ejecute la utilidad klbackup con el parámetro `-cert_only` para restaurar el certificado del Servidor de Administración y la clave privada desde la copia de seguridad que guardó en la etapa 3. En la línea de comandos, ejecute el siguiente comando: `/opt/kaspersky/ksc64/sbin/klbackup -path <ruta a la copia de seguridad del certificado del Servidor de administración> -restore -cert_only`.

8 Actualice el Agente de red a la versión más reciente

Actualice el Agente de red para Linux a la misma versión que Kaspersky Security Center.

9. Asegúrese de que los dispositivos administrados estén visibles en el nuevo Servidor de administración

En el Servidor de administración de Kaspersky Security Center Linux, abra la lista de dispositivos administrados (**Administración de activos** → **Dispositivos administrados**) y verifique los valores en las columnas **Visible**, **Agente de red instalado** y **Última conexión con el Servidor de administración**.

Otros métodos de migración de datos

Además del asistente de migración, existen otros métodos para transferir los objetos actuales, pero solo permiten transferir tareas y directivas:

- Exporte las tareas de Kaspersky Security Center Windows y, luego, impórtelas en Kaspersky Security Center Linux.
- Exporte directivas específicas de Kaspersky Security Center Windows y luego impórtelas en Kaspersky Security Center Linux. Los perfiles de las directivas que seleccione se exportarán e importarán junto con las directivas.

Exportación de objetos de grupo desde Kaspersky Security Center Windows

La estructura del grupo de administración de la migración, incluidos los dispositivos administrados y otros objetos de grupo de Kaspersky Security Center Windows a Kaspersky Security Center Linux, requiere que primero seleccione los datos para exportar y cree un archivo de exportación. El archivo de exportación contiene información sobre todos los objetos de grupo que desea migrar. El archivo de exportación se utilizará para la importación posterior a Kaspersky Security Center Linux.

Puede exportar los siguientes objetos:

- Tareas y directivas de aplicaciones administradas
- Tareas globales
- Selecciones de dispositivos personalizados
- Estructura del grupo de administración y dispositivos incluidos
- Etiquetas que se asignaron a los dispositivos en migración

Antes de iniciar la exportación, lea la información general sobre la migración a Kaspersky Security Center Linux. Elija el método de migración: puede utilizar o no la jerarquía de servidores de administración de Kaspersky Security Center Windows y Kaspersky Security Center Linux.

Para exportar dispositivos administrados y objetos afines a través del Asistente de migración, haga lo siguiente:

1. Realice una de las siguientes acciones (dependiendo de si los servidores de administración de Kaspersky Security Center Windows y Kaspersky Security Center Linux están organizados en una jerarquía):

   - Si los servidores están organizados en una jerarquía, abra Kaspersky Security Center Web Console y cambie al servidor de Kaspersky Security Center Windows.

   - Si los servidores no están organizados en una jerarquía, abra una instancia de Kaspersky Security Center Web Console conectada a Kaspersky Security Center Windows.

2. En el menú principal, vaya a **Operaciones** → **Migración**.

3. Seleccione **Migrar a Kaspersky Security Center Linux o a Open Single Management Platform** para iniciar el asistente y seguir los pasos.

4. Seleccione el grupo o subgrupo de administración que desee exportar. Asegúrese de que el grupo o subgrupo de administración seleccionado no tenga más de 10 000 dispositivos.

5. Seleccione las aplicaciones administradas cuyas tareas y directivas desee exportar. Seleccione solo aquellas aplicaciones que sean compatibles con Kaspersky Security Center Linux. Los objetos de las aplicaciones incompatibles se exportarán de todos modos, pero no podrán utilizarse.

6. Utilice los vínculos que verá en el lado izquierdo para seleccionar las tareas globales, las selecciones de dispositivos y los informes que desee exportar. Puede usar el vínculo **Objetos de grupo** para excluir los roles personalizados, los usuarios internos, los grupos de seguridad internos y las categorías de aplicaciones personalizadas que no desee exportar.

Se crea el archivo de exportación (archivo ZIP). Dependiendo de si realiza o no una migración compatible con la jerarquía del Servidor de administración, el archivo de exportación se guarda de la siguiente manera:

- Si los Servidores están organizados en una jerarquía, el archivo de exportación se guarda en la carpeta temporal del servidor de Kaspersky Security Center Web Console.

- Si los Servidores no están organizados en una jerarquía, el archivo de exportación se descarga en su dispositivo.

Para una migración compatible con la jerarquía del Servidor de administración, la importación se inicia automáticamente después de una exportación exitosa. Para una migración no compatible con la jerarquía del Servidor de administración, puede importar manualmente el archivo de exportación guardado a Kaspersky Security Center Linux.

Importar el archivo de exportación en Kaspersky Security Center Linux

Para transferir información sobre dispositivos administrados, objetos y sus configuraciones que exportó desde Kaspersky Security Center Windows, debe importarla a Kaspersky Security Center Linux o Kaspersky Next XDR Expert.

Para importar dispositivos administrados y objetos afines a través del Asistente de migración, haga lo siguiente:

1. Realice una de las siguientes acciones (dependiendo de si los servidores de administración de Kaspersky Security Center Windows y Kaspersky Security Center Linux están organizados en una jerarquía):

   - Si los servidores están organizados en una jerarquía, continúe con el siguiente paso del Asistente de migración una vez completada la exportación. La importación comienza automáticamente después de una exportación exitosa dentro de este asistente (consulte el paso 2 de esta instrucción).

   - Si los Servidores no están organizados en una jerarquía:

     a. Abra la aplicación Kaspersky Security Center Web Console conectada a Kaspersky Security Center Linux o Kaspersky Next XDR Expert.

     b. En el menú principal, vaya a **Operaciones** → **Migración**.

     c. Seleccione el archivo de exportación (archivo ZIP) que creó y descargó durante la exportación desde Kaspersky Security Center Windows. Se iniciará la carga del archivo de exportación.

2. Una vez que el archivo de exportación se haya cargado correctamente, podrá continuar con la importación. Si desea especificar otro archivo de exportación, haga clic en el vínculo **Cambiar** y, luego, seleccione el archivo deseado.

3. Se muestra toda la jerarquía de grupos de administración de Kaspersky Security Center Linux.

   Seleccione la casilla de verificación junto al grupo de administración de destino al que se deben restaurar los objetos de grupo de administración exportado (dispositivos administrados, directivas, tareas y otros objetos de grupo).

4. Comenzará la importación de objetos de grupo. No podrá minimizar el Asistente de migración ni realizar ninguna operación simultánea durante la importación. Espere a que los íconos de actualización (🔄) ubicados junto a los elementos de la lista de objetos cambien por marcas de verificación verdes (✓) y se complete la importación.

5. Una vez que concluya la importación, verá la estructura de grupos de administración exportada (incluidos los detalles de los dispositivos) en el grupo de administración de destino que haya seleccionado. Si intenta restaurar un objeto que tenga el mismo nombre que un objeto existente, se agregará un sufijo secuencial al nombre del objeto restaurado.

> Si una tarea migrada contiene los datos de la cuenta con la cual ha de ejecutarse, una vez que se complete la importación, deberá abrir la tarea e ingresar la contraseña nuevamente.

Si la importación se completó con un error, puede realizar una de las siguientes acciones:

- Para la migración con soporte de jerarquía del Servidor de administración, puede comenzar a importar el archivo de exportación nuevamente.

- Para la migración sin compatibilidad con la jerarquía del Servidor de administración, puede iniciar el Asistente de migración para seleccionar otro archivo de exportación y luego importarlo nuevamente.

Puede comprobar si los objetos de grupo incluidos en el alcance de la exportación se han importado correctamente a Kaspersky Security Center Linux. Para ello, vaya a la sección **Administración de activos** y asegúrese de que los objetos importados aparezcan en las subsecciones correspondientes.

Tenga en cuenta que los dispositivos administrados importados se muestran en la subsección **Dispositivos administrados**, pero son invisibles en la red y el Agente de red si no estás instalados ni ejecutándose en ellos (el valor *No* en las columnas **Visible**, **Agente de red instalado** y **Agente de red en ejecución**

Para completar la migración, debe cambiar los dispositivos administrados para que estén bajo la administración de Kaspersky Security Center Linux.

Cambiar los dispositivos administrados para que estén bajo la administración de Kaspersky Security Center Linux

Después de una importación exitosa de información sobre dispositivos administrados, objetos y su configuración a Kaspersky Security Center Linux, debe cambiar los dispositivos administrados para que estén bajo la administración de Kaspersky Security Center Linux para completar la migración.

Puede mover los dispositivos administrados para que estén bajo Kaspersky Security Center Linux mediante uno de los siguientes métodos:

- Mediante la utilidad klmover.
- Usar la tarea *Cambiar Servidor de administración*.
- Restaurar el certificado y la clave privada del Servidor de administración a partir de una copia de seguridad (solo para la migración a Kaspersky Security Center Linux 15.1 o posterior).

  Para obtener más información, consulte el paso «Mover los dispositivos administrados importados bajo la administración de Kaspersky Security Center Linux» en el escenario principal de migración de datos.
- Mediante la instalación del Agente de red en los dispositivos administrados a través de una tarea de instalación remota.

Para cambiar los dispositivos administrados para que estén bajo la administración de Kaspersky Security Center Linux instalando el Agente de red:

1. Elimine el Agente de red en los dispositivos administrados importados que se cambiarán bajo la administración de Kaspersky Security Center Linux.
2. Cambie al Servidor de Administración de Kaspersky Security Center Windows.
3. Vaya a **Administración de software** → **Paquetes de instalación** y luego abra las propiedades de un paquete de instalación existente del Agente de red.

   Si el paquete de instalación del Agente de red no está en la lista de paquetes, descargue uno nuevo.

   También puede crear y utilizar un paquete de instalación independiente para instalar el Agente de red de manera local.
4. En la pestaña **Configuración**, seleccione la sección **Conexión**. Defina los ajustes de conexión del Servidor de administración de Kaspersky Security Center Linux.

5. Cree una tarea de instalación remota para dispositivos administrados importados y luego especifique el paquete de instalación del Agente de red reconfigurado.

   Puede instalar el Agente de red a través del Servidor de administración de Kaspersky Security Center Windows o mediante un dispositivo basado en Windows que actúa como punto de distribución. Si utiliza el Servidor de administración, habilite la opción **Con los recursos del sistema operativo a través del Servidor de administración**. Si utiliza un punto de distribución, habilite la opción **Con los recursos del sistema operativo a través de los puntos de distribución**.

6. Ejecute la tarea de instalación remota.

Una vez que la tarea de instalación remota finalice exitosamente, vaya al Servidor de administración de Kaspersky Security Center Linux y asegúrese de que los dispositivos administrados estén visibles en la red y que el Agente de red esté instalado y ejecutándose en ellos (el valor *Sí* en **Visible**, **Agente de red instalado** y **Agente de red en ejecución** columnas).

Configuración del Servidor de administración

Esta sección describe el proceso de configuración y las propiedades del Servidor de administración.

Configurar la dirección de conexión con el Servidor de administración

La dirección de conexión con el Servidor de administración es la dirección de red que se usa para los siguientes propósitos:

- Como dirección predeterminada al crear los paquetes de instalación del Agente de red

  Después de la instalación del Agente de red, los dispositivos administrados se conectan al Servidor de administración con esta dirección.

- Como dirección del servidor proxy de KSN

  Los dispositivos administrados se conectan al servidor proxy KSN a través de esta dirección.

Para configurar la dirección de conexión con el Servidor de administración:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, elija la sección **General**.

3. En la ventana que se abre, en el campo **Dirección de conexión con el Servidor de administración**, especifique la nueva dirección de conexión con el Servidor de administración.

   La longitud máxima de la dirección de conexión es de 255 caracteres.

   Puede especificar la dirección de conexión con el Servidor de administración como el nombre NetBIOS, FQDN o la dirección IP del Servidor de administración.

4. Haga clic en el botón **Guardar**.

La dirección especificada se utiliza como la dirección del Servidor de administración y la dirección del servidor proxy de KSN.

Configuración de la conexión de Kaspersky Security Center Web Console al Servidor de administración

Puede configurar la conexión de Kaspersky Security Center Web Console al Servidor de administración a través de las propiedades del Servidor de administración o mediante la configuración de directivas del Servidor de administración.

Para configurar los puertos de conexión a través del Servidor de administración:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la ficha **General**, seleccione la sección **Puertos de conexión**.

3. Si es necesario, especifique el **Puerto SSL para Web Console** o especifique otros puertos de conexión con el Servidor de administración.

Los principales ajustes de conexión del servidor seleccionado quedan indicados.

Para establecer los puertos de conexión a través de la configuración de la directiva del Servidor de administración:

1. En el menú principal, vaya a **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva del Servidor de administración y luego vaya a la pestaña **Configuración de la aplicación**.

3. Si es necesario, especifique el **Puerto SSL para Web Console** o especifique otros puertos de conexión con el Servidor de administración.

   Si desactiva la opción **Abrir puerto para Web Console** y esta configuración de directiva se aplica al dispositivo, usted no podrá conectarse al Servidor de administración mediante Kaspersky Security Center Web Console. En este caso, la conexión se cerrará. Si tiene un Servidor de administración en el que no se aplica esta directiva, puede volver a conectarse a este Servidor de administración a través de Kaspersky Security Center Web Console.

Los principales ajustes de conexión del servidor seleccionado quedan indicados.

Configurar una lista de direcciones IP autorizadas a iniciar sesión en Kaspersky Security Center Linux

De forma predeterminada, cualquier dispositivo tiene permitido conectarse a Kaspersky Security Center Linux. Por ejemplo, puede instalar Kaspersky Security Center Web Console Server en cualquier dispositivo que cumpla con los requisitos, y Kaspersky Security Center Web Console Server se comunicará con Kaspersky Security Center Linux. Sin embargo, puede configurar el Servidor de administración para que las conexiones solo se permitan desde dispositivos con las direcciones IP que especifique. En este caso, si un intruso intenta conectarse a Kaspersky Security Center Linux a través del Servidor de Kaspersky Security Center Web Console instalado en un dispositivo que no está incluido en la lista de admitidos, no podrá iniciar sesión en Kaspersky Security Center Linux.

La dirección IP se verifica cuando el usuario inicia sesión en Kaspersky Security Center Linux o ejecuta una aplicación que interactúa con el Servidor de administración a través de la interfaz OpenAPI de Kaspersky Security Center Linux. En este momento, una aplicación en un dispositivo intenta establecer una conexión con el Servidor de administración. Si la dirección IP del dispositivo no está en la lista de direcciones permitidas, ocurre un error de autenticación y el evento KLAUD_EV_SERVERCONNECT indica que no se estableció conexión con el Servidor de administración.

Requisitos para la lista de direcciones IP permitidas

Las direcciones IP se controlan solo cuando las siguientes aplicaciones intentan conectarse al Servidor de administración:

- Servidor de Kaspersky Security Center Web Console

  Si utiliza Kaspersky Security Center Web Console para iniciar sesión en Kaspersky Security Center Linux, puede usar las herramientas habituales de su sistema operativo para configurar un firewall en el dispositivo que tenga instalado el Servidor de Kaspersky Security Center Web Console. El firewall puede evitar que un intruso inicie sesión en Kaspersky Security Center Linux desde un dispositivo que no sea el que tenga instalado el Servidor de Kaspersky Security Center Web Console.

- Aplicaciones que interactúan con el Servidor de administración a través de objetos de automatización de klakaut

- Aplicaciones que interactúan con el Servidor de administración a través de OpenAPI, como Kaspersky Anti Targeted Attack Platform o Kaspersky Security for Virtualization

Por consiguiente, debe especificar las direcciones de todo dispositivo que tenga instalada una de las aplicaciones anteriores.

La lista puede contener direcciones IPv4 e IPv6. No puede contener intervalos de direcciones IP.

Cómo definir una lista de direcciones IP permitidas

Si es la primera vez que crea una lista de direcciones permitidas, siga estas instrucciones.

Para definir la lista de direcciones IP que podrán iniciar sesión en Kaspersky Security Center Linux:

1. En el dispositivo en el que se encuentre instalado el Servidor de administración, abra el símbolo del sistema con una cuenta con derechos de administrador.

2. Cambie de directorio a la carpeta de instalación de Kaspersky Security Center Linux (generalmente, /opt/kaspersky/ksc64/sbin).

3. Ingrese el siguiente comando en la cuenta root:
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP addresses>" -t s`

   Introduzca las direcciones IP que haya recopilado siguiendo los criterios de más arriba. Utilice un punto y coma para separar cada dirección.

   Ejemplo para permitir que un solo dispositivo se conecte al Servidor de administración:

   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0" -t s`

   Ejemplo para permitir que varios dispositivos se conecten al Servidor de administración:

   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 198.51.100.0; 203.0.113.0" -t s`

4. Reinicie el servicio del Servidor de administración.

Para saber si la lista de direcciones IP admitidas se definió correctamente, consulte el registro de eventos de Syslog en el Servidor de administración.

Cómo modificar una lista de direcciones IP permitidas

Para modificar una lista de direcciones permitidas, puede seguir los mismos pasos que utilizó para crearla. Ejecute el mismo comando que la primera vez y defina una nueva lista:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP
addresses>" -t s
```

Si desea eliminar algunas direcciones IP de la lista de admitidos, debe reescribirla. Por ejemplo, su lista de admitidos incluye las siguientes direcciones IP: 192.0.2.0; 198.51.100.0; 203.0.113.0. Desea eliminar la dirección IP 198.51.100.0. Para hacer esto, ingrese el siguiente comando en el símbolo del sistema:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0;
203.0.113.0" -t s
```

No olvide reiniciar el servicio del Servidor de administración.

Cómo eliminar una lista de direcciones IP permitidas

Si ya ha definido una lista de direcciones IP permitidas y desea eliminarla:

1. Ingrese el siguiente comando en el símbolo del sistema en la cuenta root:
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "" -t s`
2. Reinicie el servicio del Servidor de administración.

Una vez que complete estos pasos, el control de direcciones IP quedará deshabilitado.

Configuración de las opciones de acceso a Internet para el Servidor de administración

Debe configurar el acceso a Internet para usar Kaspersky Security Network y descargar actualizaciones y bases de datos antivirus para Kaspersky Security Center Linux y las aplicaciones de Kaspersky administradas.

Para especificar la configuración de acceso a Internet para el Servidor de administración:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.
2. En la pestaña **General**, seleccione la sección **Configuración de acceso a Internet**.

3. Active la opción **Usar servidor proxy** si quiere usar un servidor proxy al conectarse a Internet. Si activa esta opción, los campos estarán disponibles para ingresar ajustes. Deberá introducir los siguientes valores de conexión del servidor proxy:

   Dirección del servidor proxy

   Dirección del servidor proxy usado para conectar Kaspersky Security Center Linux a Internet.

   Número de puerto

   Número del puerto a través del cual se establecerá la conexión proxy de Kaspersky Security Center Linux.

   No usar el servidor proxy para direcciones locales

   Ningún servidor proxy se usará para conectarse a los dispositivos en la red local.

   Autenticación del servidor proxy

   Si se selecciona esta casilla, en los campos de entrada se podrán especificar las credenciales para la autenticación del servidor proxy.

   Este campo de entrada está disponible cuando la casilla **Usar servidor proxy** está desmarcada.

   Nombre de usuario

   Cuenta de usuario con la que se establece la conexión al servidor proxy (este campo está disponible si se selecciona la casilla **Autenticación del servidor proxy**).

   Contraseña

   Contraseña que especifica el usuario con cuya cuenta se establece la conexión al servidor proxy (este campo está disponible si se selecciona la casilla **Autenticación del servidor proxy**).

   Para ver la contraseña indicada, mantenga presionado el botón **Mostrar** durante la cantidad de tiempo que sea necesario.

También puede configurar el acceso a Internet mediante el asistente de inicio rápido.

Jerarquía de Servidores de administración

Algunas empresas cliente (por ejemplo, los MSP) pueden tener varios servidores de administración en funcionamiento. Puede ser poco conveniente administrar varios Servidores de administración independientes, por lo que se puede aplicar una jerarquía. En una jerarquía, un Servidor de administración instalado en Linux puede funcionar como servidor principal o como servidor secundario. Un Servidor de administración principal instalado en Linux puede administrar servidores secundarios instalados tanto en Linux como en Windows. Un servidor principal basado en Windows puede administrar un servidor secundario basado en Linux.

La configuración "principal/secundario" de dos Servidores de administración proporciona las opciones siguientes:

- El Servidor de administración secundario hereda directivas, tareas, roles de usuario y paquetes de instalación del Servidor de administración principal. De esta forma, se evita la duplicación de configuraciones.
- Las selecciones de dispositivos en el Servidor de administración principal pueden incluir dispositivos desde los Servidores de administración secundarios.

- Los informes sobre el Servidor de administración principal pueden contener datos (incluida información detallada) de los Servidores de administración secundarios.
- El Servidor de administración principal puede actuar como origen de actualizaciones del Servidor de administración secundario.

El Servidor de administración principal solo recibe datos de Servidores de administración secundarios no virtuales dentro del alcance de las opciones antes enumeradas. Esta limitación no se aplica a los Servidores de administración virtuales, que comparten la base de datos con su Servidor de administración principal.

La jerarquía de los Servidores de administración es compatible con el modo de multiinquilinato. Este modo permite que un administrador principal administre varios clientes de forma centralizada e independiente. Cada organización u oficina cliente está aislada de las demás y se denomina inquilino. Puede asignar varios dispositivos administrados junto con sus datos, configuraciones, directivas y tareas asociados a un inquilino, y configurar los derechos de usuario por inquilino.

Un Servidor de administración principal, instalado en la infraestructura de la organización principal, actúa como inquilino principal. El Servidor de administración principal permite que los Servidores de administración secundarios o virtuales (sus inquilinos aislados) reciban y procesen de forma independiente sus propios eventos y trabajen con sus propios recursos, servicios y configuraciones.

Un proveedor de servicios que tenga varias organizaciones cliente puede proporcionar las funcionalidades de Kaspersky Security Center Linux, incluida la combinación de alertas y las acciones de respuesta, a cada organización cliente de forma independiente. Para lograr esto, el proveedor de servicios conecta Servidores de administración secundarios o virtuales como inquilinos para cada organización cliente. El proveedor de servicios brinda servicios utilizando su propio personal y recursos.

Creación de una jerarquía de servidores de administración: agregar un Servidor de administración secundario

En una jerarquía, un Servidor de administración instalado en Linux puede funcionar como servidor principal o como servidor secundario. Un Servidor de administración principal instalado en Linux puede administrar servidores secundarios instalados tanto en Linux como en Windows. Un servidor principal basado en Windows puede administrar un servidor secundario basado en Linux.

Agregado del Servidor de administración secundario (realizado en el futuro Servidor de administración principal)

Puede agregar un Servidor de administración como Servidor de administración secundario, estableciendo así una jerarquía "principal/secundario".

Para agregar un Servidor de administración secundario al que sea posible conectarse mediante Kaspersky Security Center Web Console:

1. Asegúrese de que el puerto 13000 del futuro Servidor de administración principal esté disponible.

   Este puerto se utilizará para la interacción entre el Servidor de administración principal y el Servidor de administración secundario después de crear la jerarquía.

2. Vaya a las propiedades del futuro Servidor de administración principal:

   a. En el menú principal, seleccione una sección (salvo **Marketplace**, **Navegación por la consola** y **Configuración**) y, a continuación, en la parte superior de la página, haga clic en el botón **Mostrar jerarquía**.

   b. En el panel de navegación que se abre, coloque el cursor sobre el nombre del Servidor de administración que necesite y luego haga clic en el ícono de configuración (⚙).

      También puede hacer clic en el nombre del Servidor de administración y luego, una vez que el nombre aparezca en el menú principal, seleccionarlo desde el menú principal para abrir la ventana de propiedades del servidor.

3. En la ventana de propiedades que se abre, haga clic en la pestaña **Servidores de administración**.

4. Marque la casilla adyacente al nombre del grupo de administración al que desee agregar el Servidor de administración.

5. En la línea del menú, haga clic en **Conectar Servidor de administración secundario**.

   Se inicia el Asistente para agregar un Servidor de administración secundario. Utilice el botón **SIGUIENTE** para avanzar al siguiente paso del asistente.

6. Complete los siguientes campos:

   Conectar el Servidor de administración principal a un Servidor de administración secundario en DMZ

   Seleccione esta opción si el Servidor de administración secundario está en una zona desmilitarizada (DMZ).

   Si se selecciona esta opción, el Servidor de administración principal inicia la conexión con el Servidor de administración secundario. En caso contrario, el Servidor de administración secundario inicia la conexión con el Servidor de Administración primario.

   Nombre para mostrar del Servidor secundario

   Un nombre para identificar al Servidor de administración secundario en la jerarquía. Puede usar, por ejemplo, la dirección IP del Servidor o una frase como "Servidor secundario para el grupo 1".

   Dirección del Servidor secundario

   Escriba la dirección IP o el nombre de dominio del Servidor de administración secundario.

   Este parámetro es necesario si la opción **Conectar el Servidor de administración principal al Servidor de administración secundario en DMZ** está habilitada.

   Puerto SSL del servidor

   Especifique el número del puerto SSL que se utilizará para la interacción entre los Servidores de administración principales y secundarios después de crear la jerarquía. El número de puerto predeterminado es 13000.

   Puerto de la API del servidor

   El número del puerto que Web Console utilizará para recibir conexiones del Servidor de administración secundario a través de OpenAPI. El número de puerto predeterminado es 13299.

   Al crear la jerarquía, Web Console se conecta al futuro Servidor de administración secundario, solicita las credenciales, obtiene el certificado público y realiza la configuración inicial.

   Una vez creada la jerarquía de Servidores de administración, el puerto 13299 dejará de utilizarse. Los Servidores de administración se comunicarán a través del puerto 13000.

   Certificado del Servidor de administración secundario

Agregue un archivo de certificado. Puede cargar el certificado manualmente desde su dispositivo u obtenerlo del Servidor de administración secundario.

7. Especifique la configuración de conexión y autenticación:

   - Introduzca la dirección del futuro Servidor de administración principal.
   - Seleccione la opción **Usar servidor proxy** si utiliza un servidor proxy para conectarse al Servidor de administración secundario.

     En este caso, también tiene que especificar la siguiente configuración del servidor proxy:

     - **Dirección del servidor proxy**
     - **Nombre de usuario**
     - **Contraseña**

8. Ingrese las credenciales de un usuario que tenga derechos para acceder al futuro Servidor de administración secundario.

El asistente finaliza, se establece la conexión con el futuro Servidor secundario y se crea la jerarquía "principal/secundario".

La conexión entre los Servidores de administración principal y secundario se establece a través del puerto 13000. Se recibirán y aplicarán las tareas y directivas del Servidor de administración principal. El Servidor de administración secundario se muestra en el Servidor de administración principal, en el grupo de administración donde se agregó.

La conexión falla en los siguientes casos:

- La configuración de conexión es incorrecta.

  Debe comprobar la configuración o especificar manualmente el certificado del futuro Servidor secundario.

- El futuro Servidor secundario se autentica con un certificado autofirmado generado automáticamente por Kaspersky Security Center Linux. En tal caso, el navegador podría bloquear la descarga del certificado autofirmado.

  Puede realizar una de las siguientes acciones:

  - Cree un certificado para el futuro Servidor secundario que se considere de confianza en su infraestructura y que cumpla con los requisitos para certificados personalizados.
  - Agregue el certificado autofirmado del futuro Servidor secundario a la lista de certificados de confianza del navegador. Recomendamos que utilice esta opción solo si no puede crear un certificado personalizado. Para obtener información sobre cómo agregar un certificado a la lista de certificados de confianza, consulte la documentación de su navegador.

Agregado del Servidor de administración secundario (realizado en el futuro Servidor de administración secundario)

Puede agregar un Servidor de administración secundario aunque no pueda conectarse al mismo (lo cual puede ocurrir, por ejemplo, si el Servidor no está disponible o no está conectado temporalmente o si el Servidor usa un archivo de certificado autofirmado).

Para agregar un Servidor de administración como secundario que no se pueda conectar mediante Kaspersky Security Center Web Console:

1. Envíe el archivo de certificado del futuro Servidor de administración principal al administrador del sistema de la oficina donde se encuentra el futuro Servidor de administración secundario (por ejemplo, puede escribir el archivo en un dispositivo externo, como una unidad flash o enviarlo por correo electrónico).

   El archivo del certificado se encuentra en el futuro Servidor de administración principal, en /var/opt/kaspersky/klnagent_srv/1093/cert/.

2. Solicite al administrador del sistema a cargo del futuro Servidor de administración secundario que haga lo siguiente:

   a. Haga clic en el nombre del Servidor de administración.

   b. En la página de propiedades que se abre, vaya a la sección **Jerarquía de Servidores de administración** de la pestaña **General**.

   c. Seleccione la opción **Este Servidor de administración es un servidor secundario en la jerarquía**.

   d. Seleccione el tipo de Servidor de administración principal.

   e. En el campo **Dirección del Servidor de administración principal**, ingrese el nombre de red del Servidor de administración principal futuro.

   f. Seleccione el archivo guardado anteriormente que contiene el certificado del futuro Servidor de administración principal haciendo clic en **Especificar el certificado del Servidor de administración principal**.

   g. De ser necesario, seleccione la casilla **Conectar el Servidor de administración principal a un Servidor de administración secundario en DMZ**.

   h. Si la conexión con el futuro Servidor de administración principal se establece a través de un servidor proxy, seleccione la casilla **Usar servidor proxy** y especifique los ajustes de conexión.

   i. Haga clic en el botón **Guardar**.

Así se constituye la jerarquía "principal/secundario". El Servidor de administración principal comienza a recibir conexiones del Servidor de administración secundario utilizando el puerto 13000. Se recibirán y aplicarán las tareas y directivas del Servidor de administración principal. El Servidor de administración secundario se muestra en el Servidor de administración principal, en el grupo de administración donde se agregó.

Ver la lista de servidores de administración secundarios

Para ver la lista de los Servidores de administración secundarios (incluido el virtual), haga lo siguiente:

1. En el menú principal, seleccione una sección (salvo **Marketplace**, **Navegación por la consola** y **Configuración**).
2. En la parte superior de la página, haga clic en el botón **Mostrar jerarquía**.

   En el panel de navegación que se abre, se muestra la lista de servidores de administración secundarios (incluidos los virtuales). Haga clic en alguno de los nombres para interactuar con el Servidor de administración correspondiente.

No puede continuar a los Servidores de administración virtuales si abrió el panel de navegación desde las secciones **Intervalos IP** y **Objetos eliminados**.
También se muestran los grupos de administración. Podrá administrar los grupos si abrió el panel de navegación desde las siguientes secciones: **Dispositivos administrados**, **Directivas**, **Tareas** y **Puntos de distribución**. De lo contrario, verá los grupos en color gris.

Si está conectado a su Servidor de administración principal en Kaspersky Security Center Web Console y no puede conectarse a un Servidor de administración virtual administrado por un Servidor de administración secundario, puede usar una de las siguientes estrategias:

- **Modifique la instalación existente de Kaspersky Security Center Web Console para agregar el servidor secundario a la lista de servidores de administración de confianza.** Una vez que haga esto, podrá conectarse al Servidor de administración virtual en Kaspersky Security Center Web Console.

  1. En el dispositivo en el que esté instalado Kaspersky Security Center Web Console, ejecute el archivo de instalación de Kaspersky Security Center Web Console correspondiente a la distribución de Linux que esté instalada en el dispositivo. Utilice para ello una cuenta con privilegios administrativos.

     Se iniciará el asistente de configuración. Avance por el asistente utilizando el botón **Siguiente**.
  2. Seleccione la opción **Actualizar**.
  3. En el paso **Tipo de modificación**, seleccione la opción **Editar la configuración de conexión**.
  4. En el paso **Servidores de administración de confianza**, agregue el Servidor de administración secundario necesario.
  5. En el último paso, haga clic en **Modificar** para aplicar la nueva configuración.
  6. Cuando la aplicación se haya reconfigurado, haga clic en el botón **Finalizar**.

- Use Kaspersky Security Center Web Console para conectarse directamente al Servidor de administración secundario en el que se haya creado el servidor virtual. Una vez que haga esto, podrá cambiar al Servidor de administración virtual en Kaspersky Security Center Web Console.

Administración de servidores de administración virtuales

En esta sección, se describen las siguientes acciones para administrar Servidores de administración virtuales.

- Crear Servidores de administración virtual
- Habilitar y deshabilitar Servidores de administración virtual
- Asignar un administrador para un Servidor de administración virtual
- Cambiar el Servidor de administración de los dispositivos cliente
- Eliminar Servidores de administración virtual

Crear un Servidor de administración virtual

Puede crear servidores de administración virtuales y agregarlos a grupos de administración.

Cuando crea un Servidor de administración virtual, hereda la lista de usuarios y todos los derechos de usuario del Servidor de administración principal. Si un usuario tiene derechos de acceso al Servidor principal, este usuario también tiene derechos de acceso al Servidor virtual. Después de la creación, usted configura los derechos de acceso a los servidores de forma independiente.

Para crear y agregar un Servidor de administración virtual:

1. En el menú principal, haga clic en el nombre del Servidor de administración.
2. En la página que se abre, vaya a la pestaña **Servidores de administración**.
3. Seleccione el grupo de administración al que quiere agregar el Servidor de administración virtual.
   El Servidor de administración virtual administrará los dispositivos que pertenezcan al grupo seleccionado (o a los subgrupos de ese grupo).
4. En la línea del menú, haga clic en **Nuevo Servidor de administración virtual**.
5. En la página que se abre, defina las propiedades del nuevo Servidor de administración virtual:
   - **Nombre del Servidor de administración virtual**.
   - **Dirección de conexión con el Servidor de administración**.
     Puede usar el nombre o la dirección IP del Servidor de administración.

6. En la lista de usuarios, seleccione al administrador del Servidor de administración virtual. Si lo desea, puede editar una de las cuentas existentes antes de asignarle la función de administrador o crear una nueva cuenta de usuario.

   Si es necesario, puede crear una nueva cuenta que actuará como administrador del Servidor de Administración virtual utilizando la utilidad kladduser. Para ello, utilice el siguiente comando:

   ```
   kladduser -n <user_name> -p <password> -vs <virtual_server_name>
   ```

   donde virtual_server_name es el nombre del Servidor de administración virtual.

7. Haga clic en el botón **Guardar**.

Se crea el nuevo Servidor de administración virtual y se lo agrega al grupo de administración seleccionado. El nuevo Servidor aparecerá en la pestaña **Servidores de administración**.

Si está conectado a su Servidor de administración principal en Kaspersky Security Center Web Console y no puede conectarse a un Servidor de administración virtual administrado por un Servidor de administración secundario, puede usar una de las siguientes estrategias:

- **Modifique la instalación existente de Kaspersky Security Center Web Console para agregar el servidor secundario a la lista de servidores de administración de confianza.** Una vez que haga esto, podrá conectarse al Servidor de administración virtual en Kaspersky Security Center Web Console.

  1. En el dispositivo en el que esté instalado Kaspersky Security Center Web Console, ejecute el archivo de instalación de Kaspersky Security Center Web Console correspondiente a la distribución de Linux que esté instalada en el dispositivo. Utilice para ello una cuenta con privilegios administrativos.

     Se iniciará el asistente de configuración. Avance por el asistente utilizando el botón **Siguiente**.

  2. Seleccione la opción **Actualizar**.

  3. En el paso **Tipo de modificación**, seleccione la opción **Editar la configuración de conexión**.

  4. En el paso **Servidores de administración de confianza**, agregue el Servidor de administración secundario necesario.

  5. En el último paso, haga clic en **Modificar** para aplicar la nueva configuración.

  6. Cuando la aplicación se haya reconfigurado, haga clic en el botón **Finalizar**.

- Use Kaspersky Security Center Web Console para conectarse directamente al Servidor de administración secundario en el que se haya creado el servidor virtual. Una vez que haga esto, podrá cambiar al Servidor de administración virtual en Kaspersky Security Center Web Console.

Habilitación y deshabilitación de un Servidor de administración virtual

Si crea un nuevo Servidor de administración virtual, quedará habilitado por defecto. Puede habilitarlo y deshabilitarlo en cualquier momento. Habilitar y deshabilitar un Servidor de administración virtual equivale a encender y apagar un Servidor de administración físico.

Para habilitar o deshabilitar un Servidor de administración virtual:

1. En el menú principal, haga clic en el nombre del Servidor de administración.
2. En la página que se abre, vaya a la pestaña **Servidores de administración**.
3. Seleccione el Servidor de administración virtual que desee habilitar o deshabilitar.
4. En la línea del menú, haga clic en el botón **Habilitar/deshabilitar el Servidor de administración virtual**.

Dependiendo del estado que tuviera antes de esta acción, el Servidor de administración virtual cambiará de estado a habilitado o deshabilitado. El nuevo estado aparecerá junto al nombre del Servidor de administración.

Asignar un administrador para un Servidor de administración virtual

Cuando utiliza Servidores de administración virtuales en su organización, es posible que desee asignar un administrador dedicado para cada Servidor de administración virtual. Esto puede ser útil, por ejemplo, cuando una organización crea servidores virtuales para administrar oficinas o departamentos separados o cuando un proveedor de servicios administrados (MSP) desea administrar sus inquilinos a través de servidores virtuales.

Cuando crea un Servidor de administración virtual, hereda la lista de usuarios y todos los derechos de usuario del Servidor de administración principal. Si un usuario tiene derechos de acceso al Servidor principal, este usuario también tiene derechos de acceso al Servidor virtual. Después de la creación, usted configura los derechos de acceso a los servidores de forma independiente. Si desea asignar un administrador solo para un Servidor de administración virtual, asegúrese de que el administrador no tenga derechos de acceso en el Servidor de administración principal.

Asigna un administrador para un Servidor de administración virtual otorgando al administrador derechos de acceso al Servidor de administración virtual. Puede otorgar los derechos de acceso necesarios de una de las siguientes maneras:

- Configure los derechos de acceso para el administrador manualmente
- Asigne uno o más roles de usuario para el administrador

Para iniciar sesión en Kaspersky Security Center Web Console, el administrador de un Servidor de administración virtual ingresa el nombre del Servidor de administración virtual y su nombre de usuario y contraseña. Kaspersky Security Center Web Console autentica al administrador y abre el Servidor de administración virtual al que el administrador está autorizado a acceder. El administrador no puede cambiar entre Servidores de Administración.

Requisitos previos

Antes de comenzar, asegúrese de que se cumplan las siguientes condiciones:

- Se crea el Servidor de administración virtual.
- En el Servidor de administración principal, creó una cuenta para el administrador que desea asignar al Servidor de administración virtual.
- Tiene el derecho **Modificar ACL de objeto** en el área funcional **Características generales → Permisos de usuario**.

Configurar derechos de acceso manualmente

Para asignar un administrador para un Servidor de administración virtual:

1. Cambie al Servidor de administración virtual que necesite:
   a. En el menú principal, seleccione una sección (salvo **Marketplace**, **Navegación por la consola** y **Configuración**) y, a continuación, en la parte superior de la página, haga clic en el botón **Mostrar jerarquía**.
   b. En el panel de navegación que se abre, haga clic en el nombre del Servidor de administración virtual que necesite.

      > No puede cambiar a un Servidor de administración virtual desde las secciones **Intervalos IP** y **Objetos eliminados**.

      En el menú principal, el Servidor de administración cambia al que seleccionó.
2. Vaya a las propiedades del Servidor de administración; para ello, haga clic en su nombre en el menú principal.

   O bien, en el panel de navegación, pase el cursor del mouse sobre el nombre del Servidor de administración virtual requerido y luego haga clic en el ícono de configuración (⚙).

   Se abre la ventana Propiedades del Servidor de administración.
3. En la pestaña **Derechos de acceso**, haga clic en el botón **Agregar**

   Se abre una lista unificada de usuarios del Servidor de administración principal y el Servidor de administración virtual actual.
4. En la lista de usuarios, seleccione la cuenta del administrador que desea asignar para el Servidor de administración virtual y, a continuación, haga clic en el botón **Aceptar**.

   La aplicación agrega el usuario seleccionado a la lista de usuarios en la pestaña **Derechos de acceso**.
5. Marque la casilla ubicada junto a la cuenta agregada y haga clic en el botón **Derechos de acceso**.
6. Configure los derechos que tendrá el administrador sobre el Servidor de administración virtual.

Para una autenticación correcta, el administrador debe tener, por lo menos, los siguientes derechos:

- Derecho de **Leer** en el área funcional **Características generales → Funcionalidad básica**
- Derecho de **Leer** en el área funcional **Características generales → Servidores de administración virtuales**

La aplicación guarda los derechos de usuario modificados en la cuenta de administrador.

Para asignar un administrador a varios servidores de administración virtuales, siga estos pasos:

1. En el menú principal, haga clic en el nombre del Servidor de administración principal.
2. En la página que se abre, vaya a la pestaña **Derechos de acceso** y, luego, haga clic en **Asignar**.

   En la ventana **Agregar usuarios o grupos** que se abre, marque la casilla junto al usuario que desea asignar como administrador.
3. Puede cambiar a la pestaña **Grupos** para seleccionar los grupos de usuarios.
4. Haga clic en **Siguiente**.
5. Seleccione los servidores a los que desea asignarle un administrador y, luego, haga clic en **Siguiente**.
6. Seleccione las funciones de administrador que desea establecer para el usuario, si es necesario.

   Si desea establecer funciones personalizadas para el Servidor de administración actual para el usuario, vaya a las propiedades del Servidor de administración requerido, haga clic en **Establecer funciones** y, luego, seleccione las funciones personalizadas.
7. Haga clic en **Finalizar** para aplicar los cambios.

El administrador con las funciones seleccionadas ahora está asignado a varios Servidores de administración virtuales.

Para revocar los derechos de acceso del administrador, siga estos pasos:

1. Cambie al Servidor de administración requerido.
2. En el menú principal, haga clic en el nombre del Servidor de administración.
3. En la página que se abre, vaya a la pestaña **Derechos de acceso**.
4. Marque la casilla junto al usuario al que desee revocarle los derechos de acceso.
5. Haga clic en **Revocar** y confirme la acción.

Se revocan los derechos de acceso del usuario seleccionado.

Configurar derechos de acceso mediante la asignación de roles de usuario

Como alternativa, puede otorgar los derechos de acceso a un administrador del Servidor de administración virtual a través de roles de usuario. Por ejemplo, esto podría ser útil si desea asignar varios administradores en el mismo Servidor de administración virtual. Si este es el caso, puede asignar a las cuentas de los administradores la misma o más roles de usuario en lugar de configurar los mismos derechos de usuario para varios administradores.

Para asignar un administrador para un Servidor de administración virtual mediante la asignación de roles de usuario:

1. En el Servidor de administración principal, cree un nuevo rol de usuario y, a continuación, especifique todos los derechos de acceso necesarios que un administrador debe tener en el Servidor de administración virtual. Puede crear varios roles, por ejemplo, si desea separar el acceso a diferentes áreas funcionales.

2. Cambie al Servidor de administración virtual que necesite:

   a. En el menú principal, seleccione una sección (salvo **Marketplace**, **Navegación por la consola** y **Configuración**) y, a continuación, en la parte superior de la página, haga clic en el botón **Mostrar jerarquía**.

   b. En el panel de navegación que se abre, haga clic en el nombre del Servidor de administración virtual que necesite.

      No puede cambiar a un Servidor de administración virtual desde las secciones **Intervalos IP** y **Objetos eliminados**.

      En el menú principal, el Servidor de administración cambia al que seleccionó.

3. Asigne el nuevo rol o varios roles a la cuenta de administrador.

La aplicación asigna los roles a la cuenta del administrador.

Configuración de derechos de acceso al nivel de objeto

Además de asignar derechos de acceso al nivel de área funcional, puede configurar el acceso a objetos específicos en el Servidor de administración virtual, por ejemplo, a un grupo de administración específico o una tarea. Para hacer esto, cambie al Servidor de administración virtual y, a continuación, configure los derechos de acceso en las propiedades del objeto.

Cambiar los dispositivos cliente de Servidor de administración

Puede cambiar el Servidor de administración que administra los dispositivos cliente por otro, mediante la tarea *Cambiar Servidor de administración*. Cuando se completa esta tarea, los dispositivos cliente seleccionados quedan bajo el mando del Servidor de administración elegido.

No se puede utilizar la tarea *Cambiar Servidor de administración* para dispositivos cliente conectados al Servidor de administración a través de puertas de enlace de conexión. Para estos dispositivos, debe reconfigurar el Agente de red o reinstalar el Agente de red y especificar la puerta de enlace de conexión.

Para cambiar el Servidor de administración que administra ciertos dispositivos cliente:

1. En el menú principal, vaya a **Tareas**.

2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

3. En el paso **Configuración de tarea nueva** del asistente, especifique estos ajustes:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Security Center**.

   b. En el campo **Tipo de tarea**, seleccione **Cambiar Servidor de administración**.

   c. En la ventana **Nombre de la tarea**, póngale un nombre a la tarea que está creando.

      El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).

   d. Seleccione los dispositivos a los que se asignará la tarea.

      Asignar tarea a un grupo de administración

      La tarea se asignará a los dispositivos incluidos en un grupo de administración. Puede seleccionar un grupo existente o crear uno nuevo.

      Puede usar esta opción para, por ejemplo, ejecutar una tarea que envíe un mensaje a ciertos usuarios si el contenido atañe solamente a los dispositivos de un grupo de administración puntual.

      Si la tarea se asigna a un grupo de administración, la pestaña **Seguridad** no se mostrará en la ventana de propiedades de la tarea; esto se debe a que las tareas de grupo están sujetas a la configuración de seguridad de los grupos a los que se aplican.

      Especificar las direcciones de los dispositivos manualmente o importarlas de una lista

      Puede especificar los nombres DNS, las direcciones IP y las subredes IP de los dispositivos a los cuales desee asignar la tarea.

      Podría elegir esta opción si necesita que la tarea se ejecute en una subred específica. Esto puede ser útil si, por ejemplo, necesita instalar una aplicación solo en los dispositivos que utilizan los contadores o si quiere analizar los dispositivos de una subred puntual que probablemente esté infectada.

      Asignar tarea a una selección de dispositivos

      La tarea se asignará a los dispositivos incluidos en una selección de dispositivos. Puede elegir una selección existente.

      Esta opción puede ser útil para, por ejemplo, ejecutar una tarea en los dispositivos que tengan una versión específica de un sistema operativo.

4. En el paso **Alcance de la tarea** del asistente, especifique un grupo de administración, dispositivos con direcciones específicas o una selección de dispositivos.

5. En este paso del asistente, confirme que acepta las condiciones de cambio del Servidor de administración para dispositivos cliente.

6. En el siguiente paso del asistente, seleccione el Servidor de administración que desea utilizar para administrar los dispositivos seleccionados:

   Cambiar a otro Servidor de administración principal

   Para mover dispositivos cliente a otro servidor de administración principal, especifique los siguientes ajustes de conexión del servidor de administración:

   1. En el campo **Dirección del Servidor de administración**, especifique la dirección del nuevo servidor de administración principal.

   2. En el campo **Número de puerto**, especifique el número de puerto para conectarse al Servidor de administración.

      El número de puerto predeterminado es 14000.

3. Especifique el número del **Puerto SSL** en el Servidor de administración principal.

   El número de puerto predeterminado es 13000.

4. De ser necesario, active la opción **Usar servidor proxy**.

   Si esta opción está desactivada, se utiliza la conexión directa para conectar el dispositivo al Servidor de administración.

   Si esta opción está habilitada, especifique los parámetros del servidor proxy:

   - **Dirección del servidor proxy**
   - **Puerto del servidor proxy**

   Si su servidor proxy requiere autenticación, en los campos **Nombre de usuario** y **Contraseña**, indique las credenciales de la cuenta con la que se establece la conexión con el servidor proxy. Le recomendamos que utilice las credenciales de una cuenta que solamente tenga los privilegios mínimos necesarios para completar la autenticación ante el servidor proxy.

5. Si es necesario, cargue un nuevo certificado del Servidor de Administración.

Cambiar a otro Servidor virtual en este Servidor principal

Seleccione esta opción para mover los dispositivos cliente al Servidor de administración virtual en el Servidor de administración principal actual. Para ello, en la lista desplegable **Nombre del Servidor de administración virtual**, seleccione el Servidor de administración virtual necesario.

7. En el paso **Seleccione una cuenta con la que ejecutar la tarea** del asistente, especifique la configuración de la cuenta:

Cuenta predeterminada

La tarea se ejecutará utilizando la misma cuenta que la aplicación que realizará la tarea.

Esta opción está seleccionada de forma predeterminada.

Especificar cuenta

Complete los campos **Cuenta** y **Contraseña** para especificar los detalles de la cuenta con la que se ejecutará la tarea. La cuenta debe tener los derechos necesarios para realizar la tarea.

Cuenta

Cuenta con la que se ejecutará la tarea.

Contraseña

Contraseña de la cuenta con la que se ejecutará la tarea.

8. Si desea cambiar la configuración predeterminada de la tarea, en el paso **Finalizar la creación de la tarea** del asistente, active la opción **Abrir los detalles de la tarea cuando se complete la creación**.

   Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Puede cambiar la configuración por defecto más tarde, en cualquier momento.

9. Haga clic en el botón **Finalizar**.

   Se crea la tarea y se la agrega a la lista de tareas.

10. Haga clic en el nombre de la nueva tarea para abrir la ventana de propiedades de la tarea.

11. Si desea cambiar la configuración predeterminada de la tarea, en la ventana de propiedades de la tarea, especifique la configuración general de la tarea según sus necesidades.

12. Haga clic en el botón **Guardar**.

    La tarea queda creada y configurada.

13. Ejecute la tarea creada.

Una vez que se completa la tarea, los dispositivos cliente para los que se la creó quedan bajo el mando del Servidor de administración especificado en la configuración de la tarea.

Eliminación de un Servidor de administración virtual

Si elimina un Servidor de administración virtual, se eliminarán también todos los objetos que se hayan creado en el mismo, incluidas las directivas y las tareas. Los dispositivos administrados que pertenezcan a los grupos de administración controlados por el Servidor de administración virtual serán eliminados de esos grupos. Para volver a administrar esos dispositivos con Kaspersky Security Center Linux, deberá realizar un sondeo de red y mover los dispositivos del grupo "Dispositivos no asignados" a los grupos de administración que considere pertinentes.

Para eliminar un Servidor de administración virtual:

1. Vaya al Servidor de administración físico principal al que pertenece el Servidor de administración virtual que se eliminará:

   a. En el menú principal, seleccione cualquier sección (salvo **Marketplace**, **Navegación por la consola** y **Configuración**) y, a continuación, en la parte superior de la página, haga clic en el botón **Mostrar jerarquía**.

   b. En el panel de navegación que aparece, haga clic en el nombre del Servidor de administración virtual requerido.

      En el menú principal, el Servidor de administración cambia al que seleccionó.

2. Vayaa las propiedades del Servidor de administración físico principal de una de las siguientes formas:

   - En el panel de navegación, coloque el cursor sobre el nombre del Servidor de administración que necesite y luego haga clic en el icono de configuración (⚙).

   - En el menú principal, haga clic en el nombre del Servidor de administración.

3. En la ventana de propiedades que se abre, vaya a la pestaña **Servidores de administración**.

4. Seleccione el Servidor de administración virtual que desee eliminar.

5. En la línea del menú, haga clic en el botón **Eliminar**.

Se elimina el Servidor de administración virtual.

Configurar el registro de eventos de conexiones del Servidor de administración

El historial de conexiones e intentos de conexión con el Servidor de administración durante su funcionamiento se puede guardar en un archivo de registro. La información en el archivo le permite rastrear no solo las conexiones desde su infraestructura de red, sino también los intentos no autorizados de acceder al servidor.

Para registrar los eventos de conexión al Servidor de administración:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la ficha **General**, seleccione la sección **Puertos de conexión**.

3. Habilite la opción **Registrar eventos de conexiones del Servidor de administración**.

Todos los eventos adicionales de las conexiones con el Servidor de administración, los resultados de autenticación y los errores de SSL se guardarán en el archivo /var/opt/kaspersky/klnagent_srv/logs/SC.syslog.

Configuración del número máximo de eventos en el repositorio de eventos

En la sección **Repositorio de eventos** de la ventana de propiedades del Servidor de administración, puede editar la configuración del almacenamiento de eventos en la base de datos del Servidor de administración limitando el número de registros de eventos o el tiempo de almacenamiento de los registros. Cuando se especifica el número máximo de eventos, la aplicación calcula una cantidad aproximada de espacio de almacenamiento requerido para el número especificado. Puede utilizar este cálculo aproximado para evaluar si tiene suficiente espacio libre en el disco para evitar el desbordamiento de la base de datos. La capacidad predeterminada de la base de datos del Servidor de administración es de 400 000 eventos. La capacidad máxima recomendada de la base de datos es de 45 millones de eventos.

La aplicación comprueba la base de datos cada 10 minutos. Si la cantidad de eventos alcanza el valor máximo especificado más 10 000, la aplicación elimina los eventos más antiguos para que solo quede la cantidad máxima de eventos especificada.

Cuando el Servidor de administración elimina los eventos antiguos, no puede guardar los nuevos eventos en la base de datos. Durante este período, la información sobre los eventos que se rechazaron se escribe en el registro del sistema operativo. Los nuevos eventos se ponen en cola y se guardan en la base de datos una vez finalizada la operación de borrado. De manera predeterminada, la cola se limita a 20 000 eventos. Puede personalizar el límite de la cola editando el valor del indicador KLEVP_MAX_POSTPONED_CNT.

Para limitar la cantidad de eventos que se pueden almacenar en el repositorio de eventos en el Servidor de administración:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la ficha **General**, seleccione la sección **Repositorio de eventos**. Especifique el número máximo de eventos almacenados en la base de datos.

3. Haga clic en el botón **Guardar**.

Además, puede hacer lo siguiente:

- Cambiar la configuración de cualquier tarea para guardar eventos relacionados con el progreso de la misma, o guardar solo los resultados de la ejecución de la tarea.

- Reducir o deshabilitar el período de almacenamiento para los eventos del Servidor de administración, el Agente de red y las aplicaciones de Kaspersky instaladas en los dispositivos administrados.

Al hacerlo, reducirá la cantidad de eventos en la base de datos, aumentará la velocidad de ejecución de los escenarios asociados con el análisis de la tabla de eventos en la base de datos y disminuirá el riesgo de que una gran cantidad de eventos sobrescriban eventos críticos.

Mover el Servidor de administración a otro dispositivo

Si necesita usar el Servidor de administración en un nuevo dispositivo, puede moverlo de una de las siguientes maneras:

- Mueva el Servidor de administración y el servidor de la base de datos a un nuevo dispositivo (el servidor de la base de datos se puede instalar en el nuevo dispositivo junto con el Servidor de administración, o en otro dispositivo).

- Mantenga el servidor de la base de datos en el dispositivo anterior y mueva solo el Servidor de administración a un nuevo dispositivo.

Para mover el Servidor de administración y el servidor de la base de datos a un nuevo dispositivo:

1. En el dispositivo anterior, cree una copia de seguridad de los datos del Servidor de administración.

   Para ello, inicie la tarea de copia de seguridad de datos a través de Kaspersky Security Center Web Console o ejecute la utilidad klbackup.

2. En el dispositivo anterior, desconecte el Servidor de administración de la red.

3. Seleccione un nuevo dispositivo para instalar el Servidor de administración. Asegúrese de que el hardware y el software del dispositivo seleccionado cumplan con los requisitos del Servidor de administración, del Agente de red y de Kaspersky Security Center Web Console. Además, compruebe que haya puertos utilizados en el Servidor de administración disponibles.

4. Asigne la misma dirección al nuevo dispositivo.

   Al nuevo Servidor de Administración se le puede asignar un nombre NetBIOS, un FQDN y una dirección IP estática. Esto depende de la dirección del Servidor de administración que se haya configurado en el paquete de instalación del Agente de red cuando se desplegaron los agentes de red. Como alternativa, puede usar la dirección de conexión que determina el Servidor de administración al que se conecta el Agente de red (puede obtener esta dirección en los dispositivos administrados mediante la utilidad klnagchk).

5. Si es necesario, instale en otro dispositivo el sistema de administración de base de datos (DBMS) que utilizará el Servidor de administración.

   La base de datos se puede instalar en el nuevo dispositivo junto con el Servidor de administración o en otro dispositivo. Cerciórese de que este dispositivo cumpla con los requisitos de hardware y software. Cuando seleccione un DBMS, tenga en cuenta la cantidad de dispositivos cubiertos por el Servidor de administración.

6. Instale el Servidor de administración en el dispositivo seleccionado.

   Tenga en cuenta que si mueve el servidor de la base de datos al nuevo dispositivo, debe especificar la dirección local como la dirección IP del dispositivo en el que está instalada la base de datos (el elemento "h" en la instrucción Instalación de Kaspersky Security Center Linux). Si desea mantener el servidor de bases de datos en el dispositivo anterior, ingrese la dirección IP del dispositivo anterior cuando llegue al punto "h" de las instrucciones de instalación de Kaspersky Security Center Linux.

7. Una vez completada la instalación, recupere los datos del Servidor de administración en el nuevo dispositivo mediante la utilidad klbackup.

8. Abra Kaspersky Security Center Web Console y conéctese al Servidor de administración.

9. Verifique que todos los dispositivos administrados estén conectados al Servidor de administración.

10. Desinstale el Servidor de administración y el servidor de la base de datos del dispositivo anterior.

Cambiar el nombre del Servidor de administración

Los pasos para cambiar el nombre del servidor pueden variar según su entorno. Puede elegir uno de los siguientes escenarios para cambiar el nombre del servidor:

- Preservar las conexiones agregando un nuevo registro DNS.
- Preservar las conexiones cambiando a la conectividad basada en direcciones IP.
- Restaurar las conexiones interrumpidas después de cambiar el nombre del servidor.

Si tiene dificultades para cambiar el nombre del servidor, póngase en contacto con Soporte técnico.

Preservar las conexiones agregando un nuevo registro DNS

En este escenario, los dispositivos administrados y Kaspersky Security Center Web Console continúan conectándose a la dirección anterior del Servidor de administración después de cambiar el nombre del Servidor de administración. Para configurar esto, agregue uno de los siguientes tipos de registros DNS:

- Un registro A para la dirección anterior del Servidor de administración que apunte a la nueva dirección IP del Servidor de administración.
- Un registro CNAME que asigne el nombre anterior del Servidor de administración al nuevo nombre del Servidor de administración.

  Para obtener más información sobre cómo configurar los registros requeridos, consulte la documentación de su Servidor DNS.

Para preservar las conexiones agregando un nuevo registro DNS:

1. **Cambie el nombre del Servidor.**

   Debido a la forma en que se configuran los componentes durante la instalación, no puede cambiar el nombre del Servidor de administración sin reinstalarlo.

   Para cambiar el nombre del servidor:

   1. Cree una nueva copia de seguridad del Servidor de administración con la utilidad klbackup.
   2. Desinstale Kaspersky Security Center Linux y Kaspersky Security Center Web Console en todas las estaciones de trabajo del administrador.
   3. Elimine manualmente la base de datos del Servidor de administración y la base de datos de IAM. El Servidor de administración no la elimina automáticamente durante la desinstalación.
   4. Cambie el nombre del dispositivo en el sistema operativo del Servidor de administración, de acuerdo con la documentación de su sistema operativo.
   5. Instale el Servidor de administración de Kaspersky Security Center Linux mediante el nuevo FQDN del Servidor de administración.
   6. Restaure la copia de seguridad del Servidor de administración preparada previamente después de la instalación.
   7. Verifique la configuración del Servidor de IAM y, si es necesario, agregue la dirección del Servidor de administración al archivo de configuración del Servidor de IAM.
   8. Instale Web Console en todas las estaciones de trabajo del administrador especificando el nuevo FQDN del Servidor de administración en el archivo de respuesta.

2. Agregue un nuevo registro DNS para la dirección anterior del Servidor de administración.
3. Especifique la nueva dirección en la configuración del Servidor de administración en Kaspersky Security Center Web Console.
4. Ejecute la tarea **Cambiar Servidor de administración** en dispositivos con visibilidad directa del Servidor de administración. Después de eso, los dispositivos administrados podrán conectarse al Servidor de administración mediante el nuevo nombre.

   > No ejecute la tarea en dispositivos sin visibilidad directa del servidor; de lo contrario, perderán la conexión con el Servidor de administración y las pasarelas de conexión.

   Los dispositivos administrados conectados a través de pasarelas de conexión no comprueban el nombre del Servidor de administración. Por lo tanto, no se requiere ninguna acción adicional para ellos/. La información sobre la dirección del Servidor de administración no se actualizará en la salida del comando de diagnóstico klnagchk.

La conexión con el Servidor de administración se conserva después de cambiar el nombre del servidor.

Después de cambiar el nombre del servidor, la información del certificado quedará obsoleta. Dado que esto no afecta el funcionamiento de los componentes, no recomendamos reemplazar los certificados autofirmados fuera de la programación. Estos certificados se generan durante la instalación de Kaspersky Security Center y el servidor los renueva automáticamente. Se volverán a emitir con el nuevo nombre del Servidor de administración durante el siguiente reemplazo automático del certificado.

Durante la reinstalación, se emitirán nuevos certificados para el Servidor de IAM/ y el Servidor de Web Console. Si es necesario, reemplácelos con certificados personalizados emitidos por su entidad de certificación para el nuevo nombre del Servidor de administración. Consulte el siguiente artículo para obtener más información: Acerca de los certificados de Kaspersky Security Center Linux.

Preservar las conexiones cambiando a la conectividad basada en direcciones IP

En este escenario, se modifica la forma en que los dispositivos administrados se conectan al Servidor de administración. Los dispositivos se conectan mediante la dirección IP del Servidor de administración en lugar del nombre del Servidor de administración. Cambiar todos los dispositivos administrados puede llevar tiempo, según la cantidad de dispositivos y la frecuencia con la que aparecen en la red con el Servidor de administración.

Para preservar las conexiones mediante el cambio a la conectividad basada en direcciones IP:

1. **Prepare la infraestructura de Kaspersky Security Center antes de cambiar el nombre del Servidor de administración.**

   1. Conecte los dispositivos administrados al Servidor de administración mediante una dirección IP. Después de cambiar el nombre del Servidor de administración, los dispositivos que usan su nombre para la conexión se desconectarán del Servidor. Para conectarse mediante una dirección IP, ejecute la tarea Cambiar Servidor de administración en los dispositivos que tengan visibilidad directa del Servidor de administración, incluidos los dispositivos que actúan como pasarelas de conexión.

      No ejecute la tarea en dispositivos sin visibilidad directa del servidor; de lo contrario, perderán la conexión con el Servidor de administración y las pasarelas de conexión.

      Los dispositivos administrados conectados a través de pasarelas de conexión no comprueban el nombre del Servidor de administración. Por lo tanto, no se requiere ninguna acción adicional para ellos/. La información sobre la dirección del Servidor de administración no se actualizará en la salida del comando de diagnóstico klnagchk.

   2. Asegúrese de que todos los dispositivos administrados estén conectados al Servidor de administración mediante la dirección IP. Para ello, compruebe lo siguiente:

      - Los resultados del comando de diagnóstico klnagchk en la línea de dirección del Servidor de administración en los dispositivos administrados con acceso directo al Servidor de administración.
      - La información de propiedades del paquete de instalación del Agente de red en el momento de la instalación en los dispositivos.

        El Agente de red debe configurarse inicialmente para conectarse al Servidor de administración mediante una dirección IP.

Si instala el Agente de red sobre la instalación existente sin desinstalarlo primero, la dirección de conexión del Servidor de administración y el certificado especificados en la configuración del Agente de red no se actualizarán.

3. Especifique un nombre nuevo en los perfiles de conexión existentes del Servidor de administración.

4. Si utiliza el rol de Administración de dispositivos móviles (administración de dispositivos Android e iOS), siga las instrucciones Cómo cambiar la dirección del Servidor de administración en dispositivos móviles que usan Kaspersky Endpoint Security para Android con el rol MDM o KSMM.

2. **Cambie el nombre del Servidor.**

Debido a la forma en que se configuran los componentes durante la instalación, no puede cambiar el nombre del Servidor de administración sin reinstalarlo.

Para cambiar el nombre del servidor:

1. Cree una nueva copia de seguridad del Servidor de administración con la utilidad klbackup.

2. Desinstale Kaspersky Security Center Linux y Kaspersky Security Center Web Console en todas las estaciones de trabajo del administrador.

3. Elimine manualmente la base de datos del Servidor de administración y la base de datos de IAM. El Servidor de administración no la elimina automáticamente durante la desinstalación.

4. Cambie el nombre del dispositivo en el sistema operativo del Servidor de administración, de acuerdo con la documentación de su sistema operativo.

5. Instale el Servidor de administración de Kaspersky Security Center Linux mediante el nuevo FQDN del Servidor de administración.

6. Restaure la copia de seguridad del Servidor de administración preparada previamente después de la instalación.

7. Verifique la configuración del Servidor de IAM y, si es necesario, agregue la dirección del Servidor de administración al archivo de configuración del Servidor de IAM.

8. Instale Web Console en todas las estaciones de trabajo del administrador especificando el nuevo FQDN del Servidor de administración en el archivo de respuesta.

3. **Actualice las direcciones del Servidor de administración en la configuración del Servidor de administración.**

Después de cambiar el nombre del Servidor de administración, especifique la nueva dirección FQDN en la configuración del Servidor de administración en Kaspersky Security Center Web Console. Para hacerlo, verifique y actualice la dirección FQDN en cada una de las siguientes opciones de configuración:

- Dirección del servidor proxy de Kaspersky Security Network
- Servidor web
- Propiedades de los paquetes de instalación del Agente de red
- Nombre del emisor del código de seguridad (2FA)

Además, haga lo siguiente:

- Especifique el nuevo nombre del servidor en las directivas y la configuración de otras aplicaciones de Kaspersky.
- Vuelva a publicar cada paquete independiente publicado y cada paquete de dispositivo móvil.
- Vuelva a conectar los Servidores de administración secundarios si usa una jerarquía de Servidores de administración y si los servidores están conectados por nombre y no por dirección IP.

4. Ejecute la tarea **Cambiar Servidor de administración** en los dispositivos con visibilidad directa del Servidor de administración para cambiar la dirección de conexión de los dispositivos administrados al nuevo nombre del Servidor de administración.

La conexión con el Servidor de administración se conserva después de cambiar el nombre del servidor.

Después de cambiar el nombre del servidor, la información del certificado quedará obsoleta. Dado que esto no afecta el funcionamiento de los componentes, no recomendamos reemplazar los certificados autofirmados fuera de la programación. Estos certificados se generan durante la instalación de Kaspersky Security Center y el servidor los renueva automáticamente. Se volverán a emitir con el nuevo nombre del Servidor de administración durante el siguiente reemplazo automático del certificado.

Durante la reinstalación, se emitirán nuevos certificados para el Servidor de IAM/ y el Servidor de Web Console. Si es necesario, reemplácelos con certificados personalizados emitidos por su entidad de certificación para el nuevo nombre del Servidor de administración. Consulte el siguiente artículo para obtener más información: Acerca de los certificados de Kaspersky Security Center Linux.

Restauración de conexiones interrumpidas después de cambiar el nombre del servidor

El escenario es relevante en los siguientes casos:

- Si perdió la propiedad del nombre de dominio del dispositivo del Servidor de administración, pero aún tiene acceso al Servidor de administración.
- Si el Servidor de administración ya no administra los dispositivos administrados.
- Si no es posible agregar registros DNS para la dirección anterior de Kaspersky Security Center Linux por otros motivos.

Para restaurar conexiones interrumpidas después de cambiar el nombre del servidor:

1. **Cambie el nombre del Servidor.**

   Debido a la forma en que se configuran los componentes durante la instalación, no puede cambiar el nombre del Servidor de administración sin reinstalarlo.

   Para cambiar el nombre del servidor:

   1. Cree una nueva copia de seguridad del Servidor de administración con la utilidad klbackup.
   2. Desinstale Kaspersky Security Center Linux y Kaspersky Security Center Web Console en todas las estaciones de trabajo del administrador.

3. Elimine manualmente la base de datos del Servidor de administración y la base de datos de IAM. El Servidor de administración no la elimina automáticamente durante la desinstalación.

4. Cambie el nombre del dispositivo en el sistema operativo del Servidor de administración, de acuerdo con la documentación de su sistema operativo.

5. Instale el Servidor de administración de Kaspersky Security Center Linux mediante el nuevo FQDN del Servidor de administración.

6. Restaure la copia de seguridad del Servidor de administración preparada previamente después de la instalación.

7. Verifique la configuración del Servidor de IAM y, si es necesario, agregue la dirección del Servidor de administración al archivo de configuración del Servidor de IAM.

8. Instale Web Console en todas las estaciones de trabajo del administrador especificando el nuevo FQDN del Servidor de administración en el archivo de respuesta.

2. **Actualice las direcciones del Servidor de administración en la configuración del Servidor de administración.**

   Después de cambiar el nombre del Servidor de administración, especifique la nueva dirección FQDN en la configuración del Servidor de administración en Kaspersky Security Center Web Console. Para hacerlo, verifique y actualice la dirección FQDN en cada una de las siguientes opciones de configuración:

   - Dirección del servidor proxy de Kaspersky Security Network
   - Servidor web
   - Propiedades de los paquetes de instalación del Agente de red
   - Nombre del emisor del código de seguridad (2FA)

   Además, haga lo siguiente:

   - Especifique el nuevo nombre del servidor en las directivas y la configuración de otras aplicaciones de Kaspersky.
   - Vuelva a publicar cada paquete independiente publicado y cada paquete de dispositivo móvil.
   - Vuelva a conectar los Servidores de administración secundarios si usa una jerarquía de Servidores de administración y si los servidores están conectados por nombre y no por dirección IP.

3. Restaure la conexión con el Servidor de administración en los dispositivos administrados anteriormente:

   - En los dispositivos con visibilidad directa del Servidor de administración, use la utilidad klmover para especificar la dirección de conexión con el nuevo nombre del Servidor de administración. Consulte el siguiente artículo para obtener más información: Conectar Agentes de red al Servidor de administración mediante la utilidad klmover.
   - En los dispositivos que actúan como pasarelas de conexión, vuelva a instalar el Agente de red y vuelva a configurar el rol de pasarela de conexión. Consulte el siguiente artículo para obtener más información: Agregar una pasarela de conexión en la DMZ como punto de distribución.

- Los dispositivos conectados a través de pasarelas de conexión se volverán a conectar automáticamente después de que se restauren las pasarelas de conexión. El Agente de red no utiliza el nombre del Servidor de administración cuando se conecta a las pasarelas de conexión.

  No use la utilidad klmover en dispositivos conectados a través de pasarelas de conexión. Consulte el siguiente artículo para obtener más información: Mover dispositivos conectados al Servidor de administración a través de pasarelas de conexión a otro Servidor de administración.

La conexión con el Servidor de administración se restaura después de cambiar el nombre del servidor.

Después de cambiar el nombre del servidor, la información del certificado quedará desactualizada. Dado que esto no afecta el funcionamiento de los componentes, no recomendamos reemplazar los certificados autofirmados fuera de la programación. Estos certificados se generan durante la instalación de Kaspersky Security Center y el servidor los renueva automáticamente. Se volverán a emitir con el nuevo nombre del Servidor de administración durante el siguiente reemplazo automático del certificado.

Durante la reinstalación, se emitirán nuevos certificados para el Servidor de IAM/ y el Servidor de Web Console. Si es necesario, reemplácelos con certificados personalizados emitidos por su entidad de certificación para el nuevo nombre del Servidor de administración. Consulte el siguiente artículo para obtener más información: Acerca de los certificados de Kaspersky Security Center Linux.

Cambio de las credenciales de DBMS

Es posible que, a veces, deba cambiar las credenciales de DBMS, por ejemplo, para realizar una rotación de credenciales por motivos de seguridad.

Cambiar las credenciales de la base de datos del Servidor de administración

Para cambiar las credenciales del Servidor de administración y de la base de datos de IAM en un entorno Linux:

1. Detenga el Servidor de administración. Según el tipo de despliegue de Kaspersky Security Center Linux, ejecute uno de los siguientes comandos con la cuenta root:

   - Para un clúster de conmutación por error de Kaspersky Security Center Linux:

     En el nodo activo, ejecute el siguiente comando:

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

   - Para un clúster de conmutación por error de Kaspersky Security Center Linux distribuido geográficamente:

     En ambos nodos, ejecute el siguiente comando:

     ```
     crm node standby
     ```

   - Para un despliegue del Servidor de administración sin clúster:

     Ejecute el siguiente comando:

     ```
     systemctl stop kladminserver_srv.service
     systemctl stop kliam_srv.service
     ```

2. Conéctese a la base de datos del Servidor de administración con privilegios de superusuario de DBMS y ejecute el siguiente comando:

```
REASSIGN OWNED BY <old_kscdbadmin> TO <new_kscdbadmin>;
```

donde `<old_kscdbadmin>` es la cuenta de usuario de DBMS anterior que el Servidor de administración utilizaba para conectarse a su base de datos, y `<new_kscdbadmin>` es la nueva cuenta de usuario de DBMS.

3. Conéctese a la base de datos de IAM con privilegios de superusuario de DBMS y ejecute el siguiente comando:

```
REASSIGN OWNED BY <old_iamdbadmin> TO <new_iamdbadmin>;
```

donde `<old_iamdbadmin>` es la cuenta de DBMS anterior que el Servidor de administración utilizaba para conectarse a su base de datos, y `<new_iamdbadmin>` son las nuevas cuentas de DBMS.

4. Busque el archivo de configuración de IAM: /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml

5. En la sección `dbms_iam`, especifique las nuevas credenciales de la cuenta en los campos de usuario y contraseña. Asegúrese de que la cuenta exista en el DBMS y esté especificada como propietaria de la base de datos de IAM.

6. Ejecute el Servidor de administración. Según el tipo de despliegue de Kaspersky Security Center Linux, ejecute uno de los siguientes comandos con la cuenta root:

   - Para un clúster de conmutación por error de Kaspersky Security Center Linux:

     En el nodo activo, ejecute el siguiente comando:

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

   - Para un clúster de conmutación por error de Kaspersky Security Center Linux distribuido geográficamente:

     En ambos nodos, ejecute el siguiente comando:

     ```
     crm node online
     ```

   - Para un despliegue del Servidor de administración sin clúster:

     Ejecute el siguiente comando:

     ```
     systemctl start kladminserver_srv.service
     systemctl start kliam_srv.service
     ```

7. Ejecute la utilidad klsrvconfig:

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

8. Especifique un nuevo nombre de cuenta. Debe especificar las credenciales de una cuenta que exista en el DBMS.

9. Introduzca una nueva contraseña.

10. Especifique la nueva contraseña para su confirmación.

11. Espere hasta que el Servidor de administración reanude su funcionamiento y aparezca una entrada de syslog en el nodo activo que indique que el Servidor de administración está listo para realizar operaciones en la GUI.

Se modifican las credenciales de la base de datos del Servidor de administración.

Copia de seguridad y restauración de los datos del Servidor de administración

La copia de seguridad de datos le permite mover un Servidor de administración de un dispositivo a otro, sin pérdida de datos. Mediante la copia de seguridad, puede restaurar datos al mover la base de datos de un Servidor de administración a otro dispositivo, o al actualizarse a una nueva versión de Kaspersky Security Center. Además, puede utilizar la copia de seguridad de datos para trasladar los datos del Servidor de administración de Kaspersky Security Center Windows y ponerlos bajo la administración de Kaspersky Security Center Linux (no se admite el traslado de datos de Kaspersky Security Center Linux a Kaspersky Security Center Windows).

No se realiza una copia de seguridad de los complementos de administración instalados. Después de restaurar los datos del Servidor de administración a partir de una copia de seguridad, debe descargar y volver a instalar los complementos para las aplicaciones administradas.

Antes de realizar una copia de seguridad de los datos del Servidor de administración, realice las siguientes acciones:

- **Siga los requisitos para crear una copia de seguridad en el Servidor de administración 16 o anterior y restaurar en la versión 16.1 o posterior**

  - Si crea una copia de seguridad de los datos en el Servidor de administración 16 o anterior y la restaura en Servidor de administración 16.1 o posterior, la autenticación de dos factores está habilitada. Para obtener más información, consulte Acerca de la autenticación de dos factores para una cuenta.

    Para asegurarse de que los usuarios puedan iniciar sesión en Web Console con sus cuentas existentes mediante el uso de claves secretas de autenticación de dos factores configuradas, y que los scripts de automatización de OpenAPI continúen funcionando después de la restauración, debe realizar los siguientes pasos:

    - Habilitación de la autenticación de dos factores para todos los usuarios
    - Los administradores deben configurar la autenticación de dos factores para sus propias cuentas
    - Excluir cuentas de la autenticación de dos factores

      Si es necesario, agregue las cuentas de integridad utilizadas para ejecutar scripts a través de OpenAPI a la lista de exclusión.

    Si no es posible configurar la autenticación de dos factores antes de crear la copia de seguridad, las cuentas de usuario se agregarán a la lista de permitidos para autenticación de dos factores y podrán configurar la autenticación de dos factores al iniciar sesión en Web Console. Las condiciones más detalladas para agregar una cuenta a la lista de permitidos se describen en el tema Permitir a los usuarios configurar la autenticación de dos factores.

- Compruebe si se agregó un Servidor de administración virtual al grupo de administración. Si se agrega un Servidor de administración virtual, asegúrese de que se asigne un administrador a este Servidor de administración virtual antes de realizar la copia de seguridad. No puede otorgar derechos de acceso de administrador al Servidor de administración virtual después de la copia de seguridad. Tenga en cuenta que si se pierden las credenciales de la cuenta de administrador, no podrá asignar un nuevo administrador al Servidor de administrador virtual.

- Si desea hacer un respaldo o restaurar un clúster de conmutación por error de Kaspersky Security Center Linux, debe detener todo el clúster para realizar el mantenimiento y, luego, reiniciarlo cuando se complete el respaldo o la restauración.

Puede crear una copia de seguridad de los datos del Servidor de administración mediante uno de los siguientes métodos:

- Puede crear y ejecutar una tarea de copia de seguridad de datos a través de Kaspersky Security Center Web Console.

- Puede ejecutar la utilidad klbackup en el dispositivo que tiene instalado el Servidor de administración. Esta utilidad está incluida en el kit de distribución de Kaspersky Security Center. Tras la instalación del Servidor de administración, la encontrará en la raíz de la carpeta de destino especificada durante la instalación de la aplicación (por lo general, /opt/kaspersky/ksc64/sbin/klbackup).

Se guardan los siguientes datos en la copia de seguridad del Servidor de administración:

- La base de datos del Servidor de administración (directivas, tareas, configuración de las aplicaciones, eventos guardados en el Servidor de administración)

- Información de configuración de la estructura de los grupos de administración y los dispositivos cliente

- Repositorio de paquetes de distribución de aplicaciones para instalación remota

- Certificado del Servidor de administración

- Claves secretas de autenticación de dos factores configuradas para cuentas de usuario

- Lista de cuentas de usuario excluidas de la autenticación de dos factores

Puede crear una copia de seguridad de los datos del Servidor de administración creando y ejecutando una tarea de copia de seguridad de datos o utilizando la utilidad klbackup. La restauración de los datos del Servidor de administración solo se puede realizar mediante la utilidad klbackup. Para llevar a cabo la restauración en una instancia del Servidor de administración que se acaba de instalar, que esté en funcionamiento y que sea de la misma versión para la que se haya creado la copia de seguridad (o de una versión más reciente). No utilice ninguna herramienta de terceros para realizar copias de seguridad o restaurar y, si es posible, no elimine la instalación anterior de Kaspersky Security Center Linux hasta que la configuración y la transferencia de datos se hayan completado por completo.

Crear una tarea de copia de seguridad de los datos del Servidor de administración

Las tareas de copia de seguridad son tareas del Servidor de administración y se crean a través del asistente de inicio rápido. Si se elimina una tarea de copia de seguridad creada por el asistente de inicio rápido, puede crearse otra manualmente.

> La tarea *Copia de seguridad de los datos del Servidor de administración* solo puede crearse en una sola copia. Si la tarea de copia de seguridad de los datos del Servidor de administración ya fue creada para el Servidor de administración, no se mostrará en la ventana de selección del tipo de tarea.

Para crear una tarea de copia de seguridad de los datos del Servidor de administración:

1. En el menú principal, vaya a **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Avance por el asistente utilizando el botón **Siguiente**.
3. En la lista **Aplicación**, seleccione **Kaspersky Security Center 17** y en la lista **Tipo de tarea**, seleccione **Copia de seguridad de los datos del Servidor de administración**.
4. En el paso correspondiente, especifique la siguiente información:
   - Carpeta de almacenamiento de copias de seguridad:
   - Contraseña para la copia de seguridad (opcional)
   - Número máximo de copias de seguridad para guardar
5. Si desea modificar la configuración predeterminada de la tarea, active la opción **Finalizar la creación de la tarea** en el paso **Abrir los detalles de la tarea cuando se complete la creación**. Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Puede cambiar la configuración por defecto más tarde, en cualquier momento.
6. Haga clic en el botón **Finalizar**.

Se crea la tarea y se la agrega a la lista de tareas.

Uso de la utilidad klbackup para realizar copias de seguridad y recuperar datos

Puede copiar datos del Servidor de administración para crear copias de seguridad y futura recuperación mediante la utilidad klbackup que forma parte del kit de distribución de Kaspersky Security Center.

La instancia del Servidor de Administración en la que se va a realizar la restauración debe utilizar un DBMS del mismo tipo. La versión del Servidor de administración puede ser igual (con un parche idéntico o posterior) o posterior.

Si hizo una copia de seguridad de los datos del Servidor de administración incluido en Kaspersky Security Center Linux 15 o anterior al usar el DBMS MariaDB de una versión anterior, y luego recupera los datos en un dispositivo con una versión posterior de MariaDB, puede ocurrir un error. Para obtener más información, consulte Cómo restaurar los datos del Servidor de administración a partir de una copia de seguridad creada en una versión anterior de DBMS.

Los indicadores del Agente de red no se restauran cuando se utiliza la utilidad klbackup. Debe configurar los indicadores del Agente de red manualmente.

Para crear una copia de seguridad o recuperar los datos del Servidor de administración en modo no interactivo,

En el dispositivo del Servidor de administración, abra la línea de comandos y ejecute klbackup con las claves necesarias.

Sintaxis de línea de comandos de la utilidad:

```
klbackup -path <ruta a la copia de seguridad> [-linux_path <ruta a la copia de seguridad de DBMS>-node_cert <ruta al certificado>] [-logfile <archivo de registro> [-use_ts]|[-restore] [-password <contraseña>] [-cert_only]
```

Si no se especificó una contraseña en la línea de comandos de la utilidad klbackup, la utilidad solicitará que se ingrese la contraseña de modo interactivo.

Descripciones de las claves:

- `-path <ruta a la copia de seguridad>`: guardar información en la carpeta de copia de seguridad o usar datos de la carpeta de copia de seguridad para la recuperación (parámetro obligatorio).
- `-linux_path <ruta a la copia de seguridad de DBMS>`: ruta local a la carpeta con datos de la copia de seguridad de DBMS.

  La cuenta del servidor de bases de datos y la utilidad klbackup deben contar con los permisos para modificar los datos de la carpeta de la copia de seguridad de DBMS.
- `-node_cert <ruta al certificado>`: archivo de certificado del servidor para configurar el nodo del clúster de conmutación por error inactivo después de la recuperación. Si no se configura, se recuperará automáticamente del Servidor.
- `-logfile <archivo de registro>`: guardar un informe sobre la copia de seguridad y recuperación de datos del Servidor de administración.

  La cuenta del servidor de bases de datos y la utilidad klbackup deben contar con permisos para modificar los datos de la carpeta de la copia de seguridad.
- `-use_ts`: al guardar datos, copie la información a la carpeta de la copia de seguridad, a la subcarpeta con un nombre en el formato `klbackup AAAA-MM-DD # HH-MM-SS`, que incluye la fecha actual y la hora de funcionamiento en UTC. Si no se especifica una clave, la información se guarda en la raíz de la carpeta de la copia de seguridad.

Durante los intentos de guardar información en una carpeta que ya contiene una copia de seguridad, aparece un mensaje de error. No se actualiza la información.

La disponibilidad de la clave `-use_ts` permite mantener un archivo de datos del Servidor de administración. Por ejemplo, si la clave `-path` indica la carpeta `/tmp/KLBackups`, entonces la carpeta `klbackup 2022/6/19 # 11-30-18` almacena información sobre el estado del Servidor de administración con fecha de 19 de junio de 2022, a las 11:30:18 h.

- `-restore`: recuperar datos del Servidor de Administración. La recuperación de los datos se realiza a partir de la información almacenada en la carpeta de la copia de seguridad. Si no se dispone de una clave, se crea una copia de seguridad de los datos en la carpeta de la copia de seguridad.

- `-password <contraseña>`: contraseña para proteger los datos confidenciales.

  Si olvida la contraseña, no podrá recuperarla. No hay requisitos para la contraseña. La longitud de la contraseña es ilimitada y también es posible que tenga una longitud cero (es decir, sin contraseña).

  Al restaurar datos, debe especificar la misma contraseña que se ingresó durante la copia de seguridad. Si la ruta a una carpeta compartida se cambió después de la copia de seguridad, controle el funcionamiento de las tareas que usan los datos restaurados (tareas de restauración y tareas de instalación remota). Si es necesario, modifique la configuración de estas tareas. Mientras los datos se están restaurando desde una copia de seguridad, nadie debe acceder a la carpeta compartida del Servidor de administración. La cuenta desde la que se inicia la utilidad klbackup debe tener acceso completo a la carpeta compartida. Para restaurar los datos del Servidor de administración desde la copia de seguridad, le recomendamos que ejecute la utilidad en un Servidor de administración recién instalado.

- `-cert_only`: guardar o recuperar solo el certificado y la clave privada del Servidor de administración.

  Este indicador puede ser útil cuando realiza la migración desde el Servidor de administración de Kaspersky Security Center Windows al Servidor de administración de Kaspersky Security Center Linux. Además, puede migrar dispositivos administrados entre los Servidores de administración de Kaspersky Security Center Linux, así como entre los Servidores de administración de Kaspersky Security Center Windows.

Puede utilizar una copia de seguridad para migrar los datos del Servidor de administración de Kaspersky Security Center Windows y pasar a administrarlos con Kaspersky Security Center Linux.
Si utiliza MySQL o MariaDB como DBMS para Kaspersky Security Center Windows y Kaspersky Security Center Linux, el parámetro `lower_case_table_names` debe ser el mismo en el DBMS activo y el nuevo. Antes de crear una copia de seguridad de los datos, verifique la configuración `lower case table names`. Entonces, al instalar MySQL o MariaDB para Kaspersky Security Center Linux, debe asignar al parámetro `lower_case_table_names` el mismo valor que tenga especificado en Windows.

Si, durante la restauración, el certificado común del Servidor de administración se reemplaza con otro certificado de una copia de seguridad, realice los siguientes pasos para garantizar un funcionamiento correcto:
1. Vuelva a instalar Web Console para evitar el siguiente error:
El Servidor de administración utiliza un certificado que no es de confianza. Vuelva a configurar la aplicación especificando un certificado válido o póngase en contacto con el administrador principal.
2. Verifique la configuración del Servidor de IAM y, si es necesario, agregue la dirección del Servidor de administración al archivo de configuración del Servidor de IAM.

Usar la utilidad klbackup para ceder el control de los dispositivos administrados a otro Servidor de administración

La utilidad klbackup permite ceder el control de los dispositivos administrados a otro Servidor de administración Puede cambiar el Servidor de administración de Kaspersky Security Center Windows por el Servidor de administración de Kaspersky Security Center Linux mediante la utilidad klbackup tras completar la migración. También puede migrar sus dispositivos administrados entre los distintos servidores de administración de Kaspersky Security Center Linux, así como entre distintos servidores de administración de Kaspersky Security Center Windows.

Antes de empezar, **verifique los requisitos de un certificado personalizado**.

Si utiliza un certificado personalizado en lugar del autofirmado, antes de actualizar Kaspersky Security Center Linux a la versión posterior, debe asegurarse de que el certificado incluya el Nombre alternativo del sujeto (SAN). Si no lo incluye, es importante reemplazar el certificado antes de actualizar Kaspersky Security Center Linux. De lo contrario, no podrá iniciar sesión en Web Console después de la actualización.

Para asegurarse de que el certificado incluya SAN:

1. En el dispositivo en el que se encuentra instalado el Servidor de administración, ejecute el siguiente comando:

   - Para un dispositivo Linux:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout
     -ext subjectAltName
     ```

   - Para un dispositivo Windows:

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. Asegúrese de que el Nombre alternativo del sujeto (SAN) esté presente en el resultado del comando y que contenga la dirección del dispositivo del Servidor de administración.

3. Si no aparece el Nombre alternativo del sujeto, utilice la utilidad klsetsrvcert para reemplazar su certificado de usuario por un certificado que cumpla con los requisitos.

Para ceder el control de un grupo de dispositivos administrados a otro Servidor de administración mediante la utilidad klbackup:

1. En el dispositivo antiguo, cree una copia de seguridad del certificado y de la clave privada del Servidor de administración.

   Puede crear una copia de seguridad de distintas maneras:

   - Mediante la interfaz de la utilidad klbackup (solo para el Servidor de administración de Kaspersky Security Center Windows)

     Ejecute la utilidad klbackup ubicada en la carpeta de instalación de Kaspersky Security Center y luego cree una copia de seguridad usando la opción **Limitar la copia de seguridad o restauración al certificado del Servidor de administración**.

- Mediante la línea de comandos (para Kaspersky Security Center Windows y servidores de administración de Kaspersky Security Center Linux versión 15.1 o versiones posteriores)

  Ejecute la utilidad klbackup con la clave `-cert_only` desde la línea de comandos para crear una copia de seguridad del certificado y de la clave privada del Servidor de administración:

  ```
  klbackup -path <path to the backup copy of Administration Server certificate> -cert_only
  ```

2. En el dispositivo antiguo, desconecte el Servidor de administración de la red.

3. Asigne el mismo nombre de dominio al dispositivo que contenga el otro Servidor de administración.

   Al nuevo Servidor de Administración se le puede asignar un nombre NetBIOS, un FQDN y una dirección IP estática. Esto depende de la dirección del Servidor de administración que se haya configurado en el paquete de instalación del Agente de red cuando se desplegaron los agentes de red. También puede usar la dirección de conexión que define a qué Servidor de administración se conecta el Agente de administración (puede averiguar esta dirección en los dispositivos administrados mediante la utilidad klnagchk).

   Si no es posible asignar la misma dirección al dispositivo con otro Servidor de administración, debe generar un nuevo certificado del Servidor de administración y especificar este certificado en el archivo de configuración de IAM. Después de la instalación del Servidor de administración, debe cambiar manualmente los Agentes de red al nuevo Servidor de administración.

4. En el dispositivo con el otro Servidor de administración, utilice la copia de seguridad para restaurar el certificado y la clave privada del Servidor de administración.

   Puede restaurar una copia de seguridad de distintas maneras:

   - Mediante la interfaz de la utilidad klbackup (solo para el Servidor de administración de Kaspersky Security Center Windows)

     Ejecute la utilidad klbackup y luego restaure la copia de seguridad usando la opción **Limitar la copia de seguridad o restauración al certificado del Servidor de administración**.

   - Mediante la línea de comandos (para Kaspersky Security Center Windows y servidores de administración de Kaspersky Security Center Linux versión 15.1 o versiones posteriores)

     Ejecute la utilidad `klbackup` con la opción `-cert_only` desde la línea de comando para restaurar el certificado del Servidor de administración y la clave privada a partir de una copia de seguridad:

     ```
     klbackup -path <path to the backup copy of Administration Server certificate> -restore -cert_only
     ```

5. Configure la verificación de certificados del Servidor de administración y del Servidor de IAM.

Los dispositivos administrados quedarán bajo la órbita administrativa del otro Servidor de administración. Puede ir a este Servidor de administración y asegurarse de que los dispositivos administrados sean visibles en la red y que el Agente de red esté instalado y activo en ellos (las columnas **Visible**, **Agente de red instalado** y **Agente de red en ejecución** deben tener el valor *Sí*).

Cómo hacer copias de seguridad y restaurar datos del Servidor de administración si se usa MySQL o MariaDB

Puede utilizar una copia de seguridad para migrar los datos del Servidor de administración de Kaspersky Security Center Windows y ponerlos bajo la órbita administrativa de Kaspersky Security Center Linux. La migración con una copia de seguridad de datos solo se admite para la migración a Kaspersky Security Center Linux 15.2 o versiones posteriores desde cualquier versión compatible de Kaspersky Security Center Windows.

Si utiliza MySQL o MariaDB como DBMS para Kaspersky Security Center Windows y Kaspersky Security Center Linux, el parámetro `lower_case_table_names` debe ser el mismo en el DBMS activo y el nuevo. De lo contrario, los datos del Servidor de administración se migrarán incorrectamente.

Antes de realizar una copia de seguridad de los datos del Servidor de administración en Kaspersky Security Center Windows, controle el valor del parámetro `lower_case_table_names`. Si no definió este parámetro durante la instalación del DBMS, se utilizará el valor predeterminado para el parámetro. El valor predeterminado del parámetro `lower_case_table_names` para Windows es `1`.

Luego, al instalar MySQL o MariaDB para Kaspersky Security Center Linux, asigne al parámetro `lower_case_table_names` el mismo valor que tenga en Windows. Para obtener más información, consulte las instrucciones del sitio web de MySQL. Si no especifica este parámetro, se utilizará el valor predeterminado para el mismo. En sistemas operativos Linux, el valor predeterminado del parámetro `lower_case_table_names` es diferente del valor predeterminado en Windows.

Si desea instalar MySQL 8.0, definir el parámetro `lower_case_table_names` siguiendo estas instrucciones puede no dar el resultado esperado. En tal caso, primero instale MySQL 5.7, defina el parámetro `lower_case_table_names` siguiendo las instrucciones y luego actualice MySQL 5.7 a MySQL 8.0. Si el parámetro `lower_case_table_names` no es el mismo en el DBMS activo y el nuevo, los datos del Servidor de administración no se restaurarán correctamente.

Mantenimiento del Servidor de administración

El mantenimiento del Servidor de administración permite liberar espacio en la carpeta del Servidor de administración y reducir el volumen de las bases de datos al eliminar objetos que ya no son necesarios. Esto lo ayuda a mejorar el rendimiento y la fiabilidad del funcionamiento de la aplicación. Le recomendamos realizar un mantenimiento del Servidor de administración por lo menos una vez a la semana.

El mantenimiento del Servidor de administración se lleva a cabo a través de la tarea especializada. La aplicación realiza las acciones siguientes durante el mantenimiento del Servidor de administración:

- Elimina carpetas y archivos innecesarios de la carpeta de almacenamiento.
- Elimina los registros innecesarios de las tablas (también conocidos como "referencias colgantes").
- Borra la caché.

- Mantiene la base de datos (si usa PostgreSQL como DBMS):
  - Reorganiza los índices de la base de datos
  - Actualiza las estadísticas de la base de datos
  - Reduce la base de datos si es necesario

La tarea Mantenimiento del Servidor de administración es compatible con las versiones 10.3 y posteriores de MariaDB. Si usa las versiones 10.2 o anteriores de MariaDB, los administradores deben mantener este DBMS por su cuenta.

La tarea Mantenimiento del Servidor de administración se crea automáticamente al instalar Kaspersky Security Center Linux. Si ha eliminado la tarea Mantenimiento del Servidor de administración, puede crearla otra vez manualmente.

Para crear una Mantenimiento del Servidor de administración:

1. En el menú principal, vaya a **Tareas**.
2. Haga clic en el botón **Agregar**.

   Se inicia el Asistente para crear nueva tarea.
3. En la ventana **Configuración de tarea nueva** del Asistente, seleccione **Mantenimiento del Servidor de administración** como tipo de tarea y haga clic en el botón **Siguiente**.
4. Siga el resto de instrucciones del asistente.

Encontrará la nueva tarea en la lista de tareas. Solo puede haber una tarea Mantenimiento del Servidor de administración en ejecución por cada Servidor de administración. Si creó creado una tarea Mantenimiento del Servidor de administración para un Servidor de administración, no podrá crear una nueva tarea Mantenimiento del Servidor de administración.

Eliminar una jerarquía de servidores de administración

Si ya no desea tener una jerarquía de servidores de administración, puede desconectar los servidores de la jerarquía.

Para eliminar una jerarquía de servidores de administración:

1. En el menú principal, haga clic en el nombre del Servidor de administración.
2. En la página que se abre, vaya a la pestaña **Servidores de administración**.
3. Busque el grupo de administración al que pertenezca el servidor de administración secundario que desee eliminar y seleccione ese servidor.

4. En la línea del menú, haga clic en **Eliminar**.

5. En la ventana que se abre, haga clic en **Aceptar** para confirmar que desea eliminar el Servidor de administración secundario.

El Servidor de administración que supo actuar como principal y el Servidor de administración que supo actuar como secundario se vuelven independientes. La jerarquía deja de existir.

Acceso a los servidores DNS públicos

Si no es posible acceder a los servidores de Kaspersky mediante los servidores DNS del sistema, Kaspersky Security Center Linux puede utilizar los siguientes servidores DNS públicos en el siguiente orden:

1. Servidores DNS públicos 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)

Las solicitudes realizadas a estos servidores DNS pueden contener direcciones de dominio y la dirección IP pública del Servidor de administración, ya que la aplicación establece una conexión TCP/UDP con los servidores DNS. Cuando Kaspersky Security Center Linux utiliza un servidor DNS público, el procesamiento de datos se rige por la política de privacidad del servicio utilizado.

Para configurar el uso de servidores DNS públicos a través de la utilidad klscflag:

1. Ejecute el símbolo del sistema de Windows usando derechos de administrador y, a continuación, cambie su directorio actual al directorio con la utilidad klscflag. La utilidad klscflag se encuentra en la carpeta donde está instalado el Servidor de administración. La ruta de instalación predeterminada: <Disk>:\Archivos de programa (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Para deshabilitar el uso de servidores DNS públicos, ejecute el siguiente comando utilizando la cuenta root:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 1
   ```

3. Para habilitar el uso de servidores DNS públicos, ejecute el siguiente comando utilizando la cuenta root:

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

Configuración de la interfaz

Puede configurar la interfaz de Kaspersky Security Center Web Console para mostrar u ocultar distintas secciones y elementos de interfaz según las funciones que utilice.

Para configurar la interfaz de Kaspersky Security Center Web Console y adaptarla a las características que utilice:

1. En el menú principal, vaya a **Configuración → Opciones de interfaz**.
2. Habilite o deshabilite las opciones necesarias:
   - **Mostrar protección y cifrado de datos**
   - **Mostrar funciones de MDR**
   - **Mostrar alertas EDR**
3. Haga clic en el botón **Guardar**.

Una vez habilitadas las opciones necesarias, la consola muestra las secciones correspondientes en el menú principal. Por ejemplo, si habilita **Mostrar alertas EDR**, la sección **Supervisión → Alertas** aparece en el menú principal.

Conexión cifrada con un Servidor de administración

El intercambio de datos entre los dispositivos cliente y el Servidor de administración se puede realizar mediante el protocolo TLS (Seguridad de la capa de transporte). El protocolo TLS puede identificar las partes que interactúan, cifrar los datos que se transfieren y protegerlos de las modificaciones durante la transferencia. El protocolo TLS usa claves públicas para autenticar las partes que interactúan y cifrar datos.

Cuando un dispositivo cliente se conecta al Servidor de administración por primera vez, el Agente de red del dispositivo descarga una copia del certificado del Servidor de administración y lo almacena localmente.

Si instala el Agente de red en un dispositivo localmente, puede seleccionar el certificado del Servidor de administración manualmente.

La copia descargada del certificado se utiliza para verificar los permisos del Servidor de administración durante las siguientes conexiones.

Durante futuras sesiones, el Agente de red solicita el certificado del Servidor de administración en cada conexión del dispositivo al Servidor y lo compara con la copia local. Si las copias no coinciden, el dispositivo no podrá acceder al Servidor de administración.

Cifrar la comunicación con TLS

Para corregir vulnerabilidades en la red corporativa de su organización, puede habilitar el cifrado de tráfico mediante el protocolo TLS. Puede habilitar los protocolos de cifrado TLS y los conjuntos de cifrado compatibles en el Servidor de administración. Kaspersky Security Center Linux admite las versiones 1.0, 1.1, 1.2 y 1.3 del protocolo TLS. Puede seleccionar el protocolo y los conjuntos de cifrado requeridos.

Kaspersky Security Center Linux utiliza certificados autofirmados. También puede utilizar sus propios certificados. Recomendamos utilizar certificados emitidos por autoridades de certificación de confianza.

Para configurar los protocolos de cifrado permitidos y las suites de cifrado en el Servidor de administración:

1. Ejecute el símbolo del sistema de Windows usando derechos de administrador y, a continuación, cambie su directorio actual al directorio con la utilidad klscflag. La utilidad klscflag se encuentra en la carpeta donde está instalado el Servidor de administración. La ruta de instalación predeterminada: <Disk>:\Archivos de programa (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Utilice el indicador SrvUseStrictSslSettings para configurar los protocolos y los conjuntos de cifrado permitidos en el Servidor de administración. Ejecute el siguiente comando en la línea de comandos en la cuenta root:

   ```
   ./klscflag -fset -pv ".core/.independent" -s Transport -n SrvUseStrictSslSettings -v <valor> -t d
   ```

   Especifique el parámetro <valor> del indicador SrvUseStrictSslSettings flag:

   - 4—Solo están habilitados los protocolos TLS 1.2 y TLS 1.3. También están habilitados los conjuntos de cifrado con TLS_RSA_WITH_AES_256_GCM_SHA384 (estos conjuntos de cifrado son necesarios para la compatibilidad con versiones anteriores de Kaspersky Security Center Linux). Este es el valor predeterminado.

     Conjuntos de cifrado compatibles con el protocolo TLS 1.2:

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - AES256-GCM-SHA384 (conjunto de cifrado con TLS_RSA_WITH_AES_256_GCM_SHA384)
     - ECDHE-RSA-AES128-GCM-SHA256
     - ECDHE-RSA-AES128-SHA256

     Conjuntos de cifrado compatibles con el protocolo TLS 1.3:

     - TLS_AES_256_GCM_SHA384
     - TLS_CHACHA20_POLY1305_SHA256
     - TLS_AES_128_GCM_SHA256
     - TLS_AES_128_CCM_SHA256

   - 5—Solo están habilitados los protocolos TLS 1.2 y TLS 1.3. Para el protocolo TLS 1.2 y TLS 1.3, se admiten los conjuntos de cifrado específicos que se enumeran a continuación.

     Conjuntos de cifrado compatibles con el protocolo TLS 1.2:

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256

Conjuntos de cifrado compatibles con el protocolo TLS 1.3:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256

No recomendamos usar 0, 1, 2 o 3 como valor de parámetro del indicador SrvUseStrictSslSettings. Estos valores de parámetros corresponden a versiones del protocolo TLS no seguras (TLS 1.0 y TLS 1.1) y conjuntos de cifrado no seguros, y se utilizan solo para la compatibilidad con versiones anteriores de Kaspersky Security Center.

3. Reinicie los siguientes servicios de Kaspersky Security Center Linux:
   - Servidor de administración
   - Servidor web
   - Proxy de activación

Como resultado, se habilita el cifrado de tráfico mediante el protocolo TLS.

Puede utilizar los indicadores KLTR_TLS12_ENABLED y KLTR_TLS13_ENABLED para habilitar la compatibilidad con los protocolos TLS 1.2 y TLS 1.3, respectivamente. Estos indicadores están habilitados de manera predeterminada.

Para habilitar o deshabilitar la compatibilidad con los protocolos TLS 1.2 y TLS 1.3:

1. Ejecute la utilidad klscflag.

   Ejecute el símbolo del sistema de Windows usando derechos de administrador y, a continuación, cambie su directorio actual al directorio con la utilidad klscflag. La utilidad klscflag se encuentra en la carpeta donde está instalado el Servidor de administración. La ruta de instalación predeterminada: <Disk>:\Archivos de programa (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Ejecute uno de los siguientes comandos en la línea de comandos en la cuenta root:
   - Utilice este comando para habilitar o deshabilitar la compatibilidad con el protocolo TLS 1.2:

     ```
     ./klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS12_ENABLED -v <valor> -t d
     ```

   - Utilice este comando para habilitar o deshabilitar la compatibilidad con el protocolo TLS 1.3:

     ```
     ./klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS13_ENABLED -v <valor> -t d
     ```

Especifique el parámetro < `valor` > del indicador:

- `1`—Para habilitar el soporte del protocolo TLS.
- `0`—Para deshabilitar el soporte del protocolo TLS.

Configuración de la red para interactuar con servicios externos

Kaspersky Security Center Linux utiliza la siguiente configuración de red para interactuar con servicios externos.

Configuración de red

Configuración de red	Dirección	Descripción
Puerto: 443 Protocolo: HTTPS	`https://activation-v2.kaspersky.com`	Activación de la aplicación.
Puerto: 443 Protocolo: HTTPS	`https://products.s.kaspersky-labs.com`	Repositorio de paquetes de distribución de aplicaciones para instalación remota

Puerto: 443
Protocolo: 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`
		Actualizar las bases de datos, los módulos de software y las aplicaciones de Kaspersky.

Puerto: 443 Protocolo: HTTPS	`https://downloads.upd.kaspersky.com`	• Actualizar las bases de datos, los módulos de software y las aplicaciones de Kaspersky. • Comprobar si se puede acceder a los servidores de Kaspersky. Antes de descargar las bases de datos y los módulos de software de Kaspersky, Kaspersky Security Center Linux verifica que se pueda acceder a los servidores de Kaspersky. Si los servidores DNS configurados en el sistema no permiten acceder a los servidores de Kaspersky, la aplicación utiliza servidores DNS públicos.

Configuración de red	Dirección	Descripción
Puerto: 80 Protocolo: HTTP	http://p00.upd.kaspersky.com http://p01.upd.kaspersky.com http://p02.upd.kaspersky.com http://p03.upd.kaspersky.com http://p04.upd.kaspersky.com http://p05.upd.kaspersky.com http://p06.upd.kaspersky.com http://p07.upd.kaspersky.com http://p08.upd.kaspersky.com http://p09.upd.kaspersky.com http://p10.upd.kaspersky.com http://p11.upd.kaspersky.com http://p12.upd.kaspersky.com http://p13.upd.kaspersky.com http://p14.upd.kaspersky.com http://p15.upd.kaspersky.com http://p16.upd.kaspersky.com http://p17.upd.kaspersky.com http://p18.upd.kaspersky.com http://p19.upd.kaspersky.com http://downloads0.kaspersky-labs.com http://downloads1.kaspersky-labs.com http://downloads2.kaspersky-labs.com http://downloads3.kaspersky-labs.com http://downloads4.kaspersky-labs.com http://downloads5.kaspersky-labs.com http://downloads6.kaspersky-labs.com http://downloads7.kaspersky-labs.com http://downloads8.kaspersky-labs.com http://downloads9.kaspersky-labs.com http://downloads.kaspersky-labs.com http://cm.k.kaspersky-labs.com	Actualizar las bases de datos, los módulos de software y las aplicaciones de Kaspersky.
Puerto: 443 Protocolo: HTTPS	https://ds.kaspersky.com https://dc1.ksn.kaspersky-labs.com https://dc1-file.ksn.kaspersky-labs.com https://dc1-pp.ksn.kaspersky-labs.com https://dc1-st.ksn.kaspersky-labs.com/ https://dc1-cert.ksn.kaspersky-labs.com https://dc1-cf.ksn.kaspersky-labs.com https://dc1-file.ksn.kaspersky-labs.com https://dc1-kas.ksn.kaspersky-labs.com https://dc1-ml.ksn.kaspersky-labs.com https://dc1-pp.ksn.kaspersky-labs.com https://dc1-st.ksn.kaspersky-labs.com https://dc1.ksn.kaspersky-labs.com	Usar Kaspersky Security Network.

Configuración de red	Dirección	Descripción
Puerto: 443, 1443 Protocolo: HTTPS	https://ksn-file-geo.kaspersky-labs.com https://ksn-verdict-geo.kaspersky-labs.com https://ksn-url-geo.kaspersky-labs.com https://ksn-a-p2p-geo.kaspersky-labs.com https://ksn-info-geo.kaspersky-labs.com https://ksn-cinfo-geo.kaspersky-labs.com	Usar Kaspersky Security Network.
Puerto: 443, 1443 Protocolo: KSN	ksn://ksn-a-p2p-geo.kaspersky-labs.com ksn://ksn-a-stat-geo.kaspersky-labs.com ksn://ksn-ca-geo.kaspersky-labs.com ksn://ksn-cinfo-geo.kaspersky-labs.com ksn://ksn-crypto-catm-geo.kaspersky-labs.com ksn://ksn-crypto-dnscheck-geo.kaspersky-labs.com ksn://ksn-crypto-hash-geo.kaspersky-labs.com ksn://ksn-crypto-ipm-geo.kaspersky-labs.com ksn://ksn-crypto-whocalls-geo.kaspersky-labs.com ksn://ksn-crypto-wifiplus-geo.kaspersky-labs.com ksn://ksn-eu-stat-kmp.kaspersky-labs.com ksn://ksn-file-geo.kaspersky-labs.com ksn://ksn-his-geo.kaspersky-labs.com ksn://ksn-info-geo.kaspersky-labs.com ksn://ksn-kas-geo.kaspersky-labs.com ksn://ksn-kddi.kaspersky-labs.com ksn://ksn-ml-geo.kaspersky-labs.com ksn://ksn-oui-geo.kaspersky-labs.com ksn://ksn-pp.kaspersky-labs.com ksn://ksn-src.kaspersky-labs.com ksn://ksn-stat-geo.kaspersky-labs.com ksn://ksn-tcert-geo.kaspersky-labs.com ksn://ksn-url-geo.kaspersky-labs.com ksn://ksn-verdict-geo.kaspersky-labs.com ksn://mdr.ksn.kaspersky-labs.com ksn://stat-eu.ksn.kaspersky-labs.com ksn://stat-hq.ksn.kaspersky-labs.com ksn://stat-ru.ksn.kaspersky-labs.com ksn://stat-sa.ksn.kaspersky-labs.com ksn://stat-sbr.ksn.kaspersky-labs.com	Usar Kaspersky Security Network.
Puerto: 443 Protocolo: HTTPS	https://click.kaspersky.com https://redirect.kaspersky.com	Seguir los enlaces desde la interfaz.

Configuración de red	Dirección	Descripción
Puerto: 80 Protocolo: HTTP	`http://crl.kaspersky.com` `http://ocsp.kaspersky.com`	Estos servidores forman parte de la Infraestructura de clave pública (PKI) y son necesarios para verificar el estado de validez de los certificados de firma digital de Kaspersky. La CRL es una lista de certificados revocados. El OCSP le permite solicitar el estado de un certificado específico en tiempo real. Estos servidores ayudan a garantizar la seguridad de la interacción con certificados digitales y protegen contra posibles ataques.
Puerto: 443 Protocolo: HTTPS	`https://ipm-klca.kaspersky.com`	Novedades con fines publicitarios
Puerto: 443 Protocolo: HTTPS	`https://tip.kaspersky.com`	Responder a las amenazas a través de Kaspersky Threat Intelligence Portal (cuando se utiliza la funcionalidad Kaspersky Next XDR Optimum).
Puerto: 443 Protocolo: HTTPS	Para obtener la lista completa de direcciones, consulte el artículo Estructura de direcciones y dominios	Responder a las amenazas a través de Kaspersky Automated Security Awareness Platform (cuando se utiliza la funcionalidad Kaspersky Next XDR Optimum).

Para una interacción adecuada de Kaspersky Security Center Linux con servicios externos, considere las siguientes recomendaciones:
- Se debe permitir el tráfico de red no cifrado en los puertos 443 y 1443 del equipo de red y del servidor proxy de su organización.
- Cuando el Servidor de administración interactúa con los servidores de actualización de Kaspersky y los servidores de Kaspersky Security Network, es necesario evitar el secuestro del tráfico de red con sustitución de certificados (ataques MITM).

Para descargar actualizaciones a través del protocolo HTTP o HTTPS utilizando la utilidad klscflag:

1. Ejecute el símbolo del sistema de Windows usando derechos de administrador y, a continuación, cambie su directorio actual al directorio con la utilidad klscflag. La utilidad klscflag se encuentra en la carpeta donde está instalado el Servidor de administración. La ruta de instalación predeterminada: <Disk>:\Archivos de programa (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Si desea descargar actualizaciones a través del protocolo HTTP, ejecute uno de los siguientes comandos en la cuenta root:

   - En el dispositivo en el que se encuentra instalado el Servidor de administración:

     ```
     klscflag -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 1
     ```

   - En un punto de distribución:

     ```
     klscflag -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 1
     ```

   Si desea descargar actualizaciones a través del protocolo HTTPS, ejecute uno de los siguientes comandos en la cuenta root:

   - En el dispositivo en el que se encuentra instalado el Servidor de administración:

     ```
     klscflag -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 0
     ```

   - En un punto de distribución:

     ```
     klscflag -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 0
     ```

Lista global de subredes

Para cada Servidor de administración que utilice, puede configurar una lista global de subredes para almacenar la información sobre las subredes de su red. Esta lista le ayuda a hacer coincidir los pares {dirección IP, máscara} y unidades físicas y sucursales. Puede usar subredes de esta lista en las reglas y configuraciones de red.

Para añadir subredes a la lista global de subredes:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, vaya a la sección **Subredes globales**.

3. Haga clic en **Agregar**.

   Se abre la ventana **Nueva subred**.

4. Complete los siguientes campos:

   - **Nombre**
   - **Dirección de subred**
   - **Máscara de subred**
   - **Descripción**

5. Haga clic en el botón **Guardar**.

La ventana se cierra y la subred aparece en la lista de subredes.

Si es necesario, en la lista de subredes globales puede hacer lo siguiente:

- Eliminar subredes de la lista seleccionando la subred requerida y haciendo clic en el botón **Eliminar**.
- Modificar las propiedades de las subredes haciendo clic en el vínculo con el nombre de la subred requerida y luego realizando las acciones descritas en los pasos 4 a 5.

Comprobar la integridad de los módulos mediante las utilidades klscmodchk e Integrity_checker

Kaspersky Security Center para Linux incluye varios módulos binarios en forma de bibliotecas enlazadas dinámicamente, archivos ejecutables, archivos de configuración y archivos de interfaz. Un atacante podría reemplazar uno o más módulos ejecutables o archivos de la aplicación por otros archivos que contengan código malicioso. Para evitar la sustitución de módulos y archivos, Kaspersky Security Center Linux implementa una comprobación de la integridad de los componentes mediante las utilidades klscmodchk e integrity_checker. Estas utilidades comprueban los módulos y archivos en busca de cambios no autorizados o daños. Si un módulo o archivo de aplicación tiene una suma de control incorrecta, se considera dañado.

La utilidad klscmodchk realiza comprobaciones de integridad de los siguientes componentes de Kaspersky Security Center Linux:

- Servidor de administración
- Agente de red

La utilidad Integrity_checker realiza comprobaciones de integridad de los siguientes componentes de Kaspersky Security Center Linux:

- Servidor de administración
- Agente de red
- Kaspersky Security Center Web Console

Ambas utilidades verifican la comprobación de integridad del módulo según el archivo de manifiesto kl_file_integrity_manifest.xml, que es parte de la compilación de Kaspersky Security Center Linux y se encuentra en la carpeta de instalación. El archivo de manifiesto del componente contiene archivos cuya integridad es importante para el correcto funcionamiento del componente de Kaspersky Security Center Linux. También se comprueba la integridad de los archivos de manifiesto.

Se recomienda no modificar el archivo de manifiesto kl_file_integrity_manifest.xml, ya que esto invalidará la firma digital y hará que la comprobación de integridad falle.

Para realizar la comprobación de integridad del componente de Kaspersky Security Center Linux, ejecute uno de los siguientes comandos:

- `klscmodchk [ parámetros ]`

  La utilidad klscmodchk inicia la utilidad integrity_checker con el parámetro `--verbose` y verifica la integridad de los módulos.

  Parámetros de la utilidad klscmodchk:

  - `-logfile < log_file_path >`: especifique la ruta de acceso a un archivo en el disco para el registro. De forma predeterminada, la información se envía a la consola.
  - `-verbose`: muestra información ampliada durante la comprobación de integridad.

- `integrity_checker [ parámetros ] < manifest_file_path >`

  Parámetros de la utilidad integrity_checker:

  - `--help`: muestra la ayuda de la utilidad integrity_checker.
  - `--version`: muestra la versión de la utilidad integrity_checker.
  - `--verbose`: muestra información sobre el funcionamiento de la utilidad. Al realizar una comprobación de integridad, es suficiente usar este parámetro en el comando.

El resultado de la verificación de cada archivo de manifiesto se muestra junto al nombre del archivo de manifiesto en el siguiente formato:

- SUCCEEDED: integridad del archivo confirmada (código de retorno 0).
- FAILED: integridad del archivo no confirmada (código de retorno diferente de cero).

También puede configurar las comprobaciones de integridad para que se inicien automáticamente al iniciar la aplicación. De manera predeterminada, la verificación de integridad automática está deshabilitada.

Para habilitar la verificación de integridad automática:

1. En el dispositivo donde está instalado el Servidor de administración, en el símbolo del sistema, ingrese el siguiente comando:

   ```
   ./klscflag -fset -pv klserver -n KLMODCHK_ENABLE_CHECKING -t d -v 1
   ```

2. Reiniciar el dispositivo.

   La verificación de integridad automática está habilitada.

En la próxima ejecución de Kaspersky Security Center, la utilidad klscmodchk se ejecutará junto con el Servidor de administración e iniciará la verificación de la integridad de los módulos. El resultado de las verificaciones de integridad se escribe en el Registro de eventos de Kaspersky.

Descubrimiento de dispositivos conectados a la red

Esta sección describe la búsqueda y la detección de dispositivos conectados a una red.

Kaspersky Security Center Linux permite encontrar dispositivos basándose en criterios especificados. Los resultados de estas búsquedas se pueden guardar en un archivo de texto.

La función de búsqueda y la detección permite encontrar los siguientes dispositivos:

- Dispositivos administrados en grupos de administración del Servidor de administración de Open Single Management Platform y sus Servidores de administración secundarios.
- Dispositivos no asignados administrados por el Servidor de administración y sus Servidores de administración secundarios.

Escenario: Descubrir dispositivos conectados a la red

Antes de instalar las aplicaciones de seguridad, es necesario llevar a cabo un descubrimiento de dispositivos. Descubrir qué dispositivos están conectados a la red le permitirá recibir información sobre ellos y usar directivas para administrarlos. La red debe sondearse en forma periódica tanto para detectar dispositivos nuevos como para determinar si los ya descubiertos siguen conectados.

El proceso para descubrir los dispositivos conectados a la red se divide en etapas:

1. **Descubrimiento de dispositivos inicial**

   Una vez que termine con el asistente de inicio rápido, realice la detección de dispositivos manualmente.

2. **Configurando futuros sondeos**

   Asegúrese de que el sondeo de rangos IP esté habilitado y que el calendario de sondeo cumpla con las necesidades de su organización. Al configurar el horario de sondeo, utilice las recomendaciones para la red de frecuencia de sondeo.

   También puede habilitar el Sondeo de Zeroconf si su red incluye dispositivos IPv6.

   Si los dispositivos en red están incluidos en un dominio, se recomienda utilizar el sondeo del controlador de dominio.

   Utilice puntos de distribución basados en Windows para sondear las redes de Windows.

3. **Configurar reglas para que los dispositivos descubiertos se agreguen a grupos de administración (opcional)**

   Los dispositivos nuevos aparecen en la red al detectarse durante los sondeos de red. Estos se incluyen automáticamente en el grupo **Dispositivos no asignados**. Si lo desea, puede configurar las reglas para automático el traslado de estos dispositivos al grupo **Dispositivos administrados**. También puede definir reglas de retención.

   Si omite esta etapa y no configura ninguna regla, los nuevos dispositivos que se descubran se agregarán al grupo **Dispositivos no asignados** y se quedarán allí. Si lo desea, puede mover estos dispositivos manualmente al grupo **Dispositivos administrados**. Si mueve los dispositivos manualmente al grupo **Dispositivos administrados**, puede analizar la información sobre cada dispositivo y decidir si desea moverlo a un grupo de administración, y, de ser así, a qué grupo.

Resultados

Completar las etapas anteriores tiene los siguientes resultados:

- El Servidor de administración de Kaspersky Security Center Linux detecta los dispositivos que están en la red y le proporciona información sobre ellos.
- Los sondeos futuros se configuran y funcionan de acuerdo con el calendario programado.

Los dispositivos recién descubiertos se asignan de acuerdo con las reglas especificadas. Si no configura ninguna regla, los dispositivos se dejarán en el grupo **Dispositivos no asignados**.

Sondeo de la red de Windows

Acerca del sondeo de la red de Windows

El Servidor de administración de Kaspersky Security Center Linux no es compatible con el sondeo de red de Windows. Utilice puntos de distribución basados en Windows para sondear las redes de Windows.

Cuando se realiza un sondeo rápido, los puntos de distribución solo recuperan información de la lista de nombres NetBIOS correspondientes a los dispositivos de todos los dominios y grupos de trabajo de la red. Cuando se realiza un sondeo completo, se solicita la siguiente información a cada dispositivo cliente:

- Nombre del sistema operativo
- Dirección IP
- Nombre DNS
- Nombre NetBIOS

Para realizar un sondeo rápido o completo, se deben cumplir los siguientes requisitos:

- Los puertos UDP 137/138, TCP 139, UDP 445, TCP 445 deben estar disponibles en la red.
- El protocolo SMB está activado.
- Se debe utilizar el servicio Explorador de equipos de Microsoft y el equipo del navegador principal debe estar habilitado en el Servidor de administración.
- Se debe utilizar el servicio Explorador de equipos de Microsoft y el equipo explorador principal debe estar habilitado en esta cantidad de dispositivos cliente:
  - al menos un dispositivo si no hay más de 32 dispositivos conectados a la red;
  - al menos un dispositivo por cada 32 dispositivos conectados a la red.

Para realizar un sondeo completo, primero debe haberse realizado al menos un sondeo rápido.

Sondeo de intervalos IP

Kaspersky Security Center Linux lleva a cabo una operación de resolución inversa para intentar determinar, mediante consultas DNS estándar, el nombre DNS correspondiente a cada dirección IPv4 del intervalo especificado. Si esta operación tiene éxito, el servidor envía al nombre recibido un `ICMP ECHO REQUEST` (el mismo tipo de solicitud que se utiliza en el comando ping). Si el dispositivo responde, se agrega información sobre el mismo a la base de datos de Kaspersky Security Center Linux. La resolución de nombres inversa es necesaria para excluir dispositivos de red que pueden tener una dirección IP, pero que no son computadoras (por ejemplo, impresoras de red o routers).

Para que este método de sondeo funcione, debe haber un servicio de DNS local correctamente configurado. El servicio debe tener una zona de búsqueda inversa. Si no se ha configurado tal zona, el sondeo de subredes IP no dará resultados.

Inicialmente, para obtener los intervalos IP que se deben sondear, Kaspersky Security Center Linux se fija en la configuración de red del dispositivo en el que está instalado. Si la dirección del dispositivo es 192.168.0.1 y la máscara de subred es 255.255.255.0, Kaspersky Security Center Linux incluye automáticamente la red 192.168.0.0/24 en la lista de direcciones para sondear. Kaspersky Security Center Linux sondeará todas las direcciones incluidas en el intervalo que va de 192.168.0.1 a 192.168.0.254.

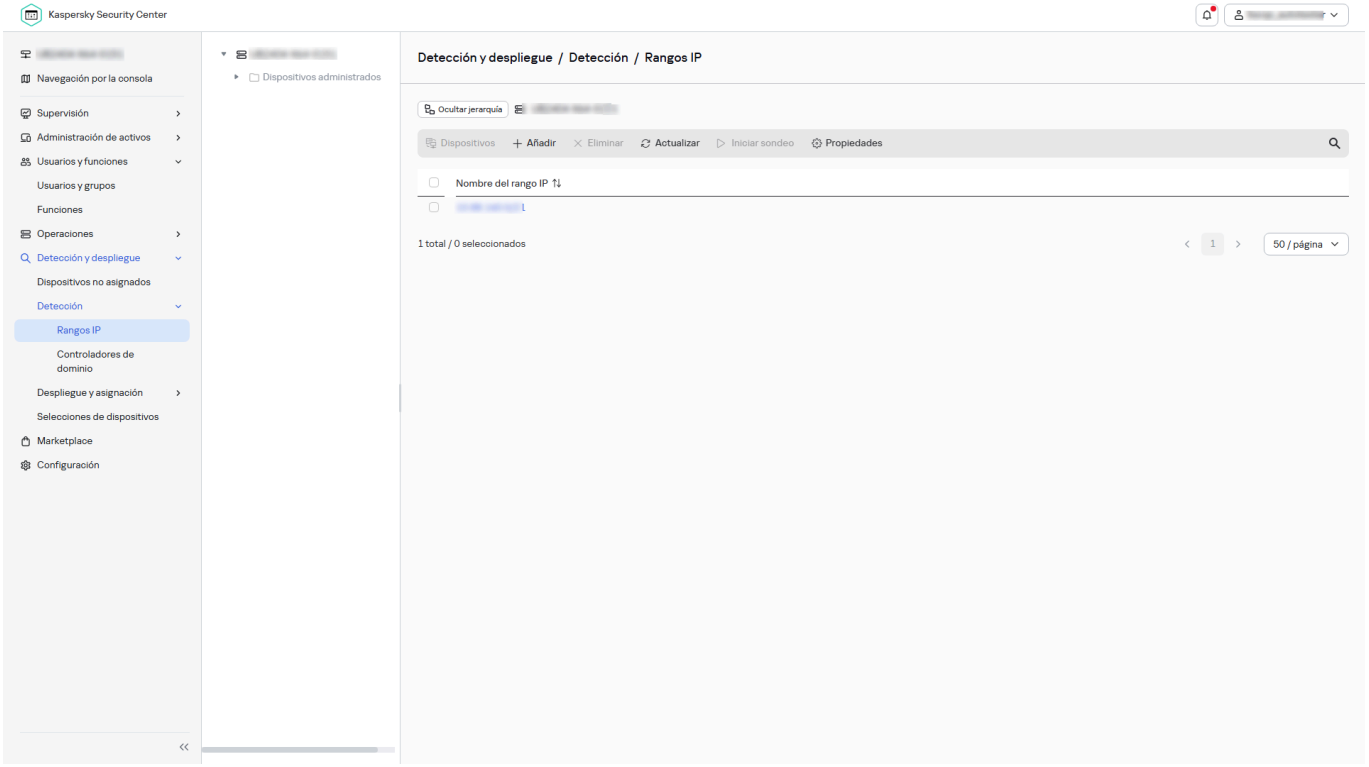
Si solo habilita el sondeo de intervalos IP, Kaspersky Security Center Linux únicamente detectará dispositivos que tengan una dirección IPv4. Si su red incluye dispositivos IPv6, active Sondeo de Zeroconf de dispositivos.

Para todos los hosts basados en Linux dentro de un controlador de dominio de Microsoft Active Directory, Samba, FreeIPA o ALD Pro, especifique el `netbios name` y los parámetros del `workgroup` en el archivo `/etc/samba/smb.conf`. Si no lo hace, es posible que los resultados del sondeo contengan hosts duplicados.

Cómo ver y modificar la configuración del sondeo de intervalos IP

Para ver y modificar las propiedades del sondeo de intervalos IP:

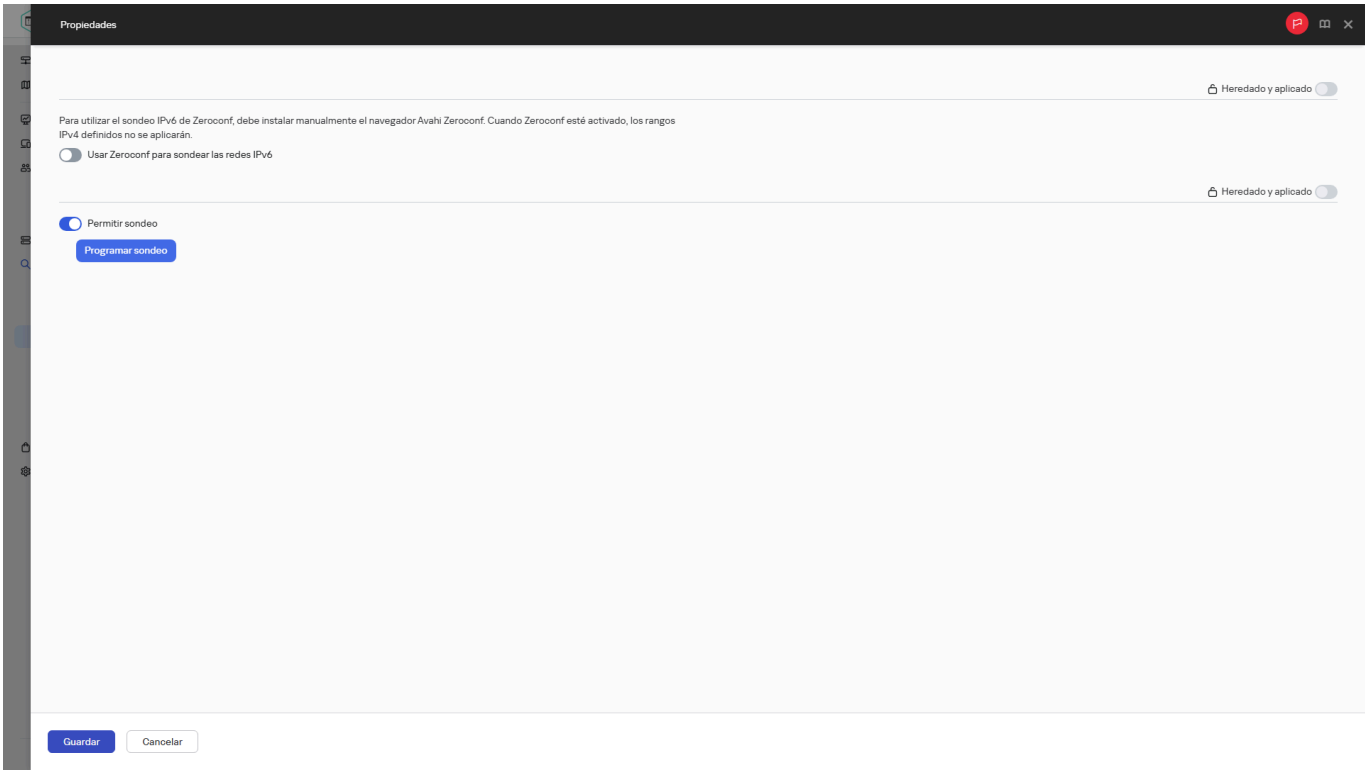
1. En el menú principal, vaya a **Descubrimiento y despliegue → Descubrimiento → Intervalos IP**.



Lista de intervalos IP

2. Haga clic en el botón **Propiedades**.

   Se abre la ventana de propiedades de sondeo de IP.



Propiedades de sondeo de IP

3. Utilizando el interruptor **Permitir sondeo**, habilite o deshabilite el sondeo de intervalos IP.

4. Configurar la programación del sondeo. De forma predeterminada, el sondeo de intervalos IP se ejecuta cada 420 minutos (7 horas).

   Al definir la frecuencia de sondeo, asegúrese de usar un valor que no supere el del parámetro Vigencia de la dirección IP. Si la función de sondeo no verifica que una dirección IP se encuentra activa durante el tiempo de vigencia de las direcciones IP, la dirección se elimina automáticamente de los resultados del sondeo. Los resultados de los sondeos tienen una vida útil por defecto de veinticuatro horas; esto se debe a que las direcciones IP dinámicas (las que se asignan mediante el protocolo de configuración dinámica de hosts, DHCP) cambian cada veinticuatro horas.

   Opciones de programación para el sondeo:

   - **Cada N días**

     Se realizará un sondeo en forma periódica, a intervalos regulares, a partir de la fecha y hora indicadas. Cada sondeo estará separado del anterior por el número de días que indique.

     De forma predeterminada, se realizará un sondeo todos los días, a partir de la fecha y hora actuales del sistema.

   - **Cada N minutos**

     Se realizará un sondeo en forma periódica, a intervalos regulares, a partir de la hora indicada. Cada sondeo estará separado del anterior por el número de minutos que indique.

   - **Por días de la semana**

     Se realizará un sondeo en forma periódica, a intervalos regulares, en el día de la semana y a la hora que indique.

   - **Mensualmente en el día de la semana seleccionado**

     Se realizará un sondeo en forma periódica, a intervalos regulares, en los días del mes y a la hora que indique.

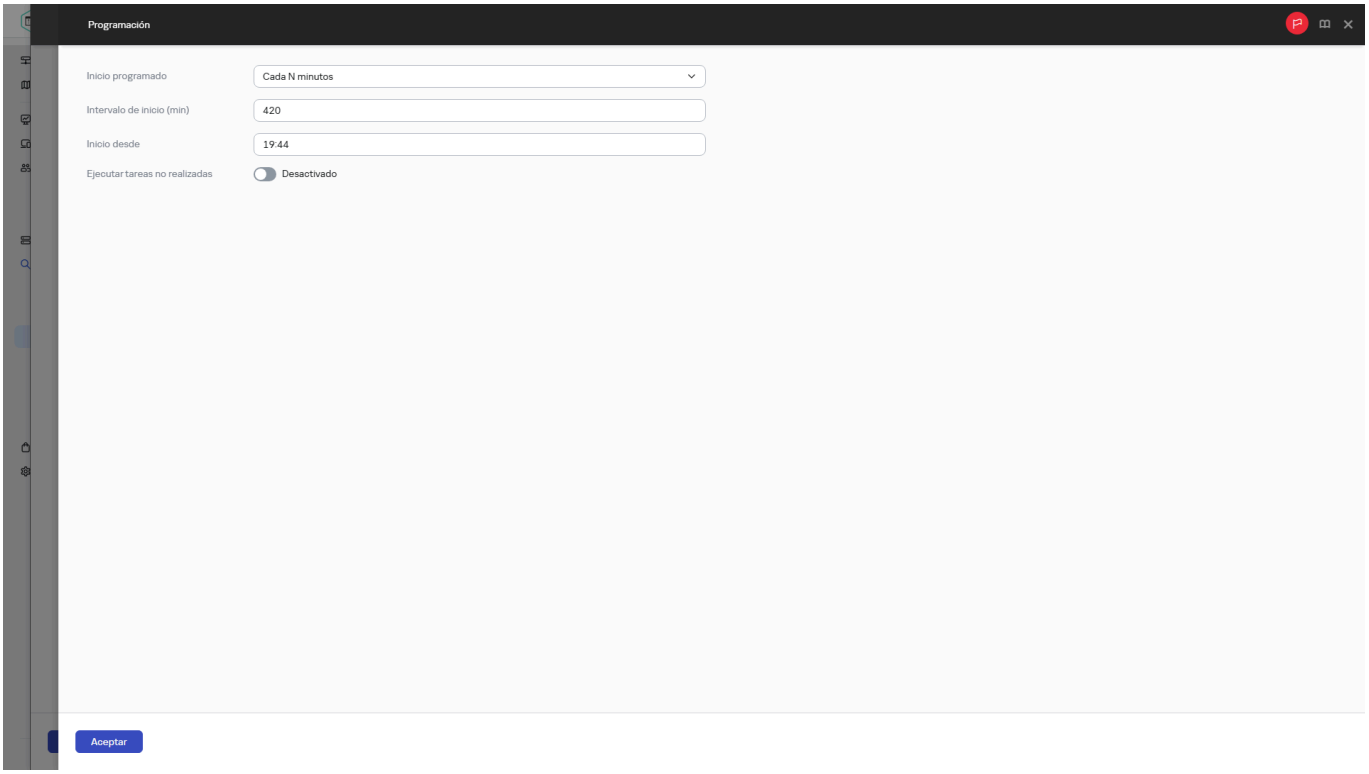
   - **Ejecutar tareas no realizadas**

     Si el Servidor de administración está apagado o no está disponible durante la hora programada para el sondeo, el Servidor de administración puede iniciar el sondeo inmediatamente después de encenderlo o esperar la próxima vez que se programe el sondeo.

     Si esta opción está habilitada, el Servidor de administración inicia el sondeo inmediatamente después de que se enciende.

     Si esta opción está desactivada, el Servidor de administración espera la próxima vez que se programe el sondeo.

Esta opción está deshabilitada de forma predeterminada.



Configuración de la programación de sondeos

5. Haga clic en el botón **Guardar**.

Las propiedades se guardan y se aplican a todos los intervalos IP.

Ejecutando la encuesta manualmente

Para ejecutar la encuesta de inmediato,

Haga clic en **Iniciar sondeo**.

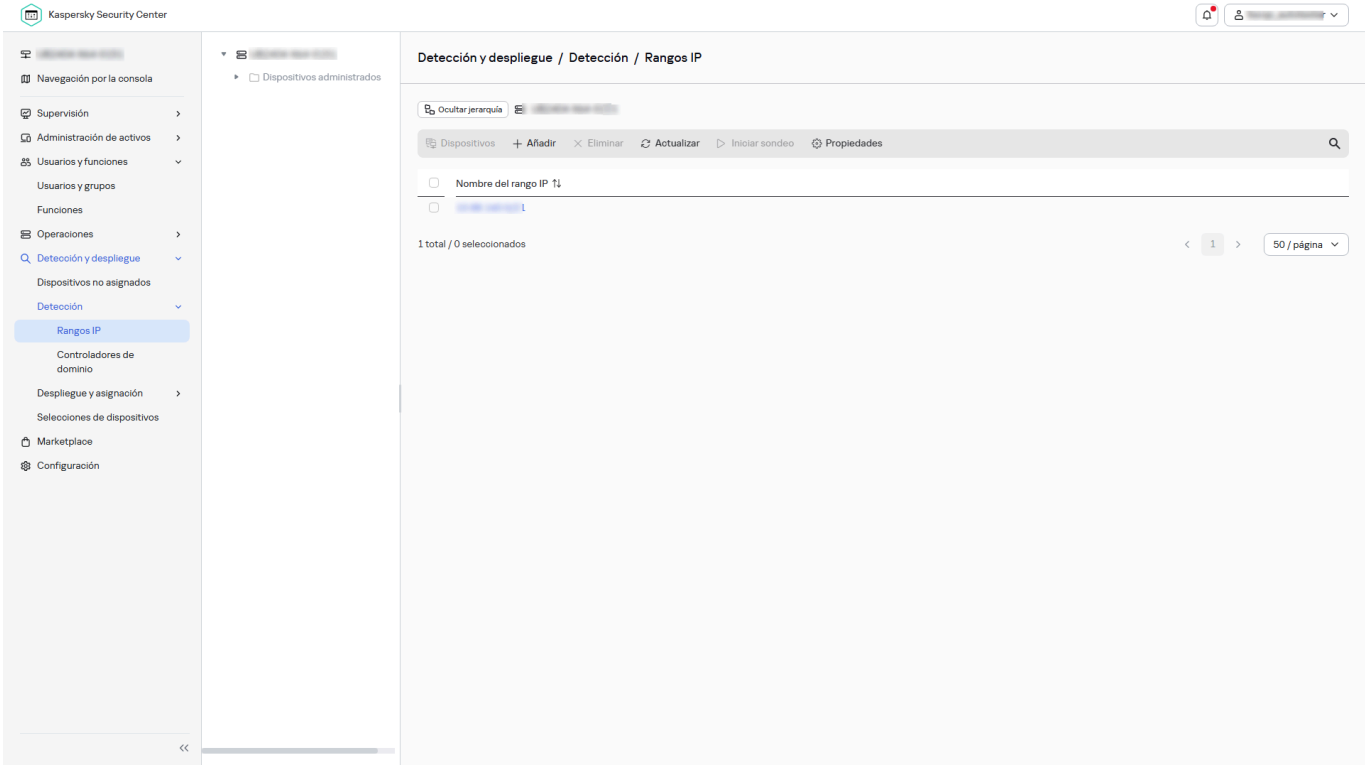
Agregar y modificar un intervalo IP

Inicialmente, para obtener los intervalos IP que se deben sondear, Kaspersky Security Center Linux se fija en la configuración de red del dispositivo en el que está instalado. Si la dirección del dispositivo es 192.168.0.1 y la máscara de subred es 255.255.255.0, Kaspersky Security Center Linux incluye automáticamente la red 192.168.0.0/24 en la lista de direcciones para sondear. Kaspersky Security Center Linux sondeará todas las direcciones incluidas en el intervalo que va de 192.168.0.1 a 192.168.0.254. Puede modificar los intervalos IP definidos automáticamente o agregar intervalos IP personalizados.

Puede crear un rango solo para direcciones IPv4. Si habilita el sondeo con Zeroconf, Kaspersky Security Center Linux sondeará la red completa.

Para agregar un nuevo intervalo IP:

1. En el menú principal, vaya a **Descubrimiento y despliegue → Descubrimiento → Intervalos IP**.



Lista de intervalos IP

2. Para agregar un nuevo intervalo IP, haga clic en el botón **Agregar**.

3. En la ventana que se abre, defina los siguientes ajustes:

   Nombre del intervalo IP

   Nombre que se le dará al intervalo IP. El nombre puede ser el intervalo en sí mismo (por ejemplo, "192.168.0.0/24").

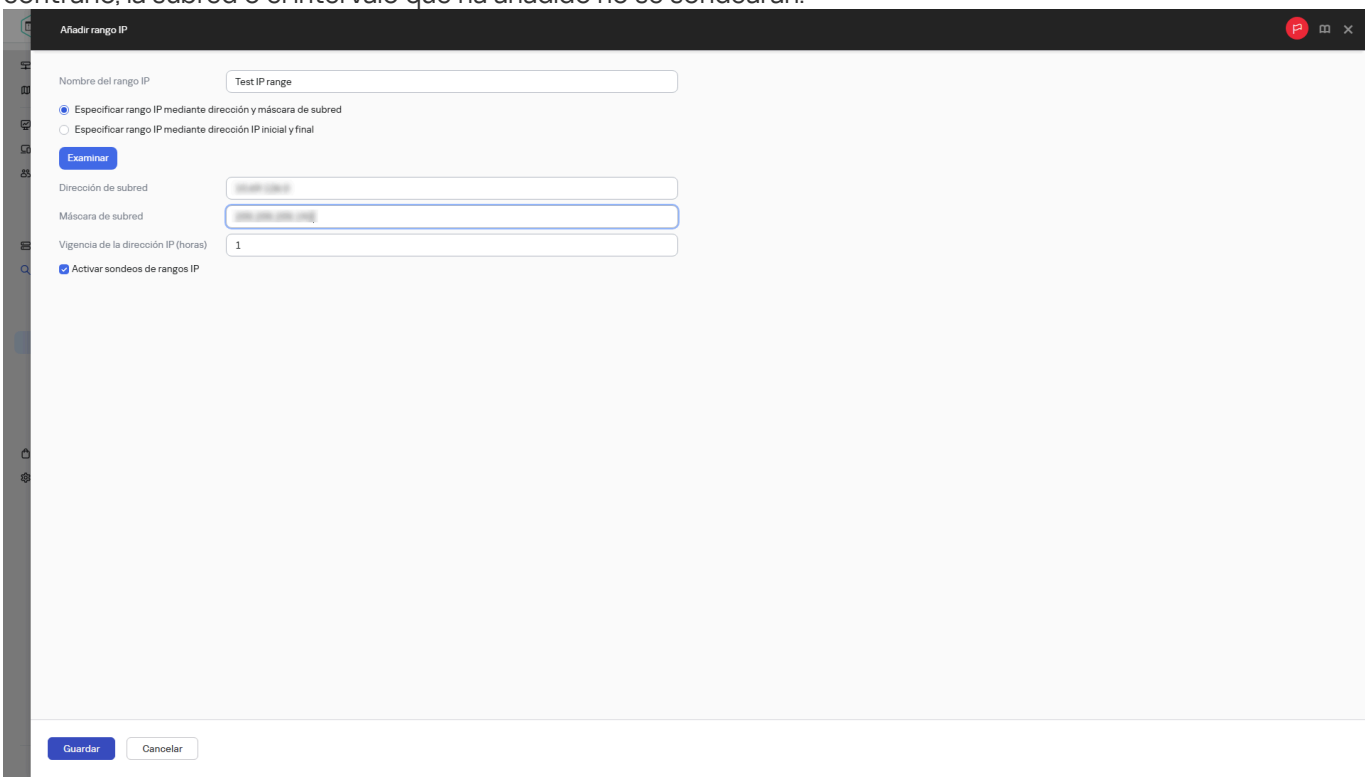
   Intervalo IP o dirección y máscara de subred

   Establezca el intervalo IP especificando las direcciones IP iniciales y finales o la dirección de subred y la máscara de subred. También puede seleccionar uno de los rangos IP existentes haciendo clic en el botón **Examinar**.

   Vigencia de la dirección IP (h)

   Al configurar este ajuste, asegúrese de que el valor supere el intervalo de sondeo establecido en la programación de sondeos. Si la función de sondeo no verifica que una dirección IP se encuentra activa durante el tiempo de vigencia de las direcciones IP, la dirección se elimina automáticamente de los resultados del sondeo. Los resultados de los sondeos tienen una vida útil por defecto de veinticuatro horas; esto se debe a que las direcciones IP dinámicas (las que se asignan mediante el protocolo de configuración dinámica de hosts, DHCP) cambian cada veinticuatro horas.

4. Seleccione **Habilitar el sondeo de intervalos IP** si desea sondear la subred o el intervalo que agregó. De lo contrario, la subred o el intervalo que ha añadido no se sondearán.



Especificar la configuración del intervalo IP

5. Haga clic en el botón **Guardar**.

   El nuevo intervalo IP se agrega a la lista de intervalos IP.

Puede ejecutar el sondeo de cada rango IP por separado usando el botón **Iniciar sondeo**. De forma predeterminada, los resultados del sondeo serán válidos por veinticuatro horas (el mismo tiempo por el que se considera vigente una dirección IP).

Para agregar una subred a un rango IP existente:

1. En el menú principal, vaya a **Descubrimiento y despliegue** → **Descubrimiento** → **Intervalos IP**.
2. Haga clic en el nombre del rango IP al que desea agregar una subred.
3. En la ventana que se abre, haga clic en el botón **Agregar**.
4. Especifique una subred usando su dirección y máscara o usando la primera y la última dirección IP en el intervalo IP. O, agregue una subred existente haciendo clic en el botón **Examinar**.
5. Haga clic en el botón **Guardar**.

   La nueva subred se agrega al rango IP.
6. Haga clic en el botón **Guardar**.

   La nueva configuración del rango IP se guarda.

Puede agregar todas las subredes que necesite. Los intervalos IP con nombre no se pueden superponer, pero no existe tal restricción para las subredes sin nombre contenidas en un intervalo IP. Puede habilitar y deshabilitar el sondeo de forma independiente para cada rango IP.

Sondeo con Zeroconf

Este tipo de sondeo solo es compatible con los puntos de distribución basados en Linux.

Kaspersky Security Center Linux puede sondear redes que tienen dispositivos con direcciones IPv6. Para realizar estos sondeos, no es necesario indicar intervalos de direcciones IP: Kaspersky Security Center Linux sondea la red completa utilizando el conjunto de tecnologías *Zeroconf*. Para comenzar a usar Zeroconf, debe instalar los componentes de avahi (avahi-utils) en el dispositivo Linux que sondea las redes, es decir, el Servidor de administración o un punto de distribución.

Al usar Zeroconf, el Servidor de administración o el punto de distribución analiza la red para detectar dispositivos compatibles con el protocolo Zeroconf y los agrega temporalmente a la lista. Luego, se realiza un ping ICMPv6 a cada dispositivo para verificar su disponibilidad, y el servicio avahi realiza una búsqueda inversa de DNS para resolver las direcciones IPv6 en nombres del DNS. La información sobre el sistema host (nombre del DNS y tipo de sistema operativo) se registra en la base de datos de Kaspersky Security Center Linux.

El alcance del sondeo con Zeroconf depende de la configuración del servicio avahi. De forma predeterminada, se realiza un sondeo por difusión dentro de una subred. Si hay varias interfaces de red configuradas en el dispositivo que aloja el Servidor de administración o el punto de distribución, el servicio avahi sondea las subredes asociadas a todas las interfaces activas.

Recomendaciones para realizar correctamente un sondeo con Zeroconf

- Asegúrese de que se hayan configurado los siguientes ajustes en el archivo /etc/avahi/avahi-daemon.conf:
  - En el Servidor de administración o el punto de distribución:
    `[server]`
    `use-ipv6=yes`
  - En los dispositivos:
    `[server]`
    `use-ipv6=yes`
    `[publish]`
    `publish-addresses=yes`
    `publish-workstation=yes`
- Asegúrese de que la siguiente línea esté presente en el archivo /etc/nsswitch.conf:
  - En el Servidor de administración o el punto de distribución:
    `mdns_minimal [NOTFOUND=return] dns`

Para habilitar el sondeo de Zeroconf:

1. En el menú principal, vaya a **Descubrimiento y despliegue → Descubrimiento → Intervalos IP**.
2. Haga clic en el botón **Propiedades**.
3. En la ventana abierta, encienda el botón **Usar Zeroconf para el sondeo de redes IPv6**.

Tras esto, Kaspersky Security Center Linux comenzará a sondear la red. En este caso, se ignoran los rangos de IP especificados.

Sondeo del controlador de dominio

Kaspersky Security Center Linux admite el sondeo de los siguientes tipos de controladores de dominio:

- Microsoft Active Directory
- Samba
- FreeIPA
- ALD Pro

Para un controlador de dominio Samba, se utiliza Samba 4 como controlador de dominio de Active Directory.

Cuando sondea un controlador de dominio, el Servidor de administración o un punto de distribución recupera información sobre la estructura del dominio, las cuentas de usuario, los grupos de seguridad y los nombres DNS de los dispositivos incluidos en el dominio.

Recomendamos utilizar el sondeo de controlador de dominio si todos los dispositivos en red son miembros de un dominio. Si algunos de los dispositivos en red no están incluidos en el dominio, estos dispositivos no podrán ser descubiertos mediante el sondeo de controlador de dominio.

Requisitos previos

Antes de sondear un controlador de dominio, asegúrese de que se permitan las conexiones al controlador de dominio a través de un firewall o servidor proxy. También asegúrese de que los siguientes protocolos estén habilitados en el controlador de dominio:

- Protocolo ligero de acceso a directorios (LDAP)
- Capa de seguridad y autenticación simple (SASL)

  Este protocolo se usa si la conexión al controlador de dominio se establece mediante la autenticación SASL. El Servidor de administración y los puntos de distribución solo admiten el mecanismo DIGEST-MD5.
- Protocolo ligero de acceso a directorios a través de la capa de sockets seguros (LDAPS)

  Este protocolo se utiliza si necesita conectarse al controlador de dominio mediante una conexión cifrada.

Asegúrese de que los siguientes puertos estén disponibles en el dispositivo controlador de dominio:

- 389 para el protocolo LDAP y autenticación simple (incluido SASL)
- 636 para el protocolo LDAPS

Para FreeIPA y ALD Pro, los protocolos LDAP y LDAPS se utilizan solo para el sondeo de dominios. Kaspersky Security Center Linux no admite la autenticación de cuentas FreeIPA a través de LDAP(S). Para permitir que los usuarios de FreeIPA y ALD Pro inicien sesión en Web Console, debe configurar la autenticación Kerberos a través del servicio de IAM.

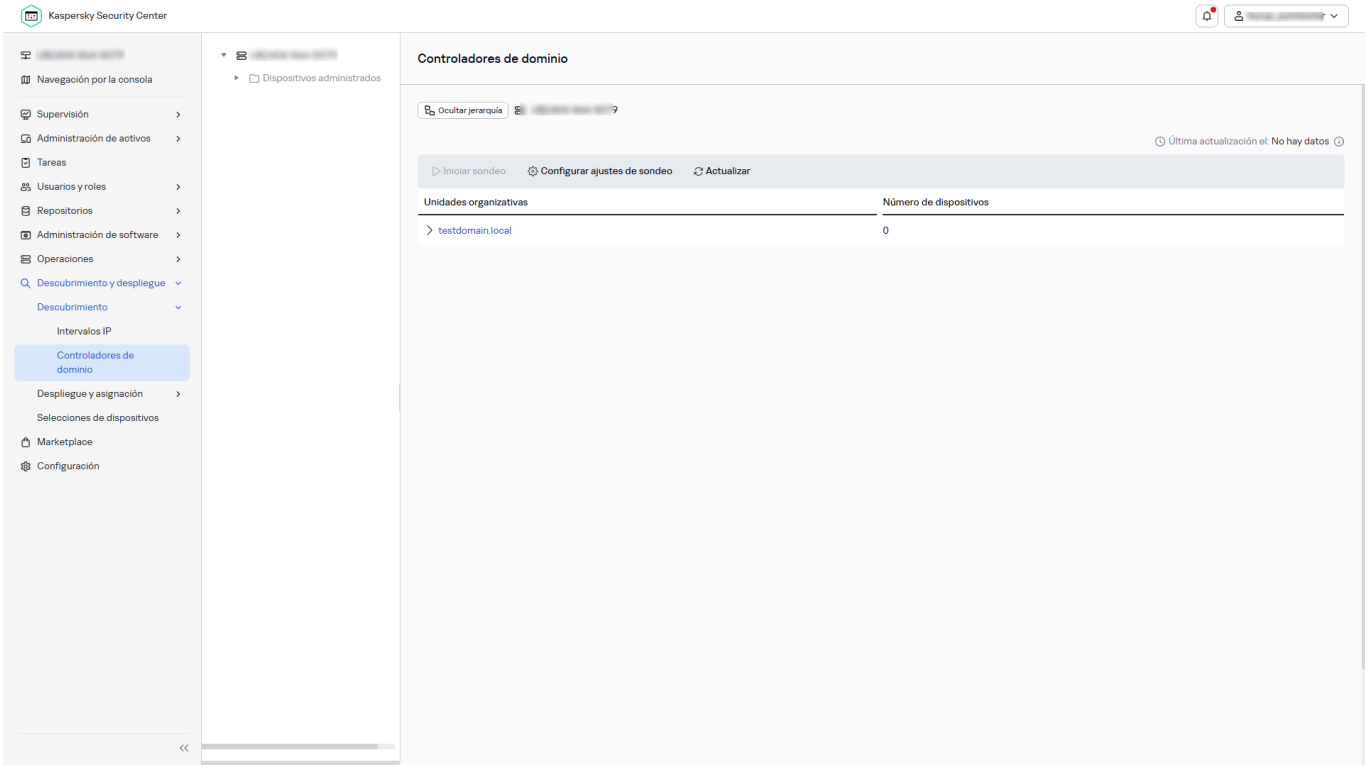
Para todos los hosts basados en Linux dentro de un controlador de dominio de Microsoft Active Directory, Samba, FreeIPA o ALD Pro, debe especificar el `netbios name` y los parámetros del `workgroup` en el archivo `/etc/samba/smb.conf`. Si no lo hace, es posible que los resultados del sondeo contengan hosts duplicados.

Si un dominio de Microsoft Active Directory contiene varios controladores de dominio, no se admite la selección de un controlador específico durante el sondeo de dominios. La conexión se establece con el primer controlador de dominio detectado. Para garantizar una autenticación adecuada con el dominio de Microsoft Active Directory, el campo Nombre alternativo del sujeto (SAN) del certificado debe incluir todas las direcciones de los controladores de dominio incluidos en este dominio, así como el nombre NetBIOS del dominio de Microsoft Active Directory.

Sondeo de controlador de dominio mediante el Servidor de administración

Para sondear un controlador de dominio mediante el Servidor de administración:

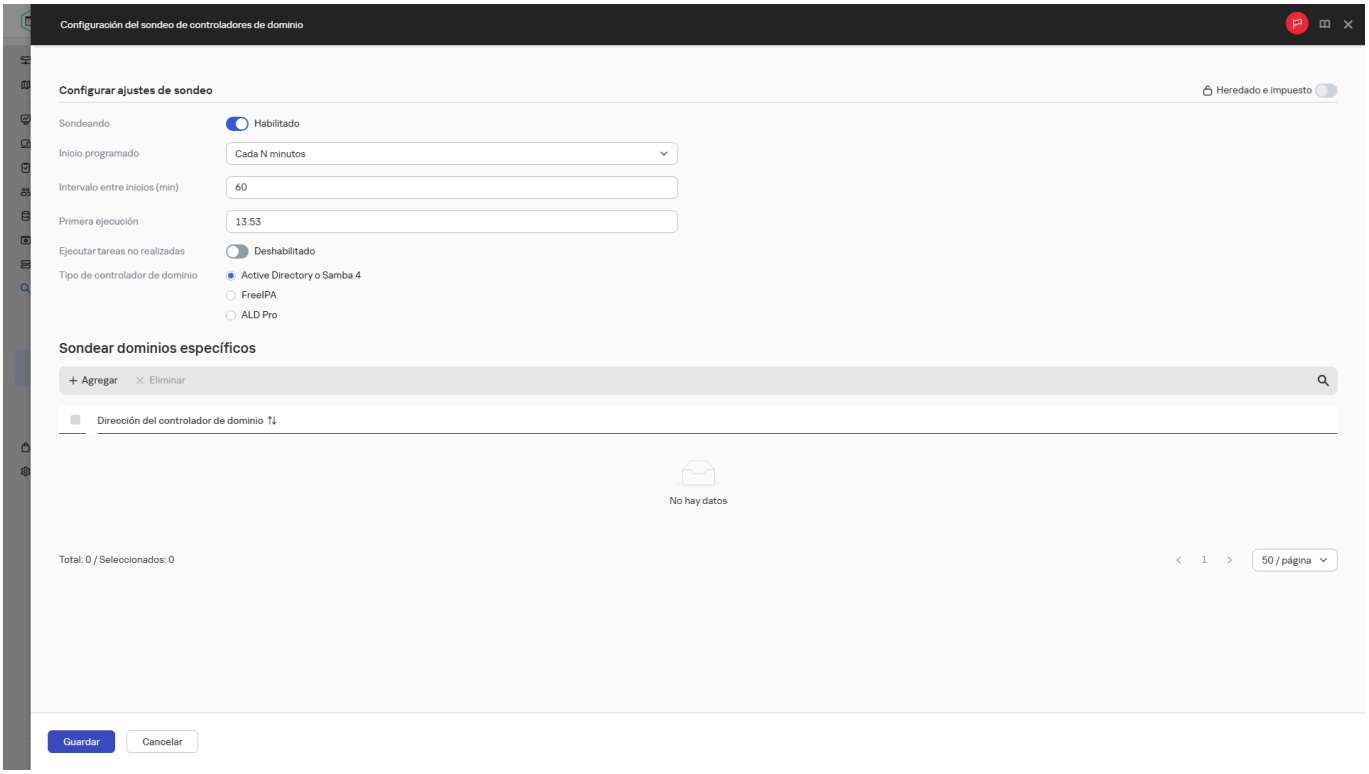
1. En el menú principal, vaya a **Descubrimiento y despliegue → Descubrimiento → Controladores de dominio**.



Ventana del sondeo del controlador de dominio

2. Haga clic en **Configurar ajustes de sondeo**.

   Se abrirá la ventana **Configuración del sondeo de controladores de dominio**.



Configuración del sondeo del controlador de dominio

3. En el campo **Sondeando**, cambie el botón de alternancia a la posición **Habilitado**.

4. En **Sondear dominios específicos**, haga clic en **Agregar** y, luego, especifique la dirección y las credenciales de usuario del controlador de dominio.

5. En la ventana **Configuración del sondeo de controladores de dominio**, haga lo siguiente:

   - Seleccione el tipo de controlador de dominio que se va a sondear: **Active Directory o Samba 4**, **FreeIPA**, **ALD Pro**.

   - Si es necesario, configure el horario de sondeo. La frecuencia de sondeo predeterminada es de una hora. Los datos recibidos en un sondeo reemplazan completamente a los datos del sondeo anterior.

     Las siguientes opciones de horarios de sondeo están disponibles:

     Cada N días

     Se realizará un sondeo en forma periódica, a intervalos regulares, a partir de la fecha y hora indicadas. Cada sondeo estará separado del anterior por el número de días que indique.

     De forma predeterminada, se realizará un sondeo todos los días, a partir de la fecha y hora actuales del sistema.

     Cada N minutos

     Se realizará un sondeo en forma periódica, a intervalos regulares, a partir de la hora indicada. Cada sondeo estará separado del anterior por el número de minutos que indique.

     Por días de la semana

     Se realizará un sondeo en forma periódica, a intervalos regulares, en el día de la semana y a la hora que indique.

     Mensualmente en el día de la semana seleccionado

Se realizará un sondeo en forma periódica, a intervalos regulares, en los días del mes y a la hora que indique.

Ejecutar tareas no realizadas

Si el Servidor de administración está apagado o no está disponible durante la hora programada para el sondeo, el Servidor de administración puede iniciar el sondeo inmediatamente después de encenderlo o esperar la próxima vez que se programe el sondeo.

Si esta opción está habilitada, el Servidor de administración inicia el sondeo inmediatamente después de que se enciende.

Si esta opción está desactivada, el Servidor de administración espera la próxima vez que se programe el sondeo.

Esta opción está deshabilitada de forma predeterminada.

Si cambia las cuentas de usuario en un grupo de seguridad del dominio, estos cambios se mostrarán en Kaspersky Security Center Linux una hora después de sondear el controlador de dominio.

6. Haga clic en **Guardar** para aplicar los cambios.
7. Si desea realizar el sondeo inmediatamente, haga clic en el botón **Iniciar sondeo**.

Sondeo de controlador de dominio mediante el uso de un punto de distribución

También puede sondear un controlador de dominio utilizando un punto de distribución. Un dispositivo administrado basado en Windows o Linux puede actuar como punto de distribución.

Para un punto de distribución de Linux, se admite el sondeo de todos los tipos de controladores de dominio.
Para un punto de distribución de Windows, solo se admite el sondeo de un controlador de dominio de Microsoft Active Directory.
No se admite el sondeo con un punto de distribución de Mac.

Para configurar el sondeo de controlador de dominio mediante el punto de distribución:

1. Abra las propiedades del punto de distribución.
2. Seleccione la sección **Sondeo del controlador de dominio**.
3. En el campo **Sondeando**, cambie el botón de alternancia a la posición **Habilitado**.
4. Si utiliza un punto de distribución Linux, seleccione el tipo de controlador de dominio que se va a sondear: **Active Directory o Samba 4**, **FreeIPA**, **ALD Pro**.

   No es necesario que especifique el mismo tipo de controlador de dominio al configurar el sondeo mediante un punto de distribución y mediante el Servidor de administración.
5. Seleccione el controlador de dominio que desea sondear.

   Si utiliza un punto de distribución de Linux, en la sección **Sondear dominios específicos**, haga clic en **Agregar** y luego especifique la dirección y las credenciales de usuario del controlador de dominio.

Si utiliza un punto de distribución de Windows, puede seleccionar una de las siguientes opciones:

- **Sondear dominio actual**
- **Sondear bosque de dominio entero**
- **Sondear dominios específicos**

6. Haga clic en el botón **Establecer programación de sondeo** para especificar las opciones de la programación de sondeo, si es necesario.

   El sondeo comenzará según el programa especificado únicamente. El inicio manual del sondeo no está disponible.

Una vez completado el sondeo, la estructura del dominio se mostrará en la sección **Controladores de dominio**.

Si configura y habilita reglas de movimiento de dispositivos, los dispositivos recién descubiertos se incluirán de forma automática en el grupo **Dispositivos administrados**. Si no se han habilitado reglas de movimiento, los dispositivos recién descubiertos se incluyen automáticamente en el grupo **Dispositivos no asignados**.

Las cuentas de usuario descubiertas se pueden utilizar para la autenticación de dominio en Kaspersky Security Center Web Console.

Autenticación y conexión a un controlador de dominio

Autenticación y conexión a un controlador de dominio al sondear un dominio

Cuando se sondea un controlador de dominio, el Servidor de administración o el punto de distribución identifican el protocolo de conexión para establecer la conexión inicial con el controlador de dominio. El protocolo se usa de allí en más para todas las futuras conexiones con el controlador de dominio Al establecer la conexión inicial con el controlador de dominio, puede cambiar las opciones de conexión mediante los indicadores del Agente de red (`KLNAG_LDAP_TLS_REQCERT` y `KLNAG_LDAP_SSL_CACERT`). Puede configurar los indicadores del Agente de red con klscflag siguiendo las indicaciones de este artículo.

La conexión inicial a un controlador de dominio se realiza de la siguiente manera:

1. El Servidor de administración o el punto de distribución intenta conectarse al controlador de dominio mediante el protocolo LDAPS.

   De forma predeterminada, la verificación del certificado no es obligatoria. Establezca el indicador `KLNAG_LDAP_TLS_REQCERT` en 1 para verificar el certificado.

   Valores posibles del indicador `KLNAG_LDAP_TLS_REQCERT`:

   - `0`: se solicita el certificado, pero si la otra parte no brinda un certificado o si la verificación del certificado genera un error, se considera que la conexión TLS se estableció correctamente (valor predeterminado).
   - `1`: se requiere una verificación estricta del certificado del servidor LDAP.

De forma predeterminada, si no se especifica el indicador `KLNAG_LDAP_SSL_CACERT`, se usa la ruta de acceso a la entidad de certificación (CA) que brinda el sistema operativo para acceder a la cadena de certificados. Utilice el indicador `KLNAG_LDAP_SSL_CACERT` para especificar una ruta personalizada.

2. Si la conexión LDAPS falla, el Servidor de administración o un punto de distribución intenta conectarse al controlador de dominio a través de una conexión TCP no cifrada mediante SASL (DIGEST-MD5).

Autenticación y conexión a un controlador de dominio al autenticar un usuario de dominio en el Servidor de administración

Cuando un usuario del dominio se autentica en el Servidor de administración, el Servidor de administración identifica el protocolo para establecer la conexión con el controlador de dominio.

Para FreeIPA y ALD Pro, los protocolos LDAP y LDAPS se utilizan solo para el sondeo de dominios. Kaspersky Security Center Linux no admite la autenticación de cuentas FreeIPA a través de LDAP(S). Para permitir que los usuarios de FreeIPA y ALD Pro inicien sesión en Web Console, debe configurar la autenticación Kerberos a través del servicio de IAM.

La conexión a un controlador de dominio se realiza de la siguiente manera:

1. El Servidor de administración intenta conectarse al controlador de dominio a través de LDAPS.

   Se requiere una verificación estricta del certificado del servidor LDAP.

   De forma predeterminada, si no se especifica el indicador `KLNAG_LDAP_SSL_CACERT`, se usa la ruta de acceso a la entidad de certificación (CA) que brinda el sistema operativo para acceder a la cadena de certificados. Utilice el indicador `KLNAG_LDAP_SSL_CACERT` para especificar una ruta personalizada.

2. Si falla la conexión LDAPS, se produce un error al conectarse al controlador de dominio y no se utilizan otros protocolos de conexión.

Configuración de indicadores

Puede usar la utilidad klscflag para configurar los indicadores.

Abra la línea de comandos y pase al directorio que contenga la utilidad klscflag. En el dispositivo del Servidor de administración, la utilidad klscflag se encuentra en el directorio de instalación. La ruta de instalación predeterminada es /opt/kaspersky/ksc64/sbin.

Por ejemplo, el siguiente comando aplica la verificación del certificado:

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_TLS_REQCERT -t d -v 1
```

Configurar un controlador de dominio Samba

Kaspersky Security Center Linux admite un controlador de dominio de Linux que se ejecuta únicamente en Samba 4.

Un controlador de dominio Samba admite las mismas extensiones de esquema que un controlador de dominio Microsoft Active Directory. Puede habilitar la compatibilidad total de un controlador de dominio Samba con un controlador de dominio Microsoft Active Directory utilizando la extensión de esquema Samba 4. Esta acción es opcional.

Recomendamos habilitar la compatibilidad total de un controlador de dominio Samba con un controlador de dominio Microsoft Active Directory. Esto garantizará la interacción correcta entre Kaspersky Security Center Linux y el controlador de dominio Samba.

Para habilitar la compatibilidad total de un controlador de dominio Samba con un controlador de dominio Microsoft Active Directory:

1. Ejecute el siguiente comando para utilizar la extensión de esquema RFC2307:

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. Habilite la actualización del esquema en un controlador de dominio Samba. Para ello, agregue la siguiente línea al archivo `/etc/samba/smb.conf`:

   ```
   dsdb:schema update allowed = true
   ```

   Si la actualización del esquema se completa con un error, deberá realizar una restauración completa del controlador de dominio que actúa como maestro de esquema.

Para todos los hosts basados en Linux dentro de un controlador de dominio Samba, especifique los parámetros `netbios name` y `workgroup` en el archivo `/etc/samba/smb.conf`. Si no lo hace, es posible que los resultados del sondeo contengan hosts duplicados.

Inventario de equipos

La lista de hardware (**Administración de activos** → **Hardware**) que usa para hacer un inventario de los equipos se completa de dos formas: automática y manualmente. Después de cada sondeo de la red, todos los dispositivos que se detectan se agregan a la lista automáticamente; sin embargo, también puede agregar los dispositivos de forma manual si no desea sondear la red. Puede agregar otros dispositivos a la lista de forma manual, como routers, impresoras o hardware del dispositivo.

En las propiedades de un dispositivo puede ver y editar información detallada acerca de ese dispositivo.

La lista de hardware puede incluir los siguientes tipos de dispositivos:

- Equipos
- Dispositivos móviles
- Dispositivos de red
- Dispositivos virtuales
- Componentes OEM
- Periféricos de equipos

- Dispositivos conectados
- Teléfonos de VoIP
- Repositorios de red

El administrador puede asignar el atributo de *Equipo de empresa* a los dispositivos detectados. Este atributo puede asignarse manualmente en las propiedades de un dispositivo o el administrador puede especificar los criterios para que los atributos se asignen automáticamente. En este caso, el atributo de *Equipo de empresa* se asigna por tipo de dispositivo.

Kaspersky Security Center Linux permite cancelar equipos. Para hacer esto, seleccione la opción **Cancelado** en las propiedades del dispositivo. Ese dispositivo no se muestra en la lista de equipos.

Un administrador puede administrar la lista de controladores lógicos programables (PLC) en la carpeta **Hardware**. Encontrará información detallada para administrar la lista de PLC en la *Guía para usuarios de Kaspersky Industrial Cyber Security for Nodes*.

Agregar información sobre los dispositivos nuevos

Para agregar información acerca de nuevos dispositivos en la red:

1. En el menú principal, vaya a **Administración de activos** → **Hardware**.
2. Haga clic en el botón **Agregar** para abrir la ventana **Nuevo dispositivo**.
3. En la ventana **Nuevo dispositivo**, en la lista desplegable **Tipo de dispositivo**, seleccione un tipo de dispositivo que desee agregar.
4. Haga clic en **Aceptar**.

   La ventana de Propiedades del dispositivo se abre en la sección **General**.
5. En la sección **General** complete los campos de entrada con datos del dispositivo. La sección **General** detalla la siguiente configuración:

   - **Dispositivo de la empresa**. Seleccione esta casilla si desea asignarle el atributo *Empresa* al dispositivo. Mediante este atributo, puede buscar dispositivos en la carpeta **Hardware**.
   - **Cancelado**. Seleccione esta casilla si no desea que el dispositivo figure en la lista de dispositivos de la carpeta **Hardware**.
6. Haga clic en **Aplicar**.

El nuevo dispositivo se mostrará en el espacio de trabajo de la página **Hardware**.

Configurar criterios usados para los dispositivos de empresa

Para configurar los criterios de detección para los dispositivos de empresa:

1. En el menú principal, vaya a **Administración de activos** → **Hardware**.
2. En la parte superior de la página **Hardware**, haga clic en el vínculo **Configurar regla para dispositivos de empresa**.

   Se invoca el panel **Configurar regla para dispositivos de empresa**.
3. En el panel **Configurar regla para dispositivos de empresa**, habilite la opción **Establecer el atributo del dispositivo de la empresa de forma automática**. Especifique los tipos de dispositivos a los que se les asigna automáticamente el atributo *Empresa*.

   > Esta opción afecta solo a los dispositivos agregados a través del sondeo de red. Para los dispositivos agregados manualmente, configure el atributo *Empresa* manualmente.
4. Haga clic en **Aceptar**.

Se configuran los criterios de detección para dispositivos empresariales.

Usar el modo dinámico para la Infraestructura de escritorio virtual (VDI) en los dispositivos cliente

Es posible utilizar máquinas virtuales temporales para implementar una infraestructura virtual en una red corporativa. Kaspersky Security Center Linux detecta las máquinas virtuales temporales y agrega información acerca de ellas a la base de datos del Servidor de administración. Después de que un usuario termina de usar una máquina virtual temporal, esta máquina se elimina de la infraestructura virtual. Sin embargo, se puede guardar un registro sobre la máquina virtual eliminada en la base de datos del Servidor de administración. Además, las máquinas virtuales inexistentes pueden aparecer en Kaspersky Security Center Web Console.

Para evitar que se guarde información sobre máquinas virtuales inexistentes, Kaspersky Security Center Linux admite el modo dinámico para la Infraestructura de Escritorio Virtual (VDI). El administrador puede habilitar la compatibilidad con el modo dinámico para VDI en las propiedades del paquete de instalación del Agente de red que se instalará en la máquina virtual temporal.

Cuando se deshabilita una máquina virtual temporal, el Agente de red notifica al Servidor de administración que la máquina se ha deshabilitado. Si la máquina virtual se ha deshabilitado correctamente, se la elimina de la lista de dispositivos conectados al Servidor de administración. Si la máquina virtual se deshabilita con errores y el Agente de red no envía una notificación sobre la máquina virtual deshabilitada al Servidor de administración, se usa un escenario de copia de seguridad. En este escenario, una máquina virtual se elimina de la lista de dispositivos conectados al Servidor de administración después de tres intentos fallidos de sincronización con el Servidor de administración.

Habilitación del modo dinámico de la Infraestructura de escritorio virtual (VDI) en las propiedades de un paquete de instalación para el Agente de red

Para habilitar el modo dinámico de la Infraestructura de escritorio virtual (VDI):

1. En el menú principal, vaya a **Administración de software** → **Paquetes de instalación**.
2. En el menú contextual del paquete de instalación del Agente de red, seleccione **Propiedades**.
   Se abrirá la ventana de **Propiedades**.
3. En la ventana **Propiedades**, seleccione la sección **Avanzado**.
4. En la sección **Avanzado**, seleccione la opción **Habilitar modo dinámico para VDI**.

El dispositivo en el que se instalará el Agente de red forma parte de VDI.

Mover los dispositivos que forman parte de la VDI a un grupo de administración

Para mover los dispositivos que formen parte de la VDI a un grupo de administración, realice lo siguiente:

1. Vaya a **Administración de activos** → **Reglas de movimiento**.
2. Haga clic en **Agregar**.
3. En la pestaña **Condiciones de la regla**, seleccione la pestaña **Máquinas virtuales**.
4. Establezca la regla **Esta es una máquina virtual** en **Sí** y **Parte de la infraestructura de escritorio virtual** en **Sí.**
5. Haga clic en **Guardar**.

Administración de dispositivos cliente

Kaspersky Security Center Linux le permite administrar dispositivos cliente:

- Vea la configuración y los estados de los dispositivos administrados, incluidos los clústeres y las matrices de servidores.
- Configure sus puntos de distribución.
- Administre las tareas.

Puede usar grupos de administración para combinar dispositivos cliente en un conjunto que se puede administrar como una sola unidad. Un dispositivo cliente puede incluirse en un solo grupo de administración. Los dispositivos se pueden asignar a un grupo automáticamente según las **Condiciones de la regla**:

- Crear reglas de movimiento de dispositivos.
- Copiar reglas de movimiento de dispositivos.
- Condiciones para una regla de movimiento de dispositivos.

Puede usar selecciones de dispositivos para filtrar dispositivos según una condición. También puede etiquetar dispositivos para crear selecciones, para buscar dispositivos y para distribuir dispositivos entre grupos de administración.

Configuración de un dispositivo administrado

Para ver la configuración de un dispositivo administrado:

1. En el menú principal, vaya a **Administración de activos** → **Dispositivos administrados**.

   Se muestra la lista de dispositivos administrados.

2. En la lista de dispositivos administrados, haga clic en el vínculo con el nombre del dispositivo de su interés.

Se muestra la ventana de propiedades del dispositivo seleccionado.

Las siguientes pestañas se muestran en la parte superior de la ventana de propiedades y representan los principales grupos de ajustes:

General

Esta pestaña incluye las siguientes secciones:

- La sección **General** muestra información general sobre el dispositivo cliente. La información se basa en los datos recibidos durante la última sincronización del dispositivo cliente con el Servidor de administración.
  - **Nombre**

    En este campo, puede ver y modificar el nombre asignado al dispositivo cliente en el grupo de administración.

- **Descripción**

  En este campo, puede ingresar una descripción adicional para el dispositivo cliente.

- **Estado del dispositivo**

  Estado del dispositivo cliente, asignado sobre la base de los criterios definidos por el administrador para el estado de protección antivirus del dispositivo y la actividad del dispositivo en la red.

- **Nombre completo del grupo**

  Grupo de administración en el que está incluido el dispositivo cliente.

- **Última actualización de las bases de datos antivirus**

  Fecha en que las bases de datos o las aplicaciones del antivirus se actualizaron por última vez en el dispositivo.

- **Conectado al Servidor de administración**

  Fecha y hora en que el Agente de red instalado en el dispositivo cliente se conectó al Servidor de administración por última vez.

- **Visible por última vez**

  Fecha y hora en que el dispositivo se vio en la red por última vez.

- **Versión del Agente de red**

  Versión del Agente de red instalado.

- **Creado**

  Fecha de creación del dispositivo en Kaspersky Security Center Linux.

- **Propietario del dispositivo**

  Nombre del propietario del dispositivo. Puede asignar o quitar un usuario como propietario del dispositivo haciendo clic en el vínculo **Administrar propietario del dispositivo**.

- **No desconectar del Servidor de administración**

  Si esta opción está habilitada, se mantendrá una conexión continua entre el dispositivo administrado y el Servidor de administración. Podría habilitar esta opción si no utiliza servidores push, que brindan este tipo de conectividad.

  Si no habilita esta opción y no utiliza servidores push, el dispositivo administrado se conectará al Servidor de administración únicamente para sincronizar o transmitir información.

  El número total máximo de dispositivos con la opción **No desconectar del Servidor de administración** seleccionada es 300.

  Esta opción está deshabilitada de manera predeterminada en los dispositivos administrados. Esta opción está habilitada de manera predeterminada en el dispositivo en el que se ha instalado el Servidor de administración y no se puede deshabilitar en ese caso.

- La sección de **Red** muestra la siguiente información sobre las propiedades de red del dispositivo cliente:

  - **Dirección IP**

    Dirección IP del dispositivo.

- **Dominio de Windows**

  Grupo de trabajo que contiene el dispositivo.

- **Nombre DNS**

  El nombre de dominio DNS del dispositivo cliente.

- **Nombre NETBIOS**

  Nombre del dispositivo cliente.

- **Dirección IPv6**

- La sección **Sistema** proporciona información sobre el sistema operativo instalado en el dispositivo cliente:

  - **SO**

  - **Arquitectura de la CPU**

  - **Nombre del dispositivo**

  - **Tipo de máquina virtual**

    Fabricante de la máquina virtual.

  - **Máquina virtual dinámica como parte de VDI**

    Esta fila muestra si el dispositivo cliente es una máquina virtual dinámica como parte de VDI.

- La sección **Protección** proporciona información sobre el estado actual de la protección antivirus del dispositivo cliente:

  - **Visible**

    Estado de visibilidad del dispositivo cliente.

  - **Estado del dispositivo**

    Estado del dispositivo cliente, asignado sobre la base de los criterios definidos por el administrador para el estado de protección antivirus del dispositivo y la actividad del dispositivo en la red.

  - **Descripción del estado**

    Estado de la protección del dispositivo cliente y de la conexión con el Servidor de administración.

  - **Estado de protección**

    Este campo muestra el estado de la protección en tiempo real del dispositivo cliente.

    Si el estado se modifica en el dispositivo, el cambio no se verá reflejado en la ventana de propiedades del dispositivo sino hasta que el dispositivo se sincronice con el Servidor de administración.

  - **Último análisis completo**

    Fecha y hora del último análisis antimalware realizado en el dispositivo cliente.

  - **Virus detectados**

Cantidad total de amenazas detectadas en el dispositivo cliente desde la instalación de la aplicación de seguridad (primer análisis) o desde la última vez que el contador de amenazas se puso en cero.

- **Objetos que no se pudieron desinfectar**

  Número de archivos no procesados en el dispositivo cliente.

  Este campo no refleja el número de archivos no procesados en dispositivos móviles.

- **Estado de cifrado del disco**

  Estado del cifrado de archivos en las unidades locales del dispositivo. Para obtener una descripción de los estados, consulte la Ayuda de Kaspersky Endpoint Security para Windows.

  Solo es posible cifrar archivos en los dispositivos administrados en los que está instalado Kaspersky Endpoint Security para Windows.

- La sección **Estado del dispositivo definido por la aplicación** proporciona información sobre el estado del dispositivo definido por la aplicación administrada instalada en el dispositivo. El estado de este dispositivo puede diferir del definido por Kaspersky Security Center Linux.

Aplicaciones

Esta pestaña enumera todas las aplicaciones de Kaspersky instaladas en el dispositivo cliente. Esta pestaña contiene los botones **Iniciar** y **Detener**, que inician y detienen la aplicación de Kaspersky seleccionada (excepto el Agente de red). Puede usar estos botones si el puerto 15000 UDP está disponible en el dispositivo administrado para recibir notificaciones push del Servidor de administración. Si el dispositivo administrado no está disponible para notificaciones push, pero el modo de conexión continua al Servidor de administración está activado (la opción **No desconectar del Servidor de administración** en la sección **General** está activada), los botones **Iniciar** y **Detener** también están disponibles. De lo contrario, cuando intenta iniciar o detener la aplicación, se muestra un mensaje de error. También puede hacer clic en el nombre de una aplicación para ver información general sobre la aplicación, los ajustes de configuración de la misma y una lista de los eventos ocurridos en el dispositivo.

Directivas y perfiles de directivas activos

Esta pestaña enumera las directivas y los perfiles de directivas que están asignados al dispositivo administrado en un momento dado.

Tareas

La pestaña **Tareas** permite administrar las tareas del dispositivo cliente. Utilice esta sección para crear tareas nuevas, ver la lista de tareas existentes, ver los resultados de ejecución de las tareas e iniciar, detener, eliminar y reconfigurar las tareas existentes. La lista de tareas mostrada se basa en los datos recibidos durante la última sesión de sincronización entre el cliente y el Servidor de administración. El Servidor de administración solicita detalles sobre el estado de las tareas al dispositivo cliente. Si el puerto 15000 UDP está disponible en el dispositivo administrado para recibir notificaciones push del Servidor de administración, se muestra el estado de la tarea y se activan los botones para administrar la tarea. Si servidor push no puede comunicarse con el dispositivo administrado, pero el modo de conexión continua al Servidor de administración está habilitado (la opción **No desconectar del Servidor de administración** en la sección **General** está habilitada), las acciones con tareas también están disponibles.

Si no se establece una conexión, no se muestra el estado y los botones quedan desactivados.

Eventos

La pestaña **Eventos** muestra los eventos registrados en el Servidor de administración para el dispositivo cliente seleccionado.

Puede exportar, copiar y eliminar los eventos del dispositivo.

Problemas de seguridad

En la pestaña **Problemas de seguridad**, puede ver, crear y editar problemas de seguridad para el dispositivo cliente. Los problemas de seguridad se pueden crear manualmente por el administrador o automáticamente por las aplicaciones de Kaspersky administradas que se han instalado en el dispositivo cliente. El administrador podría crear un problema de seguridad si, por ejemplo, algunos de sus usuarios han copiado malware de una unidad extraíble en más de una ocasión. En el texto del problema de seguridad, el administrador podría brindar una breve descripción del caso, delinear las acciones que recomienda tomar (por ejemplo, medidas disciplinarias contra los usuarios) y agregar un vínculo al usuario o a los usuarios.

Se denomina *procesado* al problema de seguridad para el cual se han tomado todas las medidas necesarias. La presencia de problemas de seguridad no procesados puede usarse como condición para cambiar el estado de un dispositivo a *Crítico* o *Advertencia*.

En esta sección, encontrará una lista con problemas de seguridad que se hayan creado para el dispositivo. Los problemas de seguridad se clasifican por tipo y por nivel de gravedad. El tipo de problema de seguridad lo define la aplicación de Kaspersky que crea el problema de seguridad. Si desea resaltar los problemas de seguridad procesados de la lista, marque la casilla de la columna **Procesado**.

Etiquetas

La pestaña **Etiquetas** permite administrar la lista de palabras clave que se utilizan para buscar dispositivos cliente. Aquí puede ver la lista de etiquetas existentes, asignar etiquetas incluidas en la lista, configurar reglas de etiquetado automático, agregar etiquetas nuevas, eliminar etiquetas antiguas y modificar el nombre de las etiquetas existentes.

Avanzado

Esta pestaña incluye las siguientes secciones:

- **Registro de aplicaciones**. En esta sección, puede ver un registro de las aplicaciones instaladas en el dispositivo cliente y de las actualizaciones de esas aplicaciones; también puede configurar el modo de visualización del registro de aplicaciones.

  Podrá ver información sobre las aplicaciones instaladas si el Agente de red instalado en el dispositivo cliente le envía la información necesaria al Servidor de administración. Puede configurar el envío de información al Servidor de administración en la ventana de propiedades del Agente de red o en su directiva, en la sección **Repositorios**.

  Al hacer clic en el nombre de una aplicación, se abre una ventana que contiene los detalles de la aplicación y una lista de los paquetes de actualización instalados para la aplicación.

- **Archivos ejecutables**. Esta sección muestra los archivos ejecutables almacenados en el dispositivo cliente.

- **Puntos de distribución**. Esta sección contiene una lista de los puntos de distribución con los que interactúa el dispositivo.

  - **Exportar a archivo**

    Haga clic en el botón **Exportar a archivo** para guardar en un archivo la lista de puntos de distribución con los que interactúa el dispositivo. De manera predeterminada, la aplicación exporta la lista de dispositivos a un archivo CSV.

  - **Propiedades**

    Haga clic en el botón **Propiedades** para ver y configurar el punto de distribución con el que interactúa el dispositivo.

- **Registro de hardware**. En esta sección, puede ver información sobre el hardware instalado en el dispositivo cliente.

Si el Agente de red está instalado en un dispositivo con Windows, envía al Servidor de administración la siguiente información sobre el hardware del dispositivo:

- RAM
- Dispositivos de almacenamiento
- Placa madre
- CPU
- Adaptadores de red
- Monitores
- Adaptador de video
- Tarjeta de sonido

Si el Agente de red está instalado en un dispositivo con Linux o macOS, envía al Servidor de administración la siguiente información sobre el hardware del dispositivo, si el sistema operativo la proporciona:

- Volumen total de la RAM
- Volumen total de los dispositivos de almacenamiento masivo
- Placa madre
- CPU
- Adaptadores de red

- **Actualizaciones disponibles**. Esta sección muestra las actualizaciones de software que se han encontrado en el dispositivo, pero que aún no se han instalado.

- **Vulnerabilidades de software**. Esta sección muestra información sobre las vulnerabilidades de las aplicaciones de terceros instaladas en los dispositivos cliente.

  Para guardar las vulnerabilidades en un archivo, marque las casillas ubicadas junto a las vulnerabilidades que desea guardar, y luego haga clic en el botón **Exportar a CSV** o en el botón **Exportar a TXT**.

  La sección contiene los siguientes ajustes:

  - **Mostrar solo las vulnerabilidades que pueden repararse**

    Si habilita esta opción, la sección mostrará las vulnerabilidades que se puedan reparar con un parche.

    Si deshabilita esta opción, la sección mostrará tanto las vulnerabilidades que se puedan reparar con un parche como las vulnerabilidades para las que no exista parche publicado.

    Esta opción está activada de forma predeterminada.

  - **Prop. de la vulnerabilidad**

Haga clic en el nombre de una vulnerabilidad de software de la lista para ver las propiedades de la vulnerabilidad de software seleccionada en una ventana aparte. En la ventana, puede hacer lo siguiente:

- Ignorar la vulnerabilidad de software en el dispositivo administrado (en Kaspersky Security Center Web Console).
- Ver la lista de reparaciones recomendadas para la vulnerabilidad.
- Especificar manualmente las actualizaciones de software que se usarán para reparar la vulnerabilidad (en Kaspersky Security Center Web Console).
- Ver las instancias de la vulnerabilidad.
- Ver la lista de tareas existentes que permiten reparar la vulnerabilidad y crear tareas de reparación nuevas.

- **Diagnóstico remoto**. En esta sección, puede realizar un diagnóstico remoto de dispositivos cliente.

Si usa un DBMS PostgreSQL, MariaDB o MySQL, la pestaña **Eventos** puede mostrar una lista incompleta de eventos para el dispositivo cliente seleccionado. Esto ocurre cuando el DBMS almacena una gran cantidad de eventos. Realice una de las siguientes acciones si desea aumentar la cantidad de eventos mostrados:

- Eliminación de eventos innecesarios.
- Reducción del plazo de almacenamiento para eventos innecesarios.

Para ver una lista completa de eventos registrados en el Servidor de administración para el dispositivo, use Informes.

Comprobación de la conexión entre un dispositivo administrado y el Servidor de administración (utilidad klnagchk)

Puede comprobar la conexión y obtener información detallada sobre la configuración de la conexión entre un dispositivo cliente y el Servidor de administración mediante la utilidad klnagchk. La utilidad klnagchk se encuentra en la carpeta de instalación del Agente de red.

Al iniciarse desde la línea de comandos, la utilidad klnagchk puede realizar las siguientes acciones (dependiendo de las claves en uso):

- Se muestra en la pantalla o registra los valores de la configuración usada para conectar el Agente de red instalado en el dispositivo con el Servidor de administración.
- Registra en un archivo de registro del evento las estadísticas del Agente de red (desde el último inicio) y los resultados de la operación de la utilidad, o bien muestra la información en pantalla.
- Intenta establecer conexión entre el Agente de red y el Servidor de administración.

  Si falla el intento de conexión, la utilidad envía un paquete ICMP para comprobar el estado del dispositivo donde está instalado el Servidor de administración.

Para comprobar la conexión entre un dispositivo cliente y el Servidor de administración mediante la utilidad klnagchk:

En el dispositivo con el Agente de red instalado, inicie la utilidad klnagchk desde la línea de comandos con una cuenta de administrador local.

Sintaxis de línea de comandos de la utilidad:

```
klnagchk [-logfile <nombre del archivo>] [-sp] [-savecert <ruta al archivo del certificado>] [-restart][-sendhb]
```

Descripciones de las claves:

- `-logfile <nombre del archivo>`: registra en un archivo de registro los valores de la configuración de conexión entre el Agente de red y el Servidor de administración y los resultados de la operación de la utilidad.

  De manera predeterminada, la información se guarda en el flujo saliente estándar (stdout). Si la clave no está en uso, la configuración, los resultados y mensajes de error se muestran en pantalla.

- `-sp`: muestra la contraseña para la autenticación del usuario en el servidor proxy.

  La clave está en uso si la conexión al Servidor de administración se establece a través de un servidor proxy.

- `-savecert <nombre del archivo>`: guarda el certificado utilizado para acceder al Servidor de administración, en un archivo especificado.

- `-restart`: inicia el Agente de red una vez completada la utilidad.

- `-sendhb`: inicia la sincronización del Agente de red con el Servidor de administración.

Después del inicio, la utilidad klnagchk accede a los archivos de configuración del Agente de red y muestra los parámetros de conexión. Estos parámetros se especifican durante la instalación del Agente de red y en la configuración de la directiva del Agente de red:

- `Current device`: nombre de red de Windows del dispositivo cliente.

- `Network Agent version`: número completo de la versión del Agente de red (con parches) instalada en el dispositivo.

- `Server address`: dirección del Servidor de administración.

- `Use SSL`: parámetro que indica si se utiliza una conexión segura al conectarse al Servidor de administración.

  Valores posibles:

  - 0: no se utiliza una conexión segura.

  - 1: se utiliza una conexión segura.

- `Compress traffic`: parámetro que indica si el tráfico entre el dispositivo cliente y el Servidor de administración está comprimido.

- `Server SSL ports`: números de puertos válidos para la comunicación con el Servidor de administración cuando se utiliza una conexión segura.

- `Server ports`: números de puertos válidos para la comunicación con el Servidor de administración cuando se utiliza una conexión normal.

- `Use proxy server`: parámetro que indica si se utiliza un servidor proxy.

  Valores posibles:

  - 0: no se utiliza un servidor proxy.
  - 1: se utiliza un servidor proxy.

- `Address`: dirección y puerto del servidor proxy, separados por dos puntos. Este parámetro se muestra solo si se utiliza un servidor proxy.
- `User name`: nombre de usuario para acceder al servidor proxy. Este parámetro se muestra solo si se utiliza un servidor proxy.
- `Password`: contraseña para acceder al servidor proxy. Este parámetro se muestra solo si se utiliza un servidor proxy. Para mostrar la contraseña del servidor proxy, debe usar la clave `sp` en el comando.
- `Certificate`: parámetro que indica si el dispositivo cliente tiene un certificado del Servidor de administración. Es posible que no exista un certificado, por ejemplo, si el Agente de red nunca se conectó correctamente al Servidor de administración.

  Valores posibles:

  - `not installed`: el dispositivo cliente no tiene un certificado de servidor de administración.
  - `present`: el dispositivo cliente tiene un certificado del Servidor de administración.

- `Open UDP port`: parámetro que indica si el Agente de red usa el puerto UDP para recibir solicitudes de sincronización del Servidor de administración.

  Valores posibles:

  - 0: el puerto UDP está cerrado para recibir solicitudes de sincronización del Servidor de administración.
  - 1: el puerto UDP está abierto para recibir solicitudes de sincronización del Servidor de administración.

- `UDP ports`: números de puerto UDP que puede usar el Agente de red.
- `Location name`: ubicación de red del dispositivo.
- `State of network location`: parámetro que indica si el dispositivo cliente se puede cambiar de un perfil de conexión del Servidor de administración a otro.

  Valores posibles:

  - `Enabled`: el perfil de conexión del servidor de administración se puede cambiar para el dispositivo cliente.
  - `Disabled`: el perfil de conexión del Servidor de administración no se puede cambiar para el dispositivo cliente.

- `Profile to use`: perfil de conexión para el Servidor de administración.
- `Condition`: dirección IP y máscara de subred de la red a la que está conectado el dispositivo cliente.
- `Ping period, minutes`: intervalo estándar entre sincronizaciones.
- `Conn timeout, s`: tiempo de espera de conexión.

- `RW timeout, s`: tiempo de espera de conexión de las operaciones de lectura y escritura.
- `Host ID`: ID del dispositivo en la red. El `Device ID` es único entre los dispositivos cliente administrados por el mismo Servidor de administración.
- `Locations of connection gateways`: parámetros para conectar el dispositivo cliente al Servidor de administración a través de la puerta de enlace de conexión.
- `Location of distribution points`: parámetros para conectar el dispositivo cliente al Servidor de administración a través del punto de distribución.
- `Connection with server`: parámetro que indica si la puerta de enlace de conexión tiene una conexión continua al Servidor de administración. El parámetro solo se muestra si el dispositivo cliente actúa como puerta de enlace de conexión.

  Valores posibles:

  - `active`: la pasarela de conexión tiene una conexión continua al Servidor de administración.
  - `inactive`: la pasarela de conexión no tiene una conexión continua al Servidor de administración.
- `Connection with server through connection gateway`: parámetro que indica si la conexión al Servidor de Administración a través de una pasarela de conexión se establece correctamente. El parámetro solo se muestra si el dispositivo cliente actúa como puerta de enlace de conexión.

  Valores posibles:

  - `active`: la conexión al Servidor de administración a través de una pasarela de conexión se estableció correctamente.
  - `inactive`: la conexión al Servidor de administración a través de una pasarela de conexión se estableció incorrectamente.

Además, el resultado de la utilidad klnagchk puede contener una de las siguientes líneas:

- `Administration Server is installed on this device`: la utilidad klnagchk se ejecuta en el dispositivo del Servidor de administración.
- `This device has been assigned a connection gateway but is not yet registered on Administration Server`: la utilidad klnagchk se ejecuta en el dispositivo en el que está instalado el Agente de red, en el modo de pasarela de conexión. La puerta de enlace de conexión configurada está esperando una conexión del Servidor de administración, pero el Servidor de administración no enumera el dispositivo entre los dispositivos administrados. Debe asegurarse de que el Servidor de administración inicia una conexión a la puerta de enlace de conexión.
- `This device is a connection gateway`: la utilidad klnagchk se ejecuta en el dispositivo que actúa como pasarela de conexión.
- `Acts as a distribution point`: la utilidad klnagchk se ejecuta en el dispositivo que actúa como punto de distribución.

La utilidad klnagchk comprueba el estado del servicio del Agente de red. Si el servicio no se está ejecutando, la utilidad se detiene. Si el servicio se está ejecutando, la utilidad muestra las siguientes estadísticas de conexión:

- `Ping count`: número de intentos de conectar el dispositivo cliente al Servidor de administración.
- `Succ. pings`: número de intentos exitosos de conectar el dispositivo cliente al Servidor de administración.
- `Sync count`: número de intentos de sincronizar la configuración del dispositivo cliente con la configuración del Servidor de administración.
- `Succ. syncs`: número de intentos exitosos de sincronizar la configuración del dispositivo cliente con el Servidor de administración.
- `Last ping`: fecha y hora de la última conexión.

Debe usar los parámetros `Ping count` y `Succ. pings` al analizar la conexión entre el Servidor de administración y el Agente de red. La configuración del dispositivo cliente se sincroniza con la configuración del Servidor de administración solo si se modificó la configuración del Servidor de administración (por ejemplo, si se agregaron nuevas tareas o se modificó la configuración de la directiva). De lo contrario, los valores de los parámetros `Ping count` y `Succ. pings` permanecen sin cambios.

Para obtener más información sobre cómo solucionar problemas relacionados con la conexión del Agente de red al Servidor de administración, consulte las Preguntas frecuentes de Kaspersky Security Center Linux.

Reglas de movimiento de dispositivos

Recomendamos que automatice la asignación de dispositivos a grupos de administración a través de las *reglas de movimiento de dispositivos*. Una regla de movimiento de dispositivos consta de tres partes principales: nombre, condición de ejecución (expresión lógica con atributos del dispositivo) y grupo de administración de destino. Una regla mueve un dispositivo al grupo de administración de destino si los atributos del dispositivo cumplen la condición de ejecución de la regla.

Toda regla de movimiento de dispositivos tiene una prioridad. El Servidor de administración comprueba los atributos del dispositivo en cuanto a si cumplen con la condición de ejecución de cada regla, en orden ascendente de prioridad. Si los atributos del dispositivo cumplen con la condición de ejecución de una regla, el dispositivo se mueve al grupo de destino, y con esto cesa el procesamiento de la regla en este dispositivo. Si los atributos de dispositivo cumplen con las condiciones de varias reglas, el dispositivo se mueve al grupo de destino de la regla con la prioridad más alta (es decir, la que tiene la clasificación más alta en la lista de reglas).

Las reglas de movimiento de dispositivos se pueden crear implícitamente. Por ejemplo, en las propiedades de un paquete de instalación o una tarea de instalación remota, puede especificar el grupo de administración al cual el dispositivo se debe mover después de que Agente de red se instala en este. Además, las reglas de movimiento de dispositivos pueden ser creadas explícitamente por el administrador de Kaspersky Security Center Linux, en la sección **Administración de activos → Reglas de movimiento**.

La regla de movimiento predeterminada está diseñada para la asignación inicial de dispositivos a grupos de administración, que se ejecuta una sola vez. La regla mueve dispositivos desde el grupo de Dispositivos no asignados solo una vez. Si un dispositivo se movió una vez mediante esta regla, la regla no lo volverá a mover, incluso si devuelve el dispositivo al grupo de dispositivos no asignados manualmente. Este es el modo recomendado de aplicar las reglas de movimiento.

Puede mover dispositivos que ya se han asignado a algunos grupos de administración. Para hacer esto, en las propiedades de una regla, borre la casilla de verificación **Solo mover dispositivos que no pertenezcan a un grupo de administración**.

Aplicar reglas de movimiento a dispositivos que ya se han asignado a algunos grupos de administración aumenta considerablemente la carga en el Servidor de administración.

La casilla **Solo mover dispositivos que no pertenezcan a un grupo de administración** está bloqueada en las propiedades de las reglas de movimiento creadas automáticamente. Esas reglas se crean cuando agrega la tarea *Instalar la aplicación de forma remota* o crea un paquete de instalación independiente.

Puede crear una regla móvil que afectaría a un dispositivo solo repetidamente.

Recomendamos encarecidamente no mueva un solo dispositivo desde un grupo al otro repetidamente (por ejemplo, a fin de aplicar una directiva especial a ese dispositivo, ejecutar una tarea de grupo especial o actualizar el dispositivo a través de un punto de distribución específico).

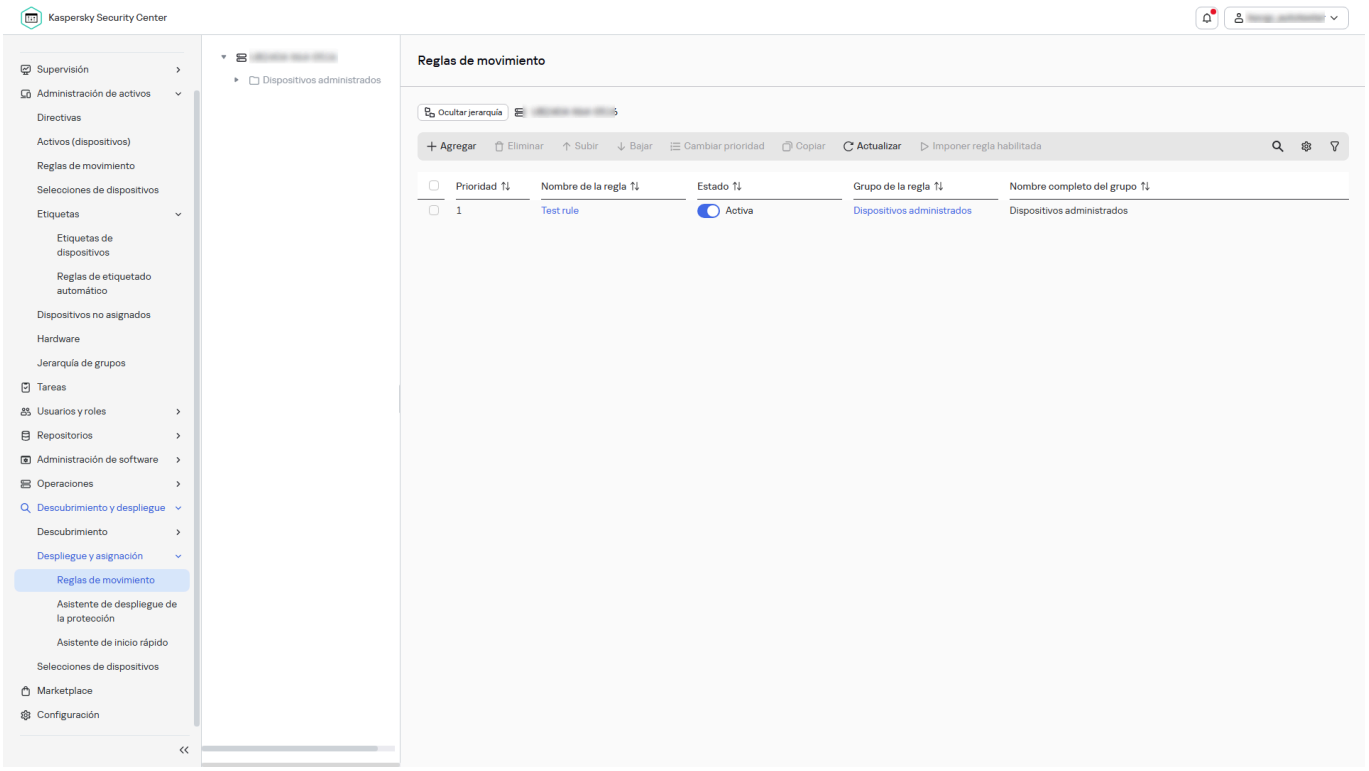
Tales situaciones no se admiten, porque aumentan la carga en el Servidor de administración y el tráfico de red a un grado extremo. Estas situaciones también entran en conflicto con los principios operativos de Kaspersky Security Center Linux (en particular en el área de derechos de acceso, eventos e informes). Se debe encontrar otra solución; por ejemplo, a través del uso de perfiles de directivas, tareas para selecciones de dispositivos, asignación de Agentes de red según el escenario estándar, entre otras cosas.

Crear reglas de movimiento de dispositivos

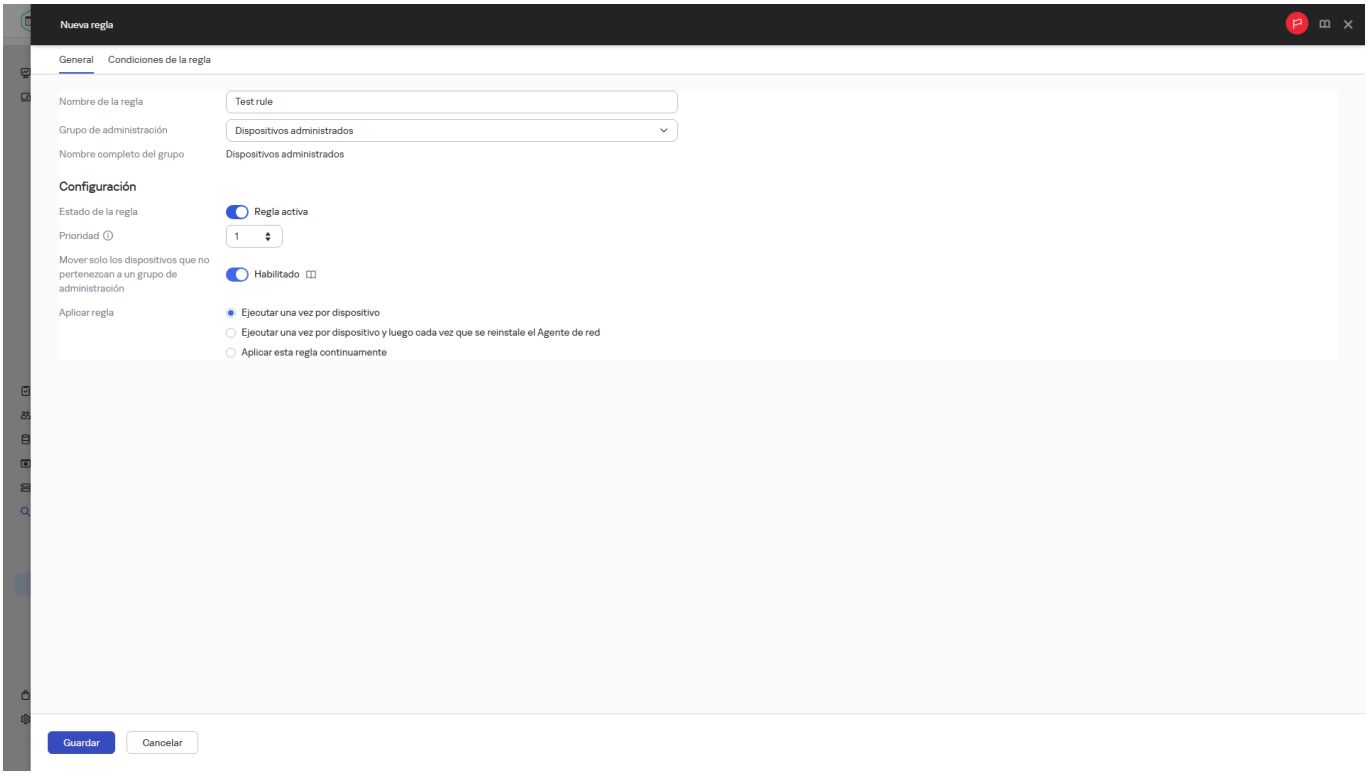
Puede configurar reglas de movimiento de dispositivos; es decir, reglas que asignan automáticamente dispositivos a grupos de administración.

Para crear una regla de movimiento:

1. En el menú principal, vaya a **Administración de activos → Reglas de movimiento**.



2. Haga clic en **Agregar**. Se abre la ventana **Nueva regla**.



3. En la ventana que se abre, especifique la siguiente información en la pestaña **General**:

Nombre de la regla

Ingrese un nombre para la nueva regla.

Cuando se copia una regla, la regla nueva recibe el nombre de la regla de origen, con el agregado de un índice numérico entre paréntesis, como (1).

Grupo de administración

Seleccione el grupo de administración al que se moverán automáticamente los dispositivos.

Estado de la regla

Si esta opción está habilitada, la regla se habilitará y empezará a operar en cuanto la guarde.

Si esta opción está deshabilitada, la regla se creará, pero no se activará. No entrará en funcionamiento hasta que habilite esta opción.

Prioridad

Puede especificar la prioridad de la regla de movimiento. La prioridad más alta es 1. Cuanto mayor sea el valor de **Prioridad**, menor será la prioridad de la regla y su posición en la lista.

Si no se asigna ninguna prioridad, a la regla se le asigna la prioridad más baja.

Al copiar una regla, a la copia de la regla se le asigna la prioridad de la regla original. Luego, la prioridad de la regla original aumenta en 1.

Mover solo los dispositivos que no pertenezcan a un grupo de administración

Si esta opción está habilitada, solo los dispositivos no asignados se moverán al grupo seleccionado.

Si esta opción está deshabilitada, tanto los dispositivos no asignados como los dispositivos que ya pertenezcan a otro grupo de administración se moverán al grupo seleccionado.

Aplicar regla

Puede seleccionar una de las siguientes opciones:

- **Ejecutar una vez por dispositivo**

  La regla se aplicará una vez por cada dispositivo que reúna los criterios especificados.

- **Ejecutar una vez por dispositivo y luego cada vez que se reinstale el Agente de red**

  La regla se aplicará una vez por cada dispositivo que reúna los criterios especificados; tras esa primera aplicación, la regla se aplicará solo cuando el Agente de red se reinstale en esos dispositivos.

- **Aplicar esta regla continuamente**

  La regla se aplicará siguiendo una programación definida automáticamente por el Servidor de administración (generalmente, una vez cada varias horas).

4. En la pestaña **Condiciones de la regla**, especifique al menos un criterio por el cual los dispositivos se mueven a un grupo de administración.

5. Haga clic en **Guardar**.

Se crea la regla de movimiento. La nueva regla aparece en la lista de reglas de movimiento.

Cuanto más alta sea la posición en la lista, mayor será la prioridad de la regla.

Para cambiar la prioridad:

1. Seleccione la casilla de una regla de movimiento.
2. Realice una de las siguientes acciones:
   - Haga clic en el botón **Cambiar prioridad** y especifique la nueva prioridad.
   - Mueva la regla hacia arriba o hacia abajo en la lista haciendo clic en los botones **Subir** o **Bajar**.
3. Haga clic en el botón **Guardar**.

Si se selecciona la opción **Aplicar esta regla continuamente**, la regla de movimiento se aplica independientemente de la configuración de prioridad. Esas reglas se aplican de acuerdo con la programación que el Servidor de administración configura automáticamente.

Si los atributos de dispositivo cumplen con las condiciones de varias reglas, el dispositivo se mueve al grupo de destino de la regla con la prioridad más alta (es decir, la que tiene la clasificación más alta en la lista de reglas).

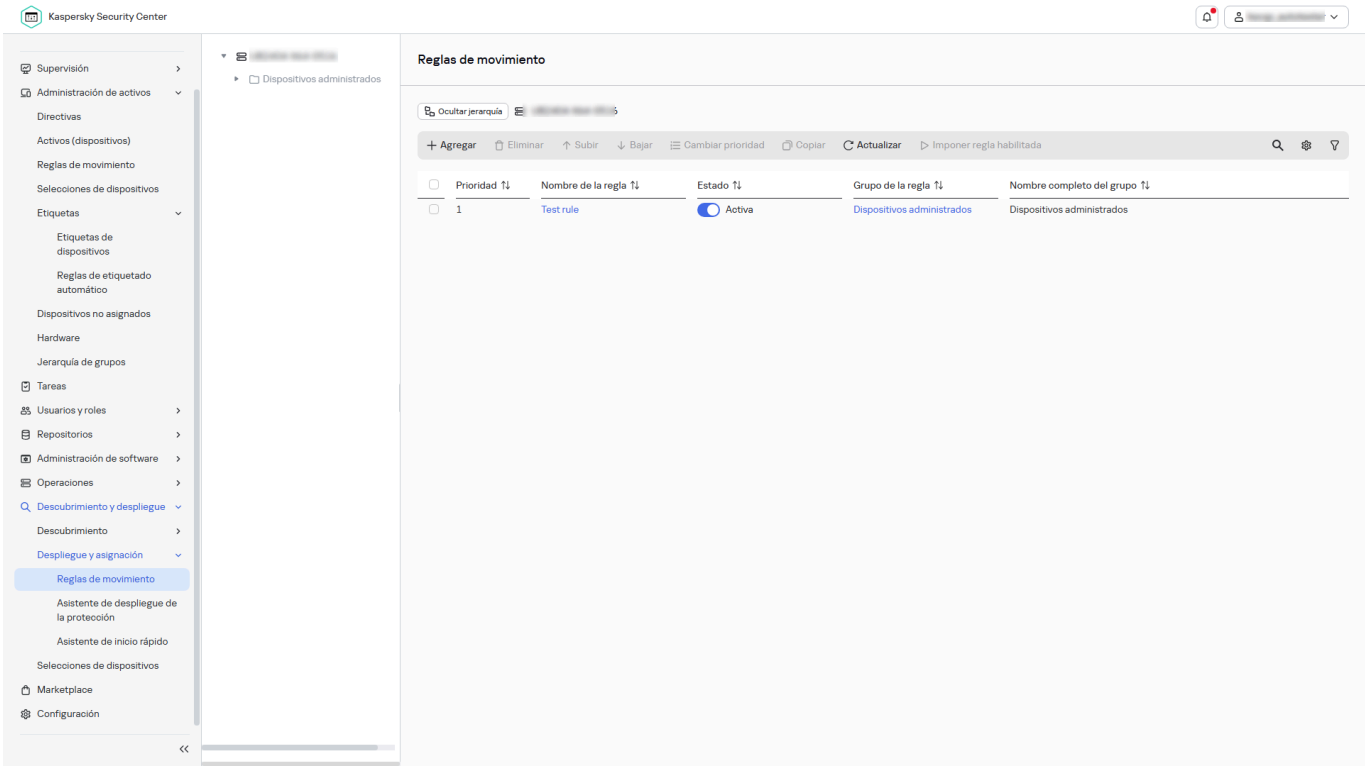
Copiar reglas de movimiento de dispositivos

Puede copiar sus reglas de movimiento de dispositivos si, por ejemplo, desea tener varias reglas de movimiento idénticas para diferentes grupos de administración de destino.

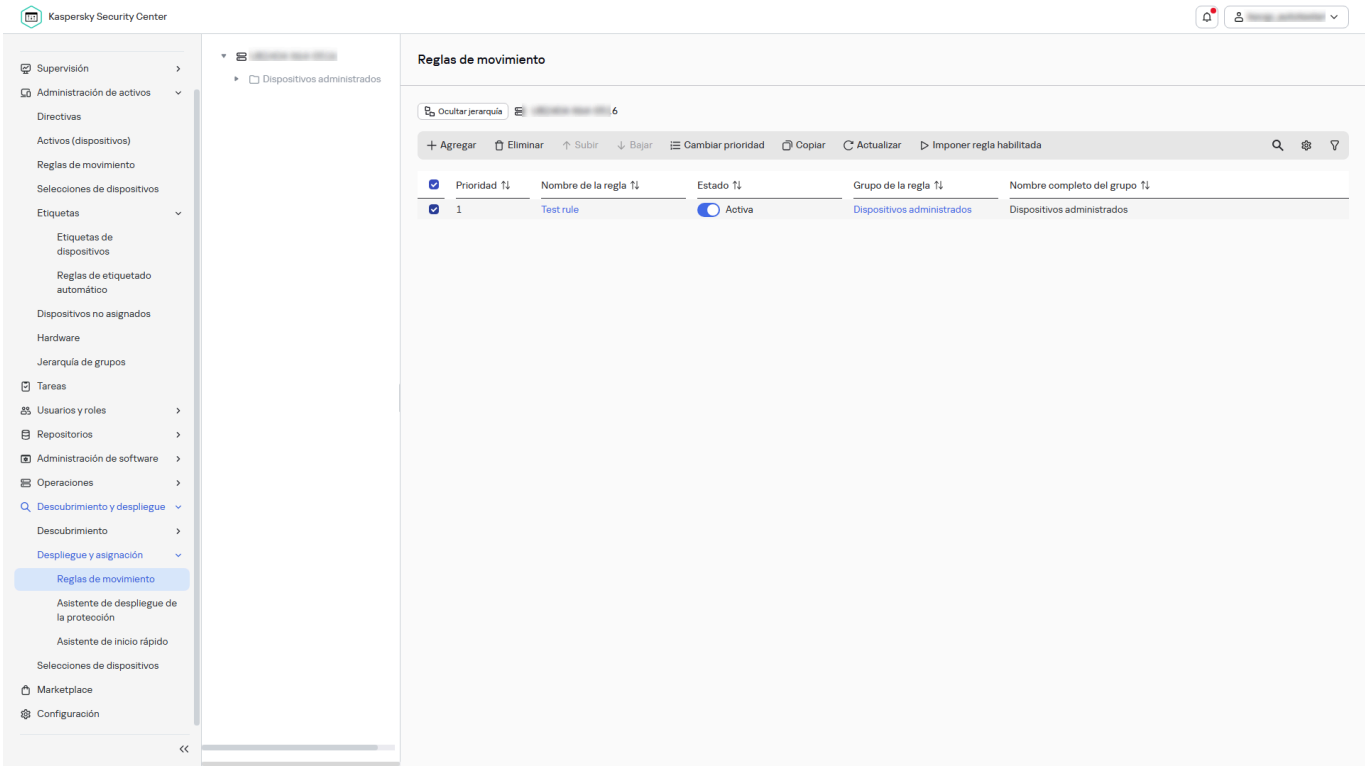
Para copiar una regla de movimiento existente:

1. Realice una de las siguientes acciones:
   - En el menú principal, vaya a **Administración de activos** → **Reglas de movimiento**.
   - En el menú principal, vaya a **Descubrimiento y despliegue** → **Despliegue y asignación** → **Reglas de movimiento**.

Se muestra la lista de reglas de movimiento.



2. Marque la casilla ubicada junto a la regla que desee copiar.



3. Haga clic en **Copiar**.

4. En la ventana que se abre, cambie la siguiente información en la pestaña **General** (si desea copiar la regla sin modificar su configuración, no haga ningún cambio):

   Nombre de la regla

   Ingrese un nombre para la nueva regla.

   Cuando se copia una regla, la regla nueva recibe el nombre de la regla de origen, con el agregado de un índice numérico entre paréntesis, como (1).

   Grupo de administración

Seleccione el grupo de administración al que se moverán automáticamente los dispositivos.

Estado de la regla

Si esta opción está habilitada, la regla se habilitará y empezará a operar en cuanto la guarde.

Si esta opción está deshabilitada, la regla se creará, pero no se activará. No entrará en funcionamiento hasta que habilite esta opción.

Prioridad

Puede especificar la prioridad de la regla de movimiento. La prioridad más alta es 1. Cuanto mayor sea el valor de **Prioridad**, menor será la prioridad de la regla y su posición en la lista.

Si no se asigna ninguna prioridad, a la regla se le asigna la prioridad más baja.

Al copiar una regla, a la copia de la regla se le asigna la prioridad de la regla original. Luego, la prioridad de la regla original aumenta en 1.

Mover solo los dispositivos que no pertenezcan a un grupo de administración

Si esta opción está habilitada, solo los dispositivos no asignados se moverán al grupo seleccionado.

Si esta opción está deshabilitada, tanto los dispositivos no asignados como los dispositivos que ya pertenezcan a otro grupo de administración se moverán al grupo seleccionado.

Aplicar regla

Puede seleccionar una de las siguientes opciones:

- **Ejecutar una vez por dispositivo**

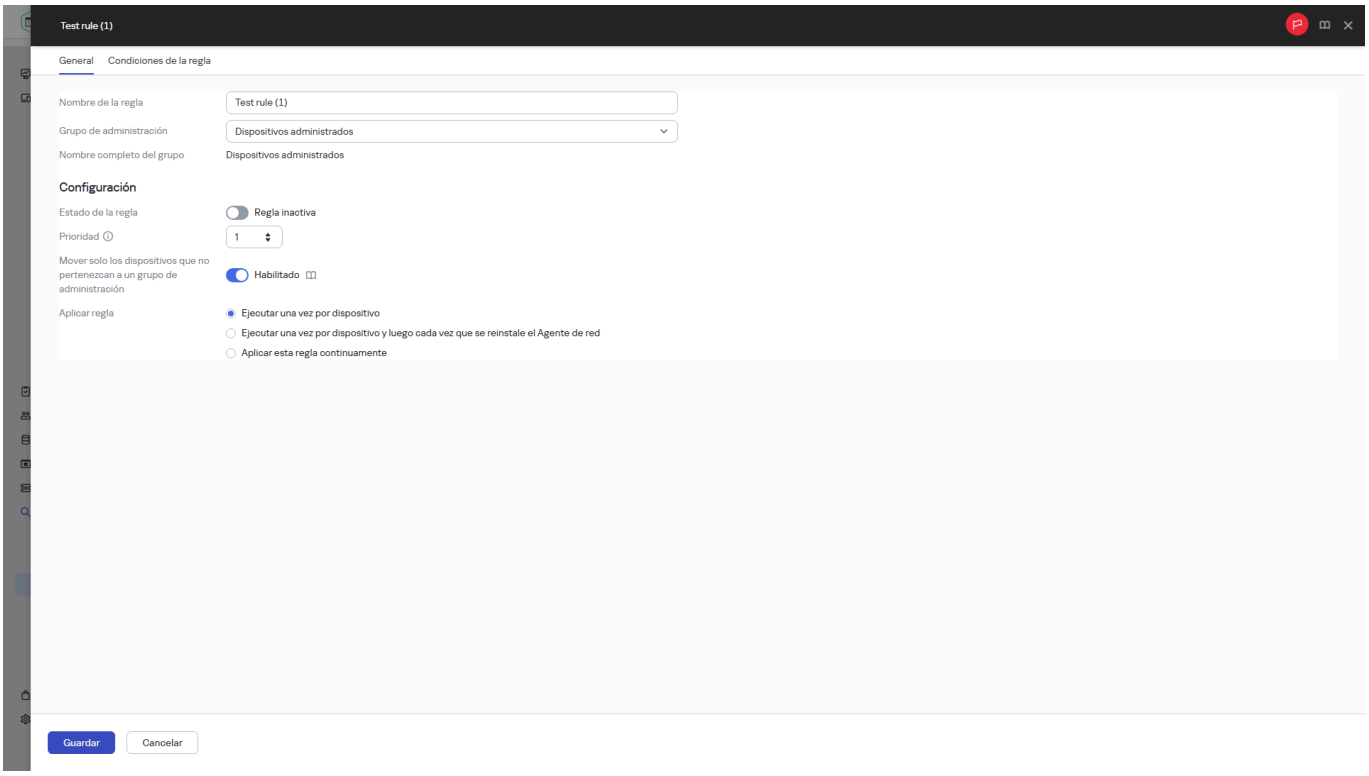
  La regla se aplicará una vez por cada dispositivo que reúna los criterios especificados.

- **Ejecutar una vez por dispositivo y luego cada vez que se reinstale el Agente de red**

  La regla se aplicará una vez por cada dispositivo que reúna los criterios especificados; tras esa primera aplicación, la regla se aplicará solo cuando el Agente de red se reinstale en esos dispositivos.

- **Aplicar esta regla continuamente**

  La regla se aplicará siguiendo una programación definida automáticamente por el Servidor de administración (generalmente, una vez cada varias horas).



5. En la pestaña **Condiciones de la regla**, especifique al menos un criterio para los dispositivos que desea que se muevan automáticamente.

6. Haga clic en **Guardar**.

Se crea la nueva regla de movimiento. La nueva regla aparece en la lista de reglas de movimiento.

Condiciones para una regla de movimiento de dispositivos

Cuando usted crea o copia una regla para mover dispositivos cliente a grupos de administración, establece en la pestaña **Condiciones de la regla** las condiciones mover los dispositivos. Para determinar qué dispositivos mover, puede utilizar los siguientes criterios:

- Etiquetas asignadas a los dispositivos cliente.
- Parámetros de red. Por ejemplo, puede mover dispositivos con direcciones IP de un rango específico.
- Propietario del dispositivo, su rol y pertenencia a grupos de seguridad.
- Aplicaciones administradas instaladas en dispositivos cliente, por ejemplo, Agente de red o Servidor de administración.
- Máquinas virtuales, que son los dispositivos cliente.
- Unidades organizativas del controlador de dominio.
- Segmentos de la nube.

A continuación, puede encontrar la descripción sobre cómo especificar esta información en una regla de movimiento de dispositivos.

Si especifica varias condiciones en la regla, se usa el operador lógico AND y todas las condiciones se aplican al mismo tiempo. Si no selecciona ninguna opción o deja algunos campos en blanco, dichas condiciones no se aplican.

Pestaña Etiquetas

En esta pestaña, puede configurar una búsqueda del dispositivo según las etiquetas para dispositivos que se añadieron anteriormente a las descripciones de los dispositivos administrados: Para hacerlo, seleccione las etiquetas pertinentes. Además, puede habilitar las siguientes opciones:

Aplicar a los dispositivos que no tengan las etiquetas especificadas

Si esta opción está habilitada, todos los dispositivos con las etiquetas especificadas se excluyen de una regla de movimiento de dispositivos. Si esta opción está deshabilitada, la regla de movimiento de dispositivos se aplica a los dispositivos con todas las etiquetas seleccionadas.

Esta opción está deshabilitada de forma predeterminada.

Aplicar si coincide al menos una etiqueta especificada

Si esta opción está habilitada, se aplica una regla de movimiento de dispositivos a los dispositivos cliente con al menos una de las etiquetas seleccionadas. Si esta opción está deshabilitada, la regla de movimiento de dispositivos se aplica a los dispositivos con todas las etiquetas seleccionadas.

Esta opción está deshabilitada de forma predeterminada.

Pestaña Red

En esta pestaña, puede especificar los datos de red de los dispositivos a los que atañe una regla de movimiento de dispositivos:

Nombre del dispositivo en la red de Windows

Nombre de red de Windows (nombre NetBIOS) del dispositivo, o la dirección IPv4 o IPv6.

Dominio de Windows

Una regla de movimiento de dispositivos se aplica a todos los dispositivos incluidos en el dominio de Windows especificado.

Nombre DNS del dispositivo

Nombre de dominio DNS del dispositivo cliente que desea mover. Complete este campo si su red incluye un servidor DNS.

> Si la intercalación con diferenciación entre mayúsculas y minúsculas está configurada para la base de datos utilizada para Kaspersky Security Center Linux, respete las mayúsculas y minúsculas cuando ingrese el nombre DNS de un dispositivo. De lo contrario, la regla de movimiento de dispositivos no funcionará.

Dominio DNS

Una regla de movimiento de dispositivos se aplica a todos los dispositivos incluidos en el sufijo DNS principal especificado. Complete este campo si su red incluye un servidor DNS.

Intervalo IP

Si habilita esta opción, podrá ingresar las direcciones IP inicial y final del intervalo IP en el que deberán estar incluidos los dispositivos pertinentes.

Esta opción está deshabilitada de forma predeterminada.

Dirección IP para establecer conexión con el Servidor de administración

Si esta opción está habilitada, puede configurar las direcciones IP mediante las cuales los dispositivos cliente se conectan al Servidor de administración. Para hacerlo, especifique el rango de IP que incluye todas las direcciones IP necesarias.

Esta opción está deshabilitada de forma predeterminada.

El dispositivo se encuentra en un subgrupo del grupo Dominios

Si esta opción está habilitada, puede seleccionar un subgrupo del grupo Dominios. Los dispositivos relevantes deben estar ubicados en el subgrupo seleccionado.

Esta opción está deshabilitada de forma predeterminada.

El dispositivo se encuentra en este intervalo IP

Si esta opción está activada, puede seleccionar un rango de IP que haya agregado previamente en la sección **Intervalos IP**. Los dispositivos relevantes deben estar incluidos en el rango IP seleccionado.

Esta opción está deshabilitada de forma predeterminada.

Perfil de conexión cambiado

Seleccione uno de los siguientes valores:

- **Sí**. Una regla de movimiento de dispositivos solo se aplica a los dispositivos cliente con un perfil de conexión modificado.
- **No**. La regla de movimiento de dispositivos solo se aplica a los dispositivos cliente cuyo perfil de conexión no cambió.
- **Ningún valor seleccionado**. La condición no se aplica.

Administrado por un Servidor de administración diferente

Seleccione uno de los siguientes valores:

- **Sí**. Una regla de movimiento de dispositivos solo se aplica a los dispositivos cliente administrados por otros Servidores de administración. Estos servidores son diferentes del servidor en el que configura la regla de movimiento de dispositivos.
- **No**. La regla de movimiento de dispositivos solo se aplica a los dispositivos cliente administrados por el Servidor de administración actual.
- **Ningún valor seleccionado**. La condición no se aplica.

Pestaña Propietario del dispositivo

En esta pestaña, puede configurar una regla de movimiento de dispositivos según el propietario del dispositivo, la pertenencia al grupo de seguridad y el rol:

Propietario del dispositivo

Seleccione el nombre de usuario del propietario del dispositivo de un grupo de seguridad interno. Obtenga más información sobre los usuarios y sus roles en esta sección.

No se puede registrar más de un usuario como propietario del dispositivo.

Membrecía del propietario del dispositivo en un grupo de seguridad de Active Directory

Seleccione un grupo de seguridad externo de Active Directory al que pertenezca el propietario del dispositivo.

El usuario puede formar parte de un grupo de seguridad de Active Directory o de un grupo incluido en este grupo de seguridad de Active Directory.

Rol del propietario del dispositivo

Seleccione el rol asignado al propietario del dispositivo. Obtenga más información sobre los roles de usuario en este artículo.

Membrecía del propietario del dispositivo en un grupo de seguridad interno

Seleccione un grupo de seguridad interno al que pertenezca el propietario del dispositivo.

Pestaña Aplicaciones

En esta pestaña, puede configurar una regla de movimiento de dispositivos basada en las aplicaciones administradas y los sistemas operativos instalados en los dispositivos cliente:

Agente de red instalado

Seleccione uno de los siguientes valores:

- **Sí**. Una regla de movimiento de dispositivos solo se aplica a los dispositivos cliente con el Agente de red instalado.
- **No**. La regla de movimiento de dispositivos solo se aplica a los dispositivos cliente en los que el Agente de red no está instalado.
- **Ningún valor seleccionado**. La condición no se aplica.

Aplicaciones

Especifique qué aplicaciones administradas deben instalarse en los dispositivos cliente, de modo que se aplique una regla de movimiento de dispositivos a estos dispositivos. Por ejemplo, puede seleccionar **Agente de red de Kaspersky Security Center 17** o **Servidor de administración de Kaspersky Security Center 17**.

Si no selecciona ninguna aplicación administrada, la condición no se aplica.

Versión del SO

Puede seleccionar dispositivos cliente en función de la versión del sistema operativo. Para ello, especifique los sistemas operativos que deben instalarse en los dispositivos cliente. Como resultado, se aplica una regla de movimiento de dispositivos a los dispositivos cliente con los sistemas operativos seleccionados.

Si no habilita esta opción, la condición no se aplica. Esta opción está deshabilitada de forma predeterminada.

Arquitectura del SO

Puede seleccionar dispositivos cliente según el tamaño de bits del sistema operativo. En el bloque **Arquitectura del sistema operativo**, puede seleccionar uno de los siguientes valores:

- **Desconocido**
- **x86**
- **AMD64**
- **IA64**

Para comprobar la arquitectura del sistema operativo de los dispositivos cliente:

1. En el menú principal, vaya a la sección **Administración de activos → Dispositivos administrados**.
2. Haga clic en el botón **Configuración de las columnas** (⚙) a la derecha.
3. Seleccione la opción **Arquitectura del SO**, y haga clic en el botón **Guardar**.

   Después, se muestra la arquitectura del sistema operativo para cada dispositivo administrado.

Administrador de paquetes del SO

Puede seleccionar los dispositivos cliente mediante el administrador de paquetes del sistema operativo. En el campo **Administrador de paquetes del SO**, puede seleccionar uno de los siguientes valores:

- rpm: para dispositivos que ejecutan los sistemas operativos Red Hat Enterprise Linux, CentOS, Fedora, SUSE y Oracle Linux
- apt (dpkg): para dispositivos que ejecutan los sistemas operativos Debian, Ubuntu y Kali
- pkg: para dispositivos que ejecutan los sistemas operativos FreeBSD y OpenBSD

Para comprobar el administrador de paquetes del sistema operativo de los dispositivos cliente, siga estos pasos:

1. En el menú principal, vaya a la sección **Administración de activos → Dispositivos administrados**.
2. Haga clic en el botón **Configuración de las columnas** (⚙) a la derecha.
3. Seleccione la opción **Administrador de paquetes del SO** y, a continuación, haga clic en el botón **Guardar**.

El administrador de paquetes del sistema operativo se muestra para cada dispositivo administrado.

Versión del paquete de servicios del SO

En este campo, puede especificar la versión del paquete de su sistema operativo (en formato *X.Y*), que determinará cómo aplicar la regla de migración a su dispositivo. De manera predeterminada, no hay una versión definida.

Certificado de usuario

Seleccione uno de los siguientes valores:

- **Instalado**. Una regla de movimiento de dispositivos solo se aplica a dispositivos móviles con un certificado para dispositivos móviles.
- **Sin instalar**. La regla de movimiento de dispositivos solo se aplica a dispositivos móviles sin un certificado para dispositivos móviles.
- **Ningún valor seleccionado**. La condición no se aplica.

Compilación del SO

Este parámetro solo es válido para sistemas operativos Windows.

Puede especificar si el sistema operativo seleccionado debe tener un número de versión igual, anterior o posterior. También puede configurar la búsqueda de una regla de movimiento para todos los números de compilación, excepto el especificado.

Número de versión del SO

Este parámetro solo es válido para sistemas operativos Windows.

Puede especificar si el sistema operativo seleccionado debe tener un número de versión igual, anterior o posterior. También puede configurar la búsqueda de una regla de movimiento para todos los números de compilación, excepto el especificado.

Pestaña Máquinas virtuales

En esta pestaña puede configurar la búsqueda de dispositivos según sean dispositivos virtuales o parte de la infraestructura de escritorio virtual (VDI):

Esta es una máquina virtual

En la lista desplegable se puede seleccionar lo siguiente:

- **N/D**. La condición no se aplica.
- **No**. Mover dispositivos que no son máquinas virtuales.
- **Sí**. Mover dispositivos que son máquinas virtuales.

Tipo de máquina virtual

Parte de la infraestructura de escritorio virtual

En la lista desplegable se puede seleccionar lo siguiente:

- **N/D**. La condición no se aplica.
- **No**. Mover dispositivos que no forman parte de la VDI.
- **Sí**. Mover de dispositivos que son parte de la VDI.

Pestaña Controlador de dominio

En esta pestaña, puede especificar que es necesario mover los dispositivos incluidos en la unidad organizativa del dominio. También puede mover dispositivos de todas las unidades organizativas secundarias de la unidad organizativa del dominio especificado:

El dispositivo está incluido en la siguiente unidad organizativa

Si esta opción está habilitada, se aplica una regla de movimiento de dispositivos a los dispositivos de la unidad organizativa del controlador de dominio especificada en la lista que hay debajo de la opción.

Esta opción está deshabilitada de forma predeterminada.

Incluir unidades organizativas secundarias

Si habilita esta opción, la selección incluirá los dispositivos de todas las unidades organizativas secundarias de la unidad organizativa del dominio especificado.

Esta opción está deshabilitada de forma predeterminada.

Mover los dispositivos de unidades secundarias a subgrupos correspondientes

Crear subgrupos correspondientes a contenedores de dispositivos recién detectados

Eliminar subgrupos no presentes en el dominio

Incluir el dispositivo en el siguiente grupo de seguridad de dominio

Si esta opción está habilitada, se aplica una regla de movimiento de dispositivos a los dispositivos del grupo de seguridad de dominio especificados en la lista que hay debajo de la opción.

Esta opción está deshabilitada de forma predeterminada.

Pestaña Segmentos de nube

En esta pestaña, puede especificar que es necesario mover los dispositivos incluidos en el segmento de la nube. También puede mover dispositivos de todas las unidades organizativas secundarias de la unidad organizativa del dominio especificado:

El dispositivo se encuentra en un segmento de la nube

Si selecciona esta opción, una regla de movimiento de dispositivos se aplica a los dispositivos cliente que pertenecen a un segmento de la nube. Puede seleccionar el segmento de nube requerido hasta una subred en la lista que hay debajo de la opción.

Esta opción está deshabilitada de forma predeterminada.

Incluir objetos secundarios

Si habilita esta opción, la selección incluirá los dispositivos de todas las unidades organizativas secundarias del segmento de la nube especificado.

Esta opción está deshabilitada de forma predeterminada.

Mover los dispositivos de objetos anidados a subgrupos correspondientes

Crear subgrupos correspondientes a contenedores de dispositivos recién detectados

Eliminar subgrupos para los que no se encuentre coincidencia en los segmentos de nube

Dispositivo encontrado mediante API

En la lista desplegable se puede seleccionar lo siguiente:

- Ningún valor seleccionado. La condición no se aplica.
- **No**. Mover dispositivos que no se detectaron mediante la API.
- **AWS**. Mover dispositivos detectados mediante la API de AWS.
- **Azure**. Mover dispositivos detectados mediante la API de Azure.
- **Google Cloud**. Mover dispositivos detectados mediante la API de Google Cloud.

Después, según el valor seleccionado, puede completar los siguientes campos:

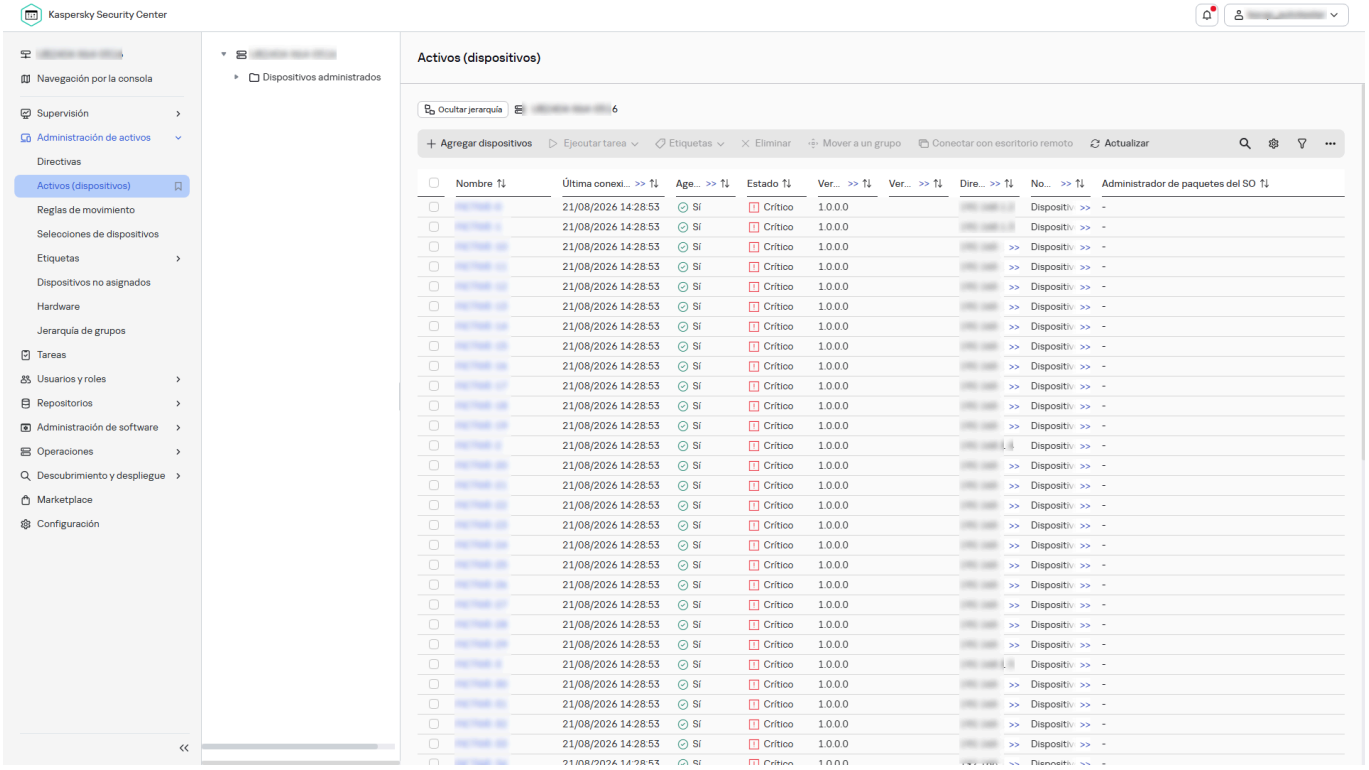
- **Subred del dispositivo de nube**.
- **Zona de disponibilidad del dispositivo de nube**.
- **Grupo de ubicación del dispositivo de nube**.

Agregar dispositivos a un grupo de administración en forma manual

Puede mover sus dispositivos a grupos de administración de distintas maneras: puede crear reglas que los muevan automáticamente, puede moverlos de un grupo de administración a otro en forma manual, o puede agregarlos manualmente a un grupo de administración puntual. En esta sección, se explica cómo agregar dispositivos a un grupo de administración de manera manual.

Para agregar uno o más dispositivos manualmente a un grupo de administración específico:

1. En el menú principal, vaya a **Administración de activos → Dispositivos administrados**.



La lista de dispositivos administrados

2. Seleccione el grupo de administración al que desea agregar los dispositivos:

   - Para el grupo root:

     En este caso, puede avanzar al próximo paso.

   - Para un subgrupo:

     a. Haga clic en el botón **Mostrar jerarquía** en la parte superior de la página.

     El nombre del botón cambia a **Ocultar jerarquía**.

     b. En la ventana que se abre, haga clic en el nombre del subgrupo.

     Verá la ruta al grupo seleccionado en la parte superior de la página. Si es necesario, puede hacer clic en un vínculo con el nombre del grupo de administración para ir al grupo. De forma predeterminada, el último vínculo de la ruta se encuentra inactivo. Además, puede cerrar la ventana de jerarquía si hace clic en el botón **Ocultar jerarquía**.

3. Haga clic en el botón **Agregar dispositivos**.

   Se inicia el Asistente para mover dispositivos.

4. Cree una lista con los dispositivos que desee agregar al grupo de administración.

   La base de datos del Servidor de administración debe tener información sobre los dispositivos que quiera agregar. No puede agregar dispositivos que nunca se hayan conectado o que la aplicación aún no haya detectado.

Elija un método para agregar los dispositivos a la lista:

- Haga clic en el botón **Agregar dispositivos** y luego elija los dispositivos de una de las siguientes maneras:
  - Seleccione los dispositivos de la lista de dispositivos detectados por el Servidor de administración.
  - Especifique las direcciones IP de los dispositivos o un intervalo de direcciones IP.

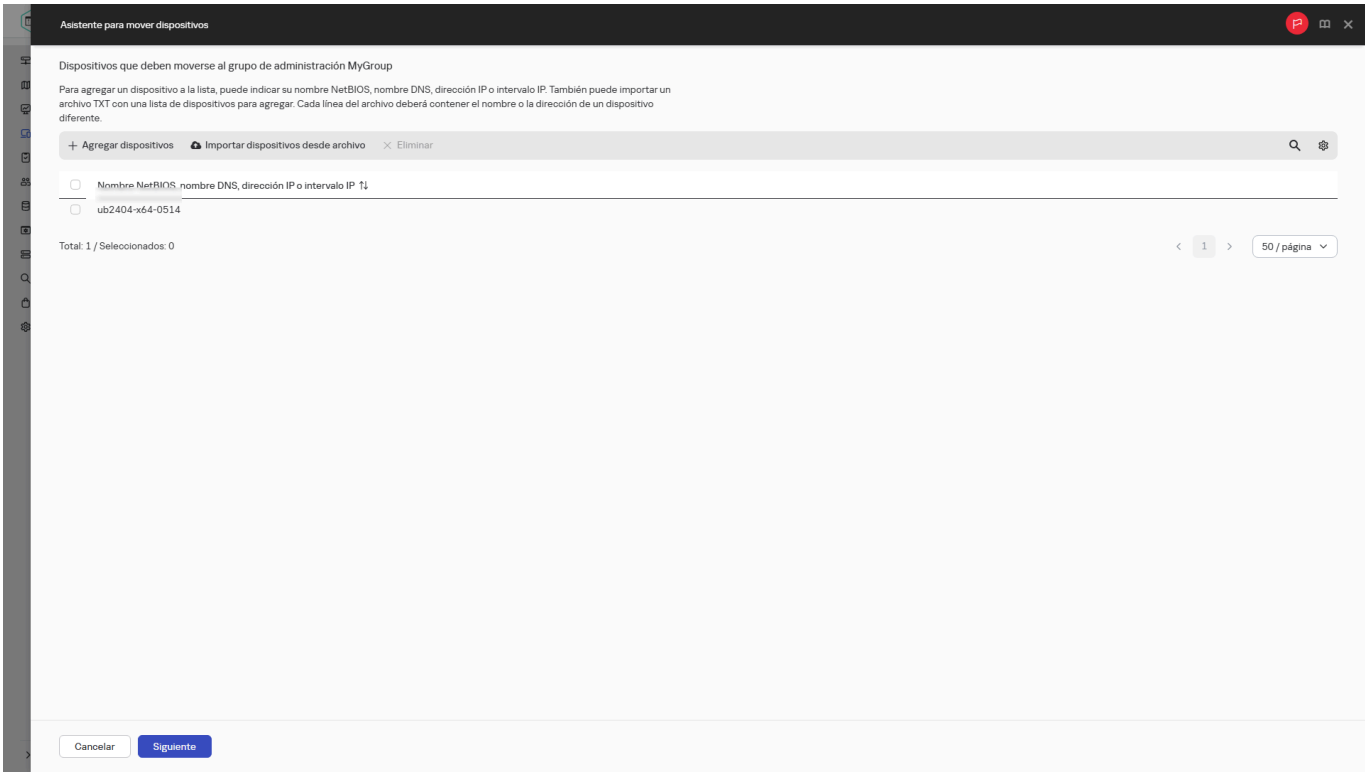
    El rango de direcciones IP no debe contener más de 1 048 576 direcciones.

  - Especifique un nombre DNS del dispositivo.

    El campo con el nombre del dispositivo no debe contener espacios en blanco, caracteres de retroceso ni ninguno de los siguientes caracteres prohibidos: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %

- Haga clic en el botón **Importar dispositivos desde archivo** para importar una lista de dispositivos desde un archivo .txt. Utilice una línea diferente para la dirección o el nombre de cada dispositivo.

  El archivo no debe contener espacios en blanco, caracteres de retroceso ni ninguno de los siguientes caracteres prohibidos: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %



Seleccionar los dispositivos que se moverán al grupo de administración

5. Revise la lista de dispositivos que se agregarán al grupo de administración. Si necesita agregar o quitar dispositivos, haga los cambios necesarios en la lista.

6. Si no ve ningún error en la lista, haga clic en el botón **Siguiente**.

El asistente procesará la lista de dispositivos y mostrará el resultado. Los dispositivos que se procesen

correctamente se agregarán al grupo de administración y aparecerán en la lista de dispositivos con nombres generados por el Servidor de administración.

Mover dispositivos o clústeres a un grupo de administración en forma manual

Puede mover dispositivos de un grupo de administración a otro, o del grupo de dispositivos no asignados a un grupo de administración.

También puede mover clústeres o conjuntos de servidores de un grupo de administración a otro. Cuando mueve un clúster o un conjunto de servidores a otro grupo, todos sus nodos se mueven con él, porque un clúster y cualquiera de sus nodos siempre pertenecen al mismo grupo de administración. Cuando selecciona un solo nodo de clúster en la pestaña **Dispositivos**, el botón **Mover a un grupo** deja de estar disponible.

Para mover uno o varios dispositivos o clústeres a un grupo de administración seleccionado:

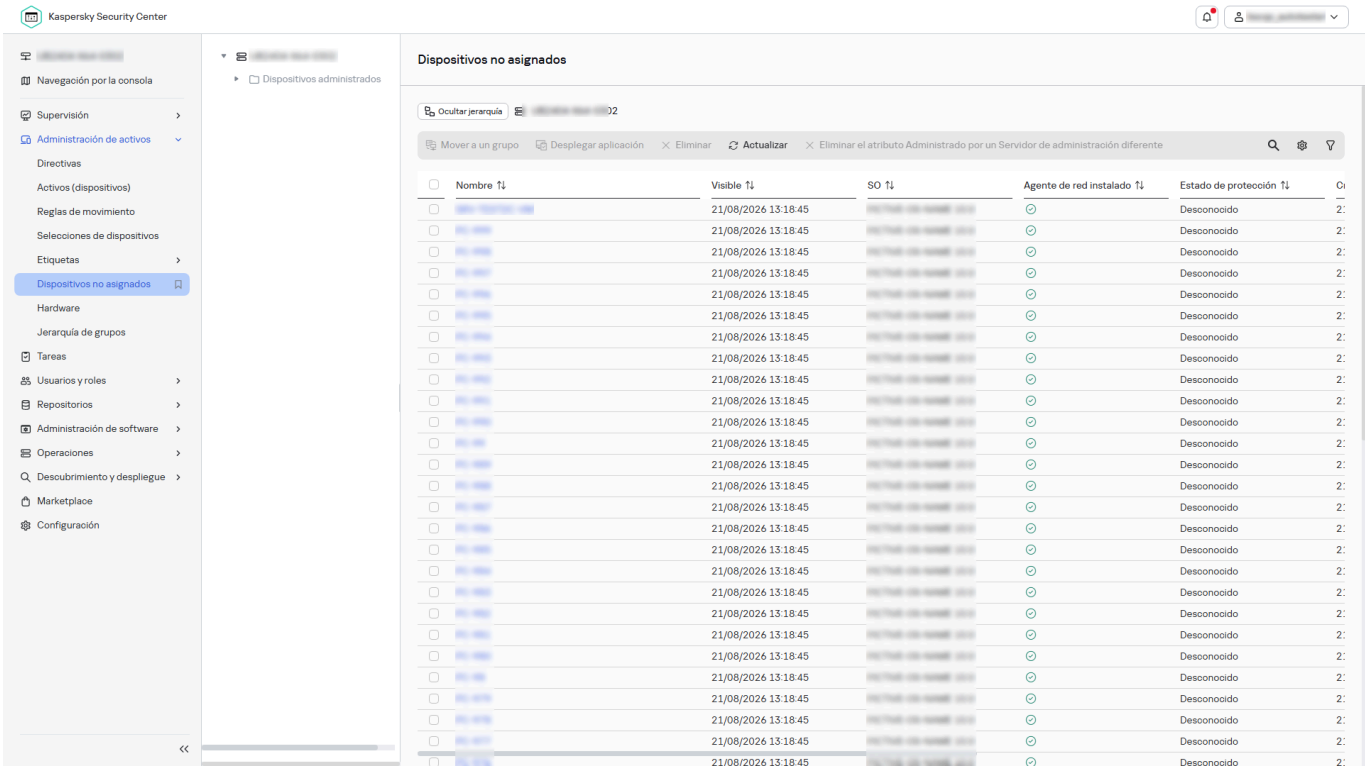
1. Abra el grupo de administración al que pertenezcan los dispositivos que desee mover. Para hacerlo, siga uno de estos pasos:

   - Para abrir un grupo de administración, en el menú principal, vaya a **Administración de activos** → **Dispositivos administrados** y, luego, seleccione el grupo de administración requerido.

     - Para el grupo raíz, puede continuar con el siguiente paso.

     - Para un subgrupo, haga clic en el botón **Mostrar jerarquía** en la parte superior de la página y, luego, en la ventana que se abre, seleccione el grupo de administración requerido.

   - Para abrir el grupo **Dispositivos no asignados**, en el menú principal, vaya a **Administración de activos** → **Dispositivos no asignados**.



La lista de dispositivos no asignados

2. Si el grupo de administración contiene clústeres o conjuntos de servidores, la sección **Dispositivos administrados** se divide en dos pestañas: **Dispositivos** y **Clústeres y conjuntos de servidores** Abra la pestaña del objeto que desea mover.

3. Active las casillas ubicadas junto a los dispositivos o clústeres que desee mover a otro grupo.

4. Haga clic en el botón **Mover a un grupo**.

5. En la jerarquía de grupos de administración, marque la casilla ubicada junto al grupo de administración al que desee mover los dispositivos o clústeres seleccionados.

6. Haga clic en el botón **Mover**.

Los dispositivos o clústeres seleccionados se moverán al grupo de administración seleccionado.

Sobre clústeres y conjuntos de servidores

Kaspersky Security Center Linux admite la tecnología de clúster. Si el Agente de red envía información al Servidor de administración que confirma que la aplicación instalada en un dispositivo cliente forma parte de una matriz de servidores, el dispositivo cliente se convierte en un nodo del clúster.

Si un grupo de administración contiene clústeres o conjuntos de servidores, la página **Dispositivos administrados** muestra dos pestañas: una para dispositivos individuales y otra para clústeres y conjuntos de servidores. Una vez que los dispositivos administrados se detectan como nodos de clúster, el clúster se agrega como un objeto individual a la pestaña **Clústeres y conjuntos de servidores**.

Los nodos de los clústeres o conjuntos de servidores se enumeran en la pestaña **Dispositivos**, junto con otros dispositivos administrados. Puede ver las propiedades de los nodos como dispositivos individuales y llevar a cabo otras operaciones, pero no puede eliminar un nodo de clúster ni moverlo a otro grupo de administración por separado de su clúster. Solo puede eliminar o mover un clúster completo.

Puede realizar las siguientes operaciones con clústeres o conjuntos de servidores:

- Ver las propiedades
- Mover el clúster o conjunto de servidores a otro grupo de administración

  Cuando mueve un clúster o un conjunto de servidores a otro grupo, todos sus nodos se mueven con él, porque un clúster y cualquiera de sus nodos siempre pertenecen al mismo grupo de administración.

- Eliminar

  Es razonable eliminar un clúster o un conjunto de servidores solo cuando el clúster o conjunto de servidores ya no existe en la red de la organización. Si un clúster aún está visible en su red y el Agente de red y la aplicación de seguridad de Kaspersky todavía están instalados en los nodos del clúster, Kaspersky Security Center Linux devuelve el clúster eliminado y sus nodos a la lista de dispositivos administrados de manera automática.

Propiedades de un clúster o conjunto de servidores

Para ver la configuración de un clúster o conjunto de servidores:

1. En el menú principal, vaya a **Administración de activos → Dispositivos administrados → Clústeres y conjuntos de servidores**.

   Se muestra la lista de clústeres y conjuntos de servidores.

2. Haga clic en el nombre del clúster o conjunto de servidores requerido.

Se muestra la ventana de propiedades del clúster o conjunto de servidores seleccionado.

General

La sección **General** muestra información general sobre el clúster o conjunto de servidores. La información se basa en los datos recibidos durante la última sincronización de los nodos del clúster con el Servidor de administración.

Nombre

Descripción

Dominio de Windows

Dominio o grupo de trabajo de Windows, que contiene el clúster o conjunto de servidores.

Nombre NETBIOS

Nombre de red de Windows del clúster o conjunto de servidores.

Nombre DNS

Nombre del dominio DNS del clúster o conjunto de servidores.

Tareas

La pestaña **Tareas** permite administrar las tareas del clúster o conjunto de servidores. Utilice esta sección para crear tareas nuevas, ver la lista de tareas existentes, ver los resultados de ejecución de las tareas e iniciar, detener, eliminar y reconfigurar las tareas existentes. Las tareas enumeradas se relacionan con la aplicación de seguridad de Kaspersky instalada en los nodos del clúster. Kaspersky Security Center Linux recibe la lista de tareas y los detalles del estado de las tareas de los nodos del clúster. Si no se puede establecer una conexión, no se mostrará ningún estado.

Nodos

Esta pestaña muestra una lista de nodos incluidos en el clúster o conjunto de servidores. Puede hacer clic en el nombre de un nodo para ver la ventana de propiedades del dispositivo.

Aplicación de Kaspersky

La ventana de propiedades también puede contener pestañas adicionales con información y configuraciones relacionadas con la aplicación de seguridad de Kaspersky instalada en los nodos del clúster.

Ajuste de puntos de distribución y puertas de enlace de conexión

Una estructura de grupos de administración en Kaspersky Security Center Linux realiza las funciones siguientes:

- Define el alcance de las directivas

  Existe otra forma de aplicar ajustes pertinentes en dispositivos: mediante el uso de *perfiles de directiva*.

- Define el alcance de las tareas de grupo

  Existe un modo de definir el alcance de las tareas de grupo que no depende de una jerarquía de grupos de administración: el uso de tareas para selecciones de dispositivos y de tareas para dispositivos específicos.

- Regula la capacidad de acceder a los distintos dispositivos, Servidores de administración secundarios y Servidores de administración virtuales

- Asigna puntos de distribución

Al momento de crear la estructura de grupos de administración, para que la asignación de puntos de distribución sea óptima, es necesario tener en cuenta la topología de la red de la organización. La distribución óptima de puntos de distribución le permite ahorrar tráfico en la red de la organización.

Dependiendo del organigrama de la organización y de la topología de la red, pueden aplicarse las siguientes configuraciones estándares a la estructura de grupos de administración:

- Oficina única

- Varias oficinas remotas pequeñas

Los dispositivos designados como puntos de distribución deben protegerse contra el acceso no autorizado por medios virtuales y físicos.

Acerca de los puntos de distribución

Los dispositivos que tengan instalado el Agente de red pueden utilizarse como punto de distribución. En este modo, el Agente de red puede distribuir actualizaciones que se pueden recuperar desde el Servidor de administración o desde los servidores de Kaspersky. En este último caso, configure la descarga de actualizaciones para un punto de distribución.

El despliegue de puntos de distribución en la red de una organización cumple los siguientes objetivos:

- Reduce la carga en el Servidor de administración.
- Optimiza el tráfico.
- Proporciona al Servidor de administración acceso a dispositivos en puntos poco accesibles de la red de la organización. La disponibilidad de un puntos de distribución en la red detrás de la NAT (con relación al Servidor de administración) permite que el Servidor de administración realice las siguientes acciones:
  - Envíe notificaciones a dispositivos mediante UDP en la red IPv4 o IPv6.
  - Sondee la red IPv4 o IPv6.
  - Realizar el despliegue inicial.
  - Actúe como un servidor push.

Un punto de distribución se asigna a un grupo de administración. En este caso, la cobertura del punto de distribución incluye todos los dispositivos dentro del grupo de administración y todos sus subgrupos. Se debe destacar, sin embargo, que el dispositivo que actúa como punto de distribución no necesariamente tiene que formar parte del grupo de administración para el que ha sido designado.

Puede hacer que un punto de distribución funcione como una puerta de enlace de conexión. En este caso, los dispositivos en la cobertura del punto de distribución se conectarán al Servidor de administración a través de la puerta de enlace, no directamente. Este modo puede ser útil en situaciones que no permitan establecer una conexión directa entre el Servidor de administración y los dispositivos administrados.

Si utiliza un dispositivo basado en Linux como punto de distribución, recomendamos encarecidamente aumentar el límite de descriptores de archivos para el servicio klnagent, ya que si el alcance del punto de distribución incluye muchos dispositivos, la cantidad máxima predeterminada de archivos que se pueden abrir puede no ser suficiente.

Configuración estándar de puntos de distribución: oficina única

En una configuración estándar de "oficina única", todos los dispositivos se encuentran en la red de la organización y tienen la capacidad de "verse" los unos a los otros. La red de la organización puede constar de varias partes independientes (redes o segmentos de red) vinculadas por canales estrechos.

Los siguientes métodos pueden emplearse para armar la estructura de grupos de administración:

- Armar la estructura de grupos de administración tomando en cuenta la topología de la red. No es necesario que la estructura de grupos de administración refleje con absoluta precisión la topología de la red. Es suficiente con que haya coincidencia entre las partes independientes de la red y ciertos grupos de administración. Puede usar la asignación automática de puntos de distribución o asignarlos manualmente.

- Armar la estructura de grupos de administración sin tener en cuenta la topología de la red. En este caso, debe deshabilitar la asignación automática de puntos de distribución y luego asignar uno o varios dispositivos para que actúen como puntos de distribución para un grupo de administración original en cada una de las partes independientes de la red; por ejemplo, para el grupo **Dispositivos administrados**. Todos los puntos de distribución estarán al mismo nivel y presentarán el mismo alcance en todos los dispositivos en la red de la organización. En este caso, cada Agente de red se conectará al punto de distribución que tenga la ruta más corta. La ruta a un punto de distribución se puede determinar con la utilidad tracert.

Configuración estándar de puntos de distribución: varias oficinas remotas pequeñas

Esta configuración estándar contempla la existencia de varias pequeñas oficinas remotas, que pueden comunicarse con una oficina central a través de Internet. Cada oficina remota está ubicada detrás de una pasarela NAT; debido a ello, las oficinas remotas están aisladas las unas de las otras y no se pueden conectar entre sí.

La configuración se debe ver reflejada en la estructura de grupos de administración: debe crearse un grupo de administración independiente para cada oficina remota (los grupos **Oficina 1** y **Oficina 2** en la siguiente imagen).



Oficinas remotas incluidas en la estructura de grupos de administración

Cada grupo de administración correspondiente a una oficina debe tener asignados uno o más puntos de distribución. Los puntos de distribución deben ser dispositivos que se encuentren en la oficina remota y deben tener una cantidad suficiente de espacio libre en disco. Los dispositivos incluidos en el grupo **Oficina 1** accederán a los puntos de distribución asignados al grupo de administración **Oficina 1**, por ejemplo.

Cuando hay usuarios que utilizan una computadora portátil para trabajar físicamente en más de una oficina, resulta necesario designar, junto con los puntos de distribución existentes, dos o más dispositivos en cada oficina remota para que actúen como puntos de distribución de un grupo de administración ubicado en un nivel superior (el grupo llamado **Grupo para oficinas** en la imagen anterior).

Ejemplo: Una computadora portátil incluida en el grupo de administración **Oficina 1** se traslada físicamente a la oficina que corresponde al grupo de administración **Oficina 2**. Luego del traslado, el Agente de red de la computadora portátil intenta acceder a los puntos de distribución asignados al grupo **Oficina 1**, pero esos puntos de distribución no están disponibles. Tras ello, el Agente de red intenta acceder a los puntos de distribución asignados al **Grupo para oficinas**. Como las oficinas remotas están aisladas entre sí, los intentos de acceder a los puntos de distribución asignados al grupo de administración **Grupo para oficinas** solo tendrán éxito cuando el Agente de red intente acceder a los puntos de distribución del grupo **Oficina 2**. Así, la computadora portátil permanecerá en el grupo de administración correspondiente a su oficina inicial, pero usará el punto de distribución de la oficina en la que se encuentre físicamente.

Cálculo de la cantidad de puntos de distribución y su configuración

Cuantos más dispositivos cliente contiene una red, más puntos de distribución se requieren. Le recomendamos que no deshabilite la asignación automática de puntos de distribución. Cuando se habilita la asignación automática de puntos de distribución, el Servidor de administración asigna puntos de distribución si el número de dispositivos cliente es bastante grande y define su configuración.

La utilización de puntos de distribución exclusivamente asignados

Si planea usar ciertos dispositivos específicos como puntos de distribución (es decir, servidores asignados exclusivamente), puede optar por no usar la asignación automática de puntos de distribución. En este caso, compruebe que los dispositivos a los que planea hacer puntos de distribución tengan el volumen suficiente de espacio libre en disco, que no se apaguen con frecuencia y que tengan el modo de suspensión desactivado.

Número de puntos de distribución dedicados en una red con un solo segmento de red, según el número de dispositivos de la red

Número de dispositivos cliente por segmento de red	Número de puntos de distribución
Menos de 300	0 (no corresponde utilizar puntos de distribución)
Más de 300	Aceptable: (N / 10 000 + 1), recomendado: (N / 5000 + 2), donde N es el número de dispositivos conectados a la red

Número de puntos de distribución dedicados en una red con varios segmentos de red, según el número de dispositivos de la red

Número de dispositivos cliente en cada segmento de red	Número de puntos de distribución
Menos de 10	0 (no corresponde utilizar puntos de distribución)
10–100	1
Más de 100	Aceptable: (N / 10 000 + 1), recomendado: (N / 5000 + 2), donde N es el número de dispositivos conectados a la red

Uso de dispositivos cliente estándar (estaciones de trabajo) como puntos de distribución

Si planea usar dispositivos cliente estándar (es decir, estaciones de trabajo) como puntos de distribución, le recomendamos que siga los lineamientos de las siguientes tablas. Al designar los puntos de distribución según estas recomendaciones, evitará las sobrecargas en los canales de comunicación y en el Servidor de administración.

Número de estaciones de trabajo designadas como puntos de distribución en una red que contiene un único segmento de red, en función del número de dispositivos en red

Número de dispositivos cliente por segmento de red	Número de puntos de distribución
Menos de 300	0 (no corresponde utilizar puntos de distribución)
Más de 300	(N / 300 + 1), donde N es el número de dispositivos en red; debe haber al menos 3 puntos de distribución

Número de estaciones de trabajo designadas como puntos de distribución en una red que contiene múltiples segmentos de red, en función del número de dispositivos en red

Número de dispositivos cliente en cada segmento de red	Número de puntos de distribución
Menos de 10	0 (no corresponde utilizar puntos de distribución)
10–30	1
31–300	2
Más de 300	(N / 300 + 1), donde N es el número de dispositivos en red; debe haber al menos 3 puntos de distribución

Cuando un punto de distribución se encuentra apagado o no está disponible por algún motivo, los dispositivos administrados en su alcance pueden obtener actualizaciones del Servidor de administración.

Asignar puntos de distribución automáticamente

Recomendamos que asigne puntos de distribución automáticamente. En este caso, Kaspersky Security Center Linux seleccionará por sí mismo qué dispositivos deben tener asignados puntos de distribución.

Los dispositivos que ejecutan Microsoft Windows en Arm no pueden actuar como puntos de distribución.

Para asignar puntos de distribución automáticamente:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, elija la sección **Puntos de distribución**.

3. Seleccione la opción **Asignar automáticamente puntos de distribución**.

   Si la asignación automática de dispositivos como puntos de distribución está habilitada, no puede configurar los puntos de distribución manualmente ni editar la lista de puntos de distribución.

4. Haga clic en el botón **Guardar**.

El Servidor de administración asigna y configura los puntos de distribución automáticamente.

Designación manual de puntos de distribución

Kaspersky Security Center Linux le permite asignar manualmente dispositivos para actuar como puntos de distribución.

Recomendamos que asigne puntos de distribución automáticamente. En este caso, Kaspersky Security Center Linux seleccionará por sí mismo qué dispositivos deben tener asignados puntos de distribución. Sin embargo, si tiene que optar por no asignar puntos de distribución automáticamente por cualquier motivo (por ejemplo, si desea utilizar servidores asignados exclusivamente), puede asignar puntos de distribución manualmente después de calcular el número y la configuración de los puntos de distribución.

Los dispositivos designados como puntos de distribución deben protegerse contra el acceso no autorizado por medios virtuales y físicos.

Los dispositivos que ejecutan Microsoft Windows en Arm no pueden actuar como puntos de distribución.

Para designar manualmente un dispositivo como punto de distribución:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, elija la sección **Puntos de distribución**.

3. Seleccione la opción **Asignar manualmente puntos de distribución**.

4. Haga clic en el botón **Asignar**.

5. Seleccione el dispositivo que quiera designar como punto de distribución.

   A la hora de seleccionar un dispositivo, tenga presentes las características de funcionamiento de los puntos de distribución y los requisitos con los que debe cumplir un dispositivo para actuar como punto de distribución.

6. Seleccione el grupo de administración que desee incluir en el alcance del punto de distribución seleccionado.

7. Haga clic en **Aceptar**.

   El punto de distribución agregado aparecerá en la lista de puntos de distribución, en la sección **Puntos de distribución**.

8. Haga clic en el punto de distribución recién agregado en la lista para abrir su ventana de propiedades.

9. En la ventana de propiedades, configure los ajustes del punto de distribución:

   - La sección **General** contiene la configuración de interacción entre el punto de distribución y los dispositivos cliente.

     Puerto SSL

     El número del puerto SSL que se usará para establecer una conexión cifrada con SSL entre el punto de distribución y los dispositivos cliente.

     El número de puerto predeterminado es 13000.

     Habilitado

     Si habilita esta opción, se utilizará la multidifusión IP para distribuir automáticamente los paquetes de instalación a los dispositivos cliente del grupo.

     Cuando necesite instalar una aplicación en un grupo de dispositivos cliente utilizando un paquete de instalación, la multidifusión IP ayudará a que el proceso se complete más rápidamente. Sin embargo, cuando se necesita instalar una aplicación en un único dispositivo cliente, la multidifusión hace que el tiempo de instalación aumente.

Dirección de multidifusión IP

La dirección IP que se utilizará para la multidifusión. Puede usar cualquier dirección IP del intervalo 224.0.0.0-239.255.255.255

De manera predeterminada, Kaspersky Security Center Linux asignará automáticamente una dirección de multidifusión IP única tomada de este intervalo.

Puerto para la multidifusión IP

Número del puerto que se usará para la multidifusión IP.

El puerto por defecto es el 15001. De forma predeterminada, si el dispositivo que tiene instalado el Servidor de administración es, además, el punto de distribución designado, se usará el puerto 13001 para las conexiones SSL.

Dirección del punto de distribución para dispositivos remotos

La dirección de red a través de la cual los dispositivos remotos se conectan al punto de distribución.

Habilitado

Las actualizaciones se distribuirán a los dispositivos administrados desde las siguientes fuentes:

- si deja esta opción habilitada: el presente punto de distribución;
- si deshabilita esta opción: otros puntos de distribución, el Servidor de administración o los servidores de actualizaciones de Kaspersky.

Si utiliza puntos de distribución para distribuir las actualizaciones, reducirá el número de descargas y verá una merma en el volumen de tráfico. Además, al distribuir la carga entre los puntos de distribución, también logrará aminorar la carga del Servidor de administración. Puede consultar Cálculo del número y la configuración de los puntos de distribución para determinar cuántos puntos de distribución necesita su red y optimizar el tráfico y la carga.

Si deshabilita esta opción, el número de descargas de actualizaciones y la carga del Servidor de administración podrían aumentar. Esta opción está activada de forma predeterminada.

Habilitado

Los paquetes de instalación se distribuirán a los dispositivos administrados desde las siguientes fuentes:

- si deja esta opción habilitada: el presente punto de distribución;
- si deshabilita esta opción: otros puntos de distribución, el Servidor de administración o los servidores de actualizaciones de Kaspersky.

Si utiliza puntos de distribución para desplegar los paquetes de instalación, reducirá el número de descargas y verá una merma en el volumen de tráfico. Además, al distribuir la carga entre los puntos de distribución, también logrará aminorar la carga del Servidor de administración. Puede calcular el número y la configuración de los puntos de distribución para determinar el número de puntos de distribución de su red y optimizar el tráfico y la carga.

Si deshabilita esta opción, el número de descargas de paquetes de instalación y la carga del Servidor de administración podrían aumentar. Esta opción está activada de forma predeterminada.

Habilitado

En Kaspersky Security Center Linux, los puntos de distribución pueden funcionar como servidores push para dispositivos que se administran a través del protocolo móvil y para dispositivos que se administran a través del Agente de red. Por ejemplo, se debe habilitar un servidor push si quiere poder forzar la sincronización de los dispositivos KasperskyOS con el Servidor de administración. Un servidor push tiene el mismo alcance de los dispositivos administrados que el punto de distribución en el que se habilitar el servidor push. Si tiene varios puntos de distribución asignados para el mismo grupo de administración, puede habilitar el servidor push en cada uno de los puntos de distribución. En este caso, el Servidor de administración equilibra la carga entre los puntos de distribución.

Puerto del servidor push

El número de puerto para el servidor push. Puede especificar el número de cualquier puerto desocupado.

- En la sección **Alcance**, especifique los grupos de administración a los que el punto de distribución distribuirá las actualizaciones.

- En la sección **Origen de actualizaciones**, puede seleccionar un origen de actualizaciones para el punto de distribución:

  Origen de actualizaciones

  Seleccione un origen de actualizaciones para el punto de distribución:

  - Seleccione **Recuperar desde el Servidor de administración** para que el punto de distribución pueda recibir actualizaciones del Servidor de administración.

  - Seleccione **Usar una tarea de descarga de actualizaciones** para que el punto de distribución pueda utilizar una tarea para recibir las actualizaciones. A continuación, indique qué tarea *Descargar actualizaciones en los repositorios de los puntos de distribución* se usará:

    - Si la tarea que desea utilizar ya existe en el dispositivo, selecciónela en la lista.

    - Si la tarea aún no existe en el dispositivo, haga clic en el vínculo **Crear tarea** para crearla. Se inicia el Asistente para crear nueva tarea. Siga los pasos del asistente.

  Descargar archivos diff

  Esta opción habilita la función de descarga de archivos diff.

  Esta opción está activada de forma predeterminada.

- Si sus puntos de distribución utilizan un servidor proxy al conectarse a Internet, en la subsección **Configuración de la conexión a Internet**, puede especificar la siguiente configuración:

  Usar servidor proxy

  Si se selecciona esta casilla, se usa un servidor proxy de Internet para conectar los puntos de distribución a los servidores de actualización de Kaspersky. En los campos de entrada, puede configurar la conexión con el servidor proxy.

  Esta casilla está desactivada por defecto.

  Dirección del servidor proxy

  Dirección del servidor proxy.

  Número de puerto

  Número de puerto que se utilizará para la conexión.

  No usar el servidor proxy para direcciones locales

Si habilita esta opción, no se usará un servidor proxy para establecer conexión con los dispositivos de la red local.

Esta opción está deshabilitada de forma predeterminada.

Autenticación del servidor proxy

Si se selecciona esta casilla, en los campos de entrada se podrán especificar las credenciales para la autenticación del servidor proxy.

Esta casilla está desactivada por defecto.

Nombre de usuario

Cuenta de usuario con la que se establece conexión con el servidor proxy.

Contraseña

Contraseña de la cuenta con la que se ejecutará la tarea.

- En la sección **Proxy de KSN**, puede configurar la aplicación para que utilice el punto de distribución para reenviar las solicitudes KSN desde los dispositivos administrados.

  Habilitar el proxy de KSN en el lado del punto de distribución

  El servicio de proxy de KSN se ejecuta en el dispositivo que se utiliza como punto de distribución. Utilice esta función para redistribuir y optimizar el tráfico de la red.

  El punto de distribución enviará a Kaspersky las estadísticas de KSN que se enumeran en la declaración de Kaspersky Security Network.

  Esta opción está deshabilitada de forma predeterminada. Esta opción solo se activa si las opciones **Usar Servidor de administración como servidor proxy** y **Acepto utilizar Kaspersky Security Network** están habilitadas en la ventana de propiedades del Servidor de administración.

  Puede asignar un nodo de un clúster activo-pasivo a un punto de distribución y habilitar el servidor proxy de KSN en ese nodo.

  Transmitir las solicitudes para KSN al Servidor de administración

  El punto de distribución envía las solicitudes KSN desde los dispositivos administrados al Servidor de administración.

  Esta opción está activada de forma predeterminada.

  Acceder a KSN Cloud/KPSN directamente a través de Internet

  El punto de distribución envía las solicitudes KSN desde los dispositivos administrados a KSN Cloud o a KPSN. Las solicitudes de KSN generadas en el punto de distribución mismo también se envían directamente a la nube de KSN Cloud o a KPSN.

  No usar el servidor proxy configurado para conectarse a KPSN

  Habilite esta opción, si tiene las configuraciones del servidor proxy configuradas en las propiedades del punto de distribución o en la directiva del Agente de red, pero su arquitectura de red requiere que use KPSN directamente. De lo contrario, las solicitudes de las aplicaciones administradas no podrán llegar a KPSN.

  Esta opción está disponible si selecciona la opción **Acceder a KSN Cloud/KPSN directamente a través de Internet**.

  Puerto

  El número del puerto de TCP que los dispositivos administrados utilizarán para conectarse al Servidor proxy de KSN. El número de puerto predeterminado es 13111.

  Usar puerto UDP

Si necesita que los dispositivos administrados se conecten al servidor proxy de KSN a través de un puerto UDP, active la opción **Usar puerto UDP** y especifique un número de puerto UDP. Esta opción está activada de forma predeterminada.

Puerto UDP

El número del puerto de UDP que los dispositivos administrados utilizarán para conectarse al Servidor proxy de KSN. El puerto UDP predeterminado de conexión al servidor proxy de KSN es 15111.

Usar HTTPS

Si necesita que los dispositivos administrados se conecten al servidor proxy de KSN a través de un puerto HTTPS, habilite la opción **Usar HTTPS** y especifique un número de **HTTPS a través del puerto**. El puerto HTTPS predeterminado de conexión al servidor proxy de KSN es 17111.

Puerto HTTPS

El número del puerto HTTPS que los dispositivos administrados usarán para conectarse al Servidor proxy de KSN. El puerto HTTPS predeterminado de conexión al servidor proxy de KSN es 17111.

- En la sección **Puerta de enlace de conexión**, puede configurar el punto de distribución para que actúe como puerta de enlace para la conexión entre las instancias del Agente de red y el Servidor de administración:

  Puerta de enlace de conexión

  Si no se puede establecer una conexión directa entre el Servidor de administración y los Agentes de red debido a la organización de su red, puede usar el punto de distribución para que actúe como la puerta de enlace de conexión entre el Servidor de administración y los Agentes de red.

  Habilite esta opción si necesita que el punto de distribución actúe como una puerta de enlace de conexión entre los Agentes de red y el Servidor de administración. Esta opción está deshabilitada de forma predeterminada.

  Establecer la conexión a la puerta de enlace de conexión desde el Servidor de administración (si la puerta de enlace está en DMZ)

  Si el Servidor de administración está ubicado fuera de la zona desmilitarizada (DMZ), en la red de área local, los Agentes de red instalados en dispositivos remotos no pueden conectarse al Servidor de administración. Puede usar un punto de distribución como puerta de enlace de conexión con conectividad inversa (el Servidor de administración establece una conexión con el punto de distribución).

  Habilite esta opción si necesita conectar el Servidor de administración a la puerta de enlace de conexión en DMZ.

  Abrir puerto local para Kaspersky Security Center Web Console

  Habilite esta opción si necesita la puerta de enlace de conexión en DMZ a fin de abrir un puerto para Web Console que está en DMZ o en Internet. Especifique el número de puerto que se usará para la conexión de Web Console al punto de distribución. El número de puerto predeterminado es 13299.

  Esta opción está disponible si habilita la opción **Establecer la conexión a la puerta de enlace de conexión desde el Servidor de administración (si la puerta de enlace está en DMZ)**.

  Al conectar dispositivos móviles al Servidor de administración a través del punto de distribución que funciona como puerta de enlace de conexión, puede habilitar las siguientes opciones:

  Abrir puerto para dispositivos móviles (solo autenticación SSL del Servidor de administración)

  Habilite esta opción si necesita que la puerta de enlace de conexión abra un puerto para los dispositivos móviles y especifique el número de puerto que usarán los dispositivos móviles a fin de conectarse con el punto de distribución. El número de puerto predeterminado es 13292. El dispositivo móvil verificará el certificado del Servidor de administración. Al establecer la conexión, solo se autentica el Servidor de administración.

Abrir puerto para dispositivos móviles (autenticación SSL bidireccional)

Habilite esta opción si necesita una puerta de enlace de conexión a fin de abrir un puerto que se usará para la autenticación bidireccional del Servidor de administración y los dispositivos móviles. El dispositivo móvil verificará el certificado del Servidor de administración y el Servidor de administración verificará el certificado para dispositivos móviles. Configure los siguientes ajustes:

- Número de puerto que usarán los dispositivos móviles para conectarse con el punto de distribución. El número de puerto predeterminado es 13293.

- Nombres de dominio DNS de la puerta de enlace de conexión que usarán los dispositivos móviles. Separe los nombres de dominio con comas. Los nombres de dominio especificados se incluirán en el certificado del punto de distribución. Si los nombres de dominio usados por los dispositivos móviles no coinciden con el nombre común en el certificado del punto de distribución, los dispositivos móviles no se conectan al punto de distribución.

  El nombre de dominio DNS predeterminado es el nombre FQDN de la puerta de enlace de conexión.

En ambos casos, los certificados se verifican solo en el punto de distribución al establecer la sesión de TLS. Los certificados no se reenvían para que los verifique el Servidor de administración. Al establecer una sesión de TLS con el dispositivo móvil, el punto de distribución utiliza el certificado del Servidor de administración para crear un túnel a fin de sincronizar el dispositivo móvil y el Servidor de administración. Si abre el puerto para la autenticación bidireccional de SSL, la única forma de distribuir el certificado para dispositivos móviles es a través de un paquete de instalación.

- Configure el sondeo de red de Windows mediante el punto de distribución basado en Windows.

  Dominios de Windows

  Puede habilitar y programar el descubrimiento de dispositivos en los dominios de Windows.

- Configurar el sondeo de controlador de dominio mediante el punto de distribución.

  Sondeo del controlador de dominio

  Puede habilitar el descubrimiento de dispositivos para los controladores de dominio.

  En el campo **Sondeando**, después de cambiar el botón de alternancia a la posición **Habilitado**, puede seleccionar controladores de dominio para el sondeo y también especificar la frecuencia de sondeo para ellos.

  Si utiliza un punto de distribución de Linux, en la sección **Sondear dominios específicos**, haga clic en **Agregar** y luego especifique la dirección y las credenciales de usuario del controlador de dominio. Además, puede especificar el tipo de dominio que se va a sondear: Active Directory o Samba, FreeIPA, ALD Pro.

  Si utiliza un punto de distribución de Windows, puede seleccionar una de las siguientes opciones:

  - **Sondear dominio actual**

  - **Sondear bosque de dominio entero**

  - **Sondear dominios específicos**

- Configure el sondeo de rangos de IP que realizará el punto de distribución.

  Sondeo de intervalos IP

  Puede habilitar el descubrimiento de dispositivos en intervalos IPv4 y en redes IPv6.

  Tras habilitar la opción **Habilitar sondeo de intervalos**, podrá agregar los intervalos que se sondearán y definir una programación para los sondeos. Puede agregar intervalos IP a la lista de los intervalos analizados.

Si habilita la opción **Usar Zeroconf para el sondeo de redes IPv6**, el punto de distribución sondeará la red IPv6 automáticamente utilizando Zeroconf, una *tecnología para crear redes sin configuración*. En ese caso, el punto de distribución sondeará la red completa; el sondeo no estará limitado a los intervalos IP que especifique. La opción **Usar Zeroconf para el sondeo de redes IPv6** está disponible si el punto de distribución ejecuta Linux. Para usar el sondeo de Zeroconf IPv6, debe instalar la utilidad avahi-browse en el punto de distribución.

- En la sección **Avanzado**, especifique la carpeta que el punto de distribución debe utilizar para almacenar los datos distribuidos.

  Usar carpeta predeterminada

  Si selecciona esta opción, la aplicación utilizará la carpeta de instalación del Agente de red en el punto de distribución.

  Usar carpeta especificada

  Si selecciona esta opción, especifique la ruta a la carpeta en el campo que verá debajo. Puede usar una carpeta local del punto de distribución o una carpeta de otro dispositivo conectado a la red corporativa.

  La cuenta de usuario que se utilice para ejecutar el Agente de red en el punto de distribución deberá tener acceso de lectura y escritura a la carpeta especificada.

10. Haga clic en **Aceptar**.

El dispositivo seleccionado se designa como punto de distribución.

Agregar una puerta de enlace de conexión ubicada en una DMZ como punto de distribución

Si el Servidor de administración se encuentra fuera de la zona desmilitarizada (DMZ), los Agentes de red instalados en dispositivos externos no pueden conectarse al Servidor de administración. En este caso, puede utilizar un punto de distribución como puerta de enlace de la conexión en DMZ. El punto de distribución abre un puerto para que el Servidor de administración cree la conexión. Cuando se inicia el Servidor de administración, se conecta a ese punto de distribución y mantiene esta conexión durante toda la sesión.

Si necesita establecer una conexión entre el Servidor de administración y sus dispositivos administrados fuera del período de sincronización entre el Agente de red y el Servidor de administración, debe habilitar un servidor push y abrir el puerto 13295 en el punto de distribución.

Le recomendamos que utilice un dispositivo especialmente asignado como puerta de enlace. Para obtener información sobre la cantidad máxima de dispositivos cliente (incluidos los dispositivos móviles), consulte la Guía de dimensionamiento.

> Una puerta de enlace de conexión no busca conectarse con el Servidor de administración; por el contrario, espera que el Servidor de administración se conecte con ella. Es por esto que, si instala una puerta de enlace de conexión en un dispositivo ubicado en su DMZ, el Servidor de administración no incluirá al dispositivo entre los dispositivos administrados. El problema puede resolverse con un procedimiento especial, que obliga al Servidor de administración a conectarse con la puerta de enlace de conexión.

Para agregar una puerta de enlace de conexión como punto de distribución:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, elija la sección **Puntos de distribución**.

3. Seleccione la opción **Asignar manualmente puntos de distribución**.

4. En la barra de herramientas, haga clic en el botón **Asignar**.

5. En el panel derecho que se abre, haga lo siguiente:

   a. Seleccione la opción **Utilizar pasarela de conexión DMZ por dirección**.

   b. En el campo **Dirección de la puerta de enlace de conexión**, especifique la dirección IP o el nombre DNS del dispositivo.

   c. Haga clic en el botón **Asignar**.

   d. El panel se cierra y el punto de distribución se muestra con el nombre **Entrada temporal para puerta de enlace de conexión**.

6. Haga clic en el botón **Guardar**.

   El Servidor de administración intenta conectarse a la puerta de enlace de conexión en la dirección que especificó. Si tiene éxito, el nombre de la entrada cambia al nombre del dispositivo de puerta de enlace de conexión. El proceso puede tomar hasta cinco minutos.

Si abre las propiedades del punto de distribución haciendo clic en el nombre **Entrada temporal para puerta de enlace de conexión**, todas las opciones aparecerán en gris. Solo puede ver la pestaña General que muestra el nombre del punto de distribución. De manera predeterminada, se utiliza el puerto (13000). Puede configurar el punto de distribución solo después de que el Servidor de administración se conecte a él. Mientras que la entrada temporal para la puerta de enlace de conexión se convierte en una entrada con nombre, la puerta de enlace de conexión también aparece en el grupo Dispositivos no asignados.

Para agregar una puerta de enlace de conexión a una red ya configurada:

1. Instale el Agente de red en el modo de puerta de enlace de conexión.

2. Vuelva a instalar el Agente de red en los dispositivos que desee conectar a la puerta de enlace de conexión recién agregada.

Modificar la lista de puntos de distribución para un grupo de administración

Puede ver la lista de puntos de distribución asignados a un grupo de administración y, si necesita agregar o quitar puntos de distribución, modificarla.

Para ver y modificar la lista de puntos de distribución asignados a un grupo de administración:

1. En el menú principal, vaya a **Administración de activos** → **Dispositivos administrados**.

2. Seleccione un grupo de administración para el que desee ver los puntos de distribución asignados. Para ello, haga clic en el botón **Mostrar jerarquía** en la parte superior de la página y, a continuación, en la ventana que se abre, haga clic en el nombre del grupo que necesite.

   Se habilitará el elemento **Puntos de distribución** en el menú.

Verá la ruta al grupo seleccionado en la parte superior de la página. Si es necesario, en esta ruta puedes hacer clic en un vínculo con el nombre del grupo de administración para ir al grupo. De forma predeterminada, el último vínculo de la ruta se encuentra inactivo.

3. En el menú principal, vaya a **Administración de activos** → **Puntos de distribución**.
4. Para agregar nuevos puntos de distribución para el grupo de administración, haga clic en el botón **Asignar**.
5. Para eliminar los puntos de distribución asignados, seleccione dispositivos de la lista y haga clic en el botón **Desasignar**.

Dependiendo de sus acciones, se agregarán nuevos puntos de distribución a la lista o se quitarán puntos de distribución de la lista.

Habilitación de un servidor push

En Kaspersky Security Center Linux, los puntos de distribución pueden funcionar como servidores push para dispositivos que se administran a través del protocolo móvil y para dispositivos que se administran a través del Agente de red. Por ejemplo, se debe habilitar un servidor push si quiere poder forzar la sincronización de los dispositivos KasperskyOS con el Servidor de administración. Un servidor push tiene el mismo alcance de los dispositivos administrados que el punto de distribución en el que se habilitar el servidor push. Si tiene varios puntos de distribución asignados para el mismo grupo de administración, puede habilitar el servidor push en cada uno de los puntos de distribución. En este caso, el Servidor de administración equilibra la carga entre los puntos de distribución.

Puede utilizar puntos de distribución como servidores push para asegurarse de que haya una conectividad continua entre un dispositivo administrado y el Servidor de administración. Se necesita conectividad continua para algunas operaciones, como ejecutar y detener tareas locales, recibir estadísticas para una aplicación administrada o crear un túnel. Si utiliza un punto de distribución como servidor push, no es necesario utilizar la opción **No desconectar del Servidor de administración** en dispositivos administrados ni enviar paquetes al puerto UDP del Agente de red.

Un servidor push soporta la carga de hasta 50 000 conexiones simultáneas.

Para habilitar un servidor push en un punto de distribución:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.
2. En la pestaña **General**, elija la sección **Puntos de distribución**.
3. Haga clic en el nombre del punto de distribución en el que desea habilitar el servidor push.

   Se abre la ventana de propiedades del punto de distribución.
4. En la sección **General**, habilite la opción **Habilitado**.
5. En el campo **Puerto del servidor push**, escriba el número de puerto. Puede especificar el número de cualquier puerto desocupado.

6. En el campo **Dirección para hosts remotos**, especifique la dirección IP o el nombre del dispositivo del punto de distribución.

7. Haga clic en **Aceptar**.

El servidor push está habilitado en el punto de distribución seleccionado.

Aumento del límite de descriptores de archivos para el servicio klnagent

Si el alcance de un punto de distribución basado en Linux incluye muchos dispositivos, el límite predeterminado de archivos que se pueden abrir (descriptores de archivos) puede no ser suficiente. Para evitar esto, puede aumentar el límite de descriptores de archivos para el servicio klnagent.

Para aumentar el límite de descriptores de archivos para el servicio klnagent:

1. En el dispositivo Linux que actúa como punto de distribución, ejecute el siguiente comando:

   ```
   systemctl edit klnagent64.service
   ```

2. Especifique los límites duros y blandos de los descriptores de archivo en el parámetro `LimitNOFILE` de la sección `[Service]`:

   `LimitNOFILE=<límite de recursos blando>:<límite de recursos duro>`

   Por ejemplo, `LimitNOFILE=32768:131072`. Tenga en cuenta que el límite blando de los descriptores de archivos debe ser menor o igual al límite duro.

3. Ejecute el siguiente comando para asegurarse de que los parámetros se especificaron correctamente:

   ```
   systemd-analyze verify klnagent64.service
   ```

   Si los parámetros se especificaron incorrectamente, este comando puede generar uno de los siguientes errores:

   - `/lib/systemd/system/klnagent64.service:11: Failed to parse resource value, ignoring: 32768:13107`

     Si ve este error, los símbolos de la línea `LimitNOFILE` no están indicados correctamente Debe verificar y corregir la línea ingresada.

   - `/lib/systemd/system/klnagent64.service:11: Soft resource limit chosen higher than hard limit, ignoring: 32768:13107`

     Si se produce este error, el límite blando de los descriptores de archivos que ingresó es mayor que el límite duro. Debe verificar la línea ingresada y asegurarse de que el límite blando de los descriptores de archivos sea menor o igual al límite duro.

4. Ejecute el siguiente comando para volver a cargar el proceso systemd:

   ```
   systemctl daemon-reload
   ```

5. Ejecute el siguiente comando para reiniciar el servicio del Agente de red:

   ```
   systemctl restart klnagent
   ```

6. Ejecute el siguiente comando para asegurarse de que los parámetros especificados se apliquen correctamente:

   `less /proc/<Id de proceso nagent>/limits`

donde el parámetro < `Id de proceso nagent` > es el identificador del proceso del Agente de Red. Puede ejecutar el siguiente comando para obtener el identificador:

```
ps -ax | grep klnagent
```

Para el punto de distribución basado en Linux, se aumenta el límite de archivos que se pueden abrir.

Acerca de los estados de los dispositivos

Kaspersky Security Center Linux le asigna un estado a cada dispositivo administrado. El estado asignado depende de que se cumplan las condiciones definidas por el usuario. En algunos casos, al asignar un estado a un dispositivo, Kaspersky Security Center Linux tiene en cuenta el indicador de visibilidad del dispositivo en la red (consulte la tabla a continuación). Por ejemplo, si a un dispositivo administrado se le asigna el estado *Crítico* por cumplirse la condición *Las bases de datos están desactualizadas*, y luego se activa el indicador de visibilidad para ese dispositivo, el estado del dispositivo cambia a *Sin inconvenientes*. Si Kaspersky Security Center Linux no encuentra un dispositivo en la red en un plazo de dos horas, el indicador de visibilidad del dispositivo se establece en *No visible*.

Los estados son los siguientes:

- *Crítico* o *Crítico/Visible*
- *Advertencia* o *Advertencia/Visible*
- *Sin inconvenientes* o *Sin inconvenientes/Visible*

En la siguiente tabla, se enumeran las condiciones predeterminadas que se deben cumplir para que se asignen los estados *Crítico* o *Advertencia* a un dispositivo, con todos los valores posibles.

Condiciones para que se asigne un estado a un dispositivo

Condición	Descripción de la condición	Valores disponibles
La aplicación de seguridad no está instalada	El Agente de red está instalado en el dispositivo, pero no hay una aplicación de seguridad instalada.	• Interruptor activado. • Interruptor desactivado.
Se detectaron demasiados virus	Una tarea de detección de virus (por ejemplo, la tarea Análisis antimalware) detectó en el dispositivo una cantidad de virus superior al valor especificado.	Más de 0.
El nivel de protección en tiempo real difiere del nivel establecido por el administrador	El dispositivo es visible en la red, pero el nivel de la protección en tiempo real no se corresponde con el que el administrador configuró (en la condición) para el estado del dispositivo.	• Detenida. • Suspendida. • En ejecución.
No se ha realizado un análisis antimalware en mucho tiempo	El dispositivo está visible en la red y tiene instalada una aplicación de seguridad, pero la tarea *Análisis antimalware* no se ha ejecutado en el intervalo de tiempo especificado. Esta condición se aplica solo a los dispositivos que se agregaron al menos siete días antes a la base de datos del Servidor de administración.	Más de 1 día.
Las bases de datos están desactualizadas	El dispositivo es visible en la red y tiene instalada una aplicación de seguridad, pero sus bases de datos antivirus no se han actualizado en el período de tiempo especificado. Esta condición se aplica solo a los dispositivos que se agregaron al menos un día antes a la base de datos del Servidor de administración.	Más de 1 día.
Sin conexión desde hace mucho tiempo	El Agente de red está instalado en el dispositivo, pero el dispositivo está apagado y no se ha conectado a un Servidor de administración durante el período de tiempo especificado.	Más de 1 día.
Se han detectado amenazas activas	El número de objetos no procesados en la carpeta **Amenazas activas** supera el valor especificado.	Más de 0 elementos.

Condición	Descripción de la condición	Valores disponibles
Tiempo requerido desde el reinicio	El dispositivo está visible en la red, pero una aplicación requirió un reinicio durante más tiempo que el intervalo de tiempo especificado.	Más de 0 minutos.
Motivo del reinicio	El dispositivo está visible en la red, pero una aplicación requiere un reinicio del dispositivo por uno de los motivos seleccionados.	• Motivo desconocido • La aplicación no se ejecutará hasta que se reinicie el equipo • Se debe reiniciar el dispositivo para completar la actualización que está ejecutando la aplicación • Se requiere reiniciar para iniciar la actualización • Se debe reiniciar el dispositivo para completar el análisis o la desinfección • Se requiere reiniciar para completar la instalación o la desinstalación remotas • Completando cifrado de datos en disco
Hay aplicaciones incompatibles instaladas	El dispositivo es visible en la red, pero, al hacer un inventario de software a través del Agente de red, se detectaron aplicaciones incompatibles instaladas en el dispositivo.	• Interruptor desactivado. • Interruptor activado.
Se detectaron vulnerabilidades de software	El dispositivo es visible en la red y tiene instalado el Agente de red, pero la tarea *Buscar vulnerabilidades y actualizaciones requeridas* ha encontrado aplicaciones instaladas en el dispositivo que tienen vulnerabilidades con el nivel de gravedad especificado.	• Crítico • Alto. • Medio. • Ignorar si la vulnerabilidad no se puede reparar. • Ignorar si hay una actualización asignada para instalarse.
Licencia caducada	El dispositivo es visible en la red, pero la licencia ha caducado.	• Interruptor desactivado. • Interruptor activado.
La licencia está por caducar	El dispositivo es visible en la red, pero la licencia instalada en el mismo caduca en menos días que el número de días especificado.	Más de 0 días.

Condición	Descripción de la condición	Valores disponibles
La búsqueda de actualizaciones de Windows Update no se ha realizado en mucho tiempo	El dispositivo es visible en la red, pero la tarea *Buscar vulnerabilidades y actualizaciones requeridas* no se ejecutó durante el intervalo de tiempo especificado.	Más de 1 día.
Estado de cifrado no válido	El Agente de red está instalado en el dispositivo, pero el resultado del cifrado del dispositivo es igual al valor especificado.	• No cumple con la directiva porque el usuario no dio su consentimiento (solo para dispositivos externos). • No cumple con la directiva debido a un error. • Se debe reiniciar el dispositivo al aplicar la directiva. • No se ha especificado una directiva de cifrado. • No compatible. • Al aplicar la directiva.
La configuración del dispositivo móvil no cumple con la directiva	Los ajustes del dispositivo móvil no son los que se encontraron en la directiva de Kaspersky Endpoint Security para Android durante el chequeo de reglas de cumplimiento normativo.	• Interruptor desactivado. • Interruptor activado.
Problemas de seguridad no procesados detectados	Se han encontrado problemas de seguridad sin procesar en el dispositivo. Los problemas de seguridad se pueden crear manualmente por el administrador o automáticamente por las aplicaciones de Kaspersky administradas que se han instalado en el dispositivo cliente.	• Interruptor desactivado. • Interruptor activado.
Estado del dispositivo definido por la aplicación	El estado del dispositivo es definido por la aplicación administrada. Los dispositivos administrados pueden tener un estado definido por las aplicaciones administradas independientemente de la configuración de Kaspersky Security Center Linux. Después de que este estado devuelve uno de los estados definidos por Kaspersky Security Center Linux, el Servidor de administración asigna a un dispositivo administrado el estado más crítico de los devueltos por la aplicación administrada y asignados por el Servidor de administración. Los estados definidos por la administración de aplicaciones tienen descripciones transferidas por las aplicaciones administradas. Puede ver las descripciones en la lista de dispositivos administrados, en la columna **Descripción del estado**.	• Interruptor desactivado. • Interruptor activado.
El dispositivo no tiene espacio en el disco	El espacio libre en el disco del dispositivo es inferior al valor especificado o el dispositivo no se pudo sincronizar con el Servidor de administración. Los estados *Crítico* o *Advertencia* cambiarán por el estado *Sin inconvenientes* cuando el dispositivo se sincronice correctamente con el Servidor de administración y el espacio libre en el dispositivo supere o iguale el valor especificado.	Más de 0 MB.
El dispositivo ha cambiado a no administrado	Durante el descubrimiento de dispositivos, el dispositivo se reconoció como visible en la red, pero hubo más de tres intentos de sincronizar el dispositivo con el Servidor de administración que terminaron con un error.	• Interruptor desactivado. • Interruptor activado.
Protección deshabilitada	El dispositivo es visible en la red, pero la aplicación de seguridad del dispositivo ha estado deshabilitada por un tiempo superior al especificado. En este caso, el estado de la aplicación de seguridad es *detenida* o *error*, y difiere del siguiente: *iniciada*, *en ejecución* o *suspendida*.	Más de 0 minutos.
La aplicación de seguridad no está en ejecución	El dispositivo es visible en la red y tiene instalada una aplicación de seguridad, pero esa aplicación no se está ejecutando.	• Interruptor desactivado. • Interruptor activado.

Kaspersky Security Center Linux permite que usted configure la conmutación automática del estado de un dispositivo en un grupo de administración cuando las condiciones especificadas se cumplen. El estado del dispositivo cliente puede hacerse pasar a *Crítico* o *Advertencia* si se cumplen las condiciones especificadas. Si no se cumplen estas condiciones, el dispositivo cliente toma el estado *Sin inconvenientes*.

Cada estado puede corresponderse con distintos valores de una misma condición. De forma predeterminada, por ejemplo, cuando la condición **Las bases de datos están desactualizadas** tiene el valor **Más de 3 días**, se asigna el estado *Advertencia* al dispositivo cliente; si el valor es **Más de 7 días**, se asigna el estado *Crítico*.

Si actualiza Kaspersky Security Center Linux desde la versión anterior, los valores de la condición **Las bases de datos están desactualizadas** para asignar el estado a *Crítico* o *Advertencia* no cambian.

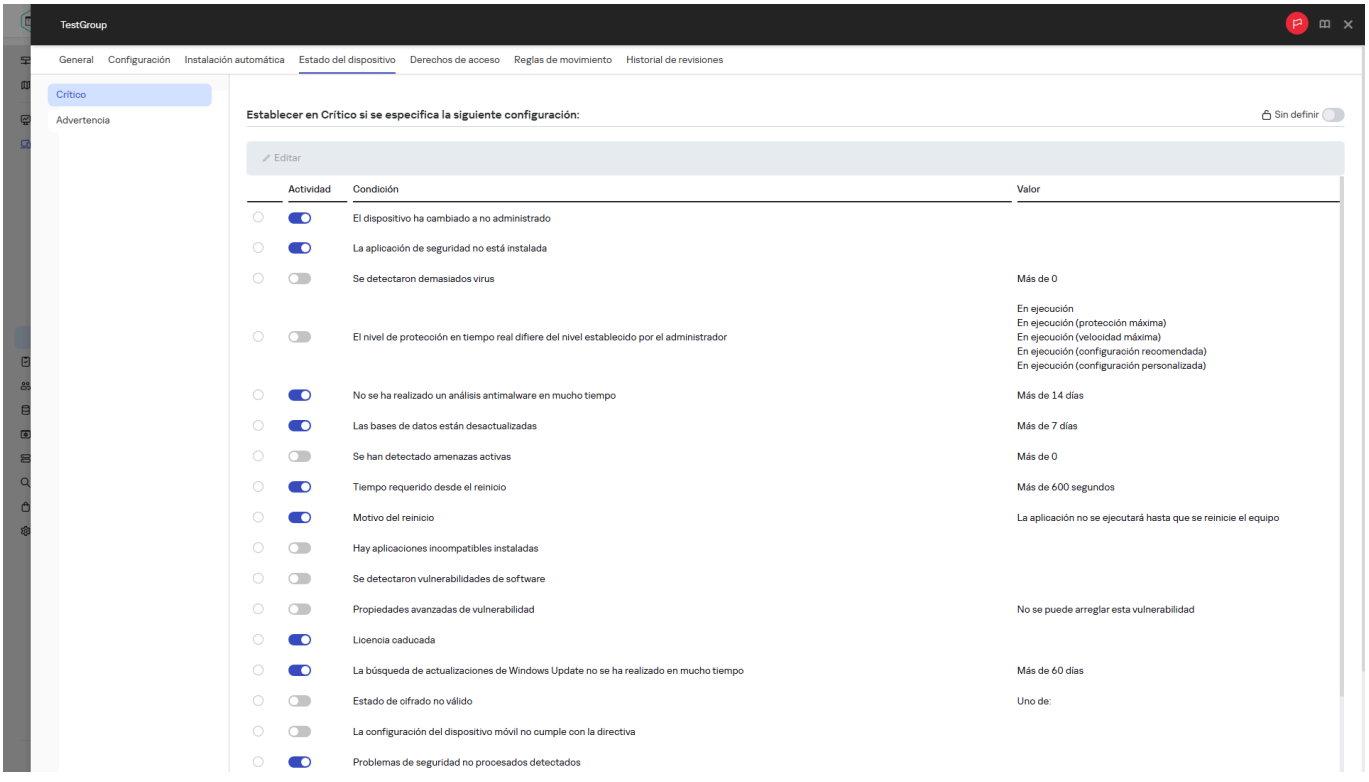
Configurar cambios de estado para los dispositivos

Puede cambiar las condiciones bajo las cuales se le asignan los estados *Crítico* o *Advertencia* a un dispositivo.

Para habilitar el cambio de estado a Crítico para los dispositivos:

1. En el menú principal, vaya a **Administración de activos** → **Jerarquía de grupos**.
2. Realice una de las siguientes acciones a fin de visualizar las propiedades del grupo de administración para el que desee cambiar el estado del dispositivo:
   - Haga clic en el nombre del grupo de administración.
   - Haga clic en el botón **Mostrar jerarquía** en la parte superior de la página. En el panel de navegación que se abre, coloque el cursor sobre el nombre del grupo que necesite y luego haga clic en el ícono de configuración (⚙).

   Se abrirá la ventana de propiedades del grupo de administración.
3. En la ventana de las propiedades, seleccione la pestaña **Estado del dispositivo**.
4. En el panel izquierdo, seleccione **Crítico**.
5. En el panel derecho, en la sección **Establecer en Crítico si se especifica la siguiente configuración**, habilite la condición bajo la cual el estado de un dispositivo cambiará a *Crítico*.



Solo podrá modificar los ajustes que no estén bloqueados en la directiva primaria.

6. En la lista, seleccione el botón de opción ubicado junto a la condición.
7. En la esquina superior izquierda de la lista, haga clic en el botón **Editar**.
8. Configure el valor necesario para la condición seleccionada.

   No es posible configurar valores para todas las condiciones.
9. Haga clic en **Aceptar**.
10. Haga clic en **Guardar** para guardar los cambios.

Cuando se cumplan las condiciones especificadas, se asignará el estado *Crítico* al dispositivo administrado.

Para habilitar el cambio de estado a Advertencia para los dispositivos:

1. En el menú principal, vaya a **Administración de activos** → **Jerarquía de grupos**.
2. En la lista de grupos que se abre, haga clic en el vínculo con el nombre del grupo que contenga los dispositivos para los que desee modificar el cambio de estado.
3. En la ventana de las propiedades que se abre, seleccione la pestaña **Estado del dispositivo**.
4. En el panel izquierdo, seleccione **Advertencia**.
5. En el panel derecho, en la sección **Establecer en Advertencia si se especifica la siguiente configuración**, habilite la condición que hará que el estado de un dispositivo cambie a *Advertencia*.

   Solo podrá modificar los ajustes que no estén bloqueados en la directiva primaria.
6. En la lista, seleccione el botón de opción ubicado junto a la condición.
7. En la esquina superior izquierda de la lista, haga clic en el botón **Editar**.
8. Configure el valor necesario para la condición seleccionada.

   No es posible configurar valores para todas las condiciones.
9. Haga clic en **Aceptar**.
10. Haga clic en **Guardar** para guardar los cambios.

Cuando se cumplan las condiciones especificadas, se asignará el estado *Advertencia* al dispositivo administrado.

Selecciones de dispositivos

Las *selecciones de dispositivos* son una herramienta para filtrar dispositivos de acuerdo con condiciones específicas. Puede usar selecciones de dispositivos para administrar varios dispositivos a la vez y, por ejemplo, moverlos de un grupo a otro o ver un informe que trate únicamente sobre ellos.

Kaspersky Security Center Linux ofrece una amplia gama de *selecciones predefinidas* (por ejemplo, **Dispositivos con estado Crítico**, **Protección deshabilitada** y **Se han detectado amenazas activas**). Las selecciones predefinidas no se pueden eliminar. De ser necesario, puede crear y configurar selecciones adicionales, llamadas *selecciones definidas por el usuario*.

En una selección definida por el usuario, se puede determinar el alcance de la búsqueda y seleccionar todos los dispositivos, los dispositivos administrados o los dispositivos no asignados. Los parámetros de búsqueda se especifican en las condiciones. Una selección de dispositivos puede tener varias condiciones con diferentes parámetros de búsqueda. Puede, por ejemplo, crear dos condiciones y especificar intervalos IP diferentes en cada una de ellas. Una selección con varias condiciones muestra los dispositivos que cumplen con cualquiera de esas condiciones. Por el contrario, los parámetros de búsqueda especificados en una condición se superponen. Si una condición especifica tanto un intervalo IP como el nombre de una aplicación instalada, se mostrarán únicamente los dispositivos que tengan asignada una dirección IP de ese intervalo y que tengan instalada esa aplicación.

Ver la lista de dispositivos de una selección de dispositivos

Kaspersky Security Center Linux le permite ver la lista de dispositivos desde una selección de dispositivos.

Para ver la lista de dispositivos de una selección de dispositivos:

1. En el menú principal, vaya a las secciones **Administración de activos** → **Selecciones de dispositivos** o **Descubrimiento y despliegue** → **Selecciones de dispositivos**.
2. En la lista de selecciones, haga clic en el nombre de la selección de dispositivos.

   La página muestra una tabla con información sobre los dispositivos incluidos en la selección de dispositivos.
3. Puede hacer lo siguiente para agrupar y filtrar los datos que conforman la tabla de dispositivos:
   - Haga clic en el ícono de configuración (⚙) y seleccione las columnas que se deban mostrar en la tabla.
   - Haga clic en el ícono de filtro (▽) y, en el menú que se abrirá, defina el criterio de filtrado.

     Se mostrará la tabla de dispositivos filtrada.

También puede ejecutar tareas para selecciones de dispositivos. Para ello, seleccione uno o varios dispositivos, haga clic en el botón **Ejecutar tarea** y seleccione **Crear tarea** para crear una tarea que se aplique a estos dispositivos, o **Aplicar tarea existente**.

Para mover los dispositivos seleccionados de la selección de dispositivos a otro grupo de administración, haga clic en el botón **Mover a un grupo** y luego seleccione el grupo de administración de destino.

Crear una selección de dispositivos

Para crear una selección de dispositivos:

1. En el menú principal, vaya a **Administración de activos** → **Selecciones de dispositivos**.

   Se muestra una página con una lista de selecciones de dispositivos.
2. Haga clic en **Agregar**.

   Se abre la ventana **Configuración de la selección de dispositivos**.
3. Escriba el nombre de la nueva selección.

4. Especifique el grupo que contiene los dispositivos que desea incluir en la selección de dispositivos:

   - **Buscar cualquier dispositivo**: Buscar dispositivos que cumplan con los criterios de selección y que estén incluidos en el grupo **Dispositivos administrados** o **Dispositivos no asignados**.
   - **Buscar dispositivos administrados**: Buscar dispositivos que cumplan con los criterios de selección y que estén incluidos en el grupo **Dispositivos administrados**.
   - **Buscar dispositivos no asignados**: Buscar dispositivos que cumplan con los criterios de selección y que estén incluidos en el grupo **Dispositivos no asignados**.

   Puede habilitar la casilla de verificación **Incluir datos de Servidores de administración secundarios** para habilitar la búsqueda de dispositivos que cumplan con los criterios de selección y que estén administrados por Servidores de administración secundarios.

5. Haga clic en **Agregar**.
6. En la ventana que se abre, especifique las condiciones que deben cumplirse para incluir los dispositivos en esta selección y, a continuación, haga clic en el botón **Guardar**.
7. Haga clic en el botón **Guardar**.

La selección de dispositivos se crea y se agrega a la lista de selecciones de dispositivos.

Configurar una selección de dispositivos

Para configurar una selección de dispositivos:

1. En el menú principal, vaya a **Administración de activos** → **Selecciones de dispositivos**.

   Se muestra una página con una lista de selecciones de dispositivos.
2. Elija la selección de dispositivos definida por el usuario pertinente y haga clic en el botón **Propiedades**.

   Se abre la ventana **Configuración de la selección de dispositivos**.
3. En la pestaña **General**, haga clic en el vínculo **Nueva condición**.
4. Especifique las condiciones que deban cumplirse para que un dispositivo se incluya o no en la selección.
5. Haga clic en el botón **Guardar**.

El cambio se aplica y se guarda.

A continuación, se presentan descripciones de las condiciones para asignar dispositivos a una selección. Las condiciones se combinan usando el operador lógico OR: la selección incluirá dispositivos que cumplan con, al menos, una de las condiciones de la lista.

General

En la sección **General**, puede cambiar el nombre de una condición de la selección y especificar si esa condición se debería invertir:

Invertir condición de selección

Esta opción está deshabilitada de forma predeterminada.

Si habilita esta opción, la condición elegida se aplicará a la inversa. La selección incluirá todos los dispositivos que no cumplan con la condición.

El siguiente ejemplo muestra la lógica del trabajo de inversión:

- **Condición**: en su dispositivo, hay un sistema operativo de tipo Linux y con número de compilación 00.0.000.
- **Condición invertida**: en su dispositivo, existe un sistema operativo con NOT (el tipo Linux y el número de compilación 00.0.000), lo que es equivalente a lo siguiente:

  Hay un sistema operativo con el tipo NOT Linux O el número de compilación NOT 00.0.000.

Por lo tanto, la selección incluirá los dispositivos con un sistema operativo, por ejemplo, del tipo Windows y el número de compilación 00.0.000, o del tipo Linux y cualquier número de compilación que no sea 00.0.000.

Infraestructura de red

En la sección **Red**, puede especificar los criterios que serán usados para incluir dispositivos en la selección según sus datos de la red:

Nombre del dispositivo

Nombre de red de Windows (nombre NetBIOS) del dispositivo, o la dirección IPv4 o IPv6.

Dominio

Muestra todos los dispositivos incluidos en el grupo de trabajo especificado.

Grupo de administración

Muestra los dispositivos incluidos en el grupo de administración especificado.

Descripción

Texto ubicado en el campo **Descripción** de la sección **General** dentro de la ventana de propiedades del dispositivo.

Para describir el texto del campo **Descripción**, puede utilizar los siguientes caracteres:

- Dentro de una palabra:
  - *****. Sustituye una cadena de cualquier largo (es decir, con cualquier número de caracteres).

    Ejemplo:

    Para describir palabras como **Servidor** o **Servidores**, puede ingresar **Servidor***.
  - **?.** Sustituye un carácter individual.

    Ejemplo:

    Para describir frases como **SUSE Linux Enterprise Server 12** o **SUSE Linux Enterprise Server 15**, puede ingresar **SUSE Linux Enterprise Server 1?**.

    La consulta no puede comenzar con un asterisco (*****) ni con un signo de interrogación (**?**).

- Para encontrar varias palabras:
  - Espacio. Muestra todos los dispositivos que tienen, en su descripción, alguna de las palabras indicadas.

  Ejemplo:

  Para encontrar una frase que contenga las palabras **secundario** o **virtual**, puede incluir la expresión **secundario virtual** en la consulta.

  - **+**. Si agrega el signo + antes de una palabra, todos los resultados de búsqueda contendrán esa palabra.

  Ejemplo:

  Para encontrar una frase que contenga las palabras **secundario** y **virtual**, ingrese la consulta **+secundario+virtual**.

  - **-**. Si agrega el signo - antes de una palabra, ningún resultado de búsqueda contendrá esa palabra.

  Ejemplo:

  Para encontrar una frase que contenga **secundario** y no contenga **virtual**, ingrese la consulta **+secundario-virtual**.

  - **"<cadena>"**. El texto que se ingresa entre comillas debe estar presente en el texto.

  Ejemplo:

  Para encontrar una frase que contenga la combinación de palabras **servidor secundario**, puede ingresar **"servidor secundario"** en la consulta.

Intervalo IP

Si habilita esta opción, podrá ingresar las direcciones IP inicial y final del intervalo IP en el que deberán estar incluidos los dispositivos pertinentes.

Esta opción está deshabilitada de forma predeterminada.

Administrado por un Servidor de administración diferente

Seleccione uno de los siguientes valores:

- **Sí**. Una regla de movimiento de dispositivos solo se aplica a los dispositivos cliente administrados por otros Servidores de administración. Estos servidores son diferentes del servidor en el que configura la regla de movimiento de dispositivos.
- **No**. La regla de movimiento de dispositivos solo se aplica a los dispositivos cliente administrados por el Servidor de administración actual.
- **Ningún valor seleccionado**. La condición no se aplica.

En la sección **Controlador de dominio**, puede configurar criterios para incluir dispositivos en una selección según la suscripción de dominio:

El dispositivo se encuentra en una unidad organizativa de dominio

Si habilita esta opción, la selección incluirá los dispositivos de la unidad organizativa del dominio especificada en el campo de entrada.

Esta opción está deshabilitada de forma predeterminada.

El dispositivo es miembro del grupo de seguridad de dominio

Si habilita esta opción, la selección incluirá los dispositivos que pertenezcan al grupo de seguridad de dominio especificado en el campo de entrada.

Esta opción está deshabilitada de forma predeterminada.

En la sección **Actividad de red**, puede establecer los criterios que se usarán para incluir dispositivos en la selección basándose en la actividad de red de los mismos:

Actúa como punto de distribución

En la lista desplegable, puede establecer el criterio que se usará para incluir dispositivos en la selección cuando se realice la búsqueda:

- **Sí**. La selección incluirá dispositivos que funcionen como punto de distribución.
- **No**. La selección no incluirá dispositivos que funcionen como punto de distribución.
- **Ningún valor seleccionado**. El criterio no se aplicará.

No desconectar del Servidor de administración

En la lista desplegable, puede establecer el criterio que se usará para incluir dispositivos en la selección cuando se realice la búsqueda:

- **Habilitado**. La selección incluirá dispositivos en los que esté activada la casilla **No desconectar del Servidor de administración**.
- **Deshabilitado**. La selección incluirá dispositivos en los que no esté activada la casilla **No desconectar del Servidor de administración**.
- **Ningún valor seleccionado**. El criterio no se aplicará.

Perfil de conexión cambiado

En la lista desplegable, puede establecer el criterio que se usará para incluir dispositivos en la selección cuando se realice la búsqueda:

- **Sí**. La selección incluirá dispositivos que se hayan conectado al Servidor de administración tras un cambio de perfil de conexión.
- **No**. La selección no incluirá dispositivos que se hayan conectado al Servidor de administración tras un cambio de perfil de conexión.
- **Ningún valor seleccionado**. El criterio no se aplicará.

Última conexión con el Servidor de administración

Puede utilizar esta casilla para establecer un criterio de búsqueda de dispositivos que se base en el momento en el que haya ocurrido la última conexión al Servidor de administración.

Si activa esta casilla, podrá usar los campos de entrada para indicar el intervalo de tiempo (fecha y hora) en el que deberá haber ocurrido la última conexión entre el Agente de red instalado en el dispositivo cliente y el Servidor de administración. La selección incluirá aquellos dispositivos que estén alcanzados por el intervalo especificado.

Si no activa esta casilla, no se aplicará este criterio.

Esta casilla está desactivada por defecto.

Nuevos dispositivos detectados por sondeo de red

Utilice esta opción para buscar dispositivos nuevos, que se hayan detectado durante los sondeos de red realizados en días recientes.

Si habilita esta opción, la selección incluirá solo aquellos dispositivos nuevos que se hayan detectado mediante el descubrimiento de dispositivos en el intervalo de días especificado en el campo **Periodo de detección (días)**.

Si deshabilita esta opción, la selección incluirá todos los dispositivos detectados por el mecanismo de descubrimiento.

Esta opción está deshabilitada de forma predeterminada.

Dispositivo visible

En la lista desplegable, puede establecer el criterio que se usará para incluir dispositivos en la selección cuando se realice la búsqueda:

- **Sí**. La selección incluirá aquellos dispositivos que sean visibles en la red.
- **No**. La selección incluirá aquellos dispositivos que no sean visibles en la red.
- **Ningún valor seleccionado**. El criterio no se aplicará.

Estados de los dispositivos

En la sección **Estado del dispositivo administrado**, puede configurar criterios para incluir dispositivos en una selección según la descripción del estado de dispositivos desde una aplicación administrada:

Estado del dispositivo

Lista desplegable en la que puede seleccionar un estado de dispositivo: *Aceptar*, *Crítico* o *Advertencia*.

Estado de protección en tiempo real

Lista desplegable en la cual puede seleccionar el estado de la protección en tiempo real. La selección incluirá aquellos dispositivos que tengan el estado de protección en tiempo real indicado.

Descripción del estado del dispositivo

En este campo, puede activar casillas correspondientes a condiciones que, al cumplirse, hacen que el dispositivo tome uno de los siguientes estados: *Aceptar, Crítico* o *Advertencia*.

En la sección **Estado de componentes en aplicaciones administradas**, puede configurar los criterios para incluir dispositivos en una selección según los estados de los componentes de las aplicaciones administradas:

Estado de Prevención de fugas de datos

Buscar dispositivos basándose en el estado de Prevención de fuga de datos (*Desconocido, Detenida, Iniciándose, En pausa, En ejecución, Error*).

Estado de protección de los servidores de colaboración

Buscar dispositivos basándose en el estado de la protección para servidores de colaboración (*Desconocido*, *Detenida*, *Iniciándose, En pausa*, *En ejecución*, *Error*).

Estado de protección antivirus en servidores de correo

Buscar dispositivos basándose en el estado de la protección para servidores de correo (*Desconocido, Detenida, Iniciándose, En pausa, En ejecución, Error).*

Estado de Sensor de Endpoint

Buscar dispositivos basándose en el estado del componente Sensor de Endpoint (*Desconocido, Detenida, Iniciándose, En pausa, En ejecución, Error*).

En la sección **Problemas que afectan al estado en las aplicaciones administradas**, puede especificar los criterios que se utilizarán para incluir dispositivos en la selección de acuerdo con la lista de posibles problemas detectados por una aplicación administrada. Si un dispositivo tiene al menos uno de los problemas elegidos, ese dispositivo se incluirá en la selección. Cuando selecciona un problema listado para varias aplicaciones, tiene la opción de seleccionar este problema en todas las listas automáticamente.

Puede activar casillas correspondientes a las descripciones de estado reportadas por la aplicación administrada. Cuando se reciban esos estados, los dispositivos correspondientes se incluirán en la selección. Si elige un estado incluido en las listas de varias aplicaciones, tendrá la opción de seleccionar todos los casos automáticamente.

Datos del sistema

En la sección **SO**, puede especificar los criterios que serán usados para incluir dispositivos en la selección según el tipo de sistema operativo.

Tipo de plataforma

Si activa esta casilla, podrá seleccionar un sistema operativo de la lista. Los dispositivos que tengan instalado ese sistema operativo se incluirán en los resultados de búsqueda.

Versión del paquete de servicios del SO

En este campo, puede especificar la versión del paquete de su sistema operativo (en formato *X.Y*), que determinará cómo aplicar la regla de migración a su dispositivo. De manera predeterminada, no hay una versión definida.

Arquitectura del SO

En la lista desplegable, puede seleccionar la arquitectura para la que deberá estar diseñado el sistema operativo. Los valores posibles son **Desconocido**, **x86**, **AMD64** e **IA64**. La arquitectura que elija determinará el modo de aplicar la regla de movimiento al dispositivo. De manera predeterminada, no hay ninguna opción seleccionada en la lista (es decir, la arquitectura del sistema operativo no está definida).

Compilación del SO

> Este parámetro solo es válido para sistemas operativos Windows.

Número de compilación del sistema operativo. Puede especificar si el sistema operativo seleccionado debe tener un número de versión igual, anterior o posterior. También puede hacer que la búsqueda incluya todos los números de compilación, excepto el especificado.

Número de versión del SO

> Este parámetro solo es válido para sistemas operativos Windows.

Identificador de versión del sistema operativo. Puede indicar si el sistema operativo seleccionado deberá tener un id. de versión igual, anterior o posterior al valor introducido. También puede hacer que la búsqueda incluya todos los id. de versión, excepto el especificado.

En la sección **Máquinas virtuales**, puede configurar los criterios que se usarán para incluir dispositivos en la selección basándose en el hecho de que sean máquinas virtuales o de que formen parte de una infraestructura de escritorios virtuales (VDI):

Esta es una máquina virtual

En la lista desplegable puede seleccionar las siguientes opciones:

- **Sin definir**.
- **No**. Buscar dispositivos que no sean máquinas virtuales.
- **Sí**. Buscar dispositivos que sean máquinas virtuales.

Tipo de máquina virtual

En la lista desplegable, puede seleccionar el desarrollador de la máquina virtual.

Esta lista desplegable estará disponible si seleccionó los valores **Sí** o **No es importante** en la lista desplegable **Es una máquina virtual**.

Parte de la infraestructura de escritorio virtual

En la lista desplegable puede seleccionar las siguientes opciones:

- **Sin definir**.
- **No**. Buscar dispositivos que no sean parte de la Infraestructura de escritorio virtual.
- **Sí**. Buscar dispositivos que sean parte de una VDI.

En la sección **Registro de hardware**, puede configurar criterios para incluir dispositivos en una selección según el hardware que tengan instalado:

Asegúrese de que la utilidad lshw esté instalada en los dispositivos Linux desde los que desea obtener detalles del hardware. Los detalles de hardware obtenidos de las máquinas virtuales pueden estar incompletos según el hipervisor que se utilice.

Dispositivo

En la lista desplegable, puede seleccionar un tipo de unidad. Los dispositivos que tengan la unidad seleccionada se incluirán en los resultados de búsqueda.

El campo permite realizar búsquedas de texto completo.

Proveedor

En la lista desplegable, puede seleccionar el nombre del fabricante de la unidad. Los dispositivos que tengan la unidad seleccionada se incluirán en los resultados de búsqueda.

El campo permite realizar búsquedas de texto completo.

Nombre del dispositivo

El dispositivo con el nombre especificado se incluirá en la selección.

Descripción

Descripción del dispositivo o unidad de hardware. Los dispositivos que tengan la descripción indicada en este campo se incluirán en la selección.

Si desea agregar una descripción a un dispositivo, puede hacerlo (en cualquier formato) a través de la ventana de propiedades del mismo. El campo permite realizar búsquedas de texto completo.

Proveedor del dispositivo

Nombre del fabricante del dispositivo. Los dispositivos producidos por el fabricante especificado en este campo se incluyen en la selección.

Puede ingresar el nombre del fabricante en la ventana de propiedades de un dispositivo.

Número de serie

Todas las unidades de hardware con el número de serie especificado en este campo se incluirán en la selección.

Número de inventario

Los equipos que tengan el número de inventario indicado en este campo se incluirán en la selección.

Usuario

Todas las unidades de hardware del usuario especificado en este campo se incluirán en la selección.

Ubicación

Ubicación de un dispositivo o una unidad de hardware (por ejemplo, en la sede central o en una sucursal). Las computadoras o dispositivos que se encuentren en la ubicación especificada en este campo se incluirán en la selección.

Puede describir la ubicación de un dispositivo en cualquier formato en la ventana de propiedades de dicho dispositivo.

Velocidad de reloj de la CPU, en MHz, desde

La frecuencia de reloj mínima de una CPU. Los equipos cuyas CPU coincidan con los intervalos especificados en estos campos de entrada (inclusive) se incluirán en la selección.

Velocidad de reloj de la CPU, en MHz, hasta

Intervalo de frecuencias de una CPU. Los equipos cuyas CPU coincidan con los intervalos especificados en estos campos de entrada (inclusive) se incluirán en la selección.

Número de núcleos de CPU virtuales, desde

El número mínimo de núcleos de CPU virtuales. Los equipos cuyas CPU coincidan con los intervalos de núcleos virtuales especificados en estos campos de entrada (inclusive) se incluirán en la selección.

Número de núcleos de CPU virtuales, a

El número máximo de núcleos de CPU virtuales. Los equipos cuyas CPU coincidan con los intervalos de núcleos virtuales especificados en estos campos de entrada (inclusive) se incluirán en la selección.

Volumen del disco duro, en GB, desde

El volumen mínimo del disco duro en el dispositivo. Los equipos cuyos discos duros coincidan con los intervalos especificados en estos campos de entrada (inclusive) se incluirán en la selección.

Volumen de disco duro, en GB, hasta

El volumen máximo del disco duro en el dispositivo. Los equipos cuyos discos duros coincidan con los intervalos especificados en estos campos de entrada (inclusive) se incluirán en la selección.

Tamaño de RAM, en MB, desde

El tamaño mínimo de la memoria RAM del dispositivo. Los dispositivos cuya RAM coincida con el intervalo de valores especificado en los campos de entrada (inclusive) se incluyen en la selección.

Tamaño de RAM, en MB, hasta

El tamaño máximo de la memoria RAM del dispositivo. Los dispositivos cuya RAM coincida con el intervalo de valores especificado en los campos de entrada (inclusive) se incluyen en la selección.

Detalles de software de terceros

En la sección **Registro de aplicaciones**, puede configurar los criterios para buscar dispositivos según aplicaciones instaladas en ellos:

Nombre de la aplicación

Lista desplegable en la que puede seleccionar una aplicación. Los dispositivos que tengan instalada la aplicación elegida se incluirán en la selección.

Versión de la aplicación

Campo de entrada en el que puede especificar la versión de la aplicación seleccionada.

Proveedor

Lista desplegable en la que puede seleccionar el desarrollador de una aplicación instalada en el dispositivo.

Estado de la aplicación

Lista desplegable en la que puede seleccionar el estado de la aplicación (*Instalada*, *Sin instalar*). Se incluirán en la selección los dispositivos que tengan o no tengan (dependiendo del estado seleccionado) la aplicación seleccionada.

Buscar por actualización

Si habilita esta opción, la búsqueda se basará en los detalles de las actualizaciones para el software instalado en los dispositivos pertinentes. Una vez que active esta casilla, los campos **Nombre de la aplicación**, **Versión de la aplicación** y **Estado de la aplicación** cambiarán a **Nombre de actualización**, **Versión de actualización** y **Estado**, respectivamente.

Esta opción está deshabilitada de forma predeterminada.

Nombre de la aplicación de seguridad incompatible

Lista desplegable en la que puede seleccionar aplicaciones de seguridad de terceros. Los dispositivos que tengan instalada la aplicación seleccionada serán incluidos en la selección cuando se realice la búsqueda.

Etiqueta de aplicación

Lista desplegable en la que puede seleccionar una etiqueta de aplicación. Se incluirán en la selección aquellos dispositivos que tengan instaladas aplicaciones que, en su descripción, contengan la etiqueta seleccionada.

Aplicar a los dispositivos que no tengan las etiquetas especificadas

Si habilita esta opción, la selección incluirá aquellos dispositivos que no contengan ninguna de las etiquetas seleccionadas en su descripción.

Si deshabilita esta opción, no se aplicará el criterio.

Esta opción está deshabilitada de forma predeterminada.

En la sección **Vulnerabilidades y actualizaciones**, puede especificar los criterios que se usarán para incluir dispositivos en la selección basándose en el origen de Windows Update que utilicen:

WUA está ahora conectado al Servidor de administración

En la lista desplegable, puede seleccionar una de las siguientes opciones de búsqueda:

- **Sí**. Si selecciona esta opción, los resultados de búsqueda incluirán aquellos dispositivos que reciban sus actualizaciones de Windows Update del Servidor de administración.
- **No**. Si selecciona esta opción, los resultados incluirán aquellos dispositivos que reciban sus actualizaciones de Windows Update de cualquier otro origen.

Detalles de las aplicaciones de Kaspersky

En la sección **Aplicaciones de Kaspersky**, puede configurar criterios para incluir dispositivos en una selección según la aplicación administrada seleccionada:

Nombre de la aplicación

En la lista desplegable, puede definir un criterio para incluir dispositivos en la selección cuando se realice una basada en el nombre de una aplicación de Kaspersky.

La lista solo contendrá los nombres de aquellas aplicaciones que tengan su respectivo complemento de administración instalado en la estación de trabajo del administrador.

Si no selecciona ninguna aplicación, este criterio no se aplicará.

Versión de la aplicación

En el campo de entrada, puede definir un criterio para incluir dispositivos en la selección cuando se realice una búsqueda basada en el número de versión de una aplicación de Kaspersky.

Si no especifica un número de versión, este criterio no se aplicará.

Nombre de la actualización crítica

En el campo de entrada, puede definir un criterio para incluir dispositivos en la selección cuando se realice una búsqueda basada en el nombre de una aplicación o en un número de paquete de actualización.

Si el campo queda en blanco, este criterio no se aplicará.

Estado de la aplicación

Lista desplegable en la que puede seleccionar el estado de la aplicación (*Instalada*, *Sin instalar*). Se incluirán en la selección los dispositivos que tengan o no tengan (dependiendo del estado seleccionado) la aplicación seleccionada.

Seleccione el período de la última actualización de módulos

Use esta opción para definir un criterio que permita buscar dispositivos según la hora en que se hayan actualizado por última vez los módulos de las aplicaciones instaladas en ellos.

Si activa esta casilla, podrá utilizar los campos de entrada para definir el intervalo de tiempo (fecha y hora) en el que deberá haber ocurrido la última actualización de módulos de las aplicaciones instaladas en los dispositivos.

Si no activa esta casilla, no se aplicará este criterio.

Esta casilla está desactivada por defecto.

El dispositivo se administra a través del Servidor de administración

Puede usar la lista desplegable para que la selección incluya aquellos dispositivos que se administren mediante Kaspersky Security Center Linux:

- **Sí**. La aplicación incluirá aquellos dispositivos que se administren mediante Kaspersky Security Center Linux.
- **No**. La selección incluye aquellos dispositivos que no se administran mediante Kaspersky Security Center.
- **Ningún valor seleccionado**. El criterio no se aplicará.

La aplicación de seguridad está instalada

Puede usar la lista desplegable para que la selección incluya aquellos dispositivos que tengan instalada la aplicación de seguridad:

- **Sí**. La selección incluirá aquellos dispositivos en los que se haya instalado la aplicación de seguridad.
- **No**. La selección incluirá aquellos dispositivos en los que no se haya instalado la aplicación de seguridad.
- **Ningún valor seleccionado**. El criterio no se aplicará.

En la sección **Protección antivirus**, puede configurar los criterios para incluir dispositivos en una selección en función de su estado de protección:

Bases de datos publicadas

Seleccione esta opción para buscar dispositivos cliente basándose en la fecha de publicación de las bases de datos antivirus. Utilice el campo de entrada para definir el intervalo de tiempo que se tomará como base para la búsqueda.

Esta opción está deshabilitada de forma predeterminada.

Registros de la base de datos

Si se habilita esta opción, podrá buscar los dispositivos cliente por el número de registros de la base de datos. En los campos de entrada puede establecer los valores umbral más bajos y más altos de los registros de la base de datos antivirus.

Esta opción está deshabilitada de forma predeterminada.

Último análisis

Habilite esta opción para buscar dispositivos cliente basándose en la hora del último análisis antimalware. Utilice los campos de entrada para definir el período en el cual deberá haber ocurrido el último análisis antimalware.

Esta opción está deshabilitada de forma predeterminada.

Amenazas detectadas

Habilite esta opción para buscar dispositivos cliente basándose en el número de virus detectados. Utilice los campos de entrada para definir los valores que se tomarán como umbral superior e inferior del número de virus detectados.

Esta opción está deshabilitada de forma predeterminada.

En la subsección **Cifrado**, puede configurar criterios para incluir dispositivos en una selección según el algoritmo de cifrado seleccionado:

Algoritmo de cifrado

Algoritmo de cifrado de bloque simétrico AES. En la lista desplegable, puede seleccionar el tamaño de la clave de cifrado (56 bits, 128 bits, 192 bits o 256 bits).

Valores disponibles: *AES56*, *AES128*, *AES192* y *AES256*.

La subsección **Componentes de las aplicaciones** contiene la lista de componentes de aquellas aplicaciones que tienen los complementos de administración correspondientes instalados en Kaspersky Next Expert View.

En la sección **Componentes de las aplicaciones**, puede definir criterios para incluir dispositivos en la selección basándose en los estados y los números de versión de los componentes vinculados a la aplicación seleccionada:

Estado

Buscar dispositivos basándose en el estado de un componente reportado por una aplicación al Servidor de administración. Puede seleccionar uno de los siguientes estados: *N/D, Detenido*, *En pausa*, *Iniciándose*, *En ejecución, Error, Sin instalar, No compatible con la licencia*. Si el componente seleccionado de la aplicación instalada en un dispositivo administrado tiene el estado especificado, el dispositivo será incluido en la selección de dispositivos.

Estados reportados por las aplicaciones:

- *Detenido*: el componente está deshabilitado y no se encuentra en funcionamiento.
- *En pausa*: el componente se encuentra suspendido (por ejemplo, porque el usuario pausó la protección en la aplicación administrada).
- *Iniciándose*: el componente está en proceso de iniciarse.
- *En ejecución*: el componente está habilitado y funciona correctamente.
- *Error*: ocurrió un error durante el funcionamiento del componente.
- *Sin instalar*: el usuario no optó por instalar el componente al realizar una instalación personalizada de la aplicación.
- *No compatible con la licencia*: la licencia no cubre el componente seleccionado.

A diferencia de los demás estados, *N/D* no es un estado reportado por las aplicaciones. Se trata de una opción que muestra que las aplicaciones no tienen información sobre el estado del componente seleccionado. Esta situación puede presentarse, por ejemplo, cuando el componente seleccionado no pertenece a ninguna de las aplicaciones instaladas en el dispositivo o cuando el dispositivo está apagado.

Versión

Buscar dispositivos basándose en el número de versión del componente seleccionado en la lista. Puede escribir un número de versión, por ejemplo `3.4.1.0`, y luego especificar si el componente seleccionado debe tener una versión igual, anterior o posterior. También puede configurar la búsqueda de todas las versiones excepto la especificada.

Etiquetas

En la sección **Etiquetas**, puede configurar criterios para dispositivos incluidos en una selección según palabras clave (etiquetas) que se agregaron anteriormente a las descripciones de dispositivos administrados:

Aplicar si coincide al menos una etiqueta especificada

Si habilita esta opción, los resultados de búsqueda mostrarán aquellos dispositivos que lleven, en su descripción, al menos una de las etiquetas seleccionadas.

Si deshabilita esta opción, los resultados de búsqueda solo mostrarán aquellos dispositivos que no tengan ninguna de las etiquetas seleccionadas en su descripción.

Esta opción está deshabilitada de forma predeterminada.

Para agregar etiquetas al criterio, haga clic en el botón **Agregar** y seleccione las etiquetas haciendo clic en el campo de entrada **Etiqueta**. Especifique si desea incluir o excluir los dispositivos con las etiquetas seleccionadas en la selección de dispositivos.

Todos los dispositivos que tengan esta etiqueta

Si selecciona esta opción, los resultados de búsqueda mostrarán aquellos dispositivos que lleven, en su descripción, la etiqueta seleccionada. La consulta de búsqueda puede incluir el asterisco, que representa una cadena de cualquier longitud (número de caracteres).

Esta opción está seleccionada de manera predeterminada.

Todos los dispositivos que no tengan esta etiqueta

Si selecciona esta opción, los resultados de búsqueda mostrarán aquellos dispositivos que no lleven en su descripción la etiqueta seleccionada. La consulta de búsqueda puede incluir el asterisco, que representa una cadena de cualquier longitud (número de caracteres).

Usuarios

En la sección **Usuarios**, puede configurar los criterios para incluir dispositivos en la selección basándose en las cuentas de usuario con las que se haya iniciado sesión en el sistema operativo.

Último usuario que inició sesión en el sistema

Si esta opción está habilitada, puede seleccionar la cuenta de usuario para configurar el criterio. Los resultados de búsqueda incluirán aquellos dispositivos en los que el usuario indicado haya sido el último en iniciar sesión.

Usuario que inició sesión en el sistema al menos una vez

Si habilita esta opción, podrá hacer clic en el botón **Examinar** para seleccionar una cuenta de usuario. Los resultados de búsqueda incluirán aquellos dispositivos en los que el usuario indicado haya iniciado sesión al menos una vez.

Propietario del dispositivo

En la sección **Propietario del dispositivo**, puede configurar los criterios a fin de incluir dispositivos en la selección de acuerdo con los propietarios del dispositivo registrados, sus roles y si pertenecen a grupos de seguridad:

Propietario del dispositivo

Seleccione el nombre de usuario del propietario del dispositivo de un grupo de seguridad interno. Obtenga más información sobre los usuarios y sus roles en esta sección.

No se puede registrar más de un usuario como propietario del dispositivo.

Membrecía del propietario del dispositivo en un grupo de seguridad de Active Directory

Seleccione un grupo de seguridad externo de Active Directory al que pertenezca el propietario del dispositivo.

El usuario puede formar parte de un grupo de seguridad de Active Directory o de un grupo incluido en este grupo de seguridad de Active Directory.

Rol del propietario del dispositivo

Seleccione el rol asignado al propietario del dispositivo. Obtenga más información sobre los roles de usuario en este artículo.

Membrecía del propietario del dispositivo en un grupo de seguridad interno

Seleccione un grupo de seguridad interno al que pertenezca el propietario del dispositivo.

Exportar la lista de dispositivos de una selección de dispositivos

Kaspersky Security Center Linux le permite guardar información sobre dispositivos de una selección de dispositivos en un archivo CSV o TXT.

Para exportar la lista de dispositivos de una selección de dispositivos, haga lo siguiente:

1. Abra la tabla de dispositivos de la selección de dispositivos como se indica más arriba.
2. Utilice una de las siguientes formas para seleccionar los dispositivos que desea exportar:
   - Para seleccionar dispositivos específicos, seleccione las casillas de verificación junto a ellos.
   - Para seleccionar todos los dispositivos de la página de la tabla actual, seleccione la casilla de verificación en el encabezado de la tabla de dispositivos y luego seleccione la casilla de verificación **Seleccionar todo en la página actual**.
   - Para seleccionar todos los dispositivos de la tabla, seleccione la casilla de verificación en el encabezado de la tabla de dispositivos y luego seleccione la casilla de verificación **Seleccionar todo**.
3. Haga clic en el botón **Exportar a CSV** o **Exportar a TXT**. Se exportará toda la información sobre los dispositivos seleccionados incluidos en la tabla.

Tenga en cuenta que si aplicó un criterio de filtro a la tabla de dispositivos, solo se exportarán los datos filtrados de las columnas mostradas.

Eliminación de dispositivos de los grupos de administración en una selección

Cuando se trabaja con la selección de dispositivos, puede eliminar los dispositivos de los grupos de administración en la misma selección, sin cambiar a los grupos de administración de los que se deben eliminar estos dispositivos.

Para eliminar los dispositivos de los grupos de administración:

1. En el menú principal, vaya a **Administración de activos → Selecciones de dispositivos** o a la sección **Descubrimiento y despliegue → Selecciones de dispositivos**.
2. En la lista de selecciones, haga clic en el nombre de la selección de dispositivos.

   La página muestra una tabla con información sobre los dispositivos incluidos en la selección de dispositivos.
3. Seleccione los dispositivos que desee eliminar y, a continuación, haga clic en **Eliminar**.

   Los dispositivos seleccionados se quitarán de los grupos de administración correspondientes.

Etiquetas de dispositivo

Kaspersky Security Center Linux permite agregar *etiquetas* a los dispositivos. Una etiqueta es un valor de cadena que se puede utilizar para agrupar, describir o encontrar dispositivos. Pueden utilizarse para crear selecciones, hallar dispositivos específicos y distribuir dispositivos en grupos de administración.

Puede etiquetar dispositivos manual o automáticamente. Si desea etiquetar un dispositivo específico, puede usar el etiquetado manual. Kaspersky Security Center Linux realiza el etiquetado automático de una de las siguientes maneras:

- Según las reglas de etiquetado especificadas.
- Mediante una aplicación.

No recomendamos que utilice diferentes formas de etiquetado para asignar la misma etiqueta. Por ejemplo, si la regla asigna una etiqueta, no se recomienda asignarla a los dispositivos manualmente.

Si las etiquetas se asignan mediante reglas, los dispositivos se etiquetan automáticamente cuando se cumplen las reglas especificadas. Cada regla está asociada a una sola etiqueta. Las reglas atienden a las propiedades de cada dispositivo, como sus atributos de red, su sistema operativo o las aplicaciones que tiene instaladas. Por ejemplo, puede configurar una regla que asignará la etiqueta `[CentOS]` a todos los dispositivos que ejecuten el sistema operativo CentOS. Podrá usar esa etiqueta para crear una selección de dispositivos, lo que lo ayudará a clasificar los dispositivos con Linux y asignar a los mismos una tarea.

Solo puede agregar una regla de etiquetado automático por etiqueta. Si crea una nueva regla para la misma etiqueta, se reemplazará la anterior.

Un dispositivo pierde una etiqueta en los siguientes casos:

- El dispositivo deja de reunir las condiciones indicadas en la regla que le asignó la etiqueta.
- Se elimina o se deshabilita la regla que le asignó al dispositivo la etiqueta.

Cada Servidor de administración tiene sus propias listas de reglas y de etiquetas, que son independientes de las listas de otros servidores de administración (esto incluye, si corresponde, el Servidor de administración principal o cualquier Servidor de administración virtual subordinado). Cada regla se aplica solo a los dispositivos del Servidor de administración en el que la regla se ha creado.

Creación de una etiqueta de dispositivo

Para crear una etiqueta de dispositivo:

1. En el menú principal, vaya a **Repositorios** → **Etiquetas de dispositivos**.
2. En la pestaña **Etiquetas de dispositivos**, haga clic en el botón **Agregar**.
   Se abre una ventana para crear la etiqueta.
3. En el campo **Etiqueta**, escriba el nombre de la etiqueta.
4. Haga clic en **Guardar** para guardar los cambios.

La nueva etiqueta aparece en la lista de etiquetas de dispositivo.

Cambiar el nombre de una etiqueta de dispositivo

Para cambiar el nombre de una etiqueta de dispositivo:

1. En el menú principal, vaya a **Repositorios** → **Etiquetas de dispositivos**.
2. En la pestaña **Etiquetas de dispositivos**, seleccione la etiqueta cuyo nombre desee cambiar.
   Se abre la ventana de propiedades de la etiqueta.
3. En el campo **Etiqueta**, cambie el nombre de etiqueta.
4. Haga clic en **Guardar** para guardar los cambios.

La etiqueta actualizada aparece en la lista de etiquetas de dispositivo.

Eliminar una etiqueta de dispositivo

Solo puede eliminar las etiquetas asignadas manualmente.

Para eliminar una etiqueta de dispositivo asignada manualmente:

1. En el menú principal, vaya a **Repositorios** → **Etiquetas de dispositivos**.
   Se muestra la lista de etiquetas.
2. En la pestaña **Etiquetas de dispositivos**, seleccione las etiquetas de dispositivos que desee eliminar.
3. A continuación, haga clic en el botón **Eliminar**.
4. En la ventana que se abre, haga clic en **Sí**.

Se elimina la etiqueta de dispositivo. La etiqueta eliminada se borra automáticamente de todos los dispositivos a los que estaba asignada.

Cuando elimina una etiqueta asignada al dispositivo mediante una regla de etiquetado automático, la regla no se elimina y la etiqueta se asigna a un nuevo dispositivo cuando el dispositivo cumple por primera vez con las condiciones de la regla. Si elimina una regla de etiquetado automático, la etiqueta especificada en las condiciones de la regla se eliminará de todos los dispositivos a los que se asignó, pero no se eliminará de la lista de etiquetas. Si es necesario, puede eliminar manualmente la etiqueta de la lista.

El dispositivo no perderá automáticamente la etiqueta eliminada si la misma fue asignada por una aplicación o por el Agente de red. Para administrar estas etiquetas, utilice la utilidad klscflag.

Ver los dispositivos que tienen asignada una etiqueta

Para ver cuáles dispositivos tienen asignada una etiqueta:

1. En el menú principal, vaya a **Repositorios** → **Etiquetas de dispositivos**.
2. En la pestaña **Etiquetas de dispositivos**, haga clic en el vínculo **Ver dispositivos** junto a la etiqueta cuya lista de dispositivos asignados desea ver.

   Se le redirigirá a la sección **Dispositivos administrados** del menú principal, donde verá los dispositivos filtrados según la etiqueta en la que haya hecho clic en el vínculo **Ver dispositivos**.
3. Para regresar a la lista de etiquetas de dispositivo, haga clic en el botón **Atrás** de su navegador.

Después de ver los dispositivos que tienen asignada la etiqueta, puede crear y asignar una nueva etiqueta o asignar la etiqueta existente a otros dispositivos. En este caso, debe eliminar el filtro por etiqueta, seleccionar los dispositivos y luego asignar la etiqueta.

Ver las etiquetas asignadas a un dispositivo

Para ver las etiquetas asignadas a un dispositivo:

1. En el menú principal, vaya a **Administración de activos** → **Dispositivos administrados**.
2. Haga clic en el nombre del dispositivo cuyas etiquetas desee ver.
3. En la ventana que se abre, que contendrá las propiedades del dispositivo, elija la pestaña **Etiquetas**.

   Se muestra la lista de etiquetas asignadas al dispositivo seleccionado. En la columna **Modo de asignación**, puede ver cómo se asignó la etiqueta.

En la barra de herramientas, puede hacer lo siguiente:

- Asignar otra etiqueta al dispositivo.
- Eliminar una etiqueta ya asignada.
- Ver una lista con todas las etiquetas de dispositivo creadas en el Servidor de administración.

No puede ver las etiquetas asignadas localmente en el dispositivo.

Etiquetar un dispositivo manualmente

Para asignar una etiqueta a un dispositivo manualmente:

1. Vea las etiquetas asignadas al dispositivo al que desee asignar otra etiqueta.
2. Haga clic en **Agregar**.
3. En la ventana que se abre, realice una de las siguientes acciones:
   - Para crear y asignar una nueva etiqueta, seleccione **Crear nueva etiqueta** y luego escriba el nombre de la nueva etiqueta.
   - Para seleccionar una etiqueta existente, seleccione **Asignar etiqueta existente** y luego, en la lista desplegable, elija la etiqueta pertinente.
4. Haga clic en **Aceptar** para aplicar los cambios.
5. Haga clic en **Guardar** para guardar los cambios.

La etiqueta seleccionada se asigna al dispositivo.

Quitarle una etiqueta a un dispositivo

Para quitarle una etiqueta a un dispositivo:

1. En el menú principal, vaya a **Administración de activos** → **Dispositivos administrados**.
2. Haga clic en el nombre del dispositivo cuyas etiquetas desee ver.
3. En la ventana que se abre, que contendrá las propiedades del dispositivo, elija la pestaña **Etiquetas**.
4. Marque la casilla de verificación adyacente a la etiqueta que desee quitar del dispositivo.
5. Al principio de la lista, haga clic en el botón **Desasignar etiqueta**.
6. En la ventana que se abre, haga clic en **Aceptar**.

El dispositivo pierde la etiqueta.

La etiqueta desasignada no se elimina. Si lo desea, puede eliminarla manualmente.

Las etiquetas asignadas a un dispositivo por una aplicación o por el Agente de red no se pueden eliminar manualmente. Para administrar estas etiquetas, utilice la utilidad klscflag.

Ver las reglas de etiquetado automático de dispositivos

Para ver las reglas que se utilizan para etiquetar dispositivos automáticamente,

Realice una de las siguientes acciones:

- En el menú principal, vaya a **Repositorios** → **Etiquetas de dispositivos** → **Reglas de etiquetado automático**.
- Vea las etiquetas asignadas a un dispositivo y luego haga clic en el botón **Configurar reglas de etiquetado automático**.

Se mostrará una lista con las reglas de etiquetado automático de dispositivos.

Modificación de una regla para etiquetar dispositivos automáticamente

Para modificar una regla para etiquetar dispositivos automáticamente:

1. Vea las reglas de etiquetado automático de dispositivos.
2. Haga clic en el nombre de la regla que desee editar.
   Se abre una ventana para configurar la regla.
3. Modifique las propiedades generales de la regla:
   a. En el campo **Nombre de la regla**, cambie el nombre de regla.
      El nombre no puede contener más de 256 caracteres.
   b. Realice una de las siguientes acciones:
      - Pase el interruptor a **Regla habilitada** para habilitar la regla.
      - Pase el interruptor a **Regla deshabilitada** para deshabilitar la regla.
4. Realice una de las siguientes acciones:
   - Si desea agregar una condición, haga clic en el botón **Agregar** y, en la ventana que se abre, especifique la configuración de la nueva condición.
   - Si desea editar una condición existente, haga clic en el nombre de la condición que desee modificar y, a continuación, edite la configuración de la condición.
   - Si desea eliminar una condición, marque la casilla adyacente al nombre de la condición que desee eliminar y haga clic en **Eliminar**.

5. Haga clic en **Aceptar** en la ventana de configuración de condiciones.

6. Haga clic en **Guardar** para guardar los cambios.

La regla modificada se muestra en la lista.

Creación de una regla para etiquetar dispositivos automáticamente

Para crear una regla para etiquetar dispositivos automáticamente:

1. Vea las reglas de etiquetado automático de dispositivos.

2. Haga clic en **Agregar**.

   Se abre una ventana para configurar la nueva regla.

3. Configure las propiedades generales de la regla:

   a. En el campo **Nombre de la regla**, escriba el nombre de la regla.

      El nombre no puede contener más de 256 caracteres.

   b. Realice una de las siguientes acciones:

      - Pase el interruptor a **Regla habilitada** para habilitar la regla.
      - Pase el interruptor a **Regla deshabilitada** para deshabilitar la regla.

   c. En el campo **Etiqueta**, escriba el nombre de una nueva etiqueta de dispositivo o seleccione una etiqueta de dispositivo de la lista.

      El nombre no puede contener más de 256 caracteres.

4. En la sección de condiciones, haga clic en el botón **Agregar** para añadir una nueva condición.

   Se abre una ventana para configurar la nueva condición.

5. Escriba el nombre de la condición.

   El nombre no puede contener más de 256 caracteres. No puede haber más de una condición con el mismo nombre dentro de una regla.

6. Configure la regla para que se active cuando se cumplan las siguientes condiciones (puede seleccionar varias condiciones):

   - **Red**: atributos de red del dispositivo, como el nombre DNS de un dispositivo o la inclusión de un dispositivo en una subred IP.

     Si la intercalación con diferenciación entre mayúsculas y minúsculas está configurada para la base de datos utilizada para Kaspersky Security Center Linux, respete las mayúsculas y minúsculas cuando ingrese el nombre DNS de un dispositivo. De lo contrario, la regla de etiquetado automático no funcionará.

- **Aplicaciones**: presencia del Agente de red en el dispositivo, tipo de sistema operativo, versión, arquitectura y administrador de paquetes.
- **Máquinas virtuales**: el hecho de que el dispositivo corresponda a un tipo concreto de máquina virtual.
- **Registro de aplicaciones**: presencia de aplicaciones de distintos proveedores en el dispositivo.

7. Haga clic en **Aceptar** para guardar los cambios.

   Si es necesario, puede especificar varias condiciones para una misma regla. En ese caso, la etiqueta se asignará a cualquier dispositivo que cumpla con al menos una condición.

8. Haga clic en **Guardar** para guardar los cambios.

La nueva regla se aplicará a los dispositivos administrados del Servidor de administración seleccionado. Si la configuración de un dispositivo cumple con las condiciones de la regla, ese dispositivo recibirá la etiqueta.

Tras la ejecución inicial, la regla se aplicará en los siguientes casos:

- automática y periódicamente, atendiendo a la carga del servidor.
- cada vez que se edite la regla.
- cada vez que la regla se aplique manualmente.
- Cada vez que el Servidor de administración detecte un cambio en la configuración de un dispositivo que reúna las condiciones de la regla o en la configuración de un grupo que contenga dicho dispositivo.

Puede crear más de una regla de etiquetado. Si crea varias reglas de etiquetado y un dispositivo cumple simultáneamente con las condiciones de todas ellas, dicho dispositivo recibirá varias etiquetas. Puede ver la lista de todas las etiquetas asignadas a un dispositivo en las propiedades del mismo.

Ejecución de reglas para etiquetar dispositivos automáticamente

Cuando se ejecuta una regla, la etiqueta definida en las propiedades de la misma se asigna a los dispositivos que reúnen las condiciones especificadas en las propiedades de esa misma regla. Solo es posible ejecutar reglas activas.

Para ejecutar reglas de etiquetado automático de dispositivos:

1. Vea las reglas de etiquetado automático de dispositivos.
2. Active las casillas de verificación ubicadas junto a las reglas activas que quiera ejecutar.
3. Haga clic en el botón **Ejecutar regla**.

Se ejecutan las reglas seleccionadas.

Eliminación de una regla para etiquetar dispositivos automáticamente

Para eliminar una regla de etiquetado automático de dispositivos:

1. Vea las reglas de etiquetado automático de dispositivos.
2. Marque la casilla ubicada junto a la regla que desee eliminar.
3. Haga clic en el botón **Eliminar**.
4. En la ventana que se abre, haga clic en **Aceptar**.

Se elimina la regla seleccionada. La etiqueta especificada en las propiedades de la regla se desasigna de los dispositivos que la tenían asignada.

La etiqueta desasignada no se elimina. Si lo desea, puede eliminarla manualmente.

Administrar las etiquetas de los dispositivos con la utilidad klscflag

Para asignar un conjunto de etiquetas a un dispositivo, debe ejecutar la utilidad klscflag en el dispositivo cliente al que desea asignar etiquetas.

La utilidad klscflag sobrescribe las etiquetas existentes asignadas al dispositivo. Esto significa que puede agregar o eliminar etiquetas especificando el conjunto de etiquetas deseado en el comando. La utilidad no tiene comandos separados para agregar o eliminar etiquetas individuales. En su lugar, modifica todo el conjunto de etiquetas.

Al especificar nombres de etiquetas en comandos como klscflag, se recomienda utilizar un enfoque de mayúsculas y minúsculas uniforme, como por ejemplo todo en mayúsculas. El uso de mayúsculas puede ayudar a evitar posibles problemas con etiquetas que difieren solo en mayúsculas y minúsculas, según la configuración del DBMS.

Para asignar una etiqueta o varias etiquetas a su dispositivo mediante la utilidad klscflag:

1. Ejecute el símbolo del sistema en una cuenta con privilegios de root y luego cambie su directorio actual al directorio con la utilidad klscflag. La utilidad klscflag se encuentra en el directorio donde está instalado el Agente de red. El directorio de instalación predeterminado es /opt/kaspersky/klnagent64/sbin/.
2. Introduzca uno de los siguientes comandos:
   - Para asignar un conjunto de etiquetas:

     ```
     /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s
     KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"NOMBRE DE LA ETIQUETA
     1\",\"NOMBRE DE LA ETIQUETA 2\",\"NOMBRE DE LA ETIQUETA 3\"]" -svt ARRAY_T -ss
     "|ss_type = \"SS_PRODINFO\";"
     ```

dónde `[\"NOMBRE DE LA ETIQUETA 1\",\"NOMBRE DE LA ETIQUETA 2\",\"NOMBRE DE LA ETIQUETA 3\"]` es la lista de etiquetas que desea asignar a su dispositivo.

Si deja los corchetes vacíos, se eliminarán todas las etiquetas del dispositivo:

```
/opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s
KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[]" -svt ARRAY_T -ss "|ss_type =
\"SS_PRODINFO\";"
```

- Para asignar una nueva etiqueta a un conjunto de etiquetas existente:

  ```
  /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s
  KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"NUEVO NOMBRE DE
  ETIQUETA\",\"NOMBRE DE LA ETIQUETA 1\",\"NOMBRE DE LA ETIQUETA 2\",\"NOMBRE DE LA
  ETIQUETA 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
  ```

  donde `NUEVO NOMBRE DE ETIQUETA` es el nombre de la etiqueta que desea asignar a su dispositivo y `NOMBRE DE ETIQUETA 1`, `NOMBRE DE ETIQUETA 2`, `NOMBRE DE ETIQUETA 3` son los nombres de las etiquetas ya asignadas al dispositivo.

- Para eliminar una etiqueta específica sin eliminar otras etiquetas ya asignadas al dispositivo, ejecute el comando con el conjunto de etiquetas actualizado.

  Por ejemplo, si sus etiquetas actuales son `NOMBRE DE ETIQUETA 1`, `NOMBRE DE ETIQUETA 2`, `NOMBRE DE ETIQUETA 3` y desea eliminar `NOMBRE DE ETIQUETA 2`, ejecute el siguiente comando:

  ```
  /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s
  KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"NOMBRE DE LA ETIQUETA
  1\",\"NOMBRE DE LA ETIQUETA 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
  ```

3. Ejecute el siguiente comando para reiniciar el servicio del Agente de red:

   ```
   systemctl restart klnagent
   ```

   La utilidad klscflag asigna a su dispositivo las etiquetas especificadas.

4. Si quiere asegurarse de que la utilidad klscflag haya asignado correctamente las etiquetas especificadas, vea las etiquetas asignadas al dispositivo.

También puede asignar etiquetas de dispositivos manualmente.

Protección y cifrado de datos

El cifrado de datos reduce el riesgo de que se filtre información corporativa o confidencial si pierde o le roban su computadora portátil o un disco duro. Cifrar la información también la mantiene a salvo de personas y aplicaciones no autorizadas.

Puede usar la función de cifrado de datos si su red tiene dispositivos Windows administrados que cuenten con Kaspersky Endpoint Security para Windows. En este caso, en dispositivos con un sistema operativo Windows, puede administrar los siguientes tipos de cifrado:

- Cifrado de unidad BitLocker
- Cifrado de disco de Kaspersky

No recomendamos habilitar el cifrado en VDI.

Al usar estos componentes de Kaspersky Endpoint Security para Windows puede, por ejemplo, habilitar o deshabilitar el cifrado, ver la lista de unidades cifradas o generar y ver informes sobre el cifrado.

Para configurar los ajustes de cifrado, debe definir la directiva de Kaspersky Endpoint Security para Windows a través de Kaspersky Security Center Linux. Kaspersky Endpoint Security para Windows realizará las operaciones de cifrado y descifrado que se indiquen en la directiva activa. Encontrará instrucciones detalladas para configurar las reglas de cifrado, así como una descripción de las funciones de cifrado, en la Ayuda de Kaspersky Endpoint Security para Windows.

La administración del cifrado para una jerarquía de Servidores de administración no está disponible actualmente en Web Console. Utilice el Servidor de administración principal para administrar dispositivos cifrados.

Puede modificar los ajustes de la interfaz de usuario para mostrar u ocultar algunos de los elementos de la interfaz que están vinculados a la función de administración del cifrado.

Ver la lista de unidades cifradas

En Kaspersky Security Center Linux, puede ver detalles sobre las unidades cifradas y sobre los dispositivos en los que se ha aplicado el cifrado de unidad completa. Si descifra la información de una unidad, la unidad desaparecerá de la lista automáticamente.

Para ver la lista de unidades cifradas:

En el menú principal, vaya a **Operaciones** → **Protección y cifrado de datos** → **Unidades cifradas**.

Si la sección no aparece en el menú, significa que está oculta. En la configuración de la interfaz de usuario, habilite la opción **Mostrar protección y cifrado de datos** para mostrar la sección.

Puede exportar la lista de unidades cifradas a un archivo CSV o TXT. Para hacerlo, haga clic en el botón **Exportar a CSV** o **Exportar a TXT**.

Ver la lista de eventos de cifrado

Cuando se realizan tareas de cifrado y descifrado de datos en los dispositivos cliente, Kaspersky Endpoint Security para Windows envía información a Kaspersky Security Center Linux sobre los siguientes tipos de eventos:

- No se puede cifrar o descifrar un archivo o crear un archivo cifrado debido a que falta espacio en disco.
- No se puede cifrar o descifrar un archivo o crear un archivo cifrado debido a problemas de licencia.
- No se puede cifrar o descifrar un archivo o crear un archivo cifrado debido a que faltan derechos de acceso.
- Se ha prohibido el acceso de la aplicación a un archivo cifrado.
- Errores desconocidos.

Para ver una lista de eventos que se produjeron al cifrar datos en dispositivos:

En el menú principal, vaya a **Operaciones** → **Protección y cifrado de datos** → **Eventos de cifrado**.

Si la sección no aparece en el menú, significa que está oculta. En la configuración de la interfaz de usuario, habilite la opción **Mostrar protección y cifrado de datos** para mostrar la sección.

Puede exportar la lista de unidades cifradas a un archivo CSV o TXT. Para hacerlo, haga clic en el botón **Exportar a CSV** o **Exportar a TXT**.

También puede examinar la lista de eventos de cifrado para cada dispositivo administrado.

Para ver los eventos de cifrado de un dispositivo administrado:

1. En el menú principal, vaya a la sección **Administración de activos** → **Dispositivos administrados**.
2. Haga clic en el nombre de un dispositivo administrado.
3. En la pestaña **General**, seleccione la sección **Protección**.
4. Haga clic en el enlace **Ver errores de cifrado de datos**.

Crear y ver informes de cifrado

Puede generar los siguientes informes:

- Informe sobre el estado de cifrado de los dispositivos administrados. Este informe proporciona detalles sobre el cifrado de datos de varios dispositivos administrados. Por ejemplo, el informe muestra el número de dispositivos a los que se aplica la directiva con reglas de cifrado configuradas. Además, puede averiguar, entre otras cosas, cuántos dispositivos deben reiniciarse. El informe también contiene información sobre la tecnología de cifrado y el algoritmo usados en cada dispositivo.
- Informe sobre el estado de cifrado de los dispositivos de almacenamiento masivo. Este informe contiene la misma información que el informe sobre el estado de cifrado de los dispositivos administrados, pero proporciona datos solo para dispositivos de almacenamiento masivo y unidades extraíbles.

- Informe sobre derechos de acceso a unidades cifradas. Este informe muestra qué cuentas de usuario tienen acceso a unidades cifradas.
- Informe sobre los errores de cifrado de archivos. Este informe contiene información sobre errores que ocurrieron durante tareas de cifrado o descifrado de datos en dispositivos.
- Informe sobre el bloqueo de acceso a los archivos cifrados. Este informe contiene información sobre el bloqueo de acceso de las aplicaciones a los archivos cifrados. Este informe es útil si un usuario o una aplicación no autorizados intenta obtener acceso a archivos o unidades cifradas.

Puede generar cualquiera de los informes en la sección **Supervisión** → **Informes**. También puede generar los siguientes informes de cifrado en la sección **Operaciones** → **Protección y cifrado de datos**:

- Informe sobre el estado de cifrado de los dispositivos de almacenamiento masivo
- Informe sobre derechos de acceso a unidades cifradas
- Informe sobre los errores de cifrado de archivos

*Para generar un informe de cifrado en la sección **Protección y cifrado de datos**:*

1. Verifique que la opción **Mostrar protección y cifrado de datos** esté habilitada en las opciones de la interfaz.
2. En el menú principal, vaya a **Operaciones** → **Protección y cifrado de datos**.
3. Seleccione una de las siguientes secciones:
   - **Unidades cifradas** genera el informe sobre el estado de cifrado de los dispositivos de almacenamiento masivo o el informe sobre derechos de acceso a unidades cifradas.
   - **Eventos de cifrado** genera el informe sobre los errores de cifrado de archivos.
4. Haga clic en el nombre del informe que desea generar.

Se inicia la generación del informe.

Brindar acceso a una unidad cifrada en modo sin conexión

Un usuario puede solicitar acceso a un dispositivo cifrado si, por ejemplo, Kaspersky Endpoint Security no está instalado en el dispositivo administrado. Si recibe una solicitud de acceso, puede crear un archivo de clave de acceso y enviárselo al usuario. Todos los casos de uso y las instrucciones detalladas se proporcionan en la Ayuda de Kaspersky Endpoint Security para la plataforma requerida.

Para otorgar acceso a una unidad cifrada en modo sin conexión en Kaspersky Endpoint Security para Windows, siga estos pasos:

1. Obtenga un archivo de solicitud de acceso de un usuario (un archivo con la extensión FDERTC). Siga las instrucciones de la Ayuda de Kaspersky Endpoint Security para Windows para generar el archivo en Kaspersky Endpoint Security para Windows.
2. En el menú principal, vaya a **Operaciones** → **Protección y cifrado de datos** → **Unidades cifradas**.

   Aparece una lista de unidades cifradas.
3. Seleccione la unidad a la que el usuario haya solicitado acceso.

4. Haga clic en el botón **Otorgar acceso al dispositivo en modo sin conexión**:

5. En la ventana que se abre, seleccione el complemento de Kaspersky Endpoint Security para Windows.

6. Siga las instrucciones proporcionadas en la Ayuda de Kaspersky Endpoint Security para Windows (vea las instrucciones para Kaspersky Security Center Web Console al final de la sección).

Tras hacerlo, el usuario aplica el archivo recibido para acceder a la unidad cifrada y leer los datos almacenados en la unidad.

Transmisión de claves de cifrado entre Servidores de administración

Si se activa la función de cifrado de datos en un dispositivo administrado, la clave de cifrado se almacena en el Servidor de administración. La clave de cifrado se utiliza para acceder a los datos cifrados y para administrar la directiva de cifrado.

La clave de cifrado debe transmitirse a otro Servidor de administración en los siguientes casos:

- Cuando reconfigura el Agente de red en un dispositivo administrado para asignar el dispositivo a otro Servidor de administración. Si este dispositivo contiene datos cifrados, la clave de cifrado debe transmitirse al Servidor de administración de destino. Si no lo hace, no se pueden descifrar los datos.

- Cuando cifra una unidad extraíble conectada a un dispositivo D1 administrado por el Servidor de administración S1 y luego se conecta esta unidad extraíble a un dispositivo D2 administrado por el Servidor de administración S2. Para acceder a los datos en la unidad extraíble, la clave de cifrado debe transmitirse desde el Servidor de administración S1 al Servidor de administración S2.

- Cuando cifra un archivo en un dispositivo D1 administrado por el Servidor de administración S1 y luego intenta acceder al archivo en un dispositivo D2 administrado por el Servidor de administración S2. Para acceder al archivo, la clave de cifrado debe transmitirse desde el Servidor de administración S1 al Servidor de administración S2.

Puede transmitir claves de cifrado de las siguientes maneras:

- Automáticamente, al habilitar la opción **Usar la jerarquía de Servidores de administración para obtener las claves de cifrado** en las propiedades de dos Servidores de administración entre los cuales se debe transmitir una clave de cifrado. Si esta opción está deshabilitada para uno de los Servidores de administración, la transmisión automática de claves de cifrado no es posible.

  Cuando habilita la opción **Usar la jerarquía de Servidores de administración para obtener las claves de cifrado** en las propiedades de un Servidor de administración, el Servidor de administración envía todas las claves de cifrado almacenadas en su repositorio al Servidor de administración principal (si hubiera) un nivel hacia arriba en la jerarquía.

  Cuando trata de acceder a los datos cifrados, el Servidor de administración primero busca la clave de cifrado en su propio repositorio. Si se habilita la opción **Usar la jerarquía de Servidores de administración para obtener las claves de cifrado** y no se encuentra la clave de cifrado necesaria en el repositorio, el Servidor de administración también envía una solicitud a los Servidores de administración principales (si hubiera) para proporcionar la clave de cifrado necesaria. La solicitud se enviará a todos los Servidores de administración principales hasta el servidor que se encuentre en el nivel más alto de la jerarquía.

- De forma manual, exportando el archivo que contiene las claves de cifrado de un Servidor de administración e importándolas a otro.

La exportación e importación de claves de cifrado son acciones que se incluyen en la función de Administración de claves de cifrado. Para realizar estas acciones, configure los derechos de acceso a la función para usuarios de Kaspersky Security Center Linux de la siguiente manera:

- Otorgue el derecho de acceso **Lectura** a la función de administración de claves de cifrado para un usuario que exporte claves de cifrado desde el Servidor de administración secundario.
- Otorgue el derecho de acceso **Escribir** a la función de administración de claves de cifrado para un usuario que importe claves de cifrado al Servidor de administración de destino.

Para habilitar la transmisión automática de las claves de cifrado entre los Servidores de administración dentro de la jerarquía, realice lo siguiente:

1. Vaya a las propiedades del Servidor de administración que necesite:
   a. En el menú principal, seleccione una sección (salvo **Marketplace**, **Navegación por la consola** y **Configuración**) y, a continuación, en la parte superior de la página, haga clic en el botón **Mostrar jerarquía**.
   b. En el panel de navegación que se abre, coloque el cursor sobre el nombre del Servidor de administración que necesite y luego haga clic en el ícono de configuración (⚙).
      También puede hacer clic en el nombre del Servidor de administración y luego, una vez que el nombre aparezca en el menú principal, seleccionarlo desde el menú principal para abrir la ventana de propiedades del servidor.
2. En la ventana de propiedades que se abre, seleccione la sección **Algoritmo de cifrado**.
3. Habilite la opción **Usar la jerarquía de Servidores de administración para obtener las claves de cifrado**.
4. Haga clic en **Guardar** para aplicar los cambios.

Las claves de cifrado se transmitirán a los Servidores de administración principales (si hubiera) en la próxima sincronización (el latido). Este Servidor de administración también proporcionará mediante solicitud una clave de cifrado desde su repositorio a un Servidor de administración secundario.

Para transmitir claves de cifrado entre Servidores de administración de forma manual:

1. Vaya a las propiedades del Servidor de administración desde donde desee exportar las claves de cifrado:
   a. En el menú principal, seleccione una sección (salvo **Marketplace**, **Navegación por la consola** y **Configuración**) y, a continuación, en la parte superior de la página, haga clic en el botón **Mostrar jerarquía**.
   b. En el panel de navegación que se abre, coloque el cursor sobre el nombre del Servidor de administración que necesite y luego haga clic en el ícono de configuración (⚙).
      También puede hacer clic en el nombre del Servidor de administración y luego, una vez que el nombre aparezca en el menú principal, seleccionarlo desde el menú principal para abrir la ventana de propiedades del servidor.
2. En la ventana de propiedades que se abre, seleccione la sección **Algoritmo de cifrado**.
3. Haga clic en **Exportar claves de cifrado**.

   Asegúrese de que un usuario que exporte claves de cifrado desde el Servidor reciba el derecho de acceso **Lectura** a la función de administración de claves de cifrado.

4. En la ventana **¿Exportar las claves de cifrado del Servidor de administración?**, haga lo siguiente:

   a. Indique la contraseña para proteger el archivo de accesos no autorizados.

   b. Especifique dónde desea guardar el archivo.

   Recuerde la contraseña. Si pierde la contraseña, no podrá recuperarla. Si la pierde, debe repetir el procedimiento de exportación. Por lo tanto, escriba la contraseña en un papel y téngalo a mano.

5. Transmita el archivo a otro Servidor de administración, por ejemplo, mediante una carpeta compartida o una unidad extraíble.

6. Vaya a las propiedades del Servidor de administración donde desee importar las claves de cifrado.

7. En la ventana de propiedades, seleccione la sección **Algoritmo de cifrado**.

8. Haga clic en **Importar claves de cifrado**.

   Asegúrese de que un usuario que importe claves de cifrado desde el Servidor reciba el derecho de acceso **Escribir** a la función de administración de claves de cifrado.

9. Seleccione el archivo que contiene las claves de cifrado.

10. Escriba la contraseña y haga clic en **Aceptar**.

Las claves de cifrado se transmiten al Servidor de administración de destino.

Cambiar los dispositivos cliente de Servidor de administración

Puede cambiar el Servidor de administración a uno diferente para dispositivos específicos de cliente. Para ello, utilice la tarea de *Cambiar Servidor de administración*.

Para cambiar el Servidor de administración que administra ciertos dispositivos cliente:

1. Conéctese al Servidor de administración que administra los dispositivos.

2. Crear una tarea de cambio del Servidor de administración

   Se inicia el Asistente para crear nueva tarea. Siga los pasos del asistente. En la ventana **Nueva tarea** del Asistente para crear nueva tarea, seleccione la aplicación **Kaspersky Security Center 17** y el tipo de tarea **Cambiar Servidor de administración**. Luego, especifique los dispositivos para los que desea cambiar el Servidor de administración:

   - **Asignar tarea a un grupo de administración**

     La tarea se asignará a los dispositivos incluidos en un grupo de administración. Puede seleccionar un grupo existente o crear uno nuevo.

     Puede usar esta opción para, por ejemplo, ejecutar una tarea que envíe un mensaje a ciertos usuarios si el contenido atañe solamente a los dispositivos de un grupo de administración puntual.

Si la tarea se asigna a un grupo de administración, la pestaña **Seguridad** no se mostrará en la ventana de propiedades de la tarea; esto se debe a que las tareas de grupo están sujetas a la configuración de seguridad de los grupos a los que se aplican.

- **Especificar las direcciones de los dispositivos manualmente o importarlas de una lista**

  Puede especificar los nombres DNS, las direcciones IP y las subredes IP de los dispositivos a los cuales desee asignar la tarea.

  Podría elegir esta opción si necesita que la tarea se ejecute en una subred específica. Esto puede ser útil si, por ejemplo, necesita instalar una aplicación solo en los dispositivos que utilizan los contadores o si quiere analizar los dispositivos de una subred puntual que probablemente esté infectada.

- **Asignar tarea a una selección de dispositivos**

  La tarea se asignará a los dispositivos incluidos en una selección de dispositivos. Puede elegir una selección existente.

  Esta opción puede ser útil para, por ejemplo, ejecutar una tarea en los dispositivos que tengan una versión específica de un sistema operativo.

3. Ejecute la tarea creada.

Una vez que se completa la tarea, los dispositivos cliente para los que se la creó quedan bajo el mando del Servidor de administración especificado en la configuración de la tarea.

Si el Servidor de administración admite el cifrado y la protección de datos y usted está creando una tarea *Cambiar Servidor de administración*, se mostrará una advertencia. La advertencia estipula que, si algunos datos cifrados se almacenan en dispositivos, después de que el Servidor nuevo comience a administrar los dispositivos, los usuarios podrán acceder solo a los datos cifrados con los cuales trabajaron anteriormente. En otros casos, no se brindará acceso a datos cifrados. Para más precisiones sobre los casos en los que se pierde el acceso a la información cifrada, consulte la Ayuda de Kaspersky Endpoint Security para Windows.

Evitar conflictos entre varios Servidores de administración

Si tiene más de un Servidor de administración en su red, pueden ver los mismos dispositivos cliente. Esto puede resultar, por ejemplo, en que el Servidor de administración instale una aplicación que ya fue instalada por otro Servidor de administración, y otros tipos de conflictos. Para evitar que una aplicación se instale en un dispositivo administrado por otro Servidor de administración, debe habilitar la opción **Instalar solo en dispositivos administrados a través de este Servidor de administración** en las propiedades de la tarea *Instalar aplicación de forma remota*.

Si habilita la opción **Instalar solo en dispositivos administrados a través de este Servidor de administración** y luego ejecuta la tarea *Instalar aplicación de forma remota*, se realiza una verificación para determinar si los dispositivos están administrados por otro Servidor de administración. Para los dispositivos administrados por otro Servidor de administración, el valor del atributo **Administrado por un Servidor de administración diferente** se establecerá en `true`. La tarea *Instalar aplicación de forma remota* no se aplicará a estos dispositivos.

Los valores del atributo **Administrado por un Servidor de administración diferente** se muestran en la columna **Administrado por un Servidor de administración diferente** en la lista de dispositivos administrados y la lista de dispositivos no asignados.

También puede usar la propiedad **Administrado por un Servidor de administración diferente** como criterio para los siguientes propósitos:

- Mostrar dispositivos administrados
- Selecciones de dispositivos
- Reglas de movimiento de dispositivos
- Reglas de etiquetado automático

Para restablecer el atributo Administrado por un Servidor de administración diferente:

1. En el menú principal de Kaspersky Security Center Web Console, vaya a **Administración de activos** → **Dispositivos no asignados**.
2. Seleccione el dispositivo requerido y, a continuación, haga clic en el botón **Eliminar el atributo Administrado por un Servidor de administración diferente**.

Se restablece el atributo **Administrado por un Servidor de administración diferente**.

Mover dispositivos conectados a un Servidor de administración mediante puertas de enlace de conexión a otro Servidor de administración

Puede mover los dispositivos conectados a un Servidor de administración mediante puertas de enlace de conexión a otro Servidor de administración. Esto puede ser necesario si, por ejemplo, instala otra versión del Servidor de administración y no desea reinstalar el Agente de red en los dispositivos, ya que ello puede llevar mucho tiempo.

Los comandos descritos en las instrucciones deben ejecutarse en los dispositivos cliente utilizando una cuenta con derechos de administrador.

Para mover un dispositivo conectado mediante una puerta de enlace de conexión a otro Servidor de administración:

1. Ejecute la utilidad klmover con el parámetro `-address <dirección del servidor>`, para cambiar al nuevo Servidor de Administración.
2. Ejecute el comando `klnagchk -nagwait -tl 4`.
3. Ejecute los siguientes comandos para establecer una nueva puerta de enlace de conexión:
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_mode -sv false -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"`
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_loc -sv "<ip o nombre de puerta de enlace>" -svt STRING_T -ss "|ss_type = \"SS_SETTINGS\";"`

     Aquí `<ip o nombre de puerta de enlace>` es la dirección de la puerta de enlace de conexión accesible desde Internet.

- `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_ssl_port -sv 13000 -svt INT_T -ss "|ss_type = \"SS_SETTINGS\";"`

  `13000` es el número del puerto TCP en el que recibe solicitudes la puerta de enlace de conexión

4. Ejecute el comando `klnagchk -restart -tl 4` para iniciar el servicio del Agente de red.

El dispositivo se mueve al nuevo Servidor de administración y se conecta a través de la nueva puerta de enlace conectada.

Ver y configurar las acciones para dispositivos inactivos

Puede recibir una notificación si se detecta que los dispositivos cliente de un grupo están inactivos. También puede hacer que esos dispositivos se eliminen automáticamente.

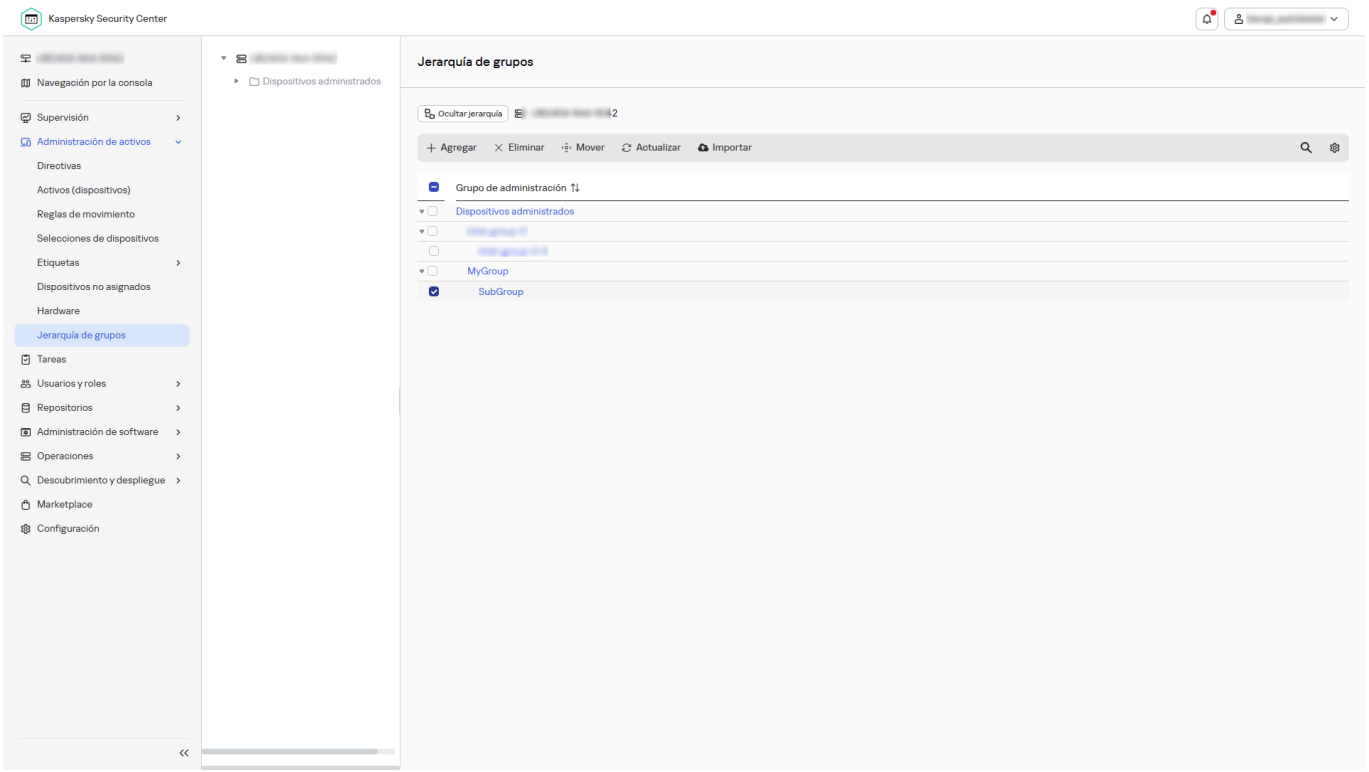
Para ver o configurar las acciones que se llevan a cabo cuando los dispositivos de un grupo están inactivos:

1. En el menú principal, vaya a **Administración de activos** → **Jerarquía de grupos**.

2. Vaya a las propiedades del grupo de administración que necesite de una de las siguientes maneras:

   - Haga clic en el nombre del grupo de administración.

   - Haga clic en el botón **Mostrar jerarquía** en la parte superior de la página. En el panel de navegación que se abre, coloque el cursor sobre el nombre del grupo que necesite y luego haga clic en el ícono de configuración (⚙).



Jerarquía de grupos de administración

Se abrirá la ventana de propiedades del grupo de administración.

3. En la ventana de propiedades, vaya a la pestaña **Configuración**.

4. En la sección **Herencia**, active o desactive las siguientes opciones:

   Heredar del grupo primario

   La configuración de la sección se heredará del grupo primario al que pertenezca el dispositivo cliente. Si esta opción está habilitada, los ajustes de la sección **Actividad de los dispositivos en la red** no se podrán modificar.

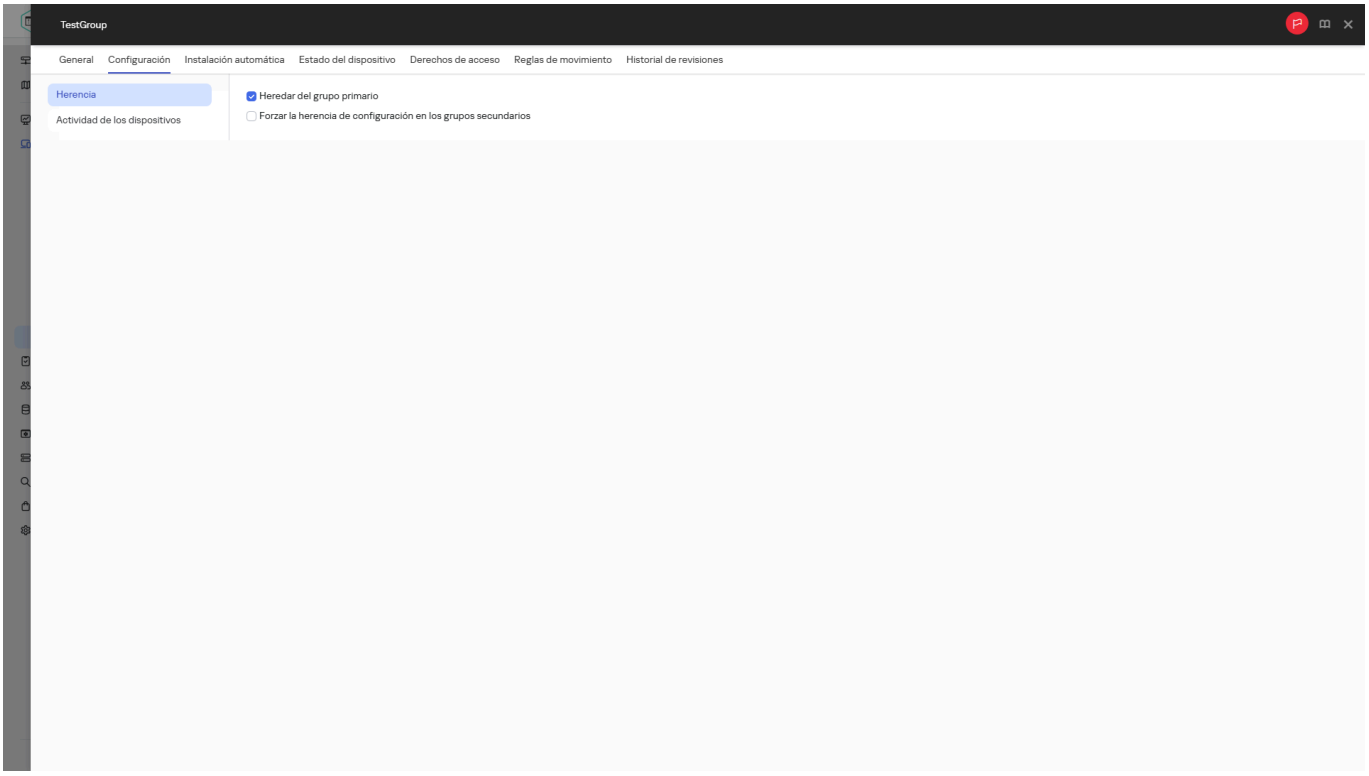
   Para que esta opción esté disponible, el grupo de administración debe tener un grupo primario.

   Esta opción está activada de forma predeterminada.

   Forzar la herencia de configuración en los grupos secundarios

   Los valores de configuración se propagarán a los grupos secundarios. Los ajustes correspondientes estarán bloqueados en las propiedades de esos grupos.

   Esta opción está deshabilitada de forma predeterminada.



Propiedades de los grupos de administración

5. En la sección **Actividad de los dispositivos**, active o deshabilite las siguientes opciones:

   Notificar al administrador si el dispositivo ha estado inactivo por más de (días)

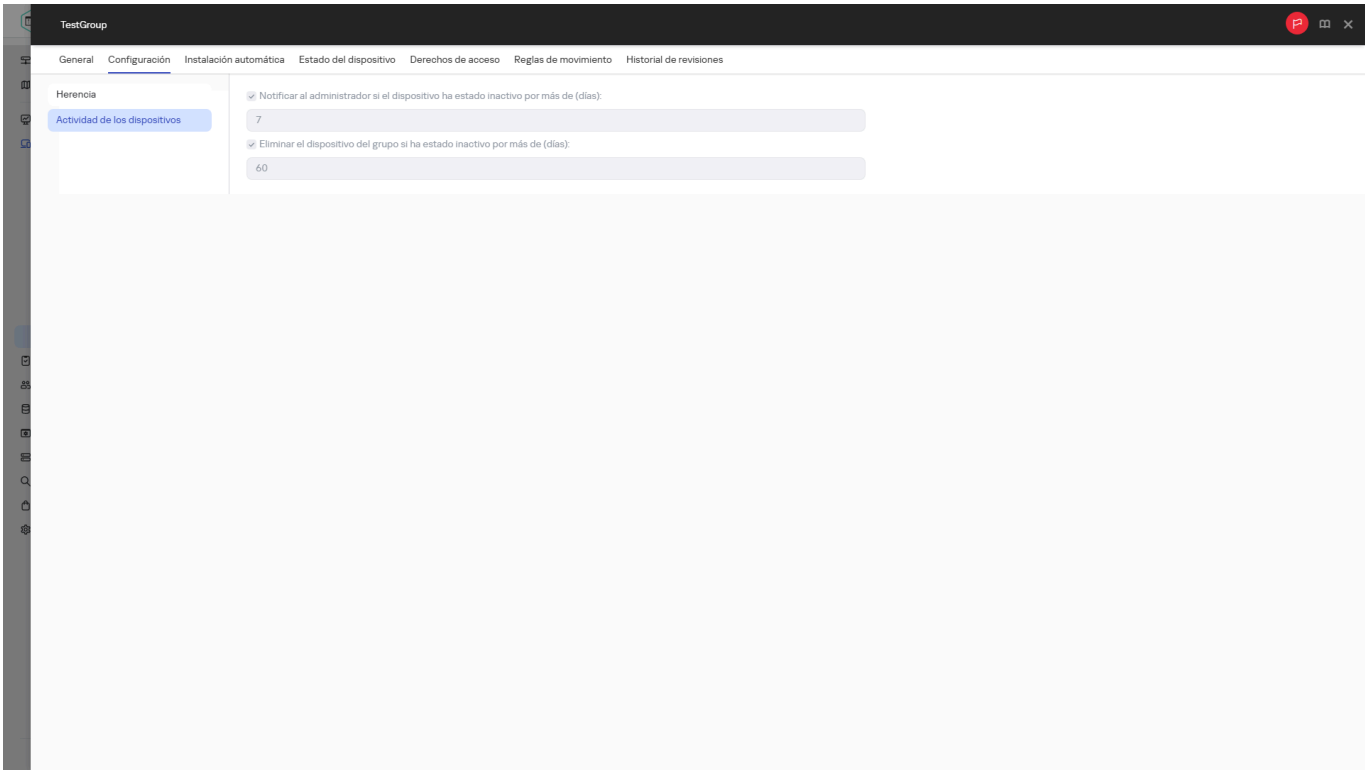
   Cuando esta opción está habilitada y se detecta que un dispositivo ha estado inactivo, el administrador recibe una notificación. Puede especificar el intervalo de tiempo que se deja pasar antes de que se cree el evento **El dispositivo ha estado inactivo en la red por mucho tiempo**. El intervalo de tiempo por defecto es de 7 días.

   Esta opción está activada de forma predeterminada.

   Eliminar el dispositivo del grupo si ha estado inactivo por más de (días)

   Si esta opción está habilitada, puede especificar el intervalo de tiempo que se deja pasar antes de que el dispositivo se elimine del grupo automáticamente. El intervalo de tiempo por defecto es de 60 días.

Esta opción está activada de forma predeterminada.



Propiedades de los grupos de administración

6. Haga clic en el botón **Guardar**.

Se guardarán y aplicarán los cambios.

Envío de mensajes a usuarios de dispositivos

Para enviar un mensaje por correo electrónico a usuarios de dispositivos:

1. En el menú principal, vaya a **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea.
3. En la lista desplegable **Tipo de tarea**, seleccione **Enviar mensaje a usuario**.
4. Seleccione una opción para elegir el grupo de administración, la selección de dispositivos o los dispositivos a los que se aplicará la tarea.
5. Ejecute la tarea creada.

Una vez finalizada la tarea, el mensaje creado se enviará a los usuarios de los dispositivos seleccionados. La tarea **Enviar mensaje a usuario** solo está disponible para dispositivos que funcionan con Windows.

Encendido, apagado y reinicio remoto de dispositivos cliente

Kaspersky Security Center Linux le permite administrar dispositivos cliente remotamente al activarlos, apagarlos o reiniciarlos.

Para administrar remotamente dispositivos cliente:

1. En el menú principal, vaya a **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea.
3. En la lista desplegable **Tipo de tarea**, seleccione **Administrar dispositivos**.
4. Seleccione una opción para elegir el grupo de administración, la selección de dispositivos o los dispositivos a los que se aplicará la tarea.
5. Seleccione el comando (encender, apagar o reiniciar).
6. Si es necesario, configure los siguientes ajustes para los comandos de apagado y reinicio:

   - Active el comutador **Solicitar confirmación del usuario** para especificar el mensaje de solicitud del usuario y los intervalos de tiempo tras los cuales desea repetir la solicitud y reiniciar o apagar los dispositivos.
   - Marque la casilla **Tiempo de espera antes del cierre forzado de aplicaciones en sesiones bloqueadas (min)** y especifique el tiempo.

   Estos ajustes se aplican solo a los dispositivos cliente Windows. Los dispositivos Linux se reiniciarán o apagarán de inmediato al completarse la tarea.
7. Ejecute la tarea creada.

Luego de finalizar la tarea, se ejecutará el comando (encender, apagar o reiniciar) en los dispositivos seleccionados.

Acceso remoto a dispositivos administrados

Kaspersky Security Center Linux le permite establecer una conexión remota a los dispositivos administrados. El administrador puede obtener acceso remoto al dispositivo administrado a través de un Agente de red instalado en el dispositivo cliente. El Agente de red permite conectarse incluso si el dispositivo cliente tiene cerrados los puertos TCP y UDP. Al establecer una conexión con el dispositivo, el administrador obtiene acceso completo a la información almacenada en este dispositivo, de manera que puede administrar las aplicaciones instaladas en él.

Los métodos para establecer una conexión remota dependen de la plataforma que se utilice en el dispositivo con Kaspersky Security Center Web Console. Kaspersky Security Center Web Console se puede instalar en un dispositivo que no sea el Servidor de administración, en un dispositivo basado en Windows o en Linux.

Desde Kaspersky Security Center Web Console instalado en un dispositivo con Linux, puede establecer las siguientes conexiones:

- A un dispositivo administrado basado en Linux mediante los siguientes métodos:
  - Conexión a escritorio remoto (RDP)
  - Computación virtual en red (VNC)
- A un dispositivo administrado basado en Windows mediante los siguientes métodos:
  - Conexión a escritorio remoto (RDP)
  - Computación virtual en red (VNC)

Desde Kaspersky Security Center Web Console instalado en un dispositivo con Windows, puede establecer las siguientes conexiones:

- A un dispositivo administrado basado en Linux mediante los siguientes métodos:
  - Conexión a escritorio remoto (RDP)
  - Computación virtual en red (VNC)
- A un dispositivo administrado basado en Windows mediante los siguientes métodos:
  - Conexión a escritorio remoto (RDP)
  - Escritorio compartido de Windows (WDS)

No se admite la conexión remota a dispositivos administrados cuando se accede a Kaspersky Security Center Web Console desde un dispositivo que ejecuta Microsoft Windows en Arm.

Para establecer una conexión remota a un dispositivo, debe contar con lo siguiente:

- Utilidad klsctunnel

  La utilidad Kaspersky se utiliza para tunelizar la conexión entre un dispositivo administrado y el Servidor de administración.

  Kaspersky Security Center Linux permite hacer túneles de conexión TCP desde Kaspersky Security Center Web Console mediante el Servidor de administración y luego mediante el Agente de red a un puerto especificado en un dispositivo administrado. Gracias a este túnel, una aplicación cliente instalada en el mismo dispositivo que Kaspersky Security Center Web Console puede conectarse a un puerto TCP de un dispositivo administrado incluso si no existe una vía de conexión directa entre Kaspersky Security Center Web Console y ese dispositivo administrado.

  La conexión entre el Servidor de administración y el dispositivo cliente remoto se debe hacer pasar por un túnel cuando el puerto que se utiliza para conectarse al Servidor de administración no está disponible en el dispositivo. El puerto del dispositivo podría no estar disponible en estos casos:

  - el dispositivo remoto está conectado a una red local en la que se utiliza el mecanismo NAT;
  - el dispositivo remoto está en la misma red local que el Servidor de administración, pero el puerto se ha cerrado con un firewall.

Puede descargar la utilidad desde Kaspersky Security Center Web Console si se establece una conexión remota mediante Web Console, o descargarla manualmente desde el sitio web de Kaspersky.

La utilidad klsctunnel se instala en el dispositivo del Servidor de administración y se usa para todos los tipos de conexión remota (RDP, VNC, WDS).

- Cliente RDP o VNC

  Una cliente RDP o VNC está instalado en el dispositivo del Servidor de administración. Este cliente le permite obtener acceso remoto al dispositivo administrado mediante la dirección y el puerto para la conexión local proporcionada por la utilidad klsctunnel.

  Se establece una conexión RDP a la sesión de escritorio remoto del usuario sin que el usuario lo sepa. Una vez que el administrador se conecta a la sesión, el usuario del dispositivo queda desconectado de la sesión sin notificación.

- Escritorio compartido de Windows (solo para dispositivos administrados basados en Windows)

  Esta función le permite conectarse a una sesión existente sin desconectar a la persona que la inició. En tal caso, el acceso al escritorio se comparte entre el administrador y el usuario que inició la sesión.

  Al conectarse con una sesión existente del escritorio remoto, el usuario de la sesión en el dispositivo recibe una solicitud de conexión del administrador. No hay información acerca de la actividad remota del dispositivo, y los resultados se guardarán en informes creados por Kaspersky Security Center Linux.

  El administrador puede configurar una auditoría de la actividad del usuario en un dispositivo cliente remoto. Cuando la función de auditoría está activada, la aplicación guarda información sobre los archivos que el administrador abre o modifica en el dispositivo cliente.

Acceso remoto desde un dispositivo basado en Linux con Kaspersky Security Center Web Console a un dispositivo administrado basado en Linux

Requisitos previos

Antes de comenzar, compruebe que hizo lo siguiente:

- En el dispositivo administrado con Linux, se instala el Agente de red 15.3 o versiones posteriores.
- En el dispositivo administrado con Linux, se instala el servidor RDP (si se conecta al dispositivo administrado mediante la conexión de escritorio remoto).
- En el dispositivo administrado con Linux, se instala el servidor VNC (si se conecta al dispositivo administrado mediante Computación virtual en red).
- Se abre el puerto para tunelizar conexiones RDP (la opción **Abrir puerto para tunelización de conexiones RDP** está habilitada en la sección **Puertos de conexión** de la ventana de propiedades del Servidor de administración).
- El administrador tiene el derecho de **Iniciar sesiones RDP** para establecer conexiones RDP (si se conecta al dispositivo administrado mediante Conexión a escritorio remoto).
- El administrador tiene el derecho **Iniciar la tunelización** para establecer la conexión de túnel para VNC (si se conecta al dispositivo administrado mediante Computación virtual en red).

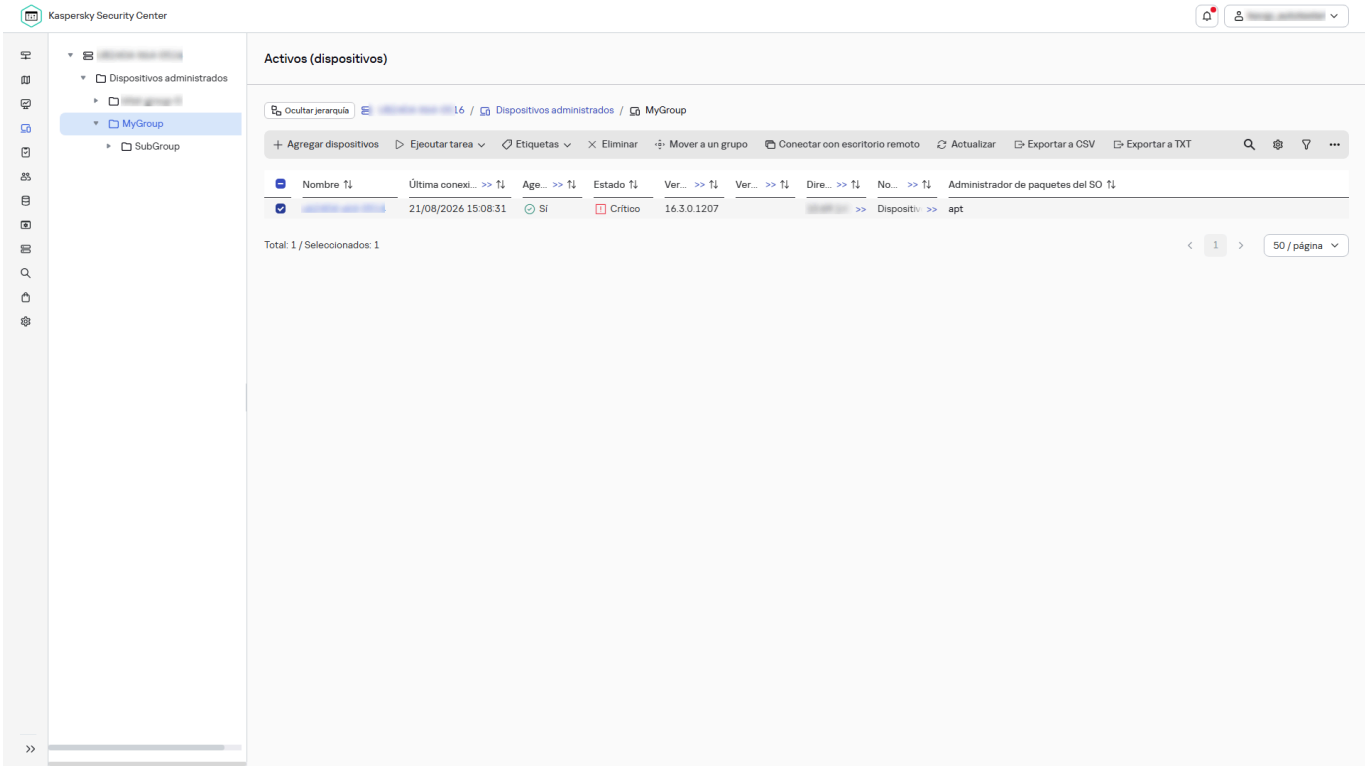
Para conectarse a un dispositivo administrado con Linux mediante RDP o VNC a través de Kaspersky Security Center Web Console abierto en un dispositivo con Linux:

1. En el menú principal, vaya a la sección **Administración de activos** → **Dispositivos administrados** o abra una selección de dispositivos.

2. Seleccione la casilla junto al dispositivo administrado al que desea conectarse de forma remota y, luego, haga clic en el botón **Conectar con escritorio remoto**.

   Se abre la ventana **Conectar con escritorio remoto**.

   Si selecciona varios dispositivos, un dispositivo móvil o un dispositivo con macOS, el botón **Conectar con escritorio remoto** se deshabilitará.



La lista de dispositivos administrados

3. Descargue la utilidad klsctunnel haciendo clic en el botón **Descargar** y, luego, ejecútela.

   Al descargar la utilidad, tenga en cuenta lo siguiente:

   - Para obtener una versión actualizada de la utilidad klsctunnel, asegúrese de que el Servidor de administración tenga acceso a los servidores de actualización de Kaspersky.

     Puede ejecutar la tarea *Descargar actualizaciones en el repositorio de la tarea del Servidor de administración* y seleccionar los servidores de actualizaciones de Kaspersky como origen de actualizaciones. Si la tarea finaliza correctamente, el Servidor de administración tendrá acceso a los servidores de actualización de Kaspersky.

   - Si el archivo de utilidad no está disponible para descargar, se muestra un mensaje de error. En este caso, descargue la utilidad manualmente y, luego, colóquela en el dispositivo del Servidor de administración en el directorio /var/opt/kaspersky/klnagent_srv.

4. En la ventana **Conectar con escritorio remoto**, especifique el puerto de conexión. El número de puerto predeterminado es 3389.

5. Genere un blob de texto con parámetros de conexión codificados haciendo clic en el botón **Generar blob** y, luego, copie y pegue el texto en el campo correspondiente en la utilidad klsctunnel.

   Un blob contiene las configuraciones necesarias para establecer una conexión entre el Servidor de administración y el dispositivo administrado. Los blobs tienen una validez de tres minutos. Si el blob caduca, genere uno nuevo.

6. En la utilidad klsctunnel, si utiliza un servidor proxy, especifique la configuración de conexión del servidor proxy.

   La utilidad klsctunnel muestra la dirección y el puerto para la conexión local de un cliente de acceso remoto.

   La utilidad permite al administrador cerrar la conexión del túnel. Si se cierra la conexión del túnel, se finaliza la conexión actual con el escritorio remoto.

7. Ejecute un cliente de acceso remoto (RDP o VNC) y conéctelo al dispositivo administrado utilizando la dirección y el puerto proporcionados por la utilidad klsctunnel.

Se establece la conexión con el dispositivo administrado. El escritorio está disponible en la ventana del cliente de acceso remoto.

Acceso remoto desde un dispositivo basado en Linux con Kaspersky Security Center Web Console a un dispositivo administrado basado en Windows

Conexión a escritorio remoto (RDP)

Requisitos previos

Antes de comenzar, compruebe que hizo lo siguiente:

- Las conexiones remotas están permitidas por el sistema operativo del dispositivo administrado.
- En el dispositivo administrado con Windows, se instala el Agente de red 13 o versiones posteriores.
- El administrador tiene el derecho **Iniciar sesiones RDP** para establecer conexiones RDP.
- Se abre el puerto para tunelizar conexiones RDP (la opción **Abrir puerto para tunelización de conexiones RDP** está habilitada en la sección **Puertos de conexión** de la ventana de propiedades del Servidor de administración).

Para conectarse a un dispositivo administrado con Windows mediante RDP a través de Kaspersky Security Center Web Console abierto en un dispositivo con Linux:

1. En el menú principal, vaya a la sección **Administración de activos** → **Dispositivos administrados** o abra una selección de dispositivos.

2. Seleccione la casilla junto al dispositivo administrado al que desea conectarse de forma remota y, luego, haga clic en el botón **Conectar con escritorio remoto**.

   Se abre la ventana **Conectar con escritorio remoto**.

   Si selecciona varios dispositivos, un dispositivo móvil o un dispositivo con macOS, el botón **Conectar con escritorio remoto** se deshabilitará.

3. En la ventana **Conectar con escritorio remoto**, seleccione el tipo de conexión **RDP**.

4. Si la conexión remota no está permitida en la configuración del sistema operativo del dispositivo administrado, permita la conexión remota de forma centralizada haciendo clic en el botón **Cambiar ajustes**.

   Si la configuración se aplica correctamente, se muestra una notificación. Además, en el dispositivo administrado, en la sección **Configuración → Sistema → Escritorio remoto**, está habilitada la opción **Habilitar escritorio remoto**.

   Si la conexión remota está permitida en la configuración del sistema operativo del dispositivo administrado, no se muestra el botón **Cambiar ajustes**.

5. Descargue la utilidad klsctunnel haciendo clic en el botón **Descargar** y, luego, ejecútela.

   Al descargar la utilidad, tenga en cuenta lo siguiente:

   - Para obtener una versión actualizada de la utilidad klsctunnel, asegúrese de que el Servidor de administración tenga acceso a los servidores de actualización de Kaspersky.

     Puede ejecutar la tarea *Descargar actualizaciones en el repositorio de la tarea del Servidor de administración* y seleccionar los servidores de actualizaciones de Kaspersky como origen de actualizaciones. Si la tarea finaliza correctamente, el Servidor de administración tendrá acceso a los servidores de actualización de Kaspersky.

   - Si el archivo de utilidad no está disponible para descargar, se muestra un mensaje de error. En este caso, descargue la utilidad manualmente y, luego, colóquela en el dispositivo del Servidor de administración en el directorio /var/opt/kaspersky/klnagent_srv.

6. Genere un blob de texto con parámetros de conexión codificados haciendo clic en el botón **Generar blob** y, luego, copie y pegue el texto en el campo correspondiente en la utilidad klsctunnel.

   Un blob contiene las configuraciones necesarias para establecer una conexión entre el Servidor de administración y el dispositivo administrado. Los blobs tienen una validez de tres minutos. Si el blob caduca, genere uno nuevo.

7. En la utilidad klsctunnel, si utiliza un servidor proxy, especifique la configuración de conexión del servidor proxy.

   La utilidad klsctunnel muestra la dirección y el puerto de la conexión al dispositivo remoto.

   La utilidad permite al administrador cerrar la conexión del túnel. Si se cierra la conexión del túnel, se finaliza la conexión actual con el escritorio remoto.

8. Ejecute un cliente RDP y conéctelo al dispositivo administrado utilizando la dirección y el puerto proporcionados por la utilidad klsctunnel.

Se establece la conexión con el dispositivo administrado. El escritorio está disponible en la ventana del cliente RDP.

Si se conecta a la sesión de escritorio remoto establecida por un usuario, lo hará sin que el usuario lo sepa. Una vez que el administrador se conecta a la sesión, el usuario del dispositivo queda desconectado de la sesión sin notificación.

Sistema de Computación virtual en red (VNC)

Requisitos previos

Antes de comenzar, compruebe que hizo lo siguiente:

- En el dispositivo administrado con Windows, se instala el Agente de red 13 o versiones posteriores.
- En el dispositivo administrado que ejecuta Windows, está instalado el servidor VNC.
- El administrador tiene el derecho **Iniciar la tunelización** para establecer la conexión de túnel para VNC.
- Se abre el puerto para tunelizar conexiones RDP (la opción **Abrir puerto para tunelización de conexiones RDP** está habilitada en la sección **Puertos de conexión** de la ventana de propiedades del Servidor de administración).

Para conectarse a un dispositivo administrado con Windows mediante VNC a través de Kaspersky Security Center Web Console abierto en un dispositivo con Linux:

1. En el menú principal, vaya a la sección **Administración de activos** → **Dispositivos administrados** o abra una selección de dispositivos.
2. Seleccione la casilla junto al dispositivo administrado al que desea conectarse de forma remota y, luego, haga clic en el botón **Conectar con escritorio remoto**.

   Se abre la ventana **Conectar con escritorio remoto**.

   Si selecciona varios dispositivos, un dispositivo móvil o un dispositivo con macOS, el botón **Conectar con escritorio remoto** se deshabilitará.
3. En la ventana **Conectar con escritorio remoto**, seleccione el tipo de conexión **VNC**.
4. Descargue la utilidad klsctunnel haciendo clic en el botón **Descargar** y, luego, ejecútela.

   Si el archivo de utilidad no está disponible para descargar, se muestra un mensaje de error. En este caso, descargue la utilidad manualmente.
5. En la ventana **Conectar con escritorio remoto**, especifique el puerto de conexión VNC. El número de puerto predeterminado es 5900.
6. Genere un blob de texto con parámetros de conexión codificados haciendo clic en el botón **Generar blob** y, luego, copie y pegue el texto en el campo correspondiente en la utilidad klsctunnel.

   Un blob contiene las configuraciones necesarias para establecer una conexión entre el Servidor de administración y el dispositivo administrado. Los blobs tienen una validez de tres minutos. Si el blob caduca, genere uno nuevo.
7. En la utilidad klsctunnel, si utiliza un servidor proxy, especifique la configuración de conexión del servidor proxy.

   La utilidad klsctunnel muestra la dirección y el puerto para la conexión local de un cliente VNC.

   La utilidad permite al usuario remoto cerrar la conexión del túnel. Si se cierra la conexión del túnel, se finaliza la conexión actual con el escritorio remoto.
8. Ejecute un cliente VNC y conéctelo al dispositivo administrado utilizando la dirección y el puerto proporcionados por la utilidad klsctunnel.

Se establece la conexión con el dispositivo administrado. El escritorio está disponible en la ventana del cliente VNC.

Acceso remoto desde un dispositivo basado en Windows con Kaspersky Security Center Web Console a un dispositivo administrado basado en Linux

Conexión a escritorio remoto (RDP)

Requisitos previos

Antes de comenzar, compruebe que hizo lo siguiente:

- En el dispositivo administrado que ejecuta Linux, está instalado el servidor RDP.
- En el dispositivo administrado con Linux, se instala el Agente de red 15.3 o versiones posteriores.
- El administrador tiene el derecho **Iniciar sesiones RDP** para establecer conexiones RDP.
- Se abre el puerto para tunelizar conexiones RDP (la opción **Abrir puerto para tunelización de conexiones RDP** está habilitada en la sección **Puertos de conexión** de la ventana de propiedades del Servidor de administración).

Para conectarse a un dispositivo administrado con Linux mediante RDP a través de Kaspersky Security Center Web Console abierto en un dispositivo con Windows:

1. En el menú principal, vaya a la sección **Administración de activos** → **Dispositivos administrados** o abra una selección de dispositivos.
2. Seleccione la casilla junto al dispositivo administrado al que desea conectarse de forma remota y, luego, haga clic en el botón **Conectar con escritorio remoto**.

   Se abre la ventana **Conectar con escritorio remoto**.

   Si selecciona varios dispositivos, un dispositivo móvil o un dispositivo con macOS, el botón **Conectar con escritorio remoto** se deshabilitará.
3. En la ventana **Conectar con escritorio remoto**, seleccione el tipo de conexión **RDP**.
4. Descargue la utilidad klsctunnel haciendo clic en el botón **Descargar** y, luego, ejecútela.

   Al descargar la utilidad, tenga en cuenta lo siguiente:

   - Para obtener una versión actualizada de la utilidad klsctunnel, asegúrese de que el Servidor de administración tenga acceso a los servidores de actualización de Kaspersky.

     Puede ejecutar la tarea *Descargar actualizaciones en el repositorio de la tarea del Servidor de administración* y seleccionar los servidores de actualizaciones de Kaspersky como origen de actualizaciones. Si la tarea finaliza correctamente, el Servidor de administración tendrá acceso a los servidores de actualización de Kaspersky.
   - Si el archivo de utilidad no está disponible para descargar, se muestra un mensaje de error. En este caso, descargue la utilidad manualmente y, luego, colóquela en el dispositivo del Servidor de administración en el directorio /var/opt/kaspersky/klnagent_srv.

5. Genere un blob de texto con parámetros de conexión codificados haciendo clic en el botón **Generar blob** y, luego, copie y pegue el texto en el campo correspondiente en la utilidad klsctunnel.

   Un blob contiene las configuraciones necesarias para establecer una conexión entre el Servidor de administración y el dispositivo administrado. Los blobs tienen una validez de tres minutos. Si el blob caduca, genere uno nuevo.

6. En la utilidad klsctunnel, si utiliza un servidor proxy, especifique la configuración de conexión del servidor proxy.

   Para ello, seleccione la casilla **Usar servidor proxy** y, luego, especifique la configuración de conexión.

7. Haga clic en el botón **Abrir puerto**.

   Se abre la ventana de inicio de sesión de Conexión a Escritorio remoto.

8. Especifique las credenciales de la cuenta con la que haya iniciado sesión en Kaspersky Security Center Web Console y, luego, conéctese al dispositivo administrado.

   La utilidad klsctunnel muestra la dirección y el puerto de la conexión al dispositivo remoto.

   La utilidad permite al administrador cerrar la conexión del túnel. Si se cierra la conexión del túnel, se finaliza la conexión actual con el escritorio remoto.

Una vez que se establezca la conexión con el dispositivo, tendrá acceso al escritorio a través de la ventana Conexión a Escritorio remoto de Microsoft Windows.

Si se conecta a la sesión de escritorio remoto establecida por un usuario, lo hará sin que el usuario lo sepa. Una vez que el administrador se conecta a la sesión, el usuario del dispositivo queda desconectado de la sesión sin notificación.

Sistema de Computación virtual en red (VNC)

Requisitos previos

Antes de comenzar, compruebe que hizo lo siguiente:

- En el dispositivo administrado con Linux, se instala el Agente de red 15.3 o versiones posteriores.
- En el dispositivo administrado que ejecuta Linux, está instalado el servidor VNC.
- El administrador tiene el derecho **Iniciar la tunelización** para establecer la conexión de túnel para VNC.
- Se abre el puerto para tunelizar conexiones RDP (la opción **Abrir puerto para tunelización de conexiones RDP** está habilitada en la sección **Puertos de conexión** de la ventana de propiedades del Servidor de administración).

Para conectarse a un dispositivo administrado con Linux mediante VNC a través de Kaspersky Security Center Web Console abierto en un dispositivo con Windows:

1. En el menú principal, vaya a la sección **Administración de activos → Dispositivos administrados** o abra una selección de dispositivos.

2. Seleccione la casilla junto al dispositivo administrado al que desea conectarse de forma remota y, luego, haga clic en el botón **Conectar con escritorio remoto**.

   Se abre la ventana **Conectar con escritorio remoto**.

Si selecciona varios dispositivos, un dispositivo móvil o un dispositivo con macOS, el botón **Conectar con escritorio remoto** se deshabilitará.

3. En la ventana **Conectar con escritorio remoto**, seleccione el tipo de conexión **VNC**.

4. Descargue la utilidad klsctunnel haciendo clic en el botón **Descargar** y, luego, ejecútela.

   Si el archivo de utilidad no está disponible para descargar, se muestra un mensaje de error. En este caso, descargue la utilidad manualmente.

5. En la ventana **Conectar con escritorio remoto**, especifique el puerto de conexión VNC. El número de puerto predeterminado es 5900.

6. Genere un blob de texto con parámetros de conexión codificados haciendo clic en el botón **Generar blob** y, luego, copie y pegue el texto en el campo correspondiente en la utilidad klsctunnel.

   Un blob contiene las configuraciones necesarias para establecer una conexión entre el Servidor de administración y el dispositivo administrado. Los blobs tienen una validez de tres minutos. Si el blob caduca, genere uno nuevo.

7. En la utilidad klsctunnel, si utiliza un servidor proxy, especifique la configuración de conexión del servidor proxy.

   Para ello, seleccione la casilla **Usar servidor proxy** y, luego, especifique la configuración de conexión.

8. Haga clic en el botón **Abrir puerto**.

   La utilidad klsctunnel muestra la dirección y el puerto para la conexión local de un cliente VNC.

   La utilidad permite al usuario remoto cerrar la conexión del túnel. Si se cierra la conexión del túnel, se finaliza la conexión actual con el escritorio remoto.

9. Ejecute un cliente VNC y conéctelo al dispositivo administrado utilizando la dirección y el puerto proporcionados por la utilidad klsctunnel.

Se establece la conexión con el dispositivo administrado. El escritorio está disponible en la ventana del cliente VNC.

Acceso remoto desde un dispositivo basado en Windows con Kaspersky Security Center Web Console a un dispositivo administrado basado en Windows

Conexión a escritorio remoto (RDP)

Requisitos previos

Antes de comenzar, compruebe que hizo lo siguiente:

- En el dispositivo administrado con Windows, se instala el Agente de red 13 o versiones posteriores.
- El administrador tiene el derecho **Iniciar sesiones RDP** para establecer conexiones RDP.

- Se abre el puerto para tunelizar conexiones RDP (la opción **Abrir puerto para tunelización de conexiones RDP** está habilitada en la sección **Puertos de conexión** de la ventana de propiedades del Servidor de administración).

- Las conexiones remotas están permitidas por el sistema operativo del dispositivo administrado.

Para conectarse a un dispositivo administrado con Windows mediante RDP a través de Kaspersky Security Center Web Console abierto en un dispositivo con Windows:

1. En el menú principal, vaya a la sección **Administración de activos** → **Dispositivos administrados** o abra una selección de dispositivos.

2. Seleccione la casilla junto al dispositivo administrado al que desea conectarse de forma remota y, luego, haga clic en el botón **Conectar con escritorio remoto**.

   Se abre la ventana **Conectar con escritorio remoto**.

   Si selecciona varios dispositivos, un dispositivo móvil o un dispositivo con macOS, el botón **Conectar con escritorio remoto** se deshabilitará.

3. En la ventana **Conectar con escritorio remoto**, seleccione el tipo de conexión **Conexión a escritorio remoto**.

4. Si la conexión remota no está permitida en la configuración del sistema operativo del dispositivo administrado, permita la conexión remota de forma centralizada haciendo clic en el botón **Cambiar ajustes**.

   Si la configuración se aplica correctamente, se muestra una notificación. Además, en el dispositivo administrado, en la sección **Configuración** → **Sistema** → **Escritorio remoto**, está habilitada la opción **Habilitar escritorio remoto**.

   Si la conexión remota está permitida en la configuración del sistema operativo del dispositivo administrado, no se muestra el botón **Cambiar ajustes**.

5. Descargue la utilidad klsctunnel haciendo clic en el botón **Descargar** y, luego, ejecútela.

   Al descargar la utilidad, tenga en cuenta lo siguiente:

   - Para obtener una versión actualizada de la utilidad klsctunnel, asegúrese de que el Servidor de administración tenga acceso a los servidores de actualización de Kaspersky.

     Puede ejecutar la tarea *Descargar actualizaciones en el repositorio de la tarea del Servidor de administración* y seleccionar los servidores de actualizaciones de Kaspersky como origen de actualizaciones. Si la tarea finaliza correctamente, el Servidor de administración tendrá acceso a los servidores de actualización de Kaspersky.

   - Si el archivo de utilidad no está disponible para descargar, se muestra un mensaje de error. En este caso, descargue la utilidad manualmente y, luego, colóquela en el dispositivo del Servidor de administración en el directorio /var/opt/kaspersky/klnagent_srv.

6. Genere un blob de texto con parámetros de conexión codificados haciendo clic en el botón **Generar blob** y, luego, copie y pegue el texto en el campo correspondiente en la utilidad klsctunnel.

   Un blob contiene las configuraciones necesarias para establecer una conexión entre el Servidor de administración y el dispositivo administrado. Los blobs tienen una validez de tres minutos. Si el blob caduca, genere uno nuevo.

7. En la utilidad klsctunnel, si utiliza un servidor proxy, especifique la configuración de conexión del servidor proxy.

   Para ello, seleccione la casilla **Usar servidor proxy** y, luego, especifique la configuración de conexión.

8. Haga clic en el botón **Abrir puerto**.

   Se abre la ventana de inicio de sesión de Conexión a Escritorio remoto.

9. Especifique las credenciales de la cuenta con la que haya iniciado sesión en Kaspersky Security Center Web Console y, luego, conéctese al dispositivo administrado.

   La utilidad klsctunnel muestra la dirección y el puerto de la conexión al dispositivo remoto.

   La utilidad permite al administrador cerrar la conexión del túnel. Si se cierra la conexión del túnel, se finaliza la conexión actual con el escritorio remoto.

   Una vez que se establezca la conexión con el dispositivo, tendrá acceso al escritorio a través de la ventana Conexión a Escritorio remoto de Microsoft Windows.

Si se conecta a la sesión de escritorio remoto establecida por un usuario, lo hará sin que el usuario lo sepa. Una vez que el administrador se conecta a la sesión, el usuario del dispositivo queda desconectado de la sesión sin notificación.

Escritorio compartido de Windows (WDS)

Requisitos previos

Antes de comenzar, compruebe que hizo lo siguiente:

- En el dispositivo administrado con Windows, se instala el Agente de red 13 o versiones posteriores.
- El administrador tiene el derecho **Conexión a sesiones de RDP existentes** para establecer la conexión WDS.
- La licencia para Administración de vulnerabilidades y parches está disponible.
- La estación de trabajo del administrador debe tener Microsoft Windows Vista o una versión de Windows posterior. El tipo de sistema operativo del dispositivo que alberga al Servidor de administración no impone restricciones con respecto a la conexión a través de Windows Desktop Sharing.

  Verifique si la función Escritorio compartido de Windows está incluida en su edición de Windows y verifique que la clave CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} esté presente en el registro de Windows.
- El dispositivo cliente debe tener Microsoft Windows Vista o una versión de Windows posterior.

Para conectarse a un dispositivo administrado con Windows mediante VNC a través de Kaspersky Security Center Web Console abierto en un dispositivo con Windows:

1. En el menú principal, vaya a la sección **Administración de activos** → **Dispositivos administrados** o abra una selección de dispositivos.
2. Seleccione la casilla junto al dispositivo administrado al que desea conectarse de forma remota y, luego, haga clic en el botón **Conectar con escritorio remoto**.

   Se abre la ventana **Conectar con escritorio remoto**.

   Si selecciona varios dispositivos, un dispositivo móvil o un dispositivo con macOS, el botón **Conectar con escritorio remoto** se deshabilitará.
3. En la ventana **Conectar con escritorio remoto**, seleccione el tipo de conexión **Windows Desktop Sharing**.

   Si Administración de vulnerabilidades y parches no está disponible, se muestra un mensaje de error.
4. Descargue la utilidad klsctunnel haciendo clic en el botón **Descargar** y, luego, ejecútela.

   Si el archivo de utilidad no está disponible para descargar, se muestra un mensaje de error. En este caso, descargue la utilidad manualmente.

5. En la lista de sesiones de usuario disponibles activas en el dispositivo seleccionado, seleccione la sesión a la que desea conectarse.

   El usuario remoto debe permitir la conexión. Si el usuario remoto se niega a conectarse o no permite la conexión durante el período de tiempo de espera, se muestra un mensaje de error.

6. Genere un blob de texto con parámetros de conexión codificados haciendo clic en el botón **Generar blob** y, luego, copie y pegue el texto en el campo correspondiente en la utilidad klsctunnel.

   Un blob contiene las configuraciones necesarias para establecer una conexión entre el Servidor de administración y el dispositivo administrado. Los blobs tienen una validez de tres minutos. Si el blob caduca, genere uno nuevo.

7. En la utilidad klsctunnel, si utiliza un servidor proxy, especifique la configuración de conexión del servidor proxy.

   Para ello, seleccione la casilla **Usar servidor proxy** y, luego, especifique la configuración de conexión.

8. Haga clic en el botón **Abrir puerto**.

   La utilidad klsctunnel muestra la dirección y el puerto para la conexión local de un cliente VNC.

   La utilidad permite al usuario remoto cerrar la conexión del túnel. Si se cierra la conexión del túnel, se finaliza la conexión actual con el escritorio remoto.

La sesión de escritorio compartido se abre en una nueva ventana. Si necesita interactuar con el dispositivo, haga clic en el ícono de menú ( ) ubicado en la esquina superior izquierda de la ventana y seleccione **Modo interactivo**.

Administración de dispositivos móviles

Para administrar la protección de dispositivos móviles a través de Kaspersky Security Center, se utiliza la función Administración de dispositivos móviles. Se necesita agregar una clave de licencia en cada dispositivo móvil para activar la aplicación de protección. Active y configure la característica Administración de dispositivos móviles si planea administrar dispositivos móviles que pertenezcan a los empleados de su organización.

La función Administración de dispositivos móviles permite administrar los dispositivos Android y iOS de los empleados. La protección está a cargo de la app Kaspersky Endpoint Security para Android y el sistema de administración para dispositivos iOS instalado en los dispositivos móviles. Estas aplicaciones móviles garantizan la protección de los dispositivos móviles contra amenazas web, virus y otros programas riesgosos. Para permitir la administración centralizada a través de Kaspersky Security Center Web Console, debe instalar los siguientes complementos de administración web en el dispositivo en el que esté instalado Kaspersky Security Center Web Console:

- Administración y protección de dispositivos móviles de Kaspersky

  El complemento Administración y protección de dispositivos móviles de Kaspersky permite usar Kaspersky Security Center Web Console para administrar dispositivos que ejecuten Android y iOS.

- Configuración del Servidor de MDM para iOS

  El complemento de configuración del Servidor de MDM para iOS puede usarse para configurar los ajustes del Servidor de MDM para iOS que se usan para conectar dispositivos iOS al Servidor de administración; permite también administrar los dispositivos iOS.

Para obtener información sobre el despliegue de la protección y la administración de dispositivos móviles, consulte la Ayuda de Kaspersky Security para dispositivos móviles y la Ayuda de Kaspersky Secure Mobility Management.

Usar Firebase Cloud Messaging

Para garantizar que los comandos se entreguen a los dispositivos Android en tiempo y forma, Kaspersky Security Center Linux utiliza el mecanismo de notificaciones push. Los dispositivos Android y el Servidor de administración intercambian notificaciones push a través de Firebase Cloud Messaging (en adelante, FCM). En Kaspersky Security Center Linux Web Console, puede definir los ajustes de Firebase Cloud Messaging que permitan conectar los dispositivos Android al servicio.

Para obtener los ajustes de Firebase Cloud Messaging, debe tener una cuenta de Google.

Para habilitar el uso de FCM:

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione **Administración de activos** → **Mobile** → **Devices**.
2. Abra el menú de 3 puntos (⋮) y seleccione **Forced Android device synchronization**.
3. En el campo **Firebase project number**, ingrese el id. del remitente de FCM.
4. En el campo **Private key**, seleccione el archivo de clave privada.

   En la siguiente sincronización con el Servidor de administración, los dispositivos Android se conectarán a Firebase Cloud Messaging.

Cuando se cambia a otro proyecto de Firebase, se debe esperar 10 minutos para que FCM reanude su ejecución.

El servicio de FCM opera en los siguientes intervalos de direcciones:

- Del lado del dispositivo Android, se requiere acceso a los puertos 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS) y 5230 (HTTPS) de las siguientes direcciones:
  - google.com
  - fcm.googleapis.com
  - oauth2.googleapis.com
  - android.apis.google.com
  - Todas las direcciones IP incluidas en el ASN 15169, perteneciente a Google
- Del lado del Servidor de administración, se requiere acceso al puerto 443 (HTTPS) de las siguientes direcciones:
  - fcm.googleapis.com
  - Todas las direcciones IP incluidas en el ASN 15169, perteneciente a Google

Si se configuró un servidor proxy en las propiedades del Servidor de administración dentro Kaspersky Security Center Web Console, se lo usará para la interacción con FCM.

Configuración de FCM: obtener el Id. del remitente y el archivo de clave privada

Para configurar FCM:

1. Regístrese en el portal de Google.
2. Vaya a la consola de Firebase.
3. Realice una de las siguientes acciones:
   - Para crear un nuevo proyecto, haga clic en **Crear un proyecto** y siga las instrucciones en pantalla.
   - Abra un proyecto existente.
4. Haga clic en el ícono de ajustes y seleccione **Configuración del proyecto**.
   Se abre la ventana **Configuración del proyecto**.
5. Seleccione la pestaña **Cloud Messaging**.
6. Recupere el id. del remitente correspondiente del campo **Id. del remitente** en la sección **API de Firebase Cloud Messaging (V1)**.
7. Seleccione la pestaña **Cuentas de servicio** y haga clic en **Generar nueva clave privada**.
8. En la ventana que se abre, haga clic en **Generar clave** para generar y descargar un archivo de clave privada.

Firebase Cloud Messaging queda configurado.

Integración con una infraestructura de claves públicas

Puede integrar la emisión de certificados con la entidad de certificación (CA) de Microsoft a través de una infraestructura de claves pública (PKI). La integración con una PKI está destinada a simplificar la emisión de certificados de usuario de dominio por parte del Servidor de administración. Una vez que se completa la integración, los certificados se emiten automáticamente.

Para obtener información detallada sobre cómo configurar la integración con una PKI para emitir certificados, consulte la Ayuda de Kaspersky Secure Mobility Management.

Puede realizar la integración con una PKI con los ajustes indicados y designar la PKI como origen de certificados para tipos específicos de certificados. Los ajustes de integración con PKI permiten establecer una plantilla predeterminada individual para todos los tipos de certificados.

Particularidades del uso de la integración con PKI para la emisión de certificados:

- La integración con PKI está desactivada de forma predeterminada. Para obtener información detallada sobre cómo activar una PKI y configurar sus ajustes, consulte la Ayuda de Kaspersky Secure Mobility Management.

- Los certificados se emiten mediante el Agente de red para Windows. Esto garantiza la integración entre el Servidor de administración y la CA de Microsoft. Como puede haber varios dispositivos con el Agente de red instalado, puede elegir el dispositivo que se conectará a la CA de Microsoft en las **Issuance rules**. Este dispositivo deberá tener un certificado de agente de inscripción (EA) instalado en el repositorio de certificados de la cuenta usada para la integración con la PKI. Este certificado es emitido por el administrador de la entidad de certificación (CA) del dominio.

- La cuenta con la que se realiza la integración con la PKI debe ser de un usuario de dominio y debe contar con el derecho *Iniciar sesión como servicio*.

- Kaspersky Security Center Linux solo puede funcionar con una integración con PKI (CA de Microsoft) a la vez.

Administrar grupos de administración

Esta sección proporciona información sobre cómo administrar grupos de administración.

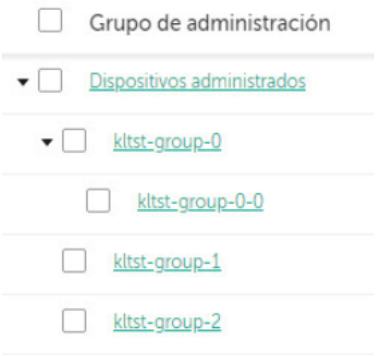
Se pueden realizar las siguientes acciones en los grupos de administración:

- Agregar cualquier número de grupos anidados de cualquier nivel de jerarquía a los grupos de administración.
- Agregar dispositivos a grupos de administración.
- Cambiar la jerarquía de los grupos de administración moviendo los dispositivos individuales y los grupos enteros a otros grupos.
- Eliminar los grupos anidados y los dispositivos de los grupos de administración.
- Agregar Servidores de administración secundarios y virtuales a los grupos de administración.
- Mover los dispositivos de los grupos de administración de un Servidor de administración a los de otro Servidor.
- Definir qué aplicaciones de Kaspersky serán automáticamente instaladas en los dispositivos incluidos en un grupo.

Puede realizar estas acciones solo si tiene el permiso **Modificar** en el área **Administración de grupos de administración** para los grupos de administración que desea administrar (o para el Servidor de administración al que pertenecen estos grupos).

Creación de grupos de administración

Inmediatamente después de la instalación de Kaspersky Security Center, la jerarquía de los grupos de administración contiene solo un grupo de administración llamado **Dispositivos administrados**. Al crear una jerarquía de grupos de administración, puede añadir dispositivos y máquinas virtuales al grupo **Dispositivos administrados** y añadir grupos anidados (vea la figura a continuación).

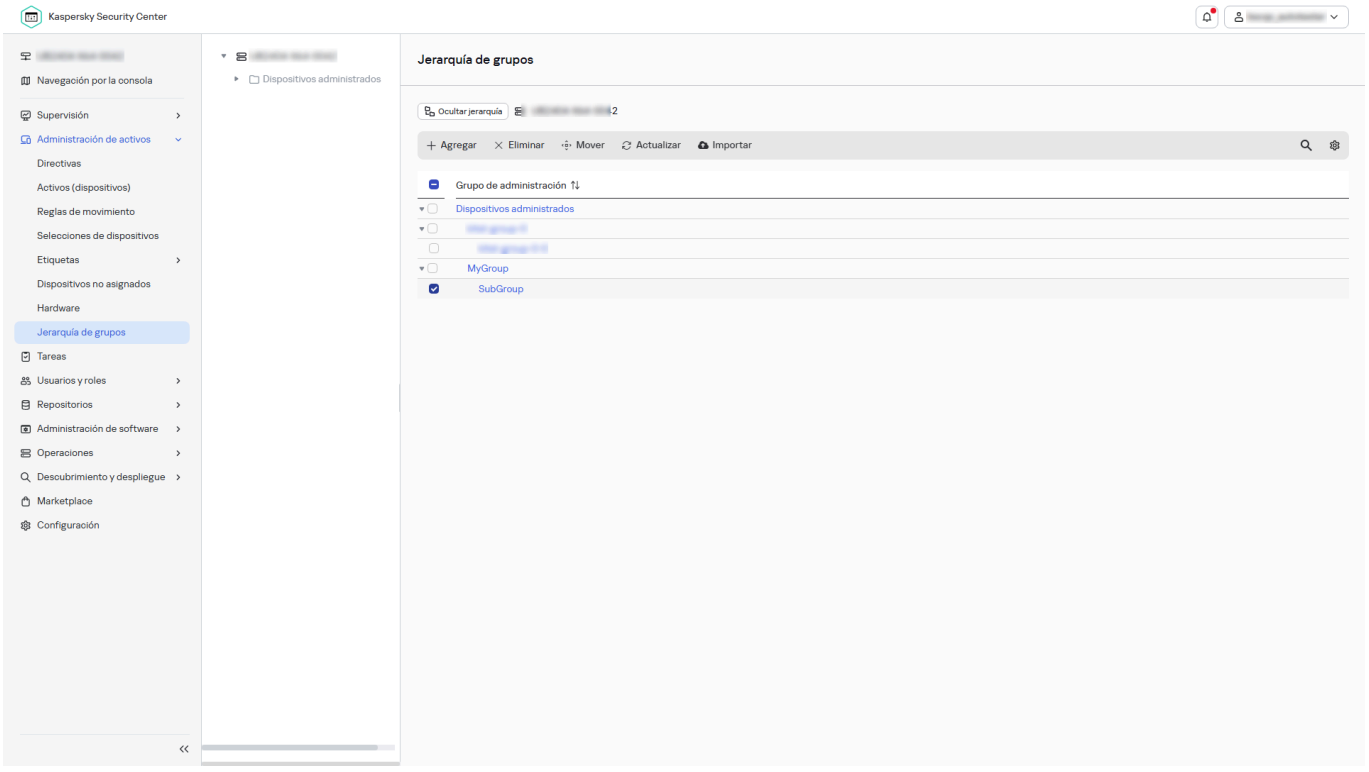


Ver jerarquía de grupos de administración

Para crear un grupo de administración:

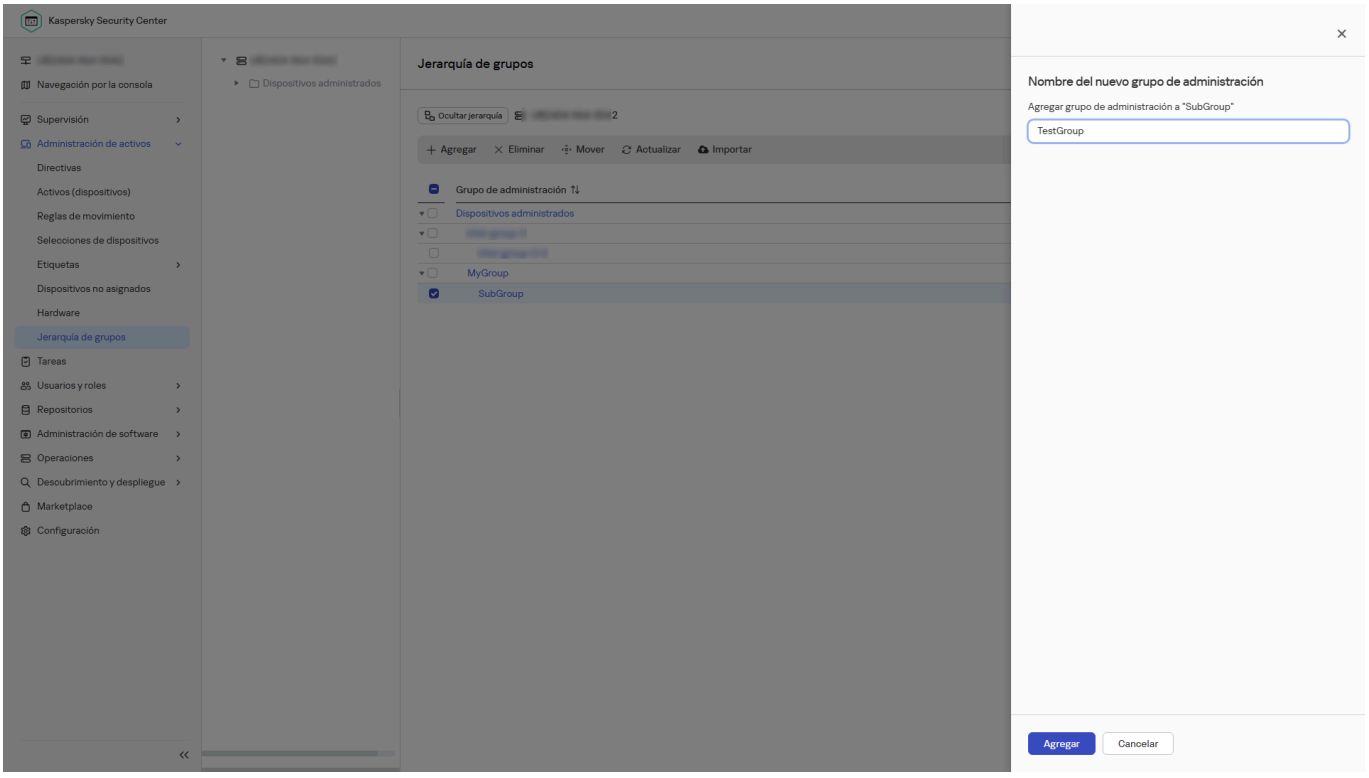
1. En el menú principal, vaya a **Administración de activos** → **Jerarquía de grupos**.

2. En la estructura del grupo de administración, seleccione el grupo de administración donde desea incluir el nuevo grupo de administración.



3. Haga clic en **Agregar**.

4. En la ventana **Nombre del nuevo grupo de administración** que se abre, introduzca el nombre del grupo y haga clic en el botón **Agregar**.



En la jerarquía de grupos de administración, aparecerá un nuevo grupo con el nombre especificado.

Para crear una estructura de grupos de administración:

1. En el menú principal, vaya a **Administración de activos** → **Jerarquía de grupos**.
2. Haga clic en **Importar**.

Se inicia el Asistente de nueva estructura de grupos de administración. Siga los pasos del asistente.

Instalación automática de aplicaciones en dispositivos de un grupo de administración

Puede especificar qué paquetes de instalación deben utilizarse para la instalación remota automática de aplicaciones Kaspersky en dispositivos cliente de un grupo de administración.

Para configurar la instalación automática de las aplicaciones en dispositivos nuevos de un grupo de administración:

1. En el menú principal, vaya a **Administración de activos** → **Jerarquía de grupos**.
2. Vaya a las propiedades del grupo de administración que necesite de una de las siguientes maneras:
   - Haga clic en el nombre del grupo de administración.
   - Haga clic en el botón **Mostrar jerarquía** en la parte superior de la página. En el panel de navegación que se abre, coloque el cursor sobre el nombre del grupo que necesite y luego haga clic en el ícono de configuración (⚙).

   Se abrirá la ventana de propiedades del grupo de administración.
3. En la ventana, vaya a la pestaña **Instalación automática**.
4. Seleccione los paquetes de instalación de las aplicaciones que desea instalar en los dispositivos y haga clic en el botón **Guardar**.

   Si selecciona varios paquetes de instalación de la misma aplicación que difieren solo en sus versiones, se guarda el paquete de instalación con la última versión.

Después de seleccionar los paquetes de instalación, se crea un grupo de tareas para la instalación de las aplicaciones en los dispositivos del grupo de administración para cada una de las aplicaciones. Estas tareas se ejecutan en los dispositivos cliente inmediatamente después de que se agregan al grupo de administración.

Traslado de grupos de administración

Puede mover grupos de administración anidados dentro de la jerarquía de grupos.

Un grupo de administración se mueve junto con todos sus grupos anidados, Servidores de administración secundarios, dispositivos, directivas de grupo y tareas. El sistema aplicará al grupo toda la configuración correspondiente a su nueva posición en la jerarquía de los grupos de administración.

El nombre del grupo debe ser único dentro de un nivel de la jerarquía. Si ya existe un grupo con el mismo nombre en la carpeta a la que se mueve el grupo de administración, debe cambiar el nombre de este último. Si no cambió el nombre del grupo que se moverá, cuando lo mueva, automáticamente se agregará un índice en formato **(<siguiente número de la secuencia>)** al nombre, por ejemplo: **(1)**, **(2)**.

No puede cambiar de nombre ni mover el grupo **Dispositivos administrados**.

Para mover un grupo de administración a otro nivel de la jerarquía de grupos de administración:

1. En el menú principal, vaya a **Administración de activos** → **Jerarquía de grupos** y luego marque la casilla junto al grupo de administración que desea mover.
2. Haga clic en el botón **Mover** en la barra de herramientas.
3. En la ventana que aparece, seleccione adónde desea mover el grupo de administración y haga clic en el botón **Mover**.

La ventana se cierra y el grupo de administración se mueve a otro nivel de la jerarquía de grupos.

Eliminación de grupos de administración

Si elimina un grupo de administración que contiene Servidores de administración secundarios, grupos anidados, dispositivos cliente, tareas de grupo o directivas creadas para este grupo, también se eliminarán todos ellos.

Antes de eliminar el grupo de administración, debe eliminar todos los Servidores de administración secundarios, grupos anidados y dispositivos cliente de ese grupo.

Para eliminar un grupo de administración:

1. En el menú principal, vaya a **Administración de activos** → **Jerarquía de grupos** y luego seleccione la casilla de verificación junto al grupo de administración que desea eliminar.
2. Haga clic en el botón **Eliminar** en la barra de herramientas.

El grupo de usuario queda eliminado.

Despliegue de las aplicaciones de Kaspersky

En esta sección se describe cómo puede usar Kaspersky Security Center Web Console para desplegar las aplicaciones de Kaspersky en los dispositivos cliente de su organización.

Procedimiento: despliegue de las aplicaciones de Kaspersky

En este escenario se explica cómo desplegar aplicaciones de Kaspersky por medio de Kaspersky Security Center Web Console. Puede utilizar el Asistente de inicio rápido y el Asistente de despliegue de la protección, o puede completar todos los pasos necesarios manualmente.

Las siguientes aplicaciones pueden desplegarse a través de Kaspersky Security Center Web Console:

- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security para Windows

Etapas

El despliegue de las aplicaciones de Kaspersky se divide en etapas:

1. **Descargar complemento web de administración para la aplicación**

   Esta etapa puede completarse con el asistente de inicio rápido. Si opta por no ejecutar el asistente, descargue los complementos manualmente.

2. **Descarga y creación de paquetes de instalación**

   Esta etapa puede completarse con el asistente de inicio rápido.

   El asistente de inicio rápido permite descargar el paquete de instalación con el complemento web de administración. Si no seleccionó esta opción al utilizar el asistente, o si sencillamente no utilizó el Asistente, descargue el paquete manualmente.

   Si no puede instalar aplicaciones de Kaspersky por medio de Kaspersky Security Center Linux en algunos dispositivos, por ejemplo, en dispositivos remotos de empleados, puede crear paquetes de instalación independientes para las aplicaciones. Si usa paquetes independientes para instalar aplicaciones de Kaspersky, no tiene que crear y ejecutar una tarea de instalación remota, ni crear y configurar tareas para Kaspersky Endpoint Security para Windows.

   Como alternativa, puede descargar los paquetes de distribución del Agente de red y de las aplicaciones de seguridad a través del sitio web de Kaspersky. Si algo impide instalar estas aplicaciones a distancia, puede usar los paquetes de distribución descargados para instalar las aplicaciones localmente.

3. **Creación, configuración y ejecución de la tarea de instalación remota**

   Este paso puede llevarse a cabo con el Asistente de despliegue de la protección. Si opta por no ejecutar el Asistente de despliegue de la protección, cree esta tarea y configúrela manualmente.

También puede crear manualmente varias tareas de instalación remotas para grupos de administración diferentes o selecciones de dispositivos diferentes. Puede desplegar diferentes versiones de una aplicación en estas tareas.

Asegúrese de que todos los dispositivos de la red se hayan descubierto; a continuación, ejecute la tarea (o las tareas) de instalación remota.

Si desea instalar el Agente de red en dispositivos con el sistema operativo SUSE Linux Enterprise Server 15, primero, instale el paquete insserv-compat para configurar el Agente de red.

Si desea instalar el Agente de Red en dispositivos que utilicen el sistema operativo RED OS 7.3.4 o posterior, o MSVSPHERE 9.2 o posterior, instale el paquete libxcrypt-compat para el correcto funcionamiento del Agente de Red.

4. **Creación y configuración de tareas**

   La tarea *Actualizar* de Kaspersky Endpoint Security for Linux requiere configuración.

   Este paso puede llevarse a cabo con el asistente de inicio rápido: el asistente creará esta tarea automáticamente y la configurará con los valores predeterminados. Si opta por no ejecutar el asistente, cree esta tarea y configúrela manualmente. Si utiliza el Asistente de inicio rápido, asegúrese de que la programación de la tarea cumpla con sus requisitos. (De manera predeterminada, el inicio programado para la tarea se establece en **Manualmente**, pero es posible que desee elegir otra opción).

5. **Creando directivas**

   Cree la directiva para Kaspersky Endpoint Security de forma manual o a través del asistente de inicio rápido. Puede usar la configuración predeterminada de la directiva. También puede modificar la configuración predeterminada de la directiva según sus necesidades en cualquier momento.

6. **Verificación de los resultados**

   Asegúrese de que el despliegue se haya completado correctamente: tiene directivas y tareas para cada aplicación, y estas aplicaciones están instaladas en los dispositivos administrados.

Resultados

Completar las etapas anteriores tiene los siguientes resultados:

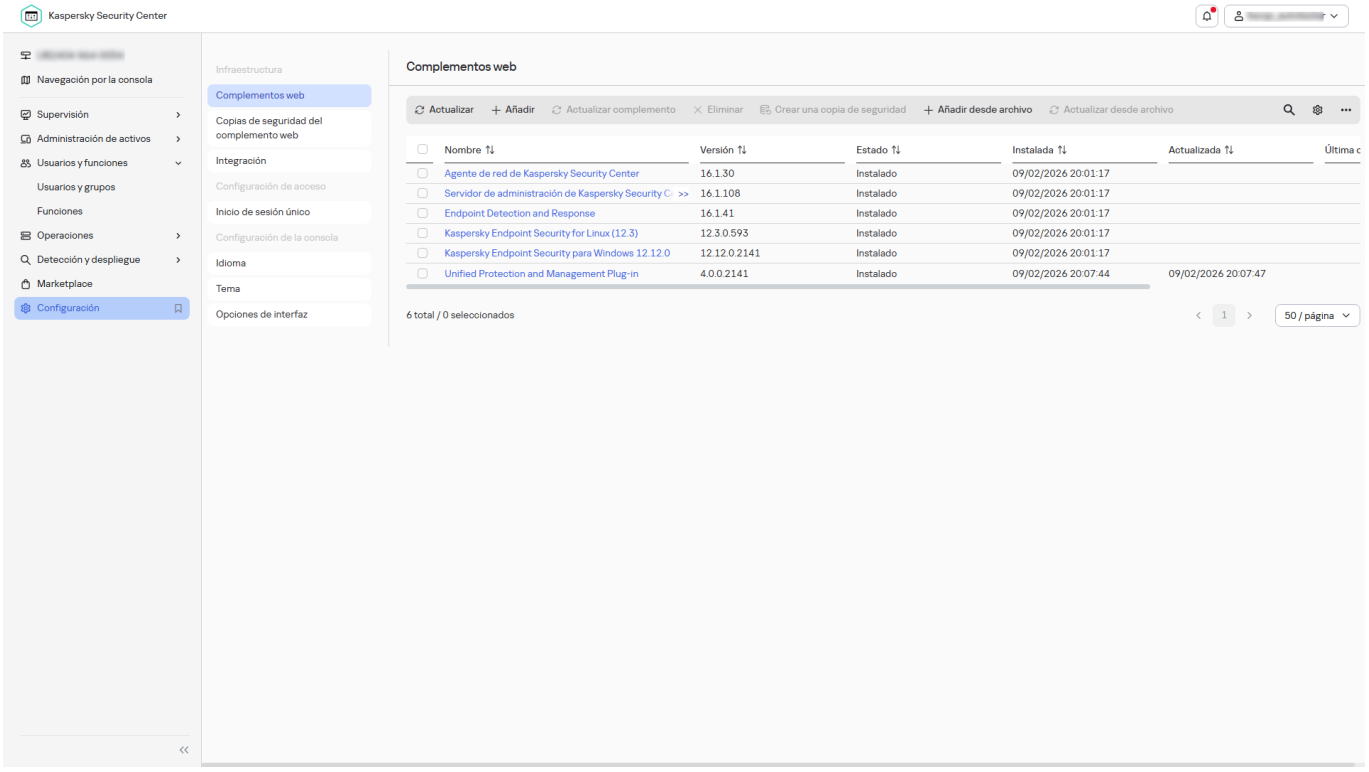
- Se crean todas las directivas y tareas necesarias para las aplicaciones seleccionadas.
- Los horarios de las tareas se configuran de acuerdo a sus necesidades.
- Las aplicaciones seleccionadas se despliegan o programan para desplegarse en los dispositivos cliente seleccionados.

Agregar complementos de administración para aplicaciones de Kaspersky

Para desplegar una aplicación de Kaspersky, por ejemplo, Kaspersky Endpoint Security for Linux o Kaspersky Endpoint Security para Windows, debe agregar e instalar el complemento web de administración de esa aplicación.

Para descargar el complemento web de administración de una aplicación de Kaspersky:

1. En el menú principal, vaya a **Configuración** → **Complementos web**.



La lista de complementos web instalados

2. En la ventana que se abre, haga clic en el botón **Agregar**.

   Se muestra una lista de complementos disponibles.

3. En la lista de complementos disponibles, haga clic en el nombre del complemento que desee descargar (por ejemplo, Kaspersky Endpoint Security for Linux) para seleccionarlo.

   Se muestra una página de descripción del complemento.

4. En la página de descripción del complemento, haga clic en **Instale el complemento**.

5. Cuando la instalación se haya completado, haga clic en **Aceptar**.

El complemento web de administración se descargará con la configuración predeterminada y aparecerá en la lista de complementos web de administración.

Puede agregar complementos y actualizar los complementos descargados desde un archivo. Puede descargar los complementos web de administración desde el sitio web de Kaspersky.

Para descargar un complemento web o actualizar un complemento web desde un archivo:

1. En el menú principal, vaya a **Configuración → Complementos web**.
2. Especifique el archivo del complemento y la firma del archivo:
   - Haga clic en **Agregar desde archivo** para descargar un complemento desde un archivo.
   - Haga clic en **Actualizar desde archivo** para descargar la actualización de un complemento desde un archivo.
3. Especifique el archivo y la firma del archivo.
4. Descargue los archivos especificados.

   El complemento web de administración se descargará del archivo y aparecerá en la lista de complementos de administración.

Paquetes

El paquete de instalación es un conjunto de archivos creados para la instalación remota de una aplicación de Kaspersky. El paquete de instalación contiene una serie de ajustes que se necesitan para instalar la aplicación y ejecutarla inmediatamente una vez que concluye la instalación. La aplicación se configura con los ajustes predeterminados. El paquete de instalación se crea usando archivos con extensiones KPD y KUD que vienen incluidos en el kit de distribución de la aplicación.

Los paquetes de instalación se generan usando los siguientes métodos:

- Automáticamente, desde paquetes de distribución especificados, en función de *descriptores* incluidos (archivos con la extensión kud que contienen reglas para instalación y análisis de resultados, y otra información).
- Desde un archivo comprimido ZIP, CAB, TAR o TAR.GZ para aplicaciones estándar o compatibles.

Los paquetes de instalación generados se organizan jerárquicamente como carpetas, con subcarpetas y archivos. Además del paquete de distribución original, un paquete de instalación contiene la configuración editable (incluida la configuración del instalador y reglas para procesar tales casos como la necesidad de reiniciar el sistema operativo a fin de completar la instalación), así como los módulos auxiliares menores.

Los valores de la configuración de instalación específicos para una aplicación individual compatible se pueden definir en la interfaz de usuario de Kaspersky Security Center Web Console, durante la creación del paquete de instalación. Al realizar la instalación remota de aplicaciones a través de herramientas de Kaspersky Security Center Linux, los paquetes de instalación se entregan a dispositivos de modo que, si se ejecuta el instalador de una aplicación, toda la configuración definida por los administradores quede a disposición para esa aplicación. Al usar herramientas de terceros para la instalación de aplicaciones de Kaspersky, solo tiene que asegurar la disponibilidad del paquete de instalación completo en el dispositivo; es decir, la disponibilidad del paquete de distribución y su configuración. Los paquetes de instalación se crean y almacenan mediante Kaspersky Security Center Linux en una subcarpeta dedicada de la carpeta compartida.

No especifique ningún detalle de cuentas privilegiadas en los parámetros de los paquetes de instalación.

No se admite el despliegue mediante directivas de grupo de Microsoft Windows.

Inmediatamente después de la instalación de Kaspersky Security Center Linux, unos paquetes de instalación se generan automáticamente; están listos para la instalación e incluyen paquetes del Agente de red y paquetes de aplicaciones de seguridad para Microsoft Windows.

A pesar de que la clave de licencia para la licencia de la aplicación se puede establecer en las propiedades del paquete de instalación, no es aconsejable utilizar este método de distribución de licencias debido a que es fácil obtener acceso de lectura a los paquetes de instalación. Lo que hay que hacer es usar claves de licencia de distribución automática o tareas de instalación de claves de licencia.

Descargar y crear paquetes de instalación para aplicaciones de Kaspersky

Puede crear paquetes de instalación de aplicaciones de Kaspersky desde los servidores web de Kaspersky si su Servidor de administración tiene acceso a Internet.

Al crear paquetes de instalación para instalar la aplicación en dispositivos Windows, si recibe el mensaje **Se produjo un error. Vuelva a intentar la descarga**:

1. Cree la marca RlUtilsArchiveDirUsed ejecutando el siguiente comando:

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

2. Ejecute el siguiente comando para reiniciar el servicio del Servidor de administración:

   ```
   systemctl restart kladminserver_srv.service
   ```

3. Descargue los módulos adicionales "Archivos para la instalación remota mediante Kaspersky Security Center" del sitio web de Kaspersky.

   Los archivos comprimidos descargados tienen los siguientes nombres:

   - ri_utils_win32.zip
   - ri_utils_arm64.zip

   No cambie el nombre de los archivos comprimidos.

4. Coloque los archivos en el directorio /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives.

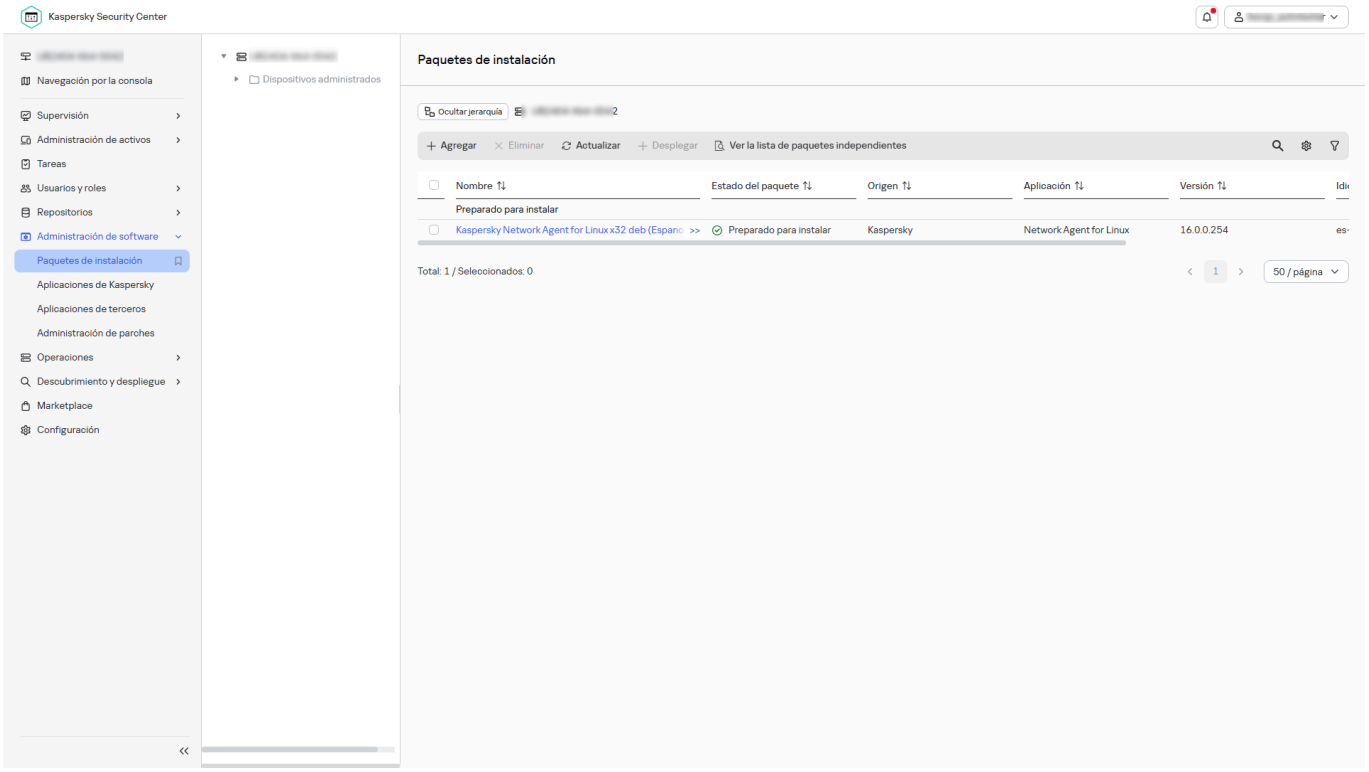
Ahora puede crear un paquete de instalación para instalar la aplicación en dispositivos Windows.

Para descargar y crear un paquete de instalación para una aplicación de Kaspersky:

1. En el menú principal, vaya a **Administración de software → Paquetes de instalación**.

   También puede ver las notificaciones sobre nuevos paquetes para aplicaciones de Kaspersky en la lista de notificaciones en pantalla. Si la lista contiene notificaciones sobre un nuevo paquete, haga clic en el vínculo ubicado junto a una notificación para abrir la lista de paquetes de instalación disponibles.

Se muestra una lista de paquetes de instalación disponibles en el Servidor de administración.

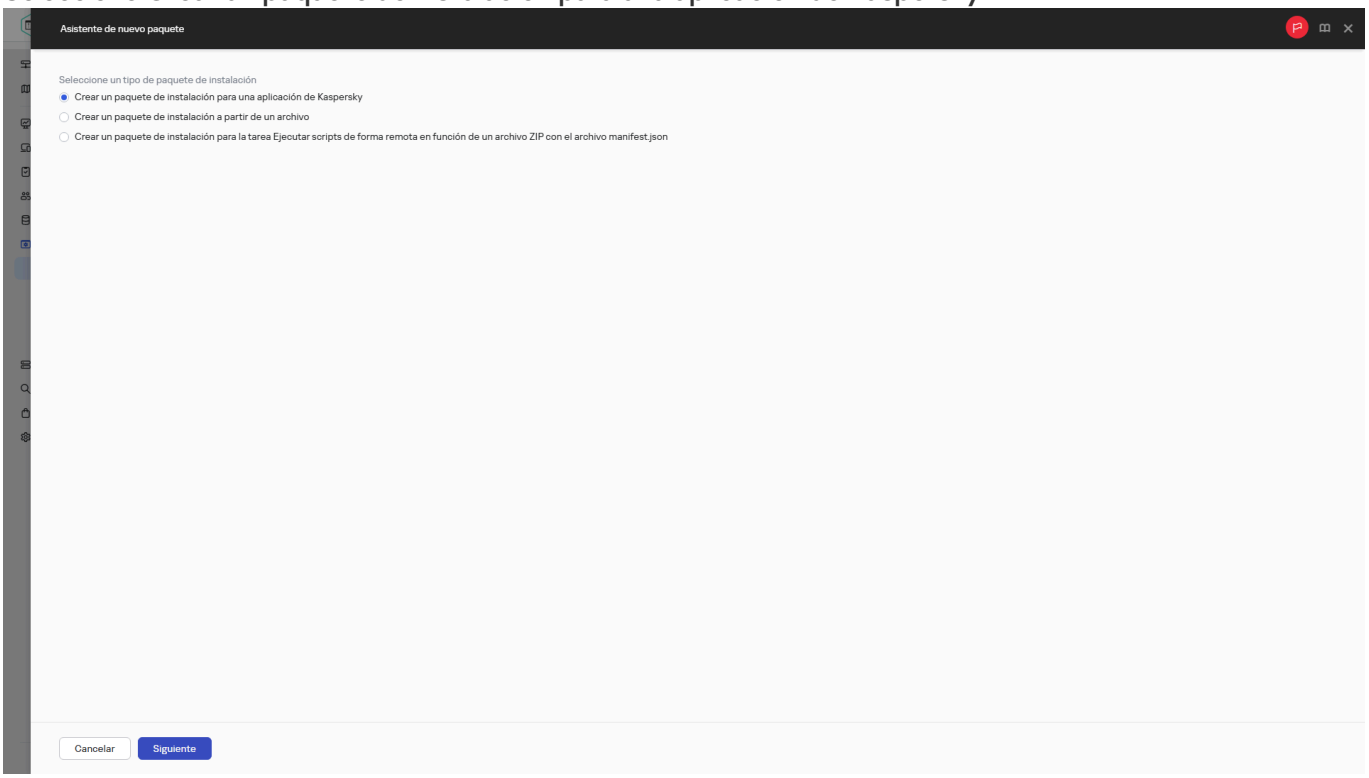


La lista de paquetes de instalación

2. Haga clic en **Agregar**.

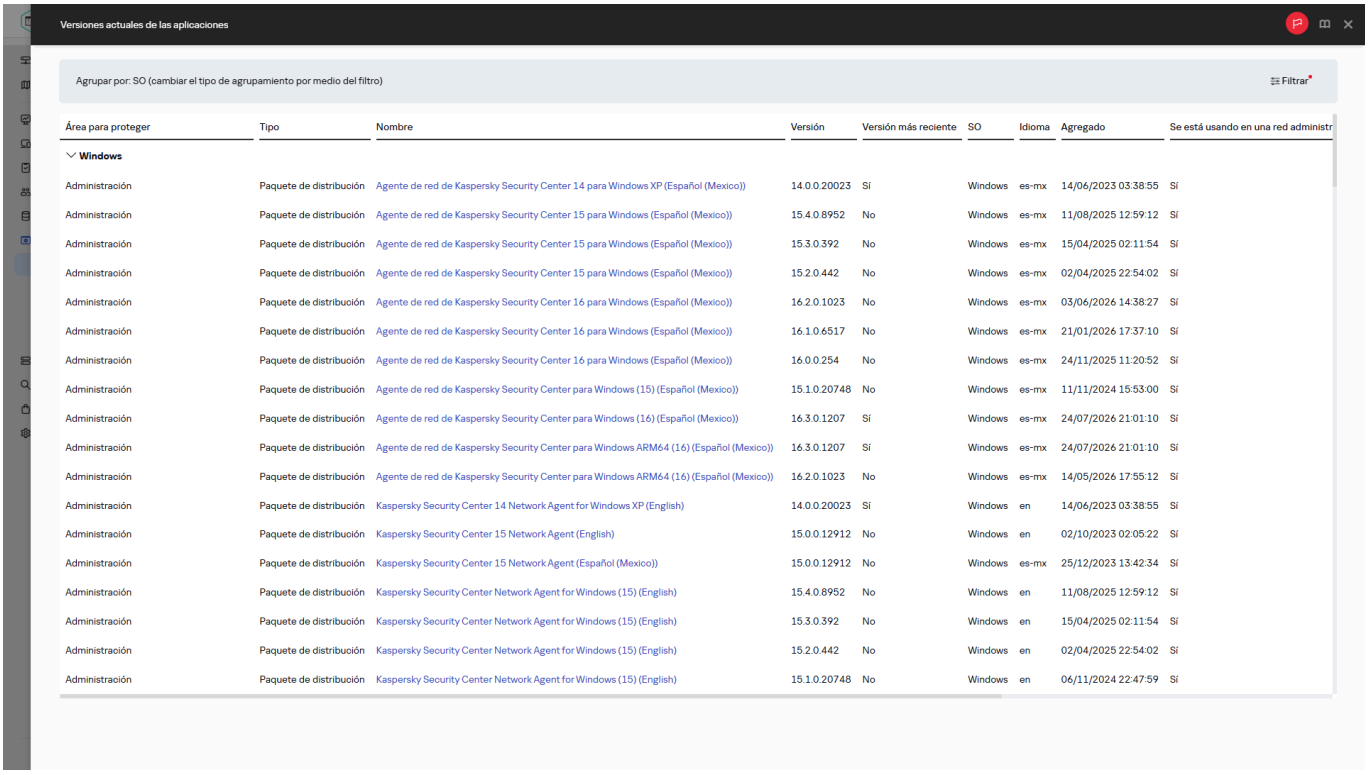
   Se inicia el Asistente de nuevo paquete. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

3. Seleccione **Crear un paquete de instalación para una aplicación de Kaspersky**.



Seleccionar el tipo de paquete de instalación

Aparecerá una lista de paquetes de instalación disponibles en los servidores web de Kaspersky. La lista contendrá únicamente paquetes de instalación de aquellas aplicaciones que sean compatibles con la versión actual de Kaspersky Security Center Linux. De forma predeterminada, la lista solo muestra las aplicaciones en inglés y el idioma que coincide con el idioma de la interfaz. Para mostrar otros idiomas, haga clic en **Filtro** y configure los ajustes del filtro.



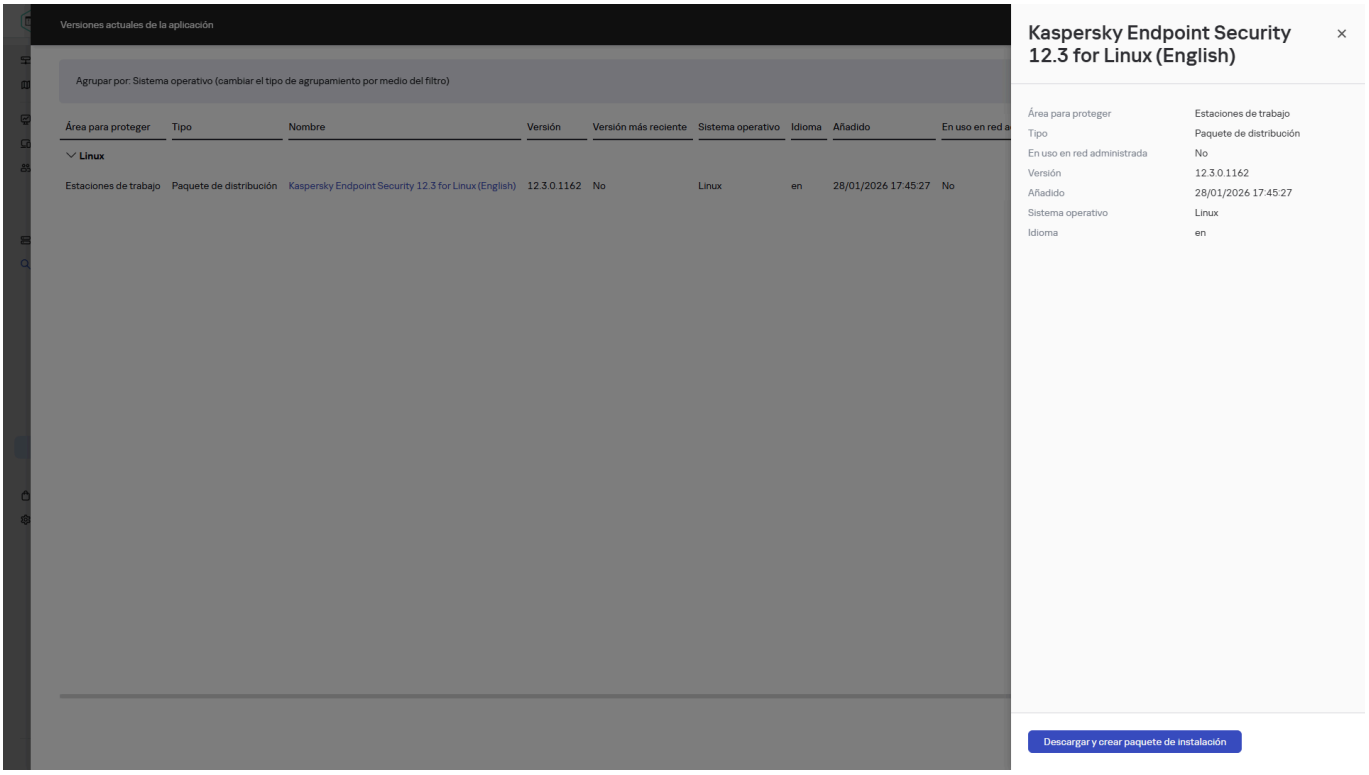
Área para proteger	Tipo	Nombre	Versión	Versión más reciente	SO	Idioma	Agregado	Se está usando en una red administr
Windows								
Administración	Paquete de distribución	Agente de red de Kaspersky Security Center 14 para Windows XP (Español (Mexico))	14.0.0.20023	Sí	Windows	es-mx	14/06/2023 03:38:55	Sí
Administración	Paquete de distribución	Agente de red de Kaspersky Security Center 15 para Windows (Español (Mexico))	15.4.0.8952	No	Windows	es-mx	11/08/2025 12:59:12	Sí
Administración	Paquete de distribución	Agente de red de Kaspersky Security Center 15 para Windows (Español (Mexico))	15.3.0.392	No	Windows	es-mx	15/04/2025 02:11:54	Sí
Administración	Paquete de distribución	Agente de red de Kaspersky Security Center 15 para Windows (Español (Mexico))	15.2.0.442	No	Windows	es-mx	02/04/2025 22:54:02	Sí
Administración	Paquete de distribución	Agente de red de Kaspersky Security Center 16 para Windows (Español (Mexico))	16.2.0.1023	No	Windows	es-mx	03/06/2026 14:38:27	Sí
Administración	Paquete de distribución	Agente de red de Kaspersky Security Center 16 para Windows (Español (Mexico))	16.1.0.6517	No	Windows	es-mx	21/01/2026 17:37:10	Sí
Administración	Paquete de distribución	Agente de red de Kaspersky Security Center 16 para Windows (Español (Mexico))	16.0.0.254	No	Windows	es-mx	24/11/2025 11:20:52	Sí
Administración	Paquete de distribución	Agente de red de Kaspersky Security Center para Windows (15) (Español (Mexico))	15.1.0.20748	No	Windows	es-mx	11/11/2024 15:53:00	Sí
Administración	Paquete de distribución	Agente de red de Kaspersky Security Center para Windows (16) (Español (Mexico))	16.3.0.1207	Sí	Windows	es-mx	24/07/2026 21:01:10	Sí
Administración	Paquete de distribución	Agente de red de Kaspersky Security Center para Windows ARM64 (16) (Español (Mexico))	16.3.0.1207	Sí	Windows	es-mx	24/07/2026 21:01:10	Sí
Administración	Paquete de distribución	Agente de red de Kaspersky Security Center para Windows ARM64 (16) (Español (Mexico))	16.2.0.1023	No	Windows	es-mx	14/05/2026 17:55:12	Sí
Administración	Paquete de distribución	Kaspersky Security Center 14 Network Agent for Windows XP (English)	14.0.0.20023	Sí	Windows	en	14/06/2023 03:38:55	Sí
Administración	Paquete de distribución	Kaspersky Security Center 15 Network Agent (English)	15.0.0.12912	No	Windows	en	02/10/2023 02:05:22	Sí
Administración	Paquete de distribución	Kaspersky Security Center 15 Network Agent (Español (Mexico))	15.0.0.12912	No	Windows	es-mx	25/12/2023 13:42:34	Sí
Administración	Paquete de distribución	Kaspersky Security Center Network Agent for Windows (15) (English)	15.4.0.8952	No	Windows	en	11/08/2025 12:59:12	Sí
Administración	Paquete de distribución	Kaspersky Security Center Network Agent for Windows (15) (English)	15.3.0.392	No	Windows	en	15/04/2025 02:11:54	Sí
Administración	Paquete de distribución	Kaspersky Security Center Network Agent for Windows (15) (English)	15.2.0.442	No	Windows	en	02/04/2025 22:54:02	Sí
Administración	Paquete de distribución	Kaspersky Security Center Network Agent for Windows (15) (English)	15.1.0.20748	No	Windows	en	06/11/2024 22:47:59	Sí

La lista de los paquetes de instalación disponibles

4. Haga clic en el nombre de un paquete de instalación (por ejemplo, "Kaspersky Endpoint Security for Linux").

   Se abrirá una ventana con información sobre el paquete de instalación.

Si esto se ajusta a las leyes y normativas aplicables, puede descargar y usar un paquete de instalación que incluya herramientas criptográficas que implementen un estándar de cifrado fuerte. Para descargar un paquete de distribución de Kaspersky Endpoint Security para Windows que sea adecuado para las necesidades de su organización, consulte la legislación del país donde se encuentren los dispositivos cliente de su organización.



Descargando el paquete de instalación

5. Lea la información y haga clic en el botón **Descargar y crear paquete de instalación**.

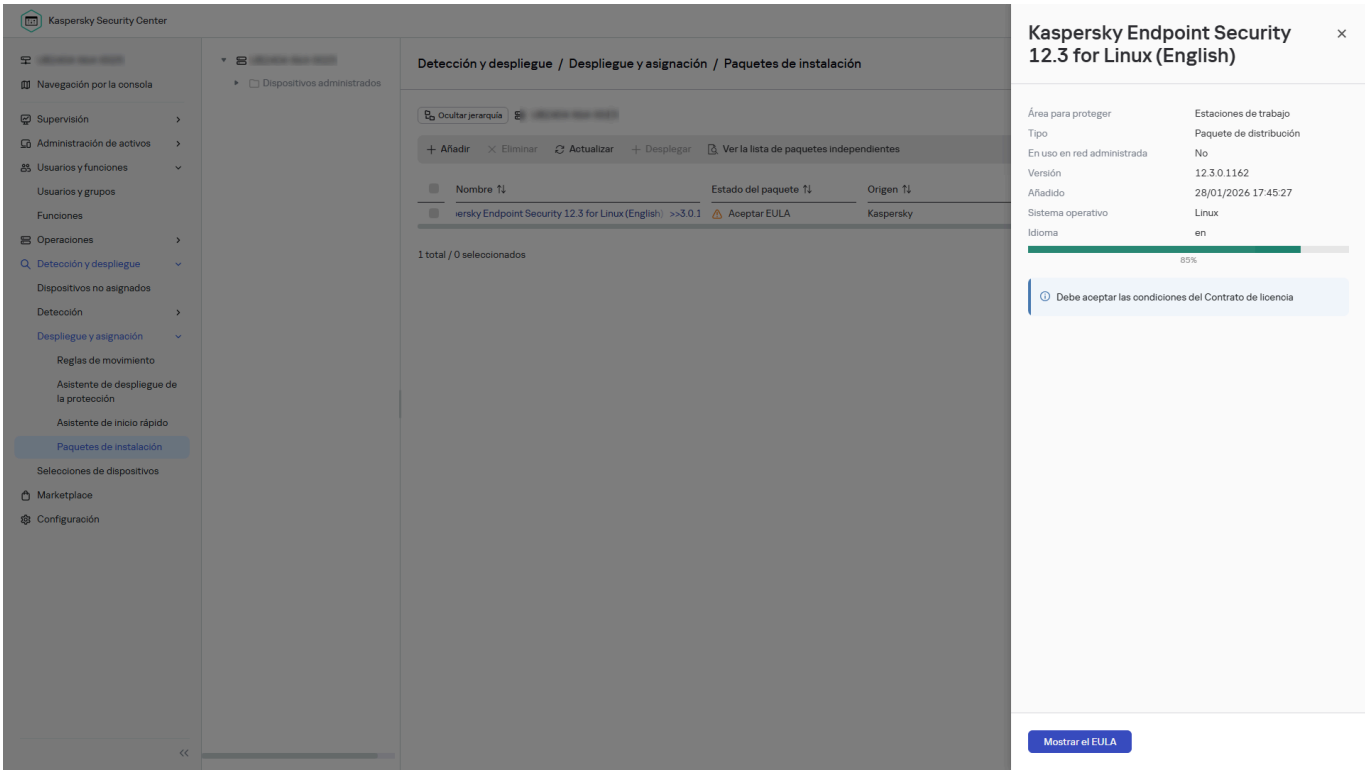
   Si no se puede convertir un paquete de distribución en uno de instalación, se mostrará el botón **Descargar y crear paquete de instalación** en lugar de **Descargar paquete de distribución**.

Para algunas aplicaciones de Kaspersky, antes del proceso de descarga y durante este, se muestra el botón **Mostrar EULA**. Si ve este botón, haga lo siguiente:

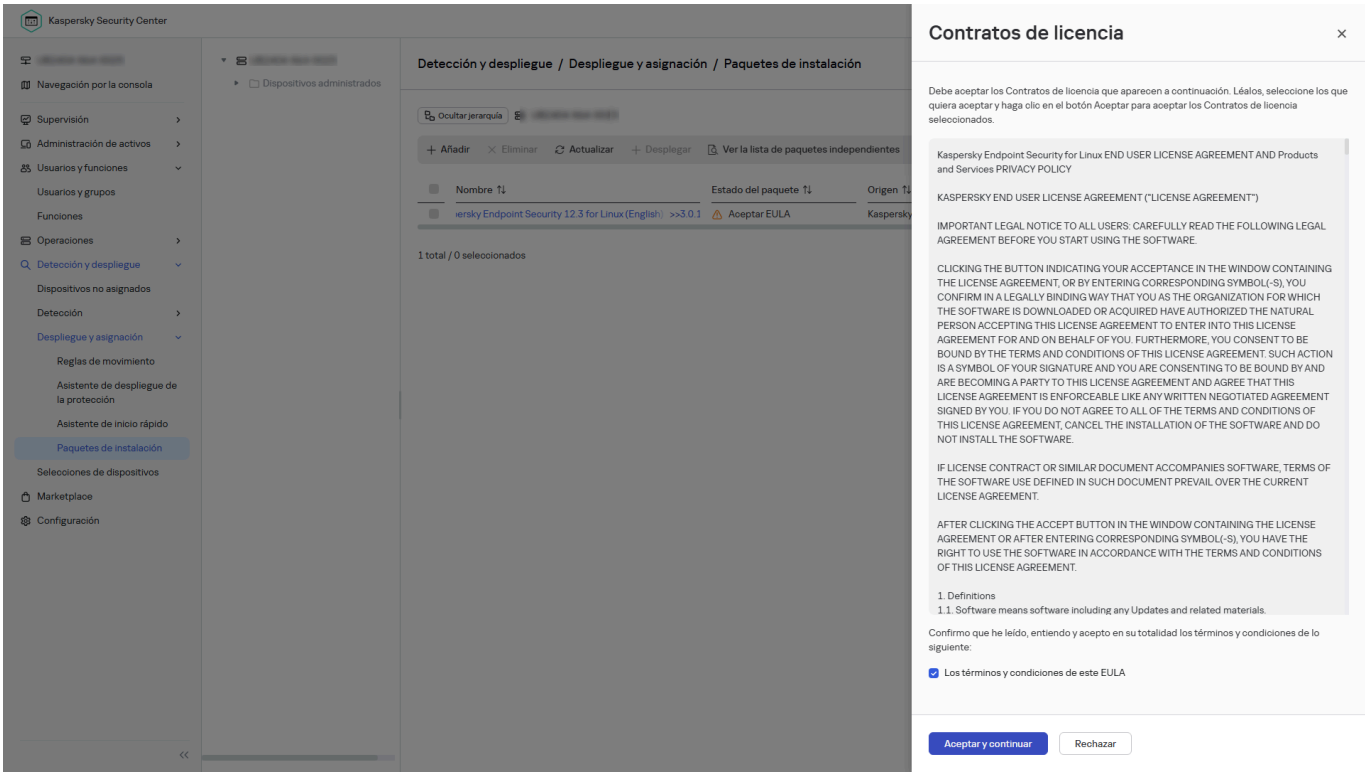
a. Haga clic en el botón **Mostrar EULA** para leer el Contrato de licencia de usuario final (EULA).

b. Lea el EULA que aparece en pantalla y haga clic en **Aceptar**.

La descarga continúa después de aceptar el EULA. Si hace clic en **Rechazar**, la descarga se detiene.



Descargando el paquete de instalación



Aceptar el EULA

Puede cerrar la ventana del asistente. En este caso, el proceso de descarga continuará en el modo de segundo plano. Puede seguir el estado de descarga del paquete de instalación, además de filtrar y ordenar los estados en la columna **Estado del paquete**.

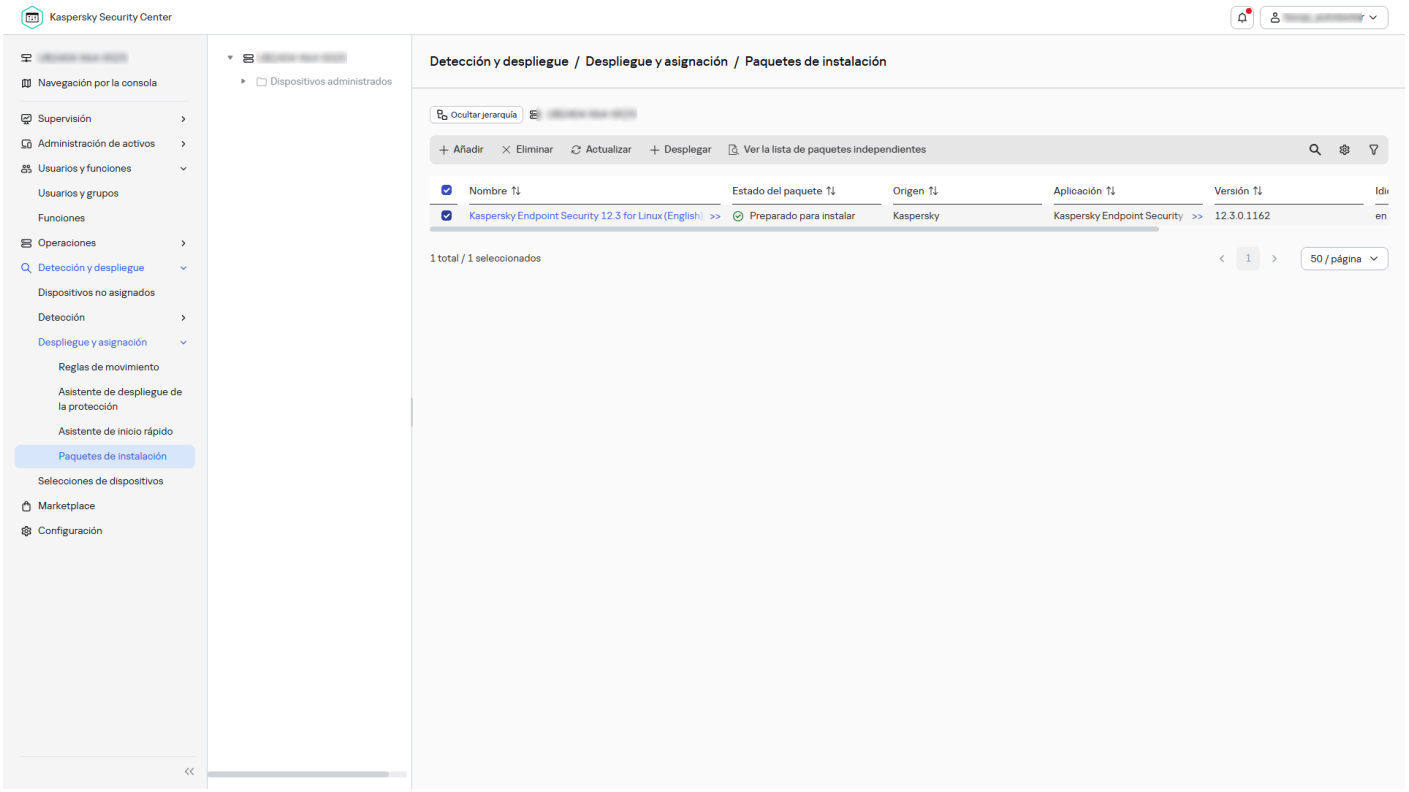
Si la descarga se detiene y el estado de descarga cambia a **Aceptar EULA**, haga clic en el nombre del paquete de instalación y haga los pasos 5.a y 5.b.

De forma predeterminada, los paquetes de instalación con estados **En curso** y **Aceptar EULA** se colocan al principio de la lista.

Si selecciona un paquete de distribución que contenga un volumen de datos mayor de lo admisible, verá un mensaje de error. Para que la aplicación le permita crear el paquete de instalación, deberá modificar el límite pertinente.

6. Cuando se complete la descarga, haga clic en el botón **Cerrar**.

El paquete de instalación seleccionado se descargará a la subcarpeta Packages de la carpeta compartida del Servidor de administración. Cuando termine la descarga, el paquete de instalación aparecerá en la lista de paquetes de instalación.



La lista de paquetes de instalación

Crear paquetes de instalación a partir de un archivo

Puede utilizar paquetes de instalación personalizada para hacer lo siguiente:

- Para instalar cualquier aplicación (como un editor de texto) en un dispositivo cliente, por ejemplo, mediante una tarea.
- para crear un paquete de instalación independiente.

Un paquete de instalación personalizada es una carpeta con un conjunto de archivos. La fuente para crear un paquete de instalación personalizada es un *archivo de almacenamiento*. El archivo de almacenamiento contiene un archivo o archivos que deben incluirse en el paquete de instalación personalizada.

Si el Servidor de administración tiene acceso al repositorio de paquetes de distribución de aplicaciones para la instalación remota, utilice la tarea **Descargar actualizaciones en el repositorio del Servidor de administración** para descargar las dependencias necesarias para crear paquetes de instalación destinados a instalar aplicaciones en dispositivos Windows.

Si el Servidor de administración no tiene acceso al repositorio de paquetes de distribución de aplicaciones para la instalación remota:

1. Cree el indicador RIUtilsArchiveDirUsed mediante la ejecución del siguiente comando:

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

2. Ejecute el siguiente comando para reiniciar el servicio del Servidor de administración:

   ```
   systemctl restart kladminserver_srv.service
   ```

3. Descargue los módulos adicionales "Archivos para la instalación remota mediante Kaspersky Security Center" del sitio web de Kaspersky.

   Los archivos comprimidos descargados tienen los siguientes nombres:

   - ri_utils_win32.zip
   - ri_utils_arm64.zip

   No cambie el nombre de los archivos comprimidos.

4. Coloque los archivos comprimidos en el directorio /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives.

   De lo contrario, al crear un paquete de instalación, se muestra el siguiente error: **No se encontraron las utilidades de instalación remota para win32**.

El Servidor de administración ahora tiene las dependencias necesarias.

Al crear un paquete de instalación personalizada, puede especificar parámetros de línea de comandos, por ejemplo, para instalar la aplicación en modo silencioso.

Vea el video para aprender a crear e implementar un paquete de instalación personalizado para Windows. La versión de texto de este tutorial para dispositivos Windows y Linux está disponible a continuación.

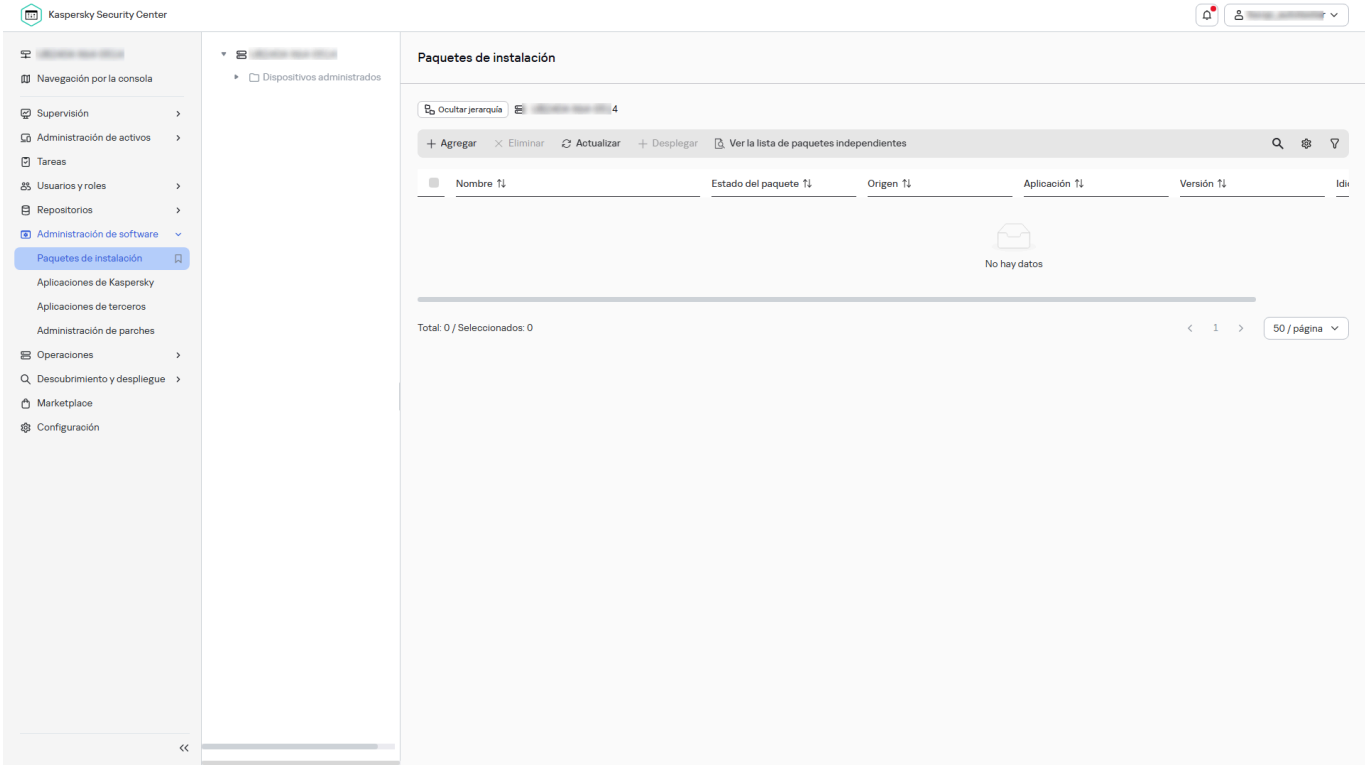


Crear e implementar un paquete de instalación personalizado a partir de un archivo para Windows. Video

Para crear un paquete de instalación personalizado:

1. En el menú principal, vaya a **Administración de software** → **Paquetes de instalación**.

   Se muestra una lista de paquetes de instalación disponibles en el Servidor de administración.

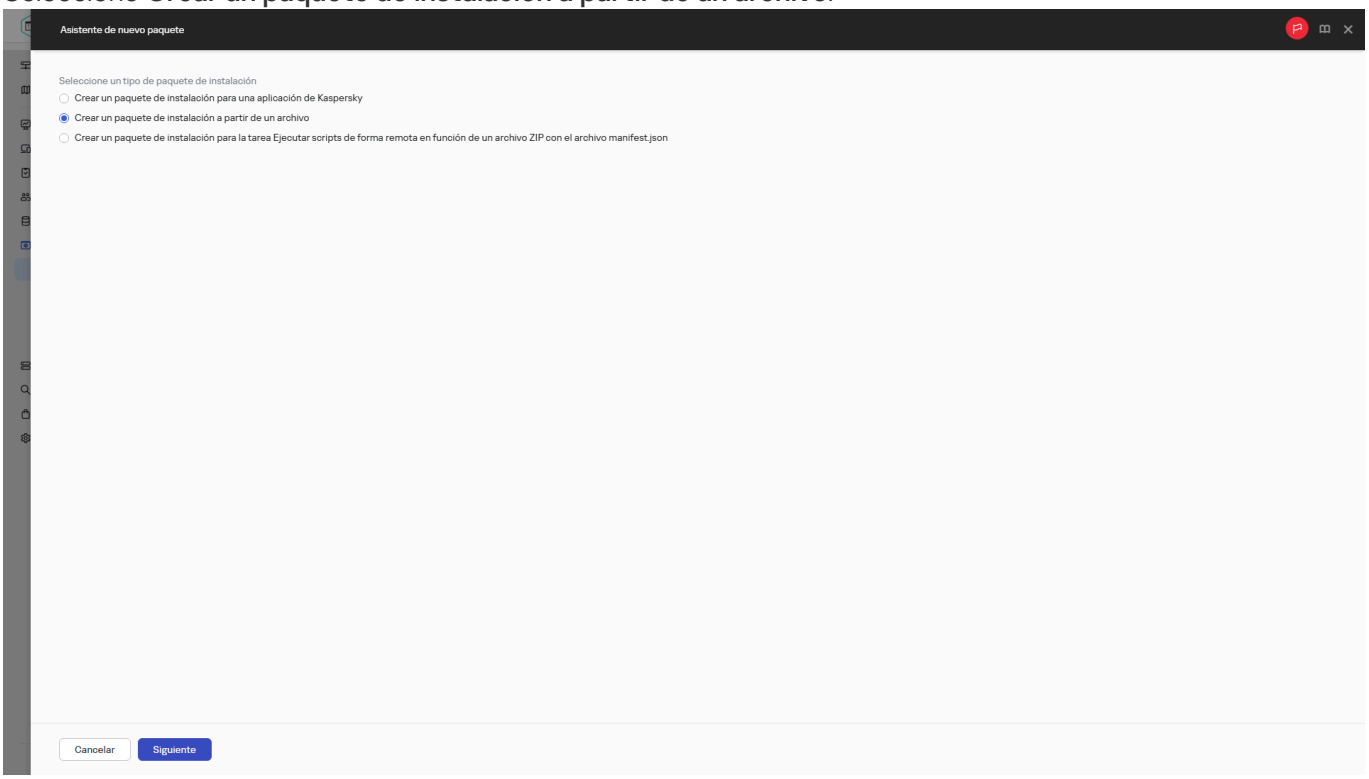


La lista de paquetes de instalación

2. Haga clic en **Agregar**.

   Se inicia el Asistente de nuevo paquete. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

3. Seleccione **Crear un paquete de instalación a partir de un archivo**.



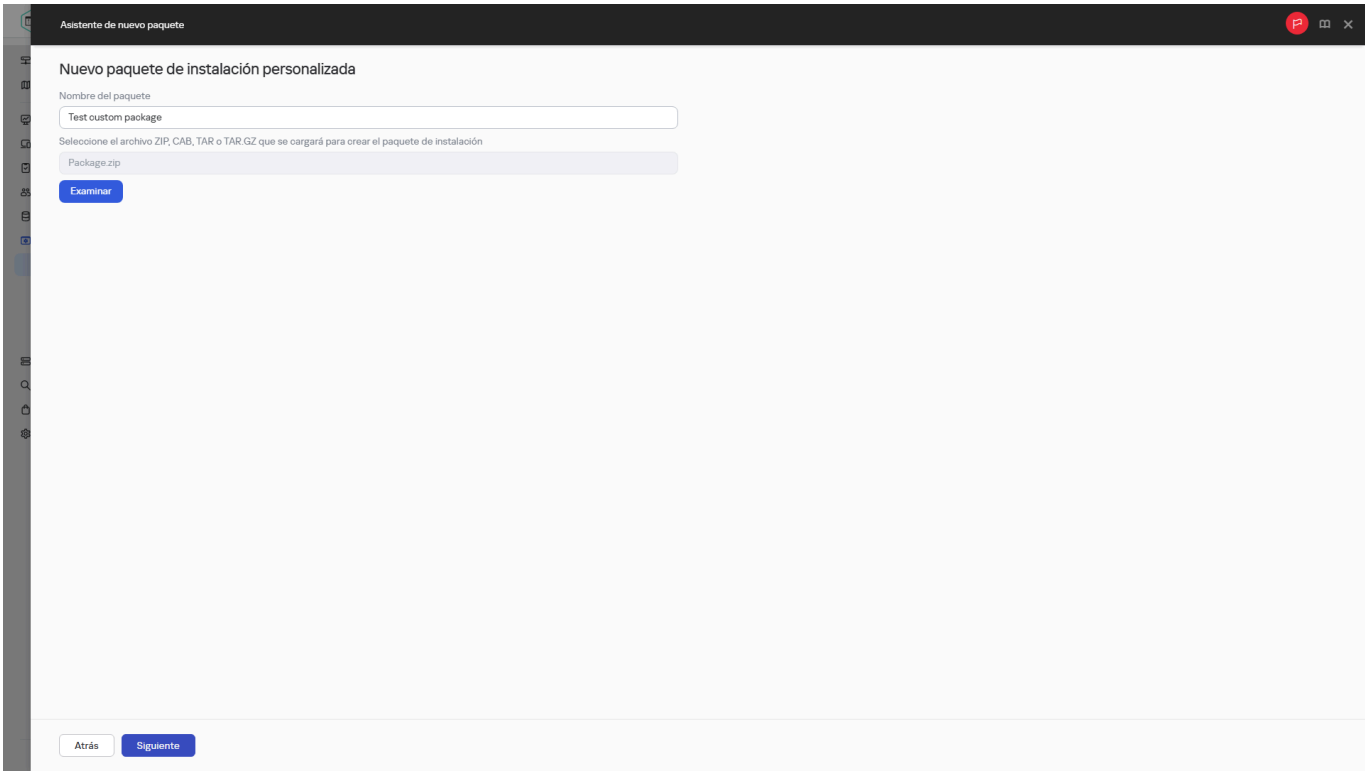
Seleccionar el tipo de paquete de instalación

4. Especifique el nombre del paquete y haga clic en el botón **Examinar**.

5. En la ventana que se abre, elija un archivo de almacenamiento ubicado en los discos disponibles.

   Puede cargar un archivo comprimido ZIP, CAB, TAR o TAR.GZ. No es posible crear un paquete de instalación a partir de un archivo autoextraíble SFX.

   Se inicia la carga de archivos en el Servidor de administración.



Especificar el archivo del paquete de instalación

6. Si especificó un archivo de una aplicación de Kaspersky, es posible que se le pida que lea y acepte el Contrato de licencia de usuario final (EULA) para la aplicación. Para continuar, debe aceptar el EULA. Seleccione la opción **Aceptar los términos y condiciones de este Contrato de licencia de usuario final** solo si ha leído, comprende y acepta en su totalidad los términos del EULA.

   Además, es posible que se le solicite que lea y acepte la Política de privacidad. Para continuar, debe aceptar la Política de privacidad. Seleccione la opción **Acepto la Política de privacidad** solo si comprende y está de acuerdo con sus datos siendo manipulados y transmitidos (incluso a países terceros) según de detalla en la Política de privacidad.

7. Seleccione un archivo (de la lista de archivos que se extraen del archivo de almacenamiento elegido) y especifique los parámetros de la línea de comandos de un archivo ejecutable.

   Cómo crear un paquete de instalación en formato deb o rpm

   1. Cree un `.sh` con los siguientes comandos:

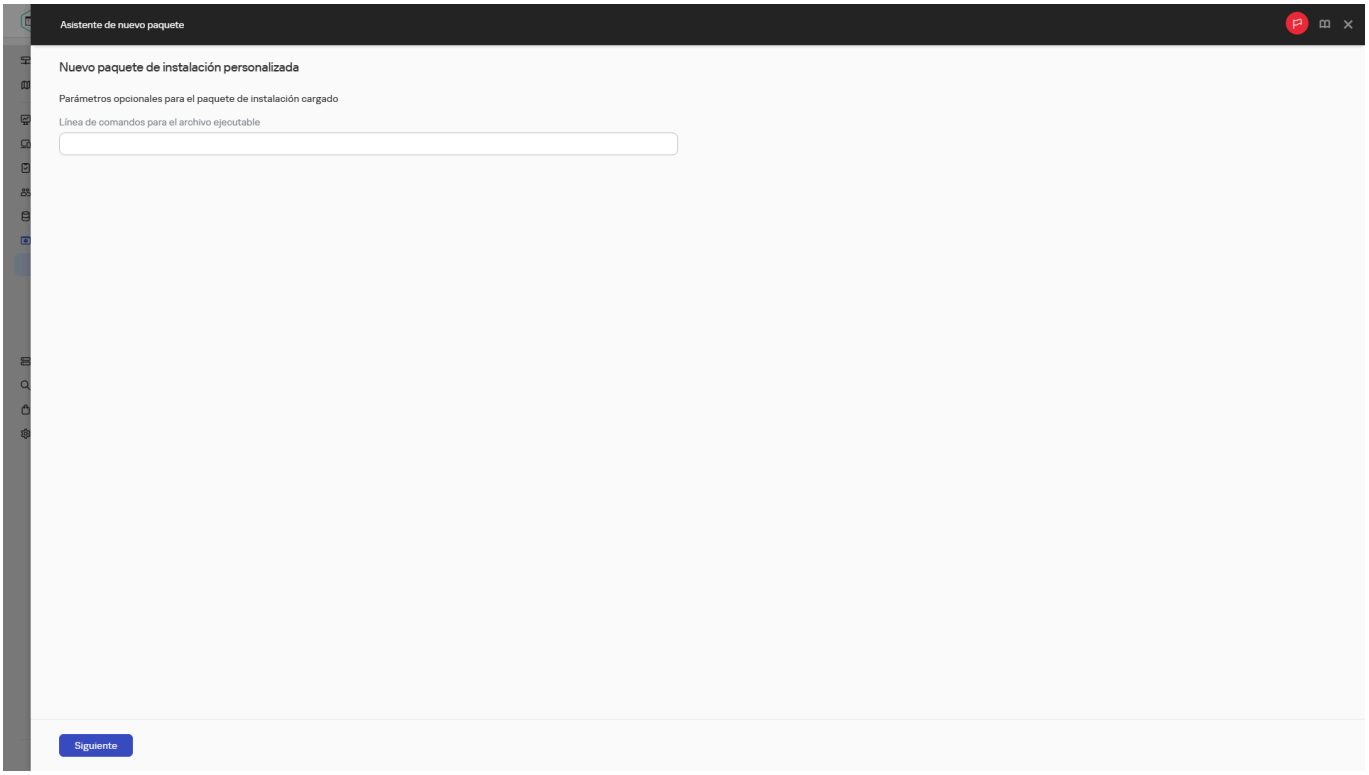
      ```
      #!/bin/sh
      script_dir="$(dirname "$0")"
      apt-get install --yes "$script_dir/<package_name>.deb" </dev/null
      ```

      El contenido del script y los comandos pueden variar según el formato del paquete y otros detalles. Puede modificar el script para adaptarlo a su configuración específica.

   2. Coloque el script creado en un archivo, junto con el archivo `.deb` o `.rpm`.

   3. Cuando cree el paquete de instalación, seleccione el script creado como archivo ejecutable.

   Puede especificar parámetros de línea de comandos para instalar la aplicación desde el paquete de instalación en modo silencioso. La especificación de los parámetros de la línea de comandos es opcional.



Especificar los parámetros opcionales de la línea de comando

   Se inicia el proceso para crear el paquete de instalación.

   El asistente le informará cuando finalice el proceso.

Si no se crea el paquete de instalación, se muestra el mensaje pertinente.

8. Haga clic en el botón **Finalizar** para cerrar el asistente.

El paquete de instalación que ha creado se descarga en la subcarpeta Paquetes de la carpeta compartida del Servidor de administración. Al concluir la descarga, el paquete de instalación aparecerá en la lista de paquetes de instalación.

En la lista de paquetes de instalación disponibles en el Servidor de administración, al hacer clic en el vínculo con el nombre de un paquete de instalación personalizado, puede hacer lo siguiente:

- Ver las siguientes propiedades del paquete de instalación:
  - **Nombre**. Nombre del paquete de instalación personalizado.
  - **Estado del paquete**. Estado de descarga del paquete de instalación.
  - **Origen**. Nombre del proveedor de la aplicación.
  - **Aplicación**. Nombre de la aplicación que contiene el paquete de instalación personalizado.
  - **Versión**. Versión de la aplicación.
  - **Idioma**. Idioma de la aplicación que contiene el paquete de instalación personalizado.
  - **Tamaño (MB)**. Tamaño del paquete de instalación.
  - **SO**. Tipo de sistema operativo para el que está destinado el paquete de instalación.
  - **Creado**. Fecha de creación del paquete de instalación.
  - **Modificado**. Fecha de modificación del paquete de instalación.
  - **Tipo**. Tipo de paquete de instalación.
- Cambie los parámetros de la línea de comandos.

Creación de paquetes de instalación independientes

Usted y los usuarios de dispositivos de su organización pueden utilizar paquetes de instalación independientes para instalar aplicaciones en dispositivos de forma manual.

Una paquete de instalación independiente es un archivo ejecutable que usted puede almacenar en el servidor web, en una carpeta compartida, enviar por correo electrónico o transferir al dispositivo cliente de otra manera. En el dispositivo cliente, el usuario puede ejecutar el archivo recibido localmente para instalar una aplicación sin utilizar Kaspersky Security Center Linux. Puede crear paquetes de instalación independientes de aplicaciones de Kaspersky y de aplicaciones de terceros. Para crear un paquete de instalación independiente para una aplicación de terceros, debe crear un paquete de instalación personalizada.

Asegúrese de que el paquete de instalación independiente no esté disponible para terceros.

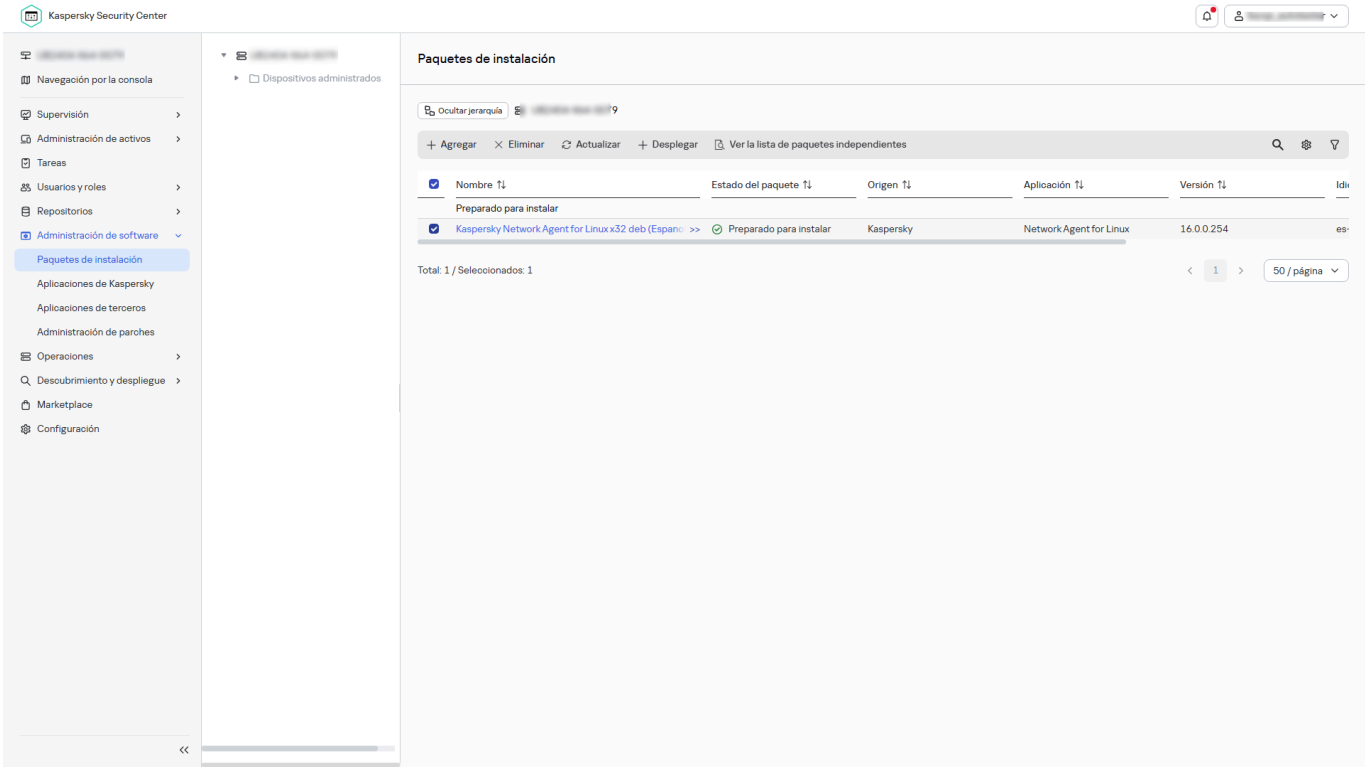
Para crear un paquete de instalación independiente:

1. En el menú principal, vaya a **Administración de software → Paquetes de instalación**.

   Se muestra una lista de paquetes de instalación disponibles en el Servidor de administración.

   > La información sobre el tamaño, el hash del archivo y la ruta no está disponible en la lista de paquetes de instalación para el paquete independiente del Agente de red o para los paquetes creados en los Servidores de administración virtuales. Estos paquetes independientes se generan en el momento de la descarga.

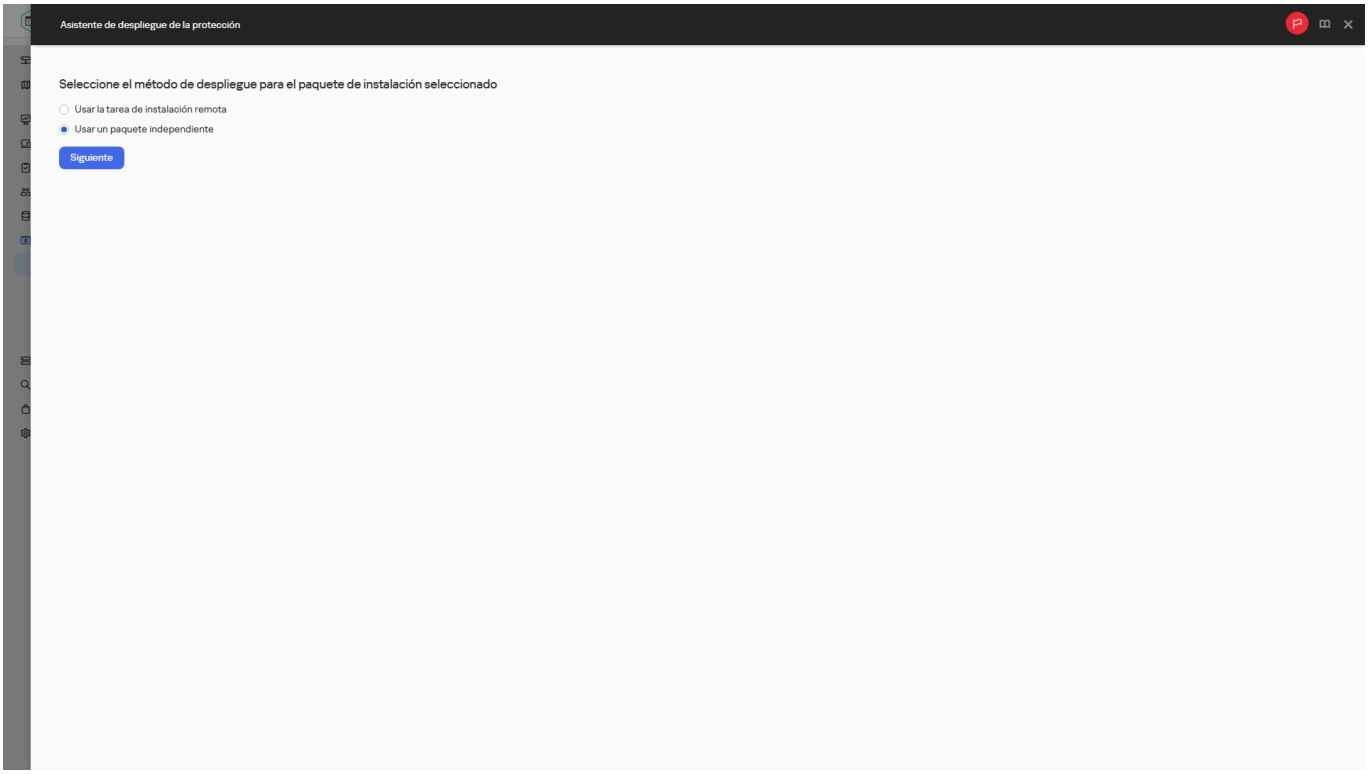
2. En la lista de paquetes de instalación, seleccione un paquete de instalación y haga clic en el botón **Desplegar** que se encuentra arriba de la lista.



La lista de paquetes de instalación

3. Seleccione la opción **Usar un paquete independiente**.

Se inicia el asistente de creación de paquetes de instalación independiente. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.



Seleccionar el método de despliegue para el paquete de instalación

4. Asegúrese de que la opción **Instalar el Agente de red junto con esta aplicación** esté habilitada si desea instalar el Agente de red junto con la aplicación seleccionada.

   La opción se muestra dependiendo de la aplicación para la que cree un paquete de instalación independiente.

   Esta opción está activada de forma predeterminada. Recomendamos que habilite esta opción si no sabe si el Agente de red está instalado en el dispositivo. Si el Agente de red ya está instalado en el dispositivo, una vez que instale el paquete de instalación independiente con el Agente de red, este último se actualizará a la versión más reciente.

   Si deshabilita esta opción, el Agente de red no se instalará en el dispositivo, y el dispositivo quedará como dispositivo no administrado.

   El asistente le indicará si el Servidor de administración ya cuenta con un paquete de instalación independiente para la aplicación seleccionada. Si esto sucede, elija una de estas acciones:

   - **Crear un paquete de instalación independiente**. Seleccione esta opción si, por ejemplo, desea crear un paquete de instalación independiente para una nueva versión de la aplicación y, al mismo tiempo, quiere conservar un paquete de instalación independiente creado para una versión más antigua de la aplicación. El nuevo paquete de instalación independiente se ubicará en otra carpeta.

   - **Utilizar un paquete de instalación independiente que ya existe**. Seleccione esta opción si desea utilizar un paquete de instalación independiente que ya exista. El proceso para crear paquetes no se iniciará.

   - **Volver a generar un paquete de instalación independiente que ya existe**. Seleccione esta opción si desea volver a crear un paquete de instalación independiente para la misma aplicación. El paquete de instalación independiente se ubicará en la misma carpeta.

5. En el paso **Mover a lista de dispositivos administrados**, la opción **No mover los dispositivos** se selecciona de manera predeterminada. Si no desea mover el dispositivo cliente a ningún grupo de administración después de la instalación del Agente de red, deje la opción seleccionada.

   Si desea que el dispositivo cliente se mueva después de la instalación del Agente de red, seleccione la opción **Mover los dispositivos no asignados a este grupo** y seleccione el grupo de administración al que desee mover el dispositivo cliente. De forma predeterminada, el dispositivo se moverá al grupo **Dispositivos administrados**.



Seleccionar el grupo de administración donde se moverá el dispositivo cliente

6. Cuando finalice el proceso de creación del paquete de instalación independiente, haga clic en el botón **FINALIZAR**.

   Se cierra el Asistente de creación de un paquete de instalación independiente.

Se crea el paquete de instalación independiente y se lo ubica en la subcarpeta PkgInst de la carpeta compartida del Servidor de administración. Puede ver la lista de paquetes independientes si hace clic en el botón **Ver la lista de paquetes independientes** que se encuentra arriba de la lista de paquetes de instalación.

Ajustes del paquete de instalación del Agente de red

Para configurar un paquete de instalación del Agente de red, haga lo siguiente:

1. En el menú principal, vaya a **Administración de software → Paquetes de instalación**.

   Se muestra una lista de paquetes de instalación disponibles en el Servidor de administración.

2. Haga clic en el nombre del paquete de instalación del Agente de red.

Se abre la ventana de propiedades del paquete de instalación del Agente de red.

La configuración de un paquete de instalación del Agente de red se agrupa en las siguientes pestañas:

- Pestaña **General**

Esta pestaña muestra la siguiente información sobre el paquete de instalación:

- Nombre del paquete de instalación
- Nombre y versión de la aplicación para la que se ha creado el paquete de instalación
- Tamaño del paquete de instalación
- Fecha de creación del paquete de instalación
- Ruta a la carpeta del paquete de instalación

- Pestaña **Configuración**

  Esta pestaña contiene la configuración necesaria para garantizar que el Agente de red funcione correctamente en cuanto concluya su instalación.

  - Sección **Configuración**

    Instalar en la carpeta predeterminada

    Si se selecciona esta opción, el Agente de red se instalará en la carpeta <Unidad>:\Archivos de programa\Kaspersky Lab\NetworkAgent. Si esta carpeta no existe, se la creará automáticamente.

    Esta opción está seleccionada de forma predeterminada.

    Instalar en la carpeta especificada

    Si se selecciona esta opción, el Agente de red se instalará en la carpeta especificada en el campo de entrada.

    Utilizar contraseña de desinstalación

    Si habilita esta opción, podrá ingresar la contraseña de desinstalación (solo disponible para el Agente de red en dispositivos con sistemas operativos Windows).

    Esta opción está deshabilitada de forma predeterminada.

    Evitar que el servicio del Agente de red se detenga o se elimine sin autorización e impedir cambios en su configuración

    Cuando esta opción está habilitada, una vez que el Agente de red se encuentre instalado en un dispositivo administrado, no se lo podrá eliminar ni reconfigurar a menos que se tengan los privilegios necesarios. El servicio del Agente de red no se podrá detener. Esta opción no tiene efecto en los controladores de dominio.

    Habilite esta opción para proteger el Agente de red en estaciones de trabajo operadas con derechos de administrador local.

    Esta opción está deshabilitada de forma predeterminada.

    Instalar automáticamente las actualizaciones y parches de estado Sin definir que estén disponibles para los componentes

    Si esta opción está activada, todas las actualizaciones y parches descargados para el Servidor de administración, el Agente de red, Kaspersky Security Center Web Console y el Servidor de MDM para iOS se instalarán automáticamente.

    Si se deshabilita esta opción, las actualizaciones y los parches que se descarguen se instalarán únicamente después de que su estado se cambie a *Aprobado*. Las actualizaciones y los parches con el estado *Sin definir* no se instalarán.

    Esta opción está activada de forma predeterminada.

- Sección **Conexión**

  En esta sección, puede configurar la conexión del Agente de red al Servidor de administración. Para establecer una conexión, pueden utilizarse los protocolos SSL o UDP. Defina los siguientes ajustes para configurar la conexión:

  Dirección del Servidor de administración

  Dirección del dispositivo en el que se encuentra instalado el Servidor de administración.

  Número de puerto

  Número de puerto que se utilizará para la conexión.

  Puerto SSL

  Número de puerto que se utilizará para la conexión mediante el protocolo SSL.

  Usar certificado del Servidor

  Si se habilita esta opción, para autenticar el acceso del Agente de red al Servidor de administración, se usará el archivo del certificado seleccionado al hacer clic en el botón **Seleccionar archivo de certificado**.

  Si se deshabilita esta opción, el archivo del certificado se obtendrá del Servidor de administración la primera vez que el Agente de red se conecte a la dirección especificada en el campo **Dirección del Servidor de administración**.

  No recomendamos que deshabilite esta opción: no se considera seguro que el Agente de red obtenga el certificado del Servidor de administración automáticamente al establecer conexión.

  Esta opción está deshabilitada de forma predeterminada.

  Usar conexión SSL

  Si se habilita esta opción, la conexión al Servidor de administración se establecerá a través de un puerto seguro utilizando el protocolo SSL.

  Esta opción está deshabilitada de forma predeterminada. Recomendamos no deshabilitar esta opción; de lo contrario, la conexión quedará desprotegida.

  Usar puerto UDP

  Si se habilita esta opción, el Agente de red se conectará al Servidor de administración a través de un puerto UDP. Esto permite administrar los dispositivos cliente y recibir información sobre ellos.

  El puerto UDP deberá estar abierto en los dispositivos administrados en los que se instale el Agente de red. Por lo tanto, recomendamos no deshabilitar esta opción.

  Esta opción está activada de forma predeterminada.

  Puerto UDP

  En este campo, puede ingresar el número de puerto que se usará para conectar el Agente de red al Servidor de administración mediante el protocolo UDP.

  El número de puerto UDP predeterminado es 15000.

  No usar servidor proxy

  Si esta opción está habilitada, se utiliza la conexión directa para conectar el dispositivo al Servidor de administración.

  Usar servidor proxy

Si esta opción está habilitada, especifique los parámetros del servidor proxy:

- **Dirección del servidor proxy**
- **Puerto del servidor proxy**

Si su servidor proxy requiere autenticación, habilite la opción **Autenticación del servidor proxy** y especifique el **Nombre de usuario** y la **Contraseña** de la cuenta con la que se establece la conexión con el servidor proxy. Le recomendamos que utilice las credenciales de una cuenta que solamente tenga los privilegios mínimos necesarios para completar la autenticación ante el servidor proxy.

Abrir puertos del Agente de red en el Firewall de Microsoft Windows

Cuando se habilita esta opción, se agregan los puertos que el Agente de red utiliza a la lista de exclusiones del Firewall de Microsoft Windows.

Esta opción está activada de forma predeterminada.

> Esta opción solo está disponible para los paquetes de instalación del Agente de red destinados a dispositivos que ejecutan Windows.

- Sección **Avanzada**

  En esta sección, puede configurar cómo se usará la puerta de enlace de conexión.

  En el grupo de configuraciones **Puerta de enlace de conexión**, puede configurar el método de conexión entre un dispositivo y el Servidor de administración:

  Usar el Agente de red como una puerta de enlace de conexión en la DMZ

  Si esta opción está habilitada, el Agente de red se utiliza como puerta de enlace de conexión en la zona desmilitarizada (DMZ) para conectarse al Servidor de administración, comunicarse con él y mantener los datos del Agente de red a salvo durante la transmisión de datos.

  Conectarse al Servidor de administración mediante una puerta de enlace de conexión

  Si esta opción está habilitada, la conexión con el Servidor de administración se establece a través de una puerta de enlace de conexión para reducir la cantidad de conexiones al Servidor de administración. Si elige esta opción, ingrese la dirección del dispositivo que actuará como puerta de enlace de conexión en el campo **Dirección de la puerta de enlace de conexión**.

  En el grupo de configuraciones de **Máquina virtual**, puede configurar la conexión para la Infraestructura de escritorio virtual (VDI) si su red incluye máquinas virtuales:

  Habilitar modo dinámico para VDI

  Si habilita esta opción, se habilitará un modo dinámico para infraestructuras de escritorios virtuales (VDI) para el Agente de red instalado en una máquina virtual.

  Esta opción está deshabilitada de forma predeterminada.

  Optimizar la configuración para VM

  Si habilita esta opción, se deshabilitarán las siguientes características de la configuración del Agente de red:

  - Recopilación de información acerca del software instalado
  - Recopilación de información acerca del hardware
  - Recopilación de información acerca de las vulnerabilidades detectadas
  - Recopilación de información acerca de las actualizaciones necesarias

  Esta opción está deshabilitada de forma predeterminada.

Si desea solicitarles automáticamente a los usuarios que se registren como propietarios del dispositivo después de instalar el Agente de red en dispositivos Linux, habilite la opción **Permitir la ejecución de la utilidad de registro de usuario luego de la instalación del Agente de red**.

Si esta opción está habilitada, la utilidad de registro del usuario como propietario del dispositivo se ejecutará después de la instalación del Agente de red. Esta opción está deshabilitada de forma predeterminada.

- Sección **Etiquetas**

  La sección **Etiquetas** muestra una lista de palabras claves (etiquetas) que se pueden agregar a los dispositivos cliente tras la instalación del Agente de red. Puede agregar etiquetas nuevas a la lista, así como eliminar las etiquetas existentes o cambiarles el nombre.

  Si la casilla junto a una etiqueta está marcada, cuando se instale el Agente de red, la etiqueta correspondiente se agregará a los dispositivos administrados de manera automática.

  Si la casilla junto a una etiqueta no está marcada, la etiqueta no se agregará automáticamente a los dispositivos administrados durante la instalación del Agente de red. De ser necesario, podrá agregar esa etiqueta manualmente a los dispositivos pertinentes.

  Si elimina una etiqueta de la lista, se la eliminará automáticamente de todos los dispositivos a los que haya sido agregada.

  > Las reglas de etiquetado automático no son aplicables a los paquetes de instalación del Agente de red destinados a dispositivos con Linux y macOS.

- Pestaña **Paquetes independientes**

  En esta pestaña, puede hacer lo siguiente:

  - Ver la lista de paquetes de instalación independientes disponibles.
  - Publicar un paquete de instalación independiente en el servidor web haciendo clic en el botón **Publicar**. El paquete de instalación independiente publicado está disponible para que lo descarguen los usuarios a quienes envió el vínculo.
  - Cancelar la publicación de un paquete de instalación independiente en el servidor web haciendo clic en el botón **Cancelar la publicación**. El paquete de instalación independiente no publicado está disponible para que lo descargue solo usted y otros administradores.
  - Descargar un paquete de instalación independiente a su dispositivo haciendo clic en el botón **Descargar**.
  - Enviar un correo electrónico con el vínculo para un paquete de instalación independiente haciendo clic en el botón **Enviar por correo electrónico**.
  - Eliminar un paquete de instalación independiente haciendo clic en el botón **Eliminar**.

- Pestaña **Historial de revisiones**

  En esta pestaña, puede ver el historial de revisiones del paquete de instalación. Puede comparar las distintas revisiones, ver revisiones específicas, guardar revisiones en un archivo, agregar descripciones a las revisiones y modificar las descripciones existentes.

Ejecución de paquetes independientes creados por Kaspersky Security Center Linux

Los métodos anteriormente descritos para el despliegue inicial del Agente de red y de otras aplicaciones no siempre se pueden implementar porque no es posible cumplir con todas las condiciones aplicables. En tales casos, puede crear un archivo ejecutable común llamado un *paquete de instalación independiente* a través de Kaspersky Security Center Linux, usando paquetes de instalación con la configuración de instalación relevante preparada por el administrador. Se puede publicar un paquete de instalación independiente en un Servidor web interno (incluido en Kaspersky Security Center Linux), si esto se considera razonable (se configuró el acceso externo a ese Servidor web para usuarios de dispositivos de destino), o en un Servidor web que viene incluido en Kaspersky Security Center Web Console. También puede copiar paquetes independientes a otro Servidor web.

Puede usar Kaspersky Security Center Linux para enviar a usuarios seleccionados un mensaje de correo electrónico que contenga un vínculo al archivo del paquete independiente en el Servidor web utilizado actualmente, solicitándoles ejecutar el archivo (ya sea en modo interactivo o con la clave "-s" para la instalación silenciosa). Puede adjuntar el paquete de instalación independiente a un mensaje de correo electrónico y luego enviarlo a los usuarios de dispositivos que no tengan acceso al Servidor web. El administrador también puede copiar el paquete independiente a una unidad extraíble, entregarlo a un dispositivo relevante, y luego ejecutarlo más adelante.

Puede crear un paquete independiente desde un paquete del Agente de red, un paquete de otra aplicación (por ejemplo, la aplicación de seguridad), o ambos. Si el paquete independiente se ha creado desde el Agente de red y otra aplicación, la instalación se inicia con el Agente de red.

Al crear un paquete independiente con el Agente de red, puede especificar el grupo de administración en el cual los dispositivos nuevos (esos que no se han asignado a ninguno de los grupos de administración) automáticamente se moverá cuando la instalación del Agente de red se complete en ellos.

Los paquetes independientes se pueden ejecutar en el modo interactivo (de forma predeterminada), mostrando el resultado para la instalación de aplicaciones que contienen, o se pueden ejecutar en el modo silencioso (cuando se ejecutan con la clave "-s"). El modo silencioso se puede utilizar para la instalación desde scripts (por ejemplo, desde scripts configurados para ejecutarse tras la instalación de una imagen de sistema operativo). El resultado de instalación en el modo silencioso está determinado por el código de devolución del proceso.

Instalación de aplicaciones con paquetes independientes

Kaspersky Security Center le permite crear paquetes de instalación independientes para aplicaciones. Un paquete de instalación independiente es un archivo ejecutable que se puede encontrar en un servidor web, enviar por correo electrónico o transferir a un dispositivo cliente de algún otro modo. El archivo recibido puede ejecutarse localmente en el dispositivo cliente para instalar una aplicación sin involucrar a Kaspersky Security Center.

Para instalar una aplicación con un paquete de instalación independiente:

1. En el menú principal, vaya a **Administración de software → Paquetes de instalación**.
2. Seleccione la casilla junto al paquete de instalación de la aplicación requerida y luego haga clic en el botón **Desplegar**.
3. En la ventana que aparece, seleccione **Usar un paquete independiente** y luego haga clic en el botón **Siguiente**.

   Se inicia el asistente de creación de paquetes de instalación independiente. Avance por el asistente utilizando el botón **Siguiente**.

4. Seleccione la opción **Crear un paquete de instalación independiente**.

5. Especifique si los dispositivos deben moverse a un grupo de administración después de la instalación del Agente de red.

6. En el paso final del asistente, seleccione un método para transferir el paquete de instalación independiente al dispositivo cliente y, a continuación, haga clic en **Finalizar** para finalizar el asistente.

7. Transfiera el paquete de instalación independiente al dispositivo cliente.

8. Ejecute el paquete de instalación independiente en el dispositivo cliente.

La aplicación ahora se encuentra instalada en el dispositivo cliente con la configuración especificada en el paquete independiente.

Al crear un paquete de instalación independiente, éste se publica automáticamente en el servidor web. En la lista de paquetes de instalación independiente creados se muestra un enlace para descargar el paquete independiente. De ser necesario, puede cancelar la publicación del paquete independiente seleccionado y publicarlo nuevamente en el servidor web. De forma predeterminada, se utiliza el puerto 8060 para la descarga de los paquetes de instalación independiente.

Conveniencia de actualizar las bases de datos en el paquete de instalación de una aplicación de seguridad

Antes de comenzar con el despliegue de la protección, debe tener en cuenta la posibilidad de actualizar las bases de datos antivirus (incluidos los módulos de los parches automáticos), que se envían junto con el paquete de distribución de la aplicación de seguridad. Es útil actualizar las bases de datos en el paquete de instalación de la aplicación antes de dar inicio al despliegue (por ejemplo, usando el comando correspondiente en el menú contextual de un paquete de instalación seleccionado). Con ello se reducirá el número de reinicios necesarios para completar el despliegue de la protección en los dispositivos de destino.

Modificación del límite de datos para paquetes de instalación personalizados

Existe un límite a la cantidad de datos que se admite descomprimir para crear un paquete de instalación personalizado. El límite predeterminado es 1 GB.

Si intenta cargar un archivo de almacenamiento que contenga un volumen de datos superior a lo permitido, verá un mensaje de error. Por ello, para crear un paquete de instalación a partir de un paquete de distribución de gran tamaño, puede ser necesario aumentar el límite predeterminado.

Para cambiar el límite de datos para paquetes de instalación personalizados:

1. En el dispositivo del Servidor de administración, abra la línea de comandos con la cuenta que se haya usado para instalar el Servidor de administración.

2. Cambie de directorio a la carpeta de instalación de Kaspersky Security Center Linux (generalmente, /opt/kaspersky/ksc64/sbin).

3. Dependiendo de cómo se haya instalado el Servidor de administración, ingrese uno de los siguientes comandos en la cuenta root:

   - Instalación local normal:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <número de bytes>
     ```

   - Instalación en el clúster de conmutación por error de Kaspersky Security Center Linux:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <número de bytes> --stp klfoc
     ```

   El valor de <número de bytes> debe ser un número de bytes en formato decimal o hexadecimal.

   Por ejemplo, si el límite requerido es de 2 GB, puede especificar el valor decimal 2147483648 o el valor hexadecimal 0x80000000. Así, para una instalación local del Servidor de administración, usaría el siguiente comando:

   ```
   klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v 2147483648
   ```

La aplicación comenzará a usar el nuevo límite de datos para los paquetes de instalación personalizados.

Distribución de paquetes de instalación a servidores de administración secundarios

A través de Kaspersky Security Center Linux, puede crear paquetes de instalación para aplicaciones desarrolladas por Kaspersky y por terceros, distribuir paquetes de instalación a sus dispositivos cliente e instalar aplicaciones utilizando esos paquetes. Para optimizar la carga del Servidor de administración principal, puede distribuir los paquetes de instalación a los servidores de administración secundarios. Los servidores secundarios transmiten luego esos paquetes a los dispositivos cliente. Concluida la distribución, puede realizarse la instalación remota de las aplicaciones en los dispositivos cliente.

Para distribuir paquetes de instalación a servidores de administración secundarios:

1. Verifique que los servidores de administración secundarios estén conectados al Servidor de administración principal.

2. En el menú principal, vaya a **Tareas**.

   Se muestra la lista de tareas.

3. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Siga los pasos del asistente.

4. En la página **Configuración de tarea nueva**, abra la lista desplegable **Aplicación** y seleccione **Kaspersky Security Center**. A continuación, en la lista desplegable **Tipo de tarea**, seleccione **Distribuir paquete de instalación**. Ingrese el nombre de la tarea.

5. En la página **Alcance de la tarea**, seleccione los dispositivos a los que se asigna la tarea de una de estas formas:

   - Si desea crear una tarea para todos los servidores de administración secundarios de un grupo de administración específico, seleccione ese grupo y cree una tarea de grupo para el mismo.

   - Si desea crear una tarea para determinados servidores de administración secundarios, seleccione esos servidores y cree una tarea para ellos.

6. En la página **Paquetes de instalación distribuidos**, seleccione los paquetes de instalación que se copiarán a los servidores de administración secundarios.

7. Seleccione la cuenta con la que se ejecutará la tarea *Distribuir paquete de instalación*. Puede usar su propia cuenta y dejar habilitada la opción **Cuenta predeterminada**. Como alternativa, puede elegir otra cuenta que tenga los derechos de acceso necesarios para ejecutar la tarea. Para ello, haga clic en **Especificar cuenta** e ingrese las credenciales de la cuenta que desee usar.

8. En la página **Finalizar la creación de la tarea**, puede habilitar la opción **Abrir los detalles de la tarea cuando se complete la creación** para que se abra la ventana de propiedades de la tarea y modificar, desde allí, la configuración de la tarea definida por defecto. Si lo prefiere, puede configurar los ajustes de la tarea en cualquier otro momento.

9. Haga clic en el botón **Finalizar**.

   En la lista de tareas, aparecerá la nueva tarea para distribuir los paquetes de instalación a los servidores de administración secundarios.

10. Ejecute la tarea manualmente o espere a que se inicie según la programación configurada para la tarea.

    Una vez que se complete la tarea, los paquetes de instalación seleccionados estarán en los servidores de administración secundarios que haya seleccionado.

Ver la lista de paquetes de instalación independientes

Puede ver la lista de paquetes de instalación independientes y las propiedades de cada paquete.

Para ver la lista de paquetes de instalación independientes para todos los paquetes de instalación:

Haga clic en el botón **Ver la lista de paquetes independientes**, ubicado encima de la lista.

En la lista de paquetes de instalación independientes, sus propiedades se muestran de la siguiente manera:

- **Nombre del paquete**. Nombre del paquete de instalación independiente. Se crea automáticamente a con el nombre y la versión de la aplicación incluida en el paquete.
- **Nombre de la aplicación**. Es el nombre de la aplicación que se incluye en el paquete de instalación independiente.
- **Versión de la aplicación**.
- **Nombre del paquete de instalación del Agente de red**. La propiedad se muestra únicamente si el Agente de red está incluido en el paquete de instalación independiente.
- **Versión del Agente de red**. La propiedad se muestra únicamente si el Agente de red está incluido en el paquete de instalación independiente.
- **Tamaño**. Tamaño del archivo en MB.
- **Grupo**. Nombre del grupo al que se mueve el dispositivo cliente después de la instalación del Agente de red.
- **Creado**. Fecha y hora de creación del paquete de instalación independiente.
- **Modificado**. Fecha y hora de modificación del paquete de instalación independiente.

- **Ruta**. Ruta completa a la carpeta donde se encuentra el paquete de instalación independiente.
- **Dirección web**. Dirección web de la ubicación del paquete de instalación independiente.
- **Hash de archivo**. La propiedad se utiliza para certificar que ningún tercero haya modificado el paquete de instalación independiente y que un usuario tiene el mismo archivo que usted creó y transfirió al usuario.

La información sobre el tamaño, el hash del archivo y la ruta no está disponible en la lista de paquetes de instalación para el paquete independiente del Agente de red o para los paquetes creados en los Servidores de administración virtuales. Estos paquetes independientes se generan en el momento de la descarga.

Para ver la lista de paquetes de instalación independientes para un paquete de instalación específico:

Seleccione el paquete de instalación de la lista y, a continuación, haga clic en el botón **Ver la lista de paquetes independientes** ubicado encima de la lista.

En la lista de paquetes de instalación independientes puede hacer lo siguiente:

- Publicar un paquete de instalación independiente en el servidor web haciendo clic en el botón **Publicar**. El paquete de instalación independiente publicado está disponible para que lo descarguen los usuarios a quienes envió el vínculo.
- Cancelar la publicación de un paquete de instalación independiente en el servidor web haciendo clic en el botón **Cancelar la publicación**. El paquete de instalación independiente no publicado está disponible para que lo descargue solo usted y otros administradores.
- Descargar un paquete de instalación independiente a su dispositivo haciendo clic en el botón **Descargar**.
- Enviar un correo electrónico con el vínculo para un paquete de instalación independiente haciendo clic en el botón **Enviar por correo electrónico**.
- Eliminar un paquete de instalación independiente haciendo clic en el botón **Eliminar**.

Instalar el Agente de red para Linux

Para administrar dispositivos en una organización, tiene que instalar el Agente de red en cada uno de ellos. La distribución de Kaspersky Security Center Linux distribuido en dispositivos corporativos normalmente comienza con la instalación del Agente de red en ellos.

Existen los siguientes métodos para instalar inicialmente el Agente de red en el dispositivo administrado con Linux:

- Conectarse al dispositivo administrado a través de SSH y ejecutar la tarea de instalación remota.
- Ejecutar el paquete de instalación en el dispositivo administrado.

Después de que se instala el Agente de red en un dispositivo, puede realizar la instalación remota de las aplicaciones de Kaspersky en ese dispositivo a través de este Agente de red. El paquete de distribución de una aplicación que se debe instalar se transfiere a través de canales de comunicación entre Agentes de red y el Servidor de administración, junto con la configuración de instalación definida por el administrador. Para transferir el paquete de distribución, puede usar nodos de distribución de relevo, es decir puntos de distribución, distribución multidifusión, etc.

Al seleccionar un método y una estrategia para instalar las aplicaciones en una red administrada, debe considerar varios factores (lista parcial):

- Configuración de red de la organización.
- Número total de dispositivos.
- Presencia de dispositivos en la red de la organización, que no son miembros de ningún dominio, y presencia de cuentas uniformes con derechos de administrador en esos dispositivos.
- Capacidad del canal entre el Servidor de administración y los dispositivos.
- Tipo de comunicación entre el Servidor de administración y subredes remotas y capacidad de los canales de la red en esas subredes.
- Configuración de seguridad aplicada en dispositivos remotos al inicio del despliegue. Estos parámetros permiten establecer la conexión remota al dispositivo administrado e iniciar la instalación.

Preparación de un dispositivo Linux para la instalación del Agente de red

Antes de la instalación del Agente de red en un dispositivo Linux, debe realizar los pasos de preparación necesarios para cualquier dispositivo Linux.

Para preparar un dispositivo que ejecute Linux para la instalación remota del Agente de red:

1. Asegúrese de que el dispositivo en el que desea instalar Network Agent for Linux cuente con una de las distribuciones de Linux compatibles.
2. Si desea instalar el Agente de red en AltOS en el modo de entorno de software cerrado, deshabilite el modo de entorno de software cerrado hasta que finalice la instalación.
3. Descargue el paquete de instalación del Agente de red mediante la interfaz de Web Console o desde el sitio web de Kaspersky.

   Si necesita instalar el Agente de red en un dispositivo que ejecuta un sistema operativo Linux con glibc 2.5, debe descargar el paquete de instalación de *Kaspersky Network Agent for Linux Legacy* mediante la interfaz de Web Console o desde el sitio web de Kaspersky.
4. Asegúrese de que el siguiente software esté instalado en el dispositivo Linux de destino:
   - Sudo (para Ubuntu 10.04, la versión de Sudo 1.7.2p1 o posterior)
   - Intérprete del lenguaje Perl versión 5.10 o posterior
   - utilidad ps
5. Pruebe la configuración del dispositivo:
   a. Compruebe si puede conectarse al dispositivo mediante un cliente SSH (por ejemplo, PuTTY).

      Si no puede conectarse al dispositivo, abra el archivo `/etc/ssh/sshd_config` y asegúrese de que las siguientes configuraciones tengan los valores respectivos que se enumeran a continuación:

      ```
      PasswordAuthentication no
      ```

```
ChallengeResponseAuthentication yes
```

> No modifique el archivo /etc/ssh/sshd_config si puede conectarse al dispositivo sin problemas; de lo contrario, es posible que se produzca un error de autenticación SSH al ejecutar una tarea de instalación remota.

Guarde el archivo (si es necesario) y reinicie el servicio SSH utilizando el comando `sudo service ssh restart`.

b. Asegúrese de que el puerto TCP 22 esté abierto y accesible en un dispositivo no asignado basado en Linux.

El puerto TCP 22 debe estar disponible para la instalación correcta del Agente de red para Linux.

c. Deshabilite la contraseña de sudo para la cuenta de usuario con la cual se conectará el dispositivo.

d. Utilice el comando `visudo` en sudo para abrir el archivo de configuración de sudoers.

En el archivo que abrió, agregue la siguiente línea al final del archivo: `<nombre de usuario> ALL = (ALL) NOPASSWD: ALL`. En este caso, `<nombre de usuario>` es la cuenta de usuario que se utilizará para la conexión del dispositivo mediante SSH. Si está utilizando el sistema operativo Astra Linux, en el archivo /etc/sudoers, agregue la última línea con el siguiente texto: `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

e. Guarde el archivo sudoers y, luego, ciérrelo.

f. Conéctese nuevamente al dispositivo a través de SSH y asegúrese de que el servicio Sudo no le solicite que ingrese una contraseña; puede hacerlo usando el comando `sudo whoami`.

6. Si desea instalar el Agente de red de manera remota en dispositivos que ejecutan el sistema operativo con el sistema de inicialización systemd, abra el archivo `/etc/systemd/logind.conf` y realice una de las siguientes acciones:

- Especifique `no` como valor para la configuración `KillUserProcesses`: `KillUserProcesses=no`.
- Para la configuración `KillExcludeUsers`, escriba el nombre de usuario de la cuenta con la cual se realizará la instalación remota, por ejemplo, `KillExcludeUsers=root`.

Dispositivo de destino Astra Linux

Si el dispositivo de destino ejecuta Astra Linux, agregue la cadena `export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` en el archivo `/home/<nombre de usuario>/.bashrc`, donde `<nombre de usuario>` es la cuenta de usuario que se utilizará para la conexión del dispositivo mediante SSH.

Dispositivo de destino OSnova

Si el dispositivo de destino ejecuta OSnova, realice lo siguiente:

a. Abra el archivo `/usr/lib/systemd/logind.conf/10-enable-kill-user-processes.conf` y luego comente la línea `#KillUserProcess=yes`.

b. Abra el archivo `/usr/lib/NESS/pam-user-session` y luego comente la línea `#loginctl terminate-session "$XDG_SESSION_ID"`.

Para aplicar el ajuste modificado, reinicie el dispositivo Linux o ejecute el siguiente comando:

```
sudo systemctl restart systemd-logind.service
```

7. Si desea instalar el Agente de red en dispositivos con el sistema operativo SUSE Linux Enterprise Server 15, primero, instale el paquete insserv-compat para configurar el Agente de red.

8. Si desea instalar el Agente de red en dispositivos que tienen el sistema operativo Astra Linux que se ejecuta en el modo de entorno de software cerrado, lleve a cabo los pasos adicionales para preparar los dispositivos Astra Linux.

9. Si desea instalar el Agente de red en dispositivos que ejecutan Ubuntu Server o Ubuntu Desktop versión 10.04, siga estos pasos adicionales para prepararlos.

10. Si desea instalar el Agente de red en un dispositivo que ejecuta un sistema operativo Linux con glibc 2.5, lleve a cabo pasos adicionales para preparar los dispositivos de destino.

11. Si está instalando el Agente de red en AltOS en modo de entorno de software cerrado, vuelva a habilitar el modo de entorno de software cerrado.

12. Si desea instalar el Agente de Red en dispositivos que utilicen el sistema operativo RED OS 7.3.4 o posterior, o MSVSPHERE 9.2 o posterior, instale el paquete libxcrypt-compat para el correcto funcionamiento del Agente de Red.

El dispositivo Linux está listo para la instalación del Agente de red. Puede instalar el Agente de red de forma remota, en modo interactivo o en modo silencioso.

Preparación de un dispositivo que ejecuta SUSE Linux Enterprise Server 15 para la instalación del Agente de red

Antes de instalar el Agente de red en un dispositivo que ejecuta SUSE Linux Enterprise Server 15, debe realizar dos procedimientos de preparación: el que se detalla en las instrucciones a continuación y los pasos de preparación generales para cualquier dispositivo Linux.

Para instalar el Agente de red en un dispositivo con el sistema operativo SUSE Linux Enterprise Server 15:

Antes de la instalación del Agente de red, ejecute el siguiente comando:

```
sudo zypper install insserv-compat
```

Esto permite instalar el paquete insserv-compat y configurar el Agente de red correctamente.

Ejecute el comando `rpm -q insserv-compat` para comprobar si el paquete ya está instalado.

Si su red incluye muchos dispositivos que ejecutan SUSE Linux Enterprise Server 15, puede usar el software especial para configurar y administrar la infraestructura de la empresa. Al usar este software, puede instalar automáticamente el paquete insserv-compat en todos los dispositivos necesarios al mismo tiempo. Por ejemplo, puede usar Puppet, Ansible o Chef, o puede crear su propio script; use cualquier método que sea conveniente para usted.

Si el dispositivo no tiene las claves de firma GPG para SUSE Linux Enterprise, puede aparecer la siguiente advertencia: `Package header is not signed!` Seleccione la opción `i` para ignorar la advertencia.

Después de preparar el dispositivo Linux, puede instalar el Agente de red de forma remota, en modo interactivo o en modo silencioso.

Preparación de un dispositivo que ejecuta Astra Linux en el modo de entorno de software cerrado para la instalación del Agente de red

Antes de la instalación del Agente de red en un dispositivo que ejecuta Astra Linux en el modo de entorno de software cerrado, debe realizar dos procedimientos de preparación: el de las instrucciones a continuación y los pasos generales de preparación para cualquier dispositivo Linux.

Ejecute los comandos provistos en estas instrucciones utilizando una cuenta con privilegios de root.

Para preparar un dispositivo que ejecuta Astra Linux en el modo de entorno de software cerrado para la instalación del Agente de red:

1. Abra el archivo `/etc/digsig/digsig_initramfs.conf` y luego especifique la siguiente configuración:

   ```
   DIGSIG_ELF_MODE=1
   ```

2. En la línea de comandos, ejecute el siguiente comando para instalar el paquete de compatibilidad:

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

3. Cree un directorio para la clave de la aplicación:

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

4. Coloque la clave de la aplicación /opt/kaspersky/klnagent64/share/kaspersky_astra_pub_key.gpg en el directorio creado en el paso anterior:

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

   Si el kit de distribución de Kaspersky Security Center Linux no incluye la clave de la aplicación kaspersky_astra_pub_key.gpg, puede descargarla haciendo clic en este enlace: https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

5. Actualice los discos RAM:

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

   Reinicie el sistema.

El dispositivo Linux está listo para la instalación del Agente de red. Puede instalar el Agente de red de forma remota, en modo interactivo o en modo silencioso.

Preparación para instalar el Agente de red en un sistema operativo Linux con glibc 2.5 (SO heredado)

Antes de instalar el Agente de red en un dispositivo que ejecuta un sistema operativo Linux con glibc 2.5 (SO heredado), debe realizar dos procedimientos de preparación: los pasos de preparación generales para cualquier dispositivo Linux y el procedimiento que se describe en este artículo.

Le recomendamos que utilice la instalación local para instalar el Agente de red en un sistema operativo Linux con glibc 2.5 (SO heredado). Si necesita usar una tarea de instalación remota para este escenario, debe realizar los pasos adicionales descritos en las instrucciones a continuación.

Ejecute los comandos provistos en este procedimiento utilizando una cuenta con privilegios de root.

Le recomendamos que utilice la instalación local para instalar el Agente de red en un sistema operativo Linux con glibc 2.5 (SO heredado). Si necesita usar una tarea de instalación remota para este escenario, debe realizar los pasos adicionales descritos en las instrucciones a continuación.

1. En el dispositivo que ejecuta un sistema operativo Linux con glibc 2.5, realice los pasos de preparación comunes para cualquier dispositivo Linux.
2. En el archivo `/etc/sudoers`, elimine la línea `Defaults requiretty`.
3. Deshabilite la lista de admitidos de algoritmos de cifrado válidos para que las conexiones SSH puedan instalar el Agente de red en el dispositivo que ejecuta un sistema operativo Linux con glibc 2.5.

   Para hacer esto, en el dispositivo con el Servidor de administración instalado, o en un dispositivo que actúa como punto de distribución cuyo alcance incluye el dispositivo de destino, ejecute el siguiente comando en la línea de comandos:

   ```
   klscflag -fset -pv ".core/.independent" -s "Transport" -n
   SSH_CLIENT_DISABLE_ALGS_PROTECT -t d -v 1
   ```

El dispositivo Linux está listo para la instalación remota del Agente de red.

Deshabilitar la lista de algoritmos de cifrado válidos admitidos puede afectar la seguridad de la conexión SSH. Recomendamos que vuelva a habilitar la lista de algoritmos de cifrado válidos admitidos de inmediato después de instalar el Agente de red. Para volver a habilitar la lista de admitidos de algoritmos de cifrado válidos, ejecute el siguiente comando:

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

Una vez que haya instalado el Agente de red y luego haya vuelto a habilitar la lista de admitidos de algoritmos de cifrado válidos, el dispositivo que ejecuta un sistema operativo Linux con glibc 2.5 (SO heredado) es ahora administrado por el Servidor de Administración.

Preparación para instalar el Agente de red en un sistema operativo Linux con OpenSSH versión 6.4 (SO heredado)

Antes de instalar el Agente de red en un dispositivo que usa OpenSSH versión 6.4 o anterior (SO heredado), debe realizar dos procedimientos de preparación: los pasos de preparación generales para cualquier dispositivo Linux y el procedimiento que se describe en este artículo.

Le recomendamos que utilice la instalación local para instalar el Agente de red en un sistema operativo Linux con glibc 2.5 (SO heredado). Si necesita usar una tarea de instalación remota para este escenario, debe realizar los pasos adicionales descritos en las instrucciones a continuación.

Ejecute los comandos provistos en estas instrucciones utilizando una cuenta con privilegios de root.

Para preparar un dispositivo que usa OpenSSH versión 6.4 o anterior para la instalación del Agente de red:

1. En el dispositivo que usa OpenSSH versión 6.4 o anterior, realice los pasos de preparación comunes para cualquier dispositivo Linux.

2. Deshabilite la lista de admitidos de algoritmos de cifrado válidos para que las conexiones SSH puedan instalar el Agente de red en el dispositivo que usa OpenSSH versión 6.4 o anterior.

   Para hacer esto, en el dispositivo con el Servidor de administración instalado, o en un dispositivo que actúa como punto de distribución cuyo alcance incluye el dispositivo de destino, ejecute el siguiente comando en la línea de comandos:

   ```
   klscflag -fset -pv ".core/.independent" -s "Transport" -n
   SSH_CLIENT_DISABLE_ALGS_PROTECT -t d -v 1
   ```

El dispositivo Linux está listo para la instalación remota del Agente de red.

Deshabilitar la lista de algoritmos de cifrado válidos admitidos puede afectar la seguridad de la conexión SSH. Recomendamos que vuelva a habilitar la lista de algoritmos de cifrado válidos admitidos de inmediato después de instalar el Agente de red. Para volver a habilitar la lista de admitidos de algoritmos de cifrado válidos, ejecute el siguiente comando:

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

Una vez que haya instalado el Agente de red y luego haya vuelto a habilitar la lista de admitidos de algoritmos de cifrado válidos, el dispositivo que ejecuta un sistema operativo Linux con glibc 2.5 (SO heredado) es ahora administrado por el Servidor de Administración.

Instalar el Agente de red en un dispositivo Linux de forma remota

Antes de instalar el Agente de red en un dispositivo basado en Linux, debe completar los pasos de preparación generales que se requieren para todos los dispositivos basados en Linux.

Después de completar los pasos generales, puede seguir las instrucciones adicionales específicas de su sistema operativo:

- Preparación de un dispositivo que ejecuta SUSE Linux Enterprise Server 15
- Preparación de un dispositivo que ejecuta Astra Linux en el modo de entorno de software cerrado
- Preparación de un dispositivo que ejecuta Ubuntu Server/Desktop versión 10.04 y 16.04
- Preparación de un dispositivo que ejecuta un sistema operativo Linux con glibc 2.5

Para instalar el Agente de red en dispositivos Linux de manera remota:

1. Descargue y cree un paquete de instalación:

   a. Antes de iniciar la instalación del paquete en el dispositivo, asegúrese de que ya tiene instaladas todas las dependencias (programas y bibliotecas) para este paquete.

      Puede ver las dependencias de cada paquete por su propia cuenta, mediante las utilidades específicas de la distribución Linux en la que se instalará el paquete. Para obtener más información sobre las utilidades, consulte la documentación de su sistema operativo.

b. Para crear un paquete de instalación remota, use los archivos siguientes:

- klnagent.kpd
- akinstall.sh
- Paquete .deb o .rpm de Agente de red

2. Cree una tarea de instalación remota con la configuración siguiente:

- En la página **Configuración** del Asistente para crear nueva tarea, seleccione la casilla **Uso de los recursos del sistema operativo a través del Servidor de administración**. Quite la selección a todo.
- En la página **Seleccione una cuenta con la que ejecutar la tarea**, especifique la configuración de la cuenta de usuario que se utiliza para la conexión del dispositivo mediante SSH.

3. Ejecute la tarea de instalación remota. Utilice la opción para el comando `su` para preservar el entorno: `-m, -p, --preserve-environment`.

Instalación del Agente de red para Linux en modo silencioso (con un archivo de respuestas)

A la hora de instalar el Agente de red en un dispositivo con Linux, puede utilizar lo que se denomina "archivo de respuestas", un archivo de texto con variables y valores que representan opciones de instalación específicas. El archivo de respuestas permite realizar la instalación en modo no interactivo, es decir, sin involucrar al usuario.

Antes de instalar el Agente de red en un dispositivo basado en Linux, debe completar los pasos de preparación generales que se requieren para todos los dispositivos basados en Linux.

Después de completar los pasos generales, puede seguir las instrucciones adicionales específicas de su sistema operativo:

- Preparación de un dispositivo que ejecuta SUSE Linux Enterprise Server 15
- Preparación de un dispositivo que ejecuta Astra Linux en el modo de entorno de software cerrado
- Preparación de un dispositivo que ejecuta Ubuntu Server/Desktop versión 10.04 y 16.04
- Preparación de un dispositivo que ejecuta un sistema operativo Linux con glibc 2.5

Para instalar el Agente de red para Linux en modo silencioso:

1. Lea el Contrato de licencia de usuario final. Siga los pasos a continuación únicamente si comprende y acepta los términos del Contrato de licencia de usuario final.

2. Cree el archivo de respuesta (en formato TXT). El archivo debe contener una lista de variables en formato NOMBRE_DE_LA_VARIABLE=valor_de_la_variable. No puede haber más de una variable por línea.

Como mínimo, el archivo de respuestas debe incluir las siguientes tres variables, que son obligatorias:

- KLNAGENT_SERVER
- KLNAGENT_AUTOINSTALL
- EULA_ACCEPTED

Si desea que la instalación remota se lleve a cabo con otros parámetros específicos, agregue las variables opcionales que correspondan. Todas las variables que puede incluir en el archivo figuran en la siguiente tabla:

Variables admitidas en el archivo de respuestas como parámetros de instalación en modo silencioso para el Agente de red para Linux

Variables admitidas en el archivo de respuestas como parámetros de instalación en modo silencioso para el Agente de red para Linux

Nombre de la variable	Obligatoria	Descripción	Valores posibles
KLNAGENT_SERVER	Sí	Contiene el nombre del Servidor de administración. El valor puede ser un nombre de dominio completo (FQDN) o una dirección IP.	Nombre DNS o dirección IP.
KLNAGENT_AUTOINSTALL	Sí	Define si la instalación se realizará en modo no interactivo.	1: Usar el modo silencioso. No se le pedirá al usuario que participe del proceso de instalación. Otro valor: No usar el modo silencioso. Se le podría pedir al usuario que participe del proceso de instalación.
EULA_ACCEPTED	Sí	Determina si el usuario está de acuerdo con el Contrato de licencia de usuario final (EULA) del agente de red. Si no se define esta variable, puede entenderse que el usuario no acepta el EULA.	1: Confirmo que he leído, entendido y aceptado completamente los términos y condiciones de este Contrato de licencia de usuario final. Otros o no especificado: No acepto los términos del Contrato de licencia (no se realiza la instalación).
KLNAGENT_PROXY_USE	No	Determina si los ajustes del servidor proxy se tendrán en cuenta para conectarse al Servidor de administración. El valor predeterminado es 0.	1: Tener en cuenta los ajustes del servidor proxy. Otro valor: Ignorar los ajustes del servidor proxy.
KLNAGENT_PROXY_ADDR	No	Define la dirección del servidor proxy que se usará al conectarse con el Servidor de administración.	Nombre DNS o dirección IP.
KLNAGENT_PROXY_LOGIN	No	Define el nombre de usuario que se usará para identificarse ante el servidor proxy.	Cualquier nombre de usuario existente.
KLNAGENT_PROXY_PASSWORD	No	Define la contraseña de usuario que se usará para identificarse ante el servidor proxy.	Cualquier secuencia de caracteres alfanuméricos que el sistema operativo permita usar como contraseña.
KLNAGENT_VM_VDI	No	Determina si el Agente de red se instalará en una imagen que luego vaya a utilizarse para crear máquinas virtuales dinámicas.	1: El Agente de red se instalará en una imagen con la que luego se crearán máquinas virtuales dinámicas. Otro valor: La aplicación no se instalará en una imagen.

KLNAGENT_VM_OPTIMIZE	No	Determina si el Agente de red usará los ajustes de configuración optimizados para hipervisores.	1: La configuración local predeterminada del Agente de red se modificará y se aplicarán los ajustes optimizados para hipervisores.
KLNAGENT_TAGS	No	Contiene la lista de etiquetas que se asignarán a la instancia del Agente de red.	Una o más etiquetas, separadas con punto y coma.
KLNAGENT_UDP_PORT	No	Define el puerto UDP que usará el Agente de red. El valor predeterminado es 15000.	Cualquier número de puerto.
KLNAGENT_PORT	No	Define el puerto no TLS que usará el Agente de red. El valor predeterminado es 14000.	Cualquier número de puerto.
KLNAGENT_SSLPORT	No	Define el puerto TLS que usará el Agente de red. El valor predeterminado es 13000.	Cualquier número de puerto.
KLNAGENT_USESSL	No	Determina si se usará el protocolo TLS para establecer la conexión.	1 (valor predeterminado): Usar TLS. Otro valor: No usar TLS.
KLNAGENT_GW_MODE	No	Determina si se usará una puerta de enlace de conexión.	1 (valor predeterminado): Mantener la configuración existente (no se usará una puerta de enlace de conexión en la primera llamada). 2: No usar una puerta de enlace de conexión. 3: Usar una puerta de enlace de conexión. Se requiere KLNAGENT_GW_ADDRESS. 4: La instancia de Agente de red actuará como puerta de enlace de conexión en una zona desmilitarizada (DMZ). Se requiere certificado de servidor.
KLNAGENT_GW_ADDRESS	No	Determina la dirección de la puerta de enlace de conexión. El valor solo se tiene en cuenta cuando KLNAGENT_GW_MODE=3.	Nombre DNS o dirección IP.
KLNAGENT_DEVICEOWNER_REGISTRATION_START	No	Permite ejecutar la utilidad para registrar a un usuario como propietario del dispositivo tras la instalación del Agente de red. Si deshabilita esta función, el usuario no podrá registrarse como propietario del dispositivo.	1: La utilidad para registrar al usuario como propietario del dispositivo se ejecutará tras la instalación del Agente de red. Otro valor: deshabilitado.
PTCH_ALLOW_APPLY_NONAPROVED_PATCHES	No	Define si se deben instalar las actualizaciones descargadas automáticamente para el Agente de red con el estado *Sin definir*.	true (valor predeterminado): estas actualizaciones se instalan automáticamente. false: las actualizaciones no se instalan automáticamente.

3. Descargue el paquete de instalación del Agente de red. La variable de entorno KLAUTOANSWERS, que especifica la ruta al archivo de respuesta, se pasa al comando de instalación. Ejecute uno de los siguientes comandos:

   - Para instalar el Agente de red de un paquete RPM a un sistema operativo de 32 bits, ejecute el siguiente comando:
     `sudo KLAUTOANSWERS=<ruta al archivo de respuesta> yum install ./klnagent-<número de compilación>.i386.rpm`

   - Para instalar el Agente de red desde un paquete RPM en un sistema operativo de 64 bits, ejecute el siguiente comando:
     `sudo KLAUTOANSWERS=<ruta al archivo de respuesta> yum install ./klnagent64-<número de compilación>.x86_64.rpm`

   - Para instalar el Agente de red de un paquete RPM en un sistema operativo de 64 bits para la arquitectura Arm, ejecute el siguiente comando:
     `sudo KLAUTOANSWERS=<ruta al archivo de respuesta> yum install ./klnagent64-<número de compilación>.aarch64.rpm`

   - Para instalar el Agente de red de un paquete DEB en un sistema operativo de 32 bits, ejecute el siguiente comando:
     `sudo KLAUTOANSWERS=<ruta al archivo de respuesta> apt install ./klnagent_<número de compilación>_i386.deb`

   - Para instalar el Agente de red de un paquete DEB en un sistema operativo de 64 bits, ejecute el siguiente comando:
     `sudo KLAUTOANSWERS=<ruta al archivo de respuesta> apt install ./klnagent64_<número de compilación>_amd64.deb`

   - Para instalar el Agente de red de un paquete DEB en un sistema operativo de 64 bits para la arquitectura Arm, ejecute el siguiente comando:
     `sudo KLAUTOANSWERS=<ruta al archivo de respuesta> apt install ./klnagent64_<número de compilación>_arm64.deb`

   Dependiendo de la configuración del sistema operativo, también puede usar los administradores de paquetes rpm, dpkg o dnf para instalar el Agente de red.

Comenzará la instalación del Agente de red para Linux en modo silencioso. No se le pedirá al usuario que participe del proceso.

Instalación del Agente de red para Linux en modo interactivo

En este artículo, se describe cómo instalar el Agente de red en dispositivos Linux en el modo interactivo, mediante la especificación paso a paso de los parámetros de instalación. También puede usar un archivo de respuestas, es decir, un archivo de texto que contiene un conjunto personalizado de parámetros de instalación: variables y sus respectivos valores. El archivo de respuestas permite realizar la instalación en modo silencioso, es decir, sin involucrar al usuario.

Antes de instalar el Agente de red en un dispositivo basado en Linux, debe completar los pasos de preparación generales que se requieren para todos los dispositivos basados en Linux.

Después de completar los pasos generales, puede seguir las instrucciones adicionales específicas de su sistema operativo:

- Preparación de un dispositivo que ejecuta SUSE Linux Enterprise Server 15
- Preparación de un dispositivo que ejecuta Astra Linux en el modo de entorno de software cerrado
- Preparación de un dispositivo que ejecuta Ubuntu Server/Desktop versión 10.04 y 16.04
- Preparación de un dispositivo que ejecuta un sistema operativo Linux con glibc 2.5

Para instalar el Agente de red en modo interactivo:

1. Descargue el paquete de instalación del Agente de red. Dependiendo de su distribución de Linux, ejecute uno de los siguientes comandos:
   - Para instalar el Agente de red desde un paquete RPM en un sistema operativo de 32 bits:
     `# yum -i klnagent-<número de compilación>.i386.rpm`
   - Para instalar el Agente de red desde un paquete RPM en un sistema operativo de 64 bits:
     `# yum -i klnagent64-<número de compilación>.x86_64.rpm`
   - Para instalar el Agente de red desde un paquete RPM en un sistema operativo de 64 bits para la arquitectura ARM:
     `# yum -i klnagent64-<número de compilación>.aarch64.rpm`
   - Para instalar el Agente de red desde un paquete DEB en un sistema operativo de 32 bits:
     `# apt install ./klnagent_<número de compilación>_i386.deb`
   - Para instalar el Agente de red desde un paquete DEB en un sistema operativo de 64 bits:
     `# apt install ./klnagent64_<número de compilación>_amd64.deb`
   - Para instalar el Agente de red desde un paquete DEB en un sistema operativo de 64 bits para la arquitectura ARM:
     `# apt install ./klnagent64_<número de compilación>_arm64.deb`
2. Ejecute la configuración del Agente de red:
   `# /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl`
3. Lea el Contrato de licencia de usuario final. El texto se muestra en la ventana de la línea de comandos. Presione la barra espaciadora para ver el siguiente segmento de texto. Luego, cuando se le solicite, ingrese uno de los siguientes valores:
   - Ingrese `y` si comprende y acepta los términos del EULA.
   - Ingrese `n` si no acepta los términos del EULA. Para usar el Agente de red, debe aceptar las condiciones del EULA.
   - Ingrese `r` para volver a mostrar el EULA.
4. Ingrese el nombre DNS o la dirección IP del Servidor de administración.
5. Ingrese el número de puerto del Servidor de administración. El número de puerto predeterminado es 14000.

6. Ingrese el número de puerto SSL del Servidor de administración. El número de puerto predeterminado es 13000.

7. Ingrese `y` si desea utilizar cifrado SSL para el tráfico entre el Agente de red y el Servidor de administración. De lo contrario, ingrese `n`.

8. Seleccione una de las siguientes opciones para configurar el Agente de red:

   - `[1]` – `Keep current connection gateway settings`.

     La configuración de la pasarela de conexión se conserva tras las actualizaciones. Tras la instalación inicial, la pasarela de conexión no está configurada.

   - `[2]` – `Do not use connection gateway.`

     Su dispositivo no se conectará al Servidor de administración a través de una puerta de enlace de conexión.

   - `[3]` –`Connect to server using connection gateway`.

     Su dispositivo se conectará al Servidor de administración a través de una puerta de enlace de conexión.

   - `[4]` – `Use as connection gateway`.

     Su dispositivo funcionará como puerta de enlace de conexión.

El Agente de red está instalado en un dispositivo Linux.

Soporte de reversión del sistema de archivos para dispositivos con Agente de red

Kaspersky Security Center Linux es una aplicación distribuida. El revertir el sistema de archivos a un estado anterior en un dispositivo con Agente de red instalado llevará a la desincronización de datos y funcionamiento incorrecto de Kaspersky Security Center Linux.

El sistema de archivos (o una parte de él) se puede revertir en los casos siguientes:

- Al copiar una imagen del disco duro.
- Al restaurar un estado de la máquina virtual por medio de la infraestructura virtual.
- Al restaurar datos desde una copia de seguridad o un punto de recuperación.

Para Kaspersky Security Center Linux, sólo son críticas las situaciones en los que el software de terceros en dispositivos con el Agente de administración instalado afecta la carpeta /var/opt/kaspersky/klnagent. Por lo tanto, siempre debe excluir esta carpeta del procedimiento de recuperación, de ser posible.

Como las reglas del lugar de trabajo de algunas organizaciones proporcionan reversiones del sistema de archivos en dispositivos, el soporte de la reversión del sistema de archivos en dispositivos con Agente de red instalado se agregó a Kaspersky Security Center Linux a partir de la versión 10 Maintenance Release 1 (Servidor de administración y Agentes de red deben ser de la versión 10 Maintenance Release 1 o posterior). Cuando se detecta, esos dispositivos automáticamente se conectan de nuevo al Servidor de administración con limpieza de datos completa y sincronización completa.

De manera predeterminada, el soporte de la detección de reversión del sistema de archivos está habilitado en Kaspersky Security Center Linux.

Siempre que sea posible, evite deshacer la carpeta /var/opt/kaspersky/klnagent en dispositivos con el Agente de red instalado, porque la resincronización completa de datos requiere una gran cantidad de recursos.

Una reversión del estado del sistema no se permite en absoluto en un dispositivo con el Servidor de administración instalado. Tampoco se aplica a la reversión de la base de datos usada por el Servidor de administración.

Puede restaurar un estado del Servidor de administración desde una copia de seguridad solo con la utilidad estándar klbackup.

Instalar el Agente de red para Windows

También puede instalar el Agente de red en dispositivos Windows de una organización para administrarlos mediante el Servidor de administración.

En Microsoft Windows XP, el Agente de red podría no realizar las siguientes operaciones correctamente: descargar actualizaciones directamente desde los servidores de Kaspersky (como un punto de distribución); funcionar como servidor proxy de KSN (como un punto de distribución); detectar vulnerabilidades de terceros (si se usa la Administración de vulnerabilidades y parches).

Antes de instalar el Agente de red en un dispositivo que ejecuta Microsoft Windows en Arm, asegúrese de que no hay ningún Agente de red para Microsoft Windows x86-64 instalado. De lo contrario, la instalación fallará.

Existen los siguientes métodos para instalar inicialmente el Agente de red en el dispositivo administrado con Windows:

- Ejecutar la tarea de instalación remota a través del punto de distribución de Windows.

  Antes de realizar una instalación remota en un dispositivo Windows no asignado, un punto de distribución basado en Windows verifica automáticamente el puerto UDP 137 para determinar el tipo de sistema operativo del dispositivo de destino. Si el puerto UDP 137 no está disponible, el punto de distribución intenta conectarse al puerto TCP 445 en el dispositivo de destino, que es necesario para realizar la instalación.

- Usar el paquete de Windows Installer (MSI) para el Agente de red con herramientas de terceros para la instalación remota de aplicaciones.

- Ejecutar el instalador de la aplicación en el dispositivo administrado.

- Enviar vínculos de usuarios del dispositivo a paquetes independientes generados por Kaspersky Security Center Linux. Los paquetes independientes son módulos ejecutables que contienen los paquetes de distribución de aplicaciones seleccionadas con su configuración definida.

Instalar el Agente de red para Windows en modo interactivo

Para instalar el Agente de red en un dispositivo de manera local:

1. En el dispositivo, ejecute el archivo ksc_<número de versión>.<número de compilación>_full_<idioma de localización>.exe del paquete de distribución que descargó de Internet.

   Se abre una ventana y se le solicita que seleccione las aplicaciones de Kaspersky que desea instalar.

2. En la ventana de selección de aplicación, haga clic en el vínculo **Instalar solo el Agente de red de Kaspersky Security Center** para iniciar el asistente de instalación del Agente de red. Siga los pasos del asistente.

   Mientras se ejecuta el asistente de instalación, puede especificar la configuración avanzada del Agente de red (ver a continuación).

3. Si quiere utilizar el dispositivo como la puerta de enlace de conexión de un grupo de administración específico, en la ventana **Puerta de enlace de conexión** del asistente de instalación, seleccione **Usar el Agente de red como una puerta de enlace de conexión en la DMZ**.

4. Para configurar el Agente de red durante la instalación en una máquina virtual:

   a. Si planea crear máquinas virtuales dinámicas desde la imagen de la máquina virtual, habilite el modo dinámico del Agente de red para infraestructura de escritorio virtual (VDI). Para hacerlo, en la ventana **Configuración avanzada** del asistente de instalación, seleccione la opción **Habilitar modo dinámico para VDI**.

      Omita este paso si no planea crear máquinas virtuales dinámicas a partir de la imagen de la máquina virtual.

   b. Optimice la operación del Agente de red para VDI. Para esto, en la ventana **Configuración avanzada** del asistente de instalación, seleccione la opción **Optimizar la configuración para VM**.

      Se desactivará el análisis de los archivos ejecutables en busca de vulnerabilidades durante el inicio del dispositivo. Además esto deshabilita el envío de información sobre los siguientes objetos al Servidor de administración:

      - Registro de hardware
      - Aplicaciones instaladas en el dispositivo
      - Actualizaciones de Microsoft Windows que deberían instalarse en el dispositivo cliente local
      - Vulnerabilidades de software detectadas en el dispositivo cliente local

      Además, podrá habilitar el envío de esta información en las propiedades del Agente de red o en la configuración de la directiva del Agente de red.

Cuando el asistente de instalación se haya completado, el Agente de red estará instalado en el dispositivo.

Puede ver las propiedades del servicio del Agente de red; también puede iniciar, detener y supervisar la actividad del Agente de red mediante las herramientas estándar de Microsoft Windows: Administración de equipos\Servicios.

Instalación del Agente de red para Windows en modo silencioso

El Agente de red puede instalarse en modo no interactivo; es decir, sin entrada interactiva de los parámetros de instalación. La instalación no interactiva usa un paquete de Windows Installer (MSI) para el Agente de red. El archivo MSI se encuentra en el paquete de distribución de Kaspersky Security Center Linux, en la carpeta Packages\NetAgent\exec.

La instalación del Agente de red desde el paquete MSI solo es posible en modo silencioso, no se admite la instalación interactiva desde el paquete MSI.

Para instalar el Agente de red en un dispositivo local en modo no interactivo:

1. Lea el Contrato de licencia de usuario final. Use el comando a continuación únicamente si comprende y acepta los términos del Contrato de licencia de usuario final.

2. Ejecute el comando
   `msiexec /i "Kaspersky Network Agent.msi" /qn <parámetros_de_instalación>`

   donde `setup_parameters` es una lista de parámetros y sus respectivos valores, separados por un espacio (`PROP1=PROP1VAL PROP2=PROP2VAL`).

   En la lista de parámetros debe incluir `EULA=1`. De lo contrario, el Agente de red no se instalará.

Si está utilizando la configuración de conexión estándar para Kaspersky Security Center y el Agente de red en dispositivos remotos, ejecute el comando:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

`/l*vx` es la clave para escribir registros. El registro se crea durante la instalación del Agente de red y se guarda en C:\windows\temp\nag_inst.log.

Además de nag_inst.log, la aplicación crea el archivo $klssinstlib.log, que contiene el registro de instalación. Este archivo se almacena en la carpeta %windir%\temp o %temp%. Para solucionar problemas, es posible que usted o un especialista del Servicio de soporte técnico de Kaspersky necesiten ambos archivos de registro: nag_inst.log y $klssinstlib.log.

Si necesita especificar adicionalmente el puerto para la conexión al Servidor de administración, ejecute el comando:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1 SERVERPORT=14000
```

El parámetro `SERVERPORT` corresponde al número de puerto para la conexión al Servidor de Administración.

Los nombres y posibles valores de los parámetros que se pueden utilizar al instalar el Agente de red en modo no interactivo se enumeran en la sección Parámetros de instalación del Agente de red.

Si desea actualizar el Agente de red con Windows Installer, ejecute el siguiente comando:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

Despliegue mediante la captura y copia de la imagen de un dispositivo

Si tiene que instalar el Agente de red en dispositivos en los cuales un sistema operativo y otro software también se deben instalar (o volver a instalar), puede usar el mecanismo de captura y copia de la imagen de ese dispositivo.

Para realizar un despliegue con una imagen de disco duro:

1. Cree un dispositivo de referencia con un sistema operativo y el software relevante instalado, incluidos el Agente de red y una aplicación de seguridad.

2. Capture la imagen de la referencia en el dispositivo y distribuya esa imagen en dispositivos nuevos a través de la tarea dedicada de Kaspersky Security Center Linux.

   Para capturar e instalar imágenes de disco, use las herramientas de terceros disponibles en la organización.

Copia de una imagen de disco con herramientas de terceros

Al aplicar herramientas de terceros para capturar la imagen de un dispositivo con el Agente de red instalado, use uno de los métodos siguientes:

- En el dispositivo de referencia, detenga el servicio del Agente de red y ejecute la utilidad klmover con la clave `-dupfix`. La utilidad klmover se incluye en el paquete de instalación del Agente de red. Evite cualquier ejecución subsiguiente del servicio del Agente de red hasta que la operación de captura de la imagen se complete.

- Asegúrese de ejecutar la utilidad klmover con la clave `-dupfix` antes de la primera ejecución del servicio del Agente de red en los dispositivos de destino. Este es un requisito obligatorio y debe realizarse en el primer inicio del sistema operativo después del despliegue de la imagen. La utilidad klmover se incluye en el paquete de instalación del Agente de red.

- Utilice el modo de clonación de disco del Agente de red.

Si la imagen del disco duro no se copió correctamente, existen métodos para resolver el problema.

También puede capturar la imagen de un dispositivo sin el Agente de red instalado. Para hacerlo, realice el despliegue de la imagen en los dispositivos de destino y luego despliegue el Agente de red. Si utiliza este método, proporcione acceso a la carpeta de red con paquetes de instalación independientes desde un dispositivo.

Modo de clonación de disco del Agente de red

La clonación del disco duro de un dispositivo de referencia es un método muy utilizado para instalar software en dispositivos nuevos. Si el Agente de red se está ejecutando en modo estándar en el disco duro del dispositivo de referencia, se presenta el siguiente problema:

Una vez que la imagen de referencia con el Agente de red se instala en los dispositivos nuevos, estos aparecen en Kaspersky Security Center Web Console como un solo dispositivo. El problema se produce porque, debido a la clonación, los datos internos de los dispositivos, que el Servidor de administración utiliza para asociar un dispositivo con su propio registro en Kaspersky Security Center Web Console, son idénticos.

El *modo de clonación de disco del Agente de red* especial le permite evitar la visualización incorrecta de dispositivos nuevos en Kaspersky Security Center Web Console luego de la clonación. Use este modo cuando desee realizar un despliegue de software (con el Agente de red) en dispositivos nuevos mediante la clonación de disco.

En el modo de clonación de disco, el Agente de red sigue ejecutándose pero no se conecta al Servidor de administración. Al salir del modo de clonación, el Agente de red elimina los datos internos que hacen que el Servidor de administración asocie varios dispositivos con un solo registro en Kaspersky Security Center Web Console. Después de completar la clonación de la imagen del dispositivo de referencia, los dispositivos nuevos se muestran en Kaspersky Security Center Web Console correctamente (con registros individuales).

Escenario de uso del modo de clonación de disco del Agente de red

1. El administrador instala el Agente de red en un dispositivo de referencia.
2. El administrador comprueba la conexión del Agente de red con el Servidor de administración usando la utilidad klnagchk.
3. El administrador habilita el modo de clonación de disco del Agente de red.
4. El administrador instala software y parches en el dispositivo, y lo reinicia tantas veces como sea necesario.
5. El administrador clona el disco duro del dispositivo de referencia en cuantos dispositivos sea necesario.
6. Cada copia clonada debe cumplir las siguientes condiciones:
    a. Se debe cambiar el nombre del dispositivo.
    b. Se debe reiniciar el dispositivo.
    c. Se debe deshabilitar el modo de clonación de disco.

Habilitación y deshabilitación del modo de clonación de disco mediante la utilidad klmover

Para activar o desactivar el modo de clonación de disco del Agente de red:

1. Ejecute la utilidad klmover en el dispositivo con el Agente de red instalado que necesita clonar.
   La utilidad klmover se encuentra en la carpeta de instalación del Agente de red.
2. Para habilitar el modo de clonación de disco, ingrese el siguiente comando en la terminal de Linux:
   `./klmover -cloningmode 1`
   El Agente de red cambia al modo de clonación de disco.

3. Para solicitar el estado actual del modo de clonación de disco, ingrese el siguiente comando en el símbolo del sistema:

   ```
   ./klmover -cloningmode
   ```

   La ventana de la utilidad indica si el modo de clonación de disco está habilitado o no.

4. Para deshabilitar el modo de clonación de disco, ingrese el siguiente comando en la línea de comandos de la utilidad:

   ```
   ./klmover -cloningmode 0
   ```

Agente de red: parámetros de instalación

La tabla a continuación describe las propiedades MSI que puede configurar al instalar el Agente de red. Todos los parámetros son opcionales, excepto EULA y SERVERADDRESS.

Parámetros de instalación del Agente de red en modo no interactivo

Propiedad MSI	Descripción	Valores disponibles
EULA	Aceptación de los términos del Contrato de licencia	• 1: Confirmo que he leído completamente, entiendo y acepto los términos y las condiciones de este Contrato de licencia de usuario final. • 0: No acepto los términos del Contrato de licencia (no se realiza la instalación). • Sin valor: no acepto los términos del Contrato de licencia (no se realiza la instalación).
DONT_USE_ANSWER_FILE	Lea la configuración de instalación desde el archivo de respuesta	• 1—No usar. • Otro valor o ningún valor—Leer.
INSTALLDIR	Ruta a la carpeta de instalación del Agente de red	Valor de cadena.
SERVERADDRESS	Dirección del Servidor de administración (obligatoria)	Valor de cadena.
SERVERPORT	Número de un puerto para la conexión al Servidor de administración	Valor numérico.
SERVERSSLPORT	Número del puerto para conexión cifrada al Servidor de administración usando el protocolo SSL	Valor numérico.
USESSL	Usar una conexión SSL o no	• 1: Usar • Otro valor o ningún valor: No usar
OPENUDPPORT	Abrir un puerto UDP o no	• 1: Abrir • Otro valor o ningún valor: No abrir
UDPPORT	Número de puerto UDP	Valor numérico.
USEPROXY	Usar un servidor proxy o no.	• 1: Usar • Otro valor o ningún valor: No usar
PROXYLOCATION (PROXYADDRESS:PROXYPORT)	Dirección del proxy y número de puerto para la conexión con el servidor proxy	Valor de cadena.
PROXYLOGIN	Cuenta para la conexión con un servidor proxy	Valor de cadena.
PROXYPASSWORD	Contraseña de la cuenta para conectarse al servidor proxy (No indique ningún detalle de las cuentas con privilegios en los parámetros de los paquetes de instalación).	Valor de cadena.
GATEWAYMODE	Modo de uso de la puerta de enlace de conexión	• 0: No usar la puerta de enlace de conexión • 1: Use este Agente de red como puerta de enlace de conexión • 2: Conectarse al Servidor de administración mediante una puerta de enlace de conexión

Propiedad MSI	Descripción	Valores disponibles
GATEWAYADDRESS	Dirección de la puerta de enlace de conexión	Valor de cadena.
CERTSELECTION	Método de recibir un certificado	• GetOnFirstConnection; Reciba un certificado del Servidor de administración • GetExistent: especificar un certificado existente. Si se selecciona esta opción, se debe definir la propiedad CERTFILE.
CERTFILE	Ruta al archivo de certificado	Valor de cadena.
VMVDI	Habilitar el modo dinámico para la Infraestructura de escritorio virtual (VDI)	• 1: Habilitar. • 0: No habilitar. • Sin valor: No habilitar.
LAUNCHPROGRAM	Ejecutar el inicio del servicio del Agente de red después de la instalación. El parámetro se ignora si VMVDI=1	• 1: Iniciar • Otro valor o ningún valor: No iniciar
NAGENTTAGS	Etiqueta para el Agente de red (tiene prioridad sobre la etiqueta dada en el archivo de respuestas)	Valor de cadena.

Instalar aplicaciones mediante la tarea de instalación remota

Kaspersky Security Center Linux permite que usted instale aplicaciones en dispositivos remotamente, mediante las tareas de instalación remotas. Las tareas se crean y se asignan a los dispositivos a través de un asistente específico. Para asignar una tarea con mayor facilidad y rapidez, puede especificar los dispositivos (hasta 1000) de distintas maneras a través de la ventana del asistente:

- **Asignar tarea a un grupo de administración**. En este caso, la tarea se asigna a los dispositivos incluidos en el grupo de administración creado anteriormente.
- **Especificar las direcciones de los dispositivos manualmente o importarlas de una lista**. Puede especificar los nombres DNS, las direcciones IP y las subredes IP de los dispositivos a los cuales desee asignar la tarea.
- **Asignar tarea a una selección de dispositivos**. En este caso, la tarea se asigna a los dispositivos incluidos en una selección creada anteriormente. Puede especificar la selección predeterminada o una personalizada que ya haya creado. Solo puede seleccionar un máximo de 1000 dispositivos.

Para evitar problemas que puedan ocurrir durante la instalación de la aplicación en un dispositivo cliente sin Agente de red instalado, debe proceder como se describe en el despliegue forzado a través de la tarea de instalación remota de Kaspersky Security Center Linux.

Acerca de las tareas de instalación remota en Kaspersky Security Center Linux

Kaspersky Security Center Linux proporciona varios mecanismos para la instalación remota de aplicaciones, que se implementan como tareas de instalación remotas (instalación forzada, instalación al copiar una imagen del disco duro). Puede crear una tarea de instalación remota tanto para un grupo de administración especificado como para dispositivos específicos o una selección de dispositivos (estas tareas se muestran en Kaspersky Security Center Web Console, en la carpeta **Tareas**). Al crear una tarea, puede seleccionar paquetes de instalación (los del Agente de red u otra aplicación) que se instalarán dentro de esta tarea, así como especificar ciertas configuraciones que definan el método de la instalación remota. Además, puede usar el Asistente de instalación remota, que se basa en la creación de una tarea de instalación remota y da como resultado la supervisión.

Las Tareas para grupos de administración afectan a ambos dispositivos incluidos en un grupo especificado y todos los dispositivos en todos los subgrupos dentro de ese grupo de administración. Una tarea cubre dispositivos de Servidores de administración secundarios incluidos en un grupo o cualquiera de sus subgrupos si la configuración correspondiente se habilita en la tarea.

Las tareas para dispositivos específicos actualizan la lista de dispositivos cliente en cada ejecución de acuerdo con el contenido de la selección en el momento en el que se inicia la tarea. Si una selección incluye dispositivos que se han conectado a Servidores de administración secundarios, la tarea también se ejecutará en esos dispositivos. Para obtener más información sobre esas configuraciones y métodos de instalación, consulte la siguiente información en esta sección.

Para asegurar la operación correcta de una tarea de instalación remota en dispositivos conectados a Servidores de administración secundarios, debe usar la tarea de retransmisión para retransmitir paquetes de instalación usados por su tarea a los Servidores de administración secundarios correspondientes de antemano.

Instalación de una aplicación de forma remota

En esta sección, se explica cómo instalar una aplicación de forma remota en los dispositivos de un grupo de administración, en dispositivos con direcciones específicas o en una selección de dispositivos.

Para instalar una aplicación en dispositivos específicos:

1. En el menú principal, vaya a **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea.
3. En la sección **Tipo de tarea**, seleccione **Instalar aplicación de forma remota**.
4. Seleccione una de las siguientes opciones:

   Asignar tarea a un grupo de administración

   La tarea se asignará a los dispositivos incluidos en un grupo de administración. Puede seleccionar un grupo existente o crear uno nuevo.

Puede usar esta opción para, por ejemplo, ejecutar una tarea que envíe un mensaje a ciertos usuarios si el contenido atañe solamente a los dispositivos de un grupo de administración puntual.

Si la tarea se asigna a un grupo de administración, la pestaña **Seguridad** no se mostrará en la ventana de propiedades de la tarea; esto se debe a que las tareas de grupo están sujetas a la configuración de seguridad de los grupos a los que se aplican.

Especificar las direcciones de los dispositivos manualmente o importarlas de una lista

Puede especificar los nombres DNS, las direcciones IP y las subredes IP de los dispositivos a los cuales desee asignar la tarea.

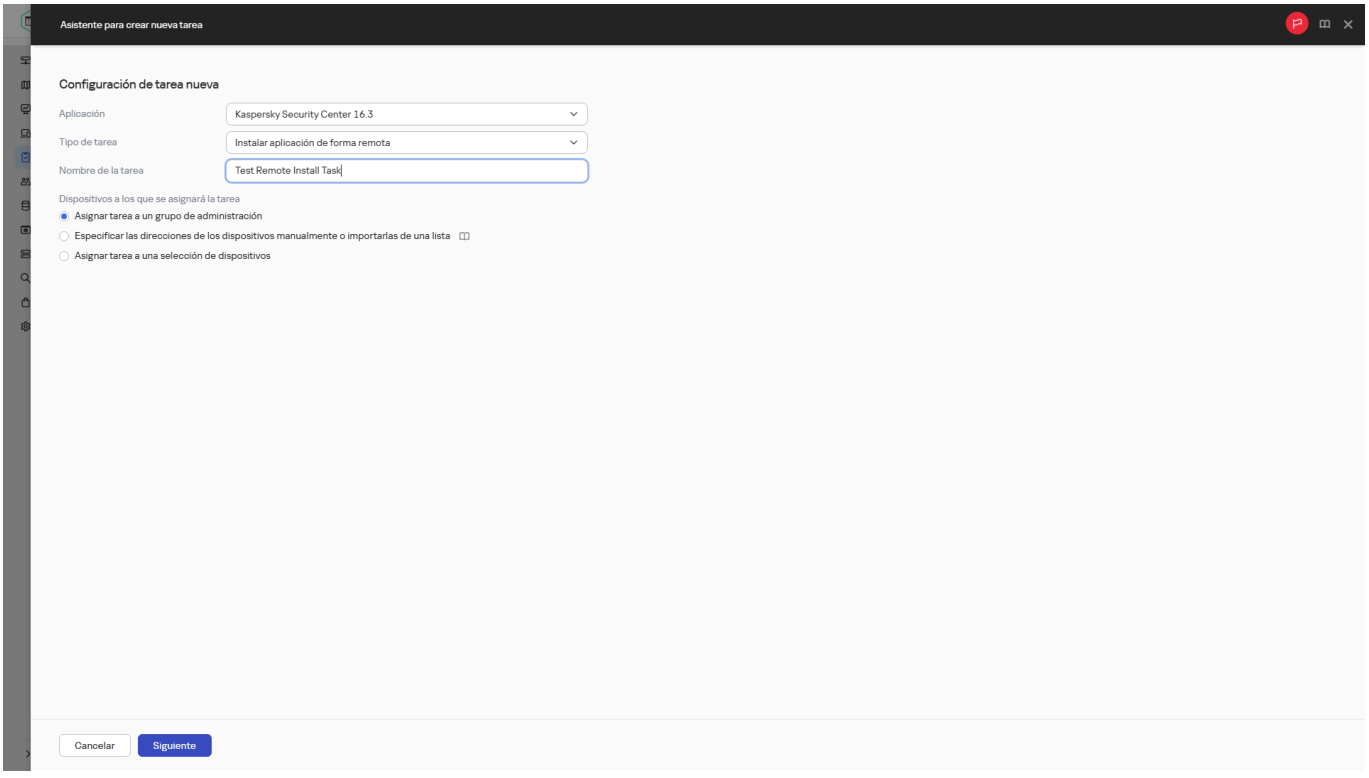
Podría elegir esta opción si necesita que la tarea se ejecute en una subred específica. Esto puede ser útil si, por ejemplo, necesita instalar una aplicación solo en los dispositivos que utilizan los contadores o si quiere analizar los dispositivos de una subred puntual que probablemente esté infectada.

Asignar tarea a una selección de dispositivos

La tarea se asignará a los dispositivos incluidos en una selección de dispositivos. Puede elegir una selección existente.

Esta opción puede ser útil para, por ejemplo, ejecutar una tarea en los dispositivos que tengan una versión específica de un sistema operativo.

La tarea *Instalar aplicación de forma remota* se creará para los dispositivos especificados. Si seleccionó la opción **Asignar tarea a un grupo de administración**, la tarea será una tarea de grupo.



Crear la tarea Instalar aplicación de forma remota

5. En el paso **Alcance de la tarea**, indique un grupo de administración, dispositivos con direcciones específicas o una selección de dispositivos.

   Los ajustes disponibles dependerán de la opción seleccionada en el paso anterior.

6. En el paso **Paquetes de instalación**, defina los siguientes ajustes:

- En el campo **Seleccione el paquete de instalación**, seleccione el paquete de instalación de la aplicación que desee instalar.

- En el grupo de configuraciones **Forzar la descarga del paquete de instalación**, puede especificar cómo se distribuyen a los dispositivos cliente los archivos que se requieren para la instalación de una aplicación:

  Con el Agente de red

  Si habilita esta opción, los paquetes de instalación se transferirán a los dispositivos cliente a través del Agente de red instalado en esos dispositivos.

  Si no habilita esta opción, los paquetes de instalación se distribuirán utilizando las herramientas provistas por el sistema operativo de los dispositivos cliente.

  Recomendamos habilitar esta opción si la tarea está asignada a dispositivos que tienen instalado el Agente de red.

  Esta opción está habilitada de manera predeterminada.

  Con los recursos del sistema operativo a través de los puntos de distribución

  Si se selecciona la casilla, los paquetes de instalación se distribuirán a los dispositivos cliente mediante los mecanismos del sistema operativo a través de un punto de distribución. Puede seleccionar esta opción si existe al menos un punto de distribución en la red.

  Si habilitó la opción **Con el Agente de red**, las herramientas del sistema operativo se utilizarán para transferir los archivos solo si las herramientas del Agente de red no están disponibles.

  Está opción se habilita de manera predeterminada para las tareas de instalación remota creadas en servidores de administración virtuales.

  La única forma de instalar una aplicación para Windows (incluido el Agente de red para Windows) en un dispositivo que no tiene instalado el Agente de red es a través de un punto de distribución basado en Windows. Por lo tanto, cuando instale una aplicación para Windows, haga lo siguiente:

  - Seleccione esta opción.
  - Asegúrese de que los dispositivos cliente de destino tengan asignado un punto de distribución.
  - Asegúrese de que el punto de distribución utilice Windows.

  Con los recursos del sistema operativo a través del Servidor de administración

  Si se habilita esta opción, los archivos se transmitirán a los dispositivos cliente a través del Servidor de administración utilizando las herramientas provistas por el sistema operativo de los dispositivos cliente. Puede habilitar esta opción si no hay ningún Agente de red instalado en el dispositivo cliente, pero el dispositivo cliente está en la misma red que el Servidor de administración.

  Esta opción está activada de forma predeterminada.

- En el campo **Número máximo de descargas simultáneas**, ingrese el número máximo permitido de dispositivos cliente a los que el Servidor de administración podrá transmitir simultáneamente los archivos.

- En el campo **Número máximo de intentos de instalación**, ingrese el límite de veces que se podrá ejecutar el instalador.

  Si se supera la cantidad de intentos indicados con este parámetro, Kaspersky Security Center Linux dejará de iniciar el instalador en el dispositivo. Para reiniciar la tarea *Instalar aplicación de forma remota*, aumente el valor del parámetro **Número máximo de intentos de instalación** e inicie la tarea. Como alternativa, cree una nueva tarea *Instalar aplicación de forma remota*.

- Si migra de una aplicación de Kaspersky a otra y su aplicación actual está protegida con contraseña, ingrese la contraseña en el campo **Contraseña para desinstalar la aplicación de Kaspersky actual**. Tenga en cuenta que, durante la migración, se desinstalará su aplicación de Kaspersky actual.

  El campo **Contraseña para desinstalar la aplicación de Kaspersky actual** solo está disponible si seleccionó la opción **Con el Agente de red** en el grupo de configuración **Forzar la descarga del paquete de instalación**.

  Puede usar la contraseña de desinstalación solo para la migración de Kaspersky Security for Windows Server a Kaspersky Endpoint Security para Windows cuando se instala Kaspersky Endpoint Security para Windows mediante la tarea Instalar aplicación de forma remota. El uso de la contraseña de desinstalación al instalar otros componentes puede causar errores de instalación.

  Para completar el escenario de migración correctamente, asegúrese de que se cumplan los siguientes requisitos previos:

  - Está utilizando el Agente de red de Kaspersky Security Center 14.2 para Windows o una versión posterior.
  - Está instalando la aplicación en dispositivos con Windows.

- Defina la configuración adicional:

  No reinstalar la aplicación si ya está instalada

  Si habilita esta opción y se detecta que la aplicación ya está instalada en el dispositivo cliente, no se la reinstalará.

  Si no habilita esta opción, la aplicación se instalará en todos los casos.

  Esta opción está activada de forma predeterminada.

  Verificar el tipo de sistema operativo antes de la descarga

  Antes de transmitir los archivos a los dispositivos cliente, Kaspersky Security Center Linux verificará si los ajustes de la utilidad de desinstalación son adecuados para el sistema operativo del dispositivo cliente. Si no lo son, Kaspersky Security Center Linux no transmitirá los archivos y no tratará de instalar la aplicación. A modo de ejemplo, si necesita instalar una aplicación en los dispositivos de un grupo de administración que contenga dispositivos con sistemas operativos diferentes, puede asignar la tarea de instalación al grupo de administración y habilitar esta opción para que la tarea no afecte a aquellos dispositivos que no tengan el sistema operativo pertinente.

  Cuando instala el Agente de red de forma remota en dispositivos no asignados, Kaspersky Security Center Linux o un punto de distribución determina automáticamente el tipo de sistema operativo del dispositivo, independientemente de la configuración **Verificar el tipo de sistema operativo antes de la descarga**.

  Asignar la instalación del paquete en las directivas de grupo de Active Directory

  Si se habilita esta opción, se instala un paquete de instalación mediante las directivas de grupo de Active Directory.

  Esta opción se encuentra disponible si se selecciona el paquete de instalación del Agente de red.

  Esta opción está deshabilitada de forma predeterminada.

  Solicitar a los usuarios que cierren las aplicaciones en ejecución

  Las aplicaciones abiertas en el dispositivo cliente podrían impedir que se lo reinicie. Si el usuario está editando un documento en un procesador de textos, por ejemplo, y no ha guardado el archivo, el procesador de textos no permitirá que el dispositivo se reinicie.

Si habilita esta opción, las aplicaciones que se estén ejecutando en un dispositivo bloqueado se cerrarán por la fuerza y, tras ello, el dispositivo se reiniciará. Los usuarios podrían perder los cambios que no hayan guardado.

Si no habilita esta opción, los dispositivos bloqueados no se reiniciarán. El estado de la tarea en tales dispositivos indicará que hay un reinicio pendiente. Los usuarios tendrán que cerrar manualmente todas las aplicaciones abiertas para luego reiniciar sus dispositivos.

Esta opción está deshabilitada de forma predeterminada.

- Seleccione los dispositivos en los que desee instalar la aplicación:

  Instalar en todos los dispositivos

  La aplicación se instalará incluso en dispositivos administrados por otros Servidores de administración.

  Esta opción está seleccionada de manera predeterminada. Si solo tiene un Servidor de administración en la red, no es necesario que cambie esta opción.

  Instalar solo en dispositivos administrados a través de este Servidor de administración

  La aplicación se instalará solo en los dispositivos administrados por este Servidor de administración. Seleccione esta opción si tiene más de un Servidor de administración en su red y desea evitar conflictos entre ellos.

- Indique si los dispositivos deberán moverse a un grupo de administración después de la instalación:

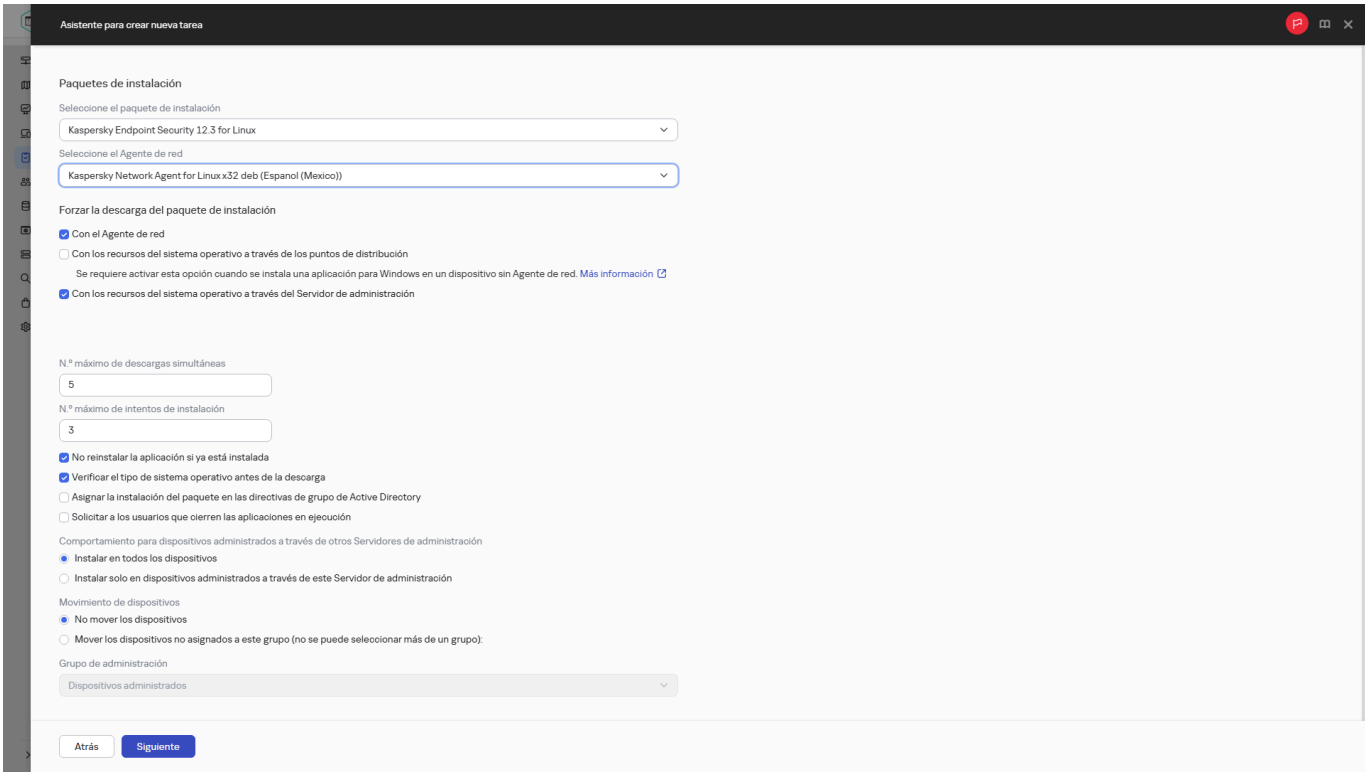
  No mover los dispositivos

  Los dispositivos se mantendrán en los grupos en los que se encuentren. Los dispositivos que no pertenezcan a ningún grupo quedarán sin asignar.

  Mover los dispositivos no asignados a este grupo (no se puede seleccionar más de un grupo)

  Los dispositivos se moverán al grupo de administración que seleccione.

  Tenga presente que la opción **No mover los dispositivos** está seleccionada de manera predeterminada. Es posible que quiera mover los dispositivos manualmente por seguridad.



Especificar la configuración de la tarea

7. En este paso del asistente, indique si los dispositivos deberán reiniciarse durante la instalación de las aplicaciones:

   No reiniciar el dispositivo

   Si se selecciona esta opción, el dispositivo no se reiniciará después de instalar la aplicación de seguridad.

   Reiniciar el dispositivo

   Si se selecciona esta opción, el dispositivo se reiniciará después de instalar la aplicación de seguridad.

8. De ser necesario, en el paso **Seleccione las cuentas con las que se accederá a los dispositivos**, agregue las cuentas que se utilizarán para iniciar la tarea *Instalar aplicación de forma remota*:

   No se necesita una cuenta (el Agente de red está instalado)

   Si selecciona esta opción, no necesitará especificar la cuenta con la que se ejecutará el instalador de la aplicación. Para ejecutar la tarea, se usará la cuenta con la que se haya iniciado el servicio del Servidor de administración.

   Esta opción no está disponible si el Agente de red no se ha instalado en los dispositivos cliente.

   Se necesita una cuenta (no se utiliza el Agente de red)

   Seleccione esta opción si el Agente de red no está instalado en los dispositivos a los que asigna la tarea de instalación remota. En este caso, puede especificar una cuenta de usuario o un certificado SSH para instalar la aplicación.

   - **Cuenta local o de dominio**. Si se selecciona esta opción, especifique la cuenta bajo la que se ejecutará el instalador de aplicación. Haga clic en el botón **Agregar**, seleccione **Cuenta local o de dominio** y, a continuación, especifique las credenciales de la cuenta de usuario.

     Puede especificar varias cuentas de usuario si, por ejemplo, ninguna de ellas tiene todos los derechos requeridos en todos los dispositivos a los que asigne esta tarea. En este caso, todas las cuentas añadidas se utilizan para ejecutar la tarea, en orden consecutivo de arriba abajo.

   - **Certificado de SSH**. Si desea instalar una aplicación en un dispositivo cliente basado en Linux, puede especificar un certificado SSH en lugar de una cuenta de usuario. Haga clic en el botón **Agregar**, seleccione **Certificado de SSH** y, a continuación, especifique las claves pública y privada del certificado.

     Para generar una clave privada, puede utilizar la utilidad ssh-keygen. Tenga en cuenta que Kaspersky Security Center Linux espera que la clave privada esté en formato PEM, pero, de manera predeterminada, la utilidad ssh-keygen genera claves SSH en formato OPENSSH. Kaspersky Security Center Linux no admite el formato OPENSSH. Para crear una clave privada en el formato PEM admitido, agregue la opción -m PEM en el comando ssh-keygen. Por ejemplo:

     ```
     ssh-keygen -m PEM -t rsa -b 4096 -C "<correo electrónico del usuario>"
     ```

9. En el paso **Finalizar la creación de la tarea**, haga clic en el botón **Finalizar** para crear la tarea y cerrar el asistente.

   Si habilitó la opción **Abrir los detalles de la tarea cuando se complete la creación**, se abrirá la ventana de configuración de la tarea. Utilice esta ventana para, de ser necesario, revisar y modificar los ajustes de la tarea o programar su ejecución.

10. En la lista de tareas, seleccione la tarea creada y haga clic en **Iniciar**.

    Como alternativa, puede esperar a que ocurra el inicio programado definido en los ajustes de la tarea.

Cuando se completa la tarea de instalación remota, la aplicación seleccionada se instala en los dispositivos especificados.

Instalación remota de aplicaciones en dispositivos macOS

Para instalar aplicaciones en dispositivos que ejecutan macOS mediante una tarea de instalación remota, siga estos pasos:

1. Cree un archivo que conste de un paquete de instalación y un script de instalación .sh.

2. Deshabilite la opción **Verificar el tipo de sistema operativo antes de la descarga** en el Asistente para crear nueva tarea.

Como alternativa, puede utilizar la tarea **Ejecutar scripts de forma remota**. El siguiente artículo describe cómo configurar archivos para esta tarea: Instalar de forma remota aplicaciones en dispositivos con la tarea Ejecución remota de scripts.

Instalar aplicaciones en los Servidores de administración secundarios

Si la versión de su Servidor de administración es 15.4 o una versión posterior, puede instalar aplicaciones en un Servidor de administración secundario solo si su versión es 15.4 o una versión posterior.

Para instalar una aplicación en Servidores de administración secundarios:

1. Establezca conexión con el Servidor de administración que controla los servidores de administración secundarios pertinentes.

2. Asegúrese de que el paquete de instalación que corresponde a la aplicación que se está instalando esté disponible en cada uno de los Servidores de administración secundarios seleccionados. Si no puede encontrar el paquete de instalación en ninguno de los servidores secundarios, distribúyalo. Para este propósito, cree una tarea con el tipo de tarea **Distribuir paquete de instalación**.

3. Crear una tarea para la instalación de una aplicación remota en Servidores de administración secundarios. Seleccione el tipo de actividad de **Instalar aplicación en el Servidor de administración secundario de forma remota**.

   El Asistente para crear nueva tarea creará la tarea para instalar de manera remota, en servidores de administración secundarios específicos, la aplicación seleccionada en el asistente.

4. Ejecute la tarea manualmente o espere a que se inicie según la programación configurada para la tarea.

Cuando se completa la tarea de instalación remota, la aplicación seleccionada se instala en los Servidores de administración secundarios.

Instalación remota de aplicaciones en dispositivos en los que se encuentra instalado el Agente de red

Si un Agente de red operable conectado al Servidor de administración principal (o a alguno de sus Servidores secundarios) está conectado en un dispositivo, puede actualizar el Agente de red en este dispositivo, así como instalar, actualizar o eliminar cualquier aplicación admitida a través del Agente de red.

Puede habilitar esta opción al seleccionar la opción **Con el Agente de red** en las propiedades de la tarea de instalación remota.

Si esta opción se selecciona, los paquetes de instalación con la configuración de instalación definida por el administrador se transferirán a los dispositivos de destino a través de canales de comunicación entre l Agente de red y el Servidor de administración.

Para optimizar la carga del Servidor de administración y minimizar el tráfico entre el Servidor de administración y los dispositivos, es útil asignar puntos de distribución en cada red remota o en cada dominio de transmisión (consulte las secciones "Acerca de los puntos de distribución" y "Creación de una estructura de grupos de administración y asignación de puntos de distribución"). En este caso, los paquetes de instalación y la configuración del instalador se distribuyen desde el Servidor de administración hacia los dispositivos de destino a través de puntos de distribución.

Además, puede usar puntos de distribución para la transmisión (multidifusión) y la distribución de paquetes de instalación, lo que permite reducir el tráfico de red considerablemente a la hora de instalar aplicaciones en forma remota.

Al transferir paquetes de instalación a los dispositivos de destino a través de canales de comunicación entre los Agentes de red y el Servidor de administración, todos los paquetes de instalación que se prepararon para la transferencia también se almacenarán en caché en la carpeta /var/opt/kaspersky/klnagent_srv/1093/.working/. Al usar múltiples paquetes de instalación de gran tamaño y de diversos tipos e involucrar a un gran número de puntos de distribución, el tamaño de esta carpeta puede aumentar significativamente.

Los archivos no se pueden eliminar desde la carpeta FTServer manualmente. Cuando los paquetes de instalación originales se eliminen, los datos correspondientes automáticamente se eliminarán de la carpeta FTServer.

Los datos recibidos en los puntos de distribución se guardan en la carpeta /var/opt/kaspersky/klnagent_srv/1103/.

Los archivos no se pueden eliminar de la carpeta $FTClTmp manualmente. Como las tareas usan los datos de esta carpeta completa, los contenidos de esta carpeta se eliminarán automáticamente.

Como los paquetes de instalación se distribuyen por canales de comunicación entre el Servidor de administración y los Agentes de red desde un repositorio intermedio en un formato optimizado para transferencias de red, ningún cambio se permite en paquetes de instalación almacenados en la carpeta original de cada paquete de instalación. Esos cambios no serán automáticamente registrados por el Servidor de administración. Si tiene que modificar los archivos de los paquetes de instalación manualmente (aunque se recomienda evitar esta situación), debe modificar cualquiera de los ajustes de un paquete de instalación en Kaspersky Security Center Web Console. La modificación de la configuración de un paquete de instalación en Kaspersky Security Center Web Console hace que el Servidor de administración actualice la imagen del paquete en la caché que se preparó para la transferencia hacia los dispositivos de destino.

El servidor envía solicitudes de eco ICMP (el mismo tipo de solicitud que se usa en el comando ping) al dispositivo de destino durante la instalación remota.

Opciones para controlar el reinicio de los dispositivos en la tarea de instalación remota

Los dispositivos a menudo necesitan un reinicio para completar la instalación remota de aplicaciones (en particular en Windows).

Si usa la tarea de instalación remota de Kaspersky Security Center Linux, en el Asistente para crear nueva tarea o en la ventana de propiedades de la tarea que se ha creado (**sección Reinicio** del sistema operativo), puede seleccionar la acción para realizar cuando el dispositivo de Windows requiera un reinicio:

- **No reiniciar el dispositivo**. En este caso, ningún reinicio automático se realizará. Para completar la instalación, debe reiniciar el dispositivo (por ejemplo, manualmente o a través de la tarea de administración del dispositivo). La información sobre el reinicio requerido se guardará en los resultados de la tarea y en el estado del dispositivo. Esta opción es conveniente para tareas de instalación en servidores y otros dispositivos donde la operación continua sea crítica.

- **Reiniciar el dispositivo**. En este caso, el dispositivo siempre se reinicia automáticamente si se requiere un reinicio para la finalización de la instalación. Esta opción es útil para tareas de instalación en dispositivos que proporcionan pausas habituales en su operación (cierre o reinicio).

- **Solicitar al usuario una acción**. A través de un recordatorio en pantalla, se le pedirá a cada usuario que reinicie su dispositivo manualmente. Puede configurar algunos ajustes avanzados para esta opción: el texto del mensaje que se le muestra al usuario, la frecuencia con la que se muestra este mensaje y el tiempo que se espera antes de reiniciar el dispositivo por la fuerza (sin que el usuario confirme el reinicio). La opción **Solicitar al usuario una acción** es la más conveniente para las estaciones de trabajo donde los usuarios necesitan la posibilidad de seleccionar el horario más cómodo para un reinicio.

Despliegue forzado con la tarea de instalación remota de Kaspersky Security Center Linux

Para desplegar por primera vez el Agente de red u otras aplicaciones, puede forzar la instalación de los paquetes de instalación seleccionados con la tarea de instalación remota de Kaspersky Security Center Linux, siempre que cada dispositivo tenga una cuenta de usuario con derechos de administrador local.

La instalación forzada también se puede usar si no se puede acceder directamente a los dispositivos mediante el Servidor de administración: por ejemplo, los dispositivos están en redes aisladas o están en una red local mientras que el elemento del Servidor de administración está en la DMZ.

En el primer despliegue, el Agente de red no está instalado. Por lo tanto, en la configuración de la tarea de instalación remota, no se puede seleccionar la distribución de los archivos necesarios para la instalación de la aplicación mediante el Agente de red. Solo puede optar por distribuir archivos con recursos del sistema operativo a través del Servidor de administración o puntos de distribución.

El servicio del Servidor de administración debe ejecutarse bajo una cuenta que tenga privilegios administrativos en los dispositivos de destino. También puede especificar una cuenta que tenga acceso al recurso compartido admin$ en la configuración de la tarea de instalación remota.

De manera predeterminada, la tarea de instalación remota se aplica a los dispositivos con las credenciales de la cuenta que se usa para ejecutar el Servidor de administración. Es importante aclarar que se trata de la cuenta utilizada para acceder al recurso compartido admin$, en lugar de la cuenta que se usa para ejecutar la tarea de instalación remota. La instalación se realiza con la Cuenta LocalSystem.

Puede especificar dispositivos de destino explícitamente (con una lista), mediante la selección del grupo de administración de Kaspersky Security Center Linux al cual pertenecen o tras crear una selección de dispositivos en función de un criterio específico. La hora de inicio de instalación es definida por la programación de la tarea. Si la configuración **Ejecutar tareas no realizadas** se habilita en las propiedades de la tarea, la tarea se puede ejecutar inmediatamente después de que los dispositivos de destino se activen, o cuando se muevan al grupo de administración de destino.

La instalación forzada consiste en el envío de paquetes de instalación a dispositivos de destino, la copia subsecuente de archivos al recurso admin$ en cada uno de los dispositivos de destino y el registro remoto de los servicios de compatibilidad en esos dispositivos. La entrega de paquetes de instalación a dispositivos de destino se realiza mediante una función de Kaspersky Security Center Linux que garantiza la interacción de la red. Las condiciones siguientes se deben cumplir en este caso:

- Se puede acceder a los dispositivos de destino desde el Servidor de administración o desde el punto de distribución.
- La resolución del nombre para los dispositivos de destino funciona correctamente en la red.
- Los usos compartidos administrativos (admin$) permanecen activados en los dispositivos de destino.
- Los siguientes servicios del sistema están en ejecución en los dispositivos de destino:
  - Servidor (LanmanServer)

    De manera predeterminada, este servicio está en ejecución.
  - Iniciador de procesos de servidor DCOM (DcomLaunch)
  - Asignador de endpoints RPC (RpcEptMapper)
  - Llamada a procedimiento remoto (RpcSs)
- El puerto TCP 445 está abierto en los dispositivos de destino para permitir el acceso remoto a través del Instrumental de administración de Windows.

  TCP 139, UDP 137 y UDP 138 se usan en protocolos más antiguos y ya no son necesarios para las aplicaciones actuales.

  En el firewall, se deben permitir puertos de acceso saliente dinámicos para las conexiones desde el Servidor de administración y los puntos de distribución a los dispositivos de destino.
- Se permiten configuraciones de seguridad de la política de dominio de Active Directory para el funcionamiento del protocolo NTLM durante el despliegue del Agente de red.

- En los dispositivos de destino que ejecutan Microsoft Windows XP, el modo de uso compartido simple de archivos está deshabilitado.
- En los dispositivos de destino, el modelo de seguridad y uso compartido de acceso se configura como *Clásico: los usuarios locales se autentican como ellos mismos*. De ninguna manera puede ser *Invitado únicamente: los usuarios locales se autentican como invitados*.
- Los dispositivos de destino son miembros del dominio, o bien se crean cuentas uniformes con derechos de administrador en los dispositivos de destino de antemano.

Para desplegar correctamente el Agente de red u otras aplicaciones en un dispositivo que no está unido a un dominio de Active Directory de Windows Server 2003 o posterior, debe deshabilitar el Control de cuentas de usuario (UAC) remoto en el dispositivo. UAC remoto es una de las razones que impide que las cuentas de administradores locales accedan a admin$, lo que es necesario para el despliegue forzado del Agente de red u otras aplicaciones. Si deshabilita UAC remoto, no interfiere con UAC local.

Durante la instalación en dispositivos nuevos que todavía no se han asignado a ninguno de los grupos de administración de Kaspersky Security Center Linux, puede abrir las propiedades de la tarea de instalación remota y especificar el grupo de administración al cual los dispositivos se moverán después de la instalación del Agente de red.

Al crear una tarea de grupo, tenga en cuenta que cada tarea de grupo afecta a todos los dispositivos en todos los grupos anidados dentro de un grupo seleccionado. Por lo tanto, debe evitar duplicar las tareas de instalación en los subgrupos.

Una forma simplificada de crear tareas para la instalación forzada de aplicaciones es la instalación automática. Para hacerlo, abra las propiedades del grupo de administración, abra la lista de paquetes de instalación y seleccione los que se deben instalar en dispositivos de este grupo. Como resultado, los paquetes de instalación seleccionados se instalarán automáticamente en todos los dispositivos de este grupo y todos sus subgrupos. El intervalo de tiempo durante el cual los paquetes se instalarán depende del rendimiento de la red y el número total de dispositivos conectados a una red.

Para reducir la carga en el Servidor de administración durante la entrega de paquetes de instalación a dispositivos de destino, puede seleccionar la instalación a través de puntos de distribución en la tarea de instalación. Tenga en cuenta que este método de instalación aplica una carga significativa a dispositivos que actúan como puntos de distribución. Por lo tanto, se recomienda seleccionar dispositivos que cumplan con los requisitos de los puntos de distribución. Si usa puntos de distribución, debe asegurarse de que estén presentes en cada una de las subredes aisladas que alojan los dispositivos de destino.

El uso de puntos de distribución como centros de instalación locales también puede ser útil al realizar la instalación en dispositivos en subredes comunicadas con el Servidor de administración mediante un canal de capacidad reducida, mientras que un canal más amplio está disponible entre dispositivos en la misma subred.

El espacio libre del disco en la partición con la carpeta /var/opt/kaspersky/KSC_Backups* debe superar, en gran cantidad, el tamaño total de los paquetes de distribución de aplicaciones instaladas.

Instalación de aplicaciones en modo no interactivo

Para instalar una aplicación en modo no interactivo:

1. En el menú principal, vaya a **Administración de software → Paquetes de instalación**.
2. Seleccione la casilla junto al paquete de instalación de la aplicación requerida o cree uno nuevo para esa aplicación.

   Los paquetes de instalación se almacenan en el Servidor de administración en la carpeta de servicios de paquetes dentro de la carpeta compartida. A cada paquete de instalación le corresponde una subcarpeta separada.

3. Abra la carpeta que almacena el paquete de instalación requerido de una de las siguientes maneras:

   - Copie en el dispositivo cliente la carpeta que corresponda al paquete de instalación relevante del Servidor de administración. A continuación, abra la carpeta copiada en el dispositivo cliente.
   - Abra desde el dispositivo cliente la carpeta compartida que equivale al paquete de instalación necesario en el Servidor de administración.

   Si la carpeta compartida está ubicada en un dispositivo con Microsoft Windows Vista instalado, seleccione el valor **Deshabilitado** para la configuración **Control de cuenta de usuario: ejecutar todos los administradores en el Modo de aprobación de administrador** (**Iniciar → Panel de control → Administración → Directiva de seguridad local → Configuración de seguridad**).

4. Según la aplicación seleccionada, realice lo siguiente:

   - Para Kaspersky Anti-Virus for Windows Workstations, Kaspersky Anti-Virus for Windows Servers y Kaspersky Security Center, diríjase a la subcarpeta exec y ejecute el archivo ejecutable (el archivo con la extensión .exe) con la tecla /s.
   - Para otras aplicaciones Kaspersky, ejecute el archivo ejecutable (un archivo con la extensión .exe) con la tecla /s desde la carpeta abierta.

   La ejecución del archivo ejecutable con las claves `EULA=1` y `PRIVACYPOLICY=1` significa que usted leyó, comprende y acepta los términos del Contrato de licencia de usuario final y la Política de privacidad, respectivamente. También está al corriente de que sus datos serán manejados y transmitidos (incluso a otros países) como se describe en la Política de privacidad. El texto del Contrato de licencia y la Política de privacidad se incluye en el kit de distribución de Kaspersky Security Center Linux. Aceptar las condiciones del Contrato de licencia y de la Política de privacidad es necesario para instalar la aplicación o actualizar una versión previa de la aplicación.

Preparación de un dispositivo de macOS para instalación remota de Agente de red

Existen los siguientes métodos para instalar inicialmente el Agente de red en el dispositivo administrado con macOS:

- Ejecutar la tarea de instalación remota en el punto de distribución de macOS.
- Enviar vínculos de usuarios del dispositivo a paquetes independientes generados por Kaspersky Security Center Linux. Los paquetes independientes son módulos ejecutables que contienen los paquetes de distribución de aplicaciones seleccionadas con su configuración definida.

Para preparar un dispositivo que ejecute macOS para la instalación remota del Agente de red:

1. Asegúrese de que sudo esté instalado en el dispositivo macOS de destino.
2. Pruebe la configuración del dispositivo:
   a. Asegúrese de que el puerto 22 esté abierto en el dispositivo cliente. Para ello, en las **Preferencias del sistema**, abra el panel **Uso compartido** y asegúrese de que la casilla **Inicio de sesión remoto** esté seleccionada.

      Puede conectarse al dispositivo cliente mediante Secure Shell (SSH) solo a través del puerto 22. No puede cambiar el número de puerto.

      Puede utilizar el comando `ssh <nombre_del_dispositivo>` para iniciar sesión en el dispositivo macOS de forma remota. Para definir quiénes podrán acceder al dispositivo macOS, utilice la opción **Permitir acceso a** del panel **Compartir**.

   b. Deshabilite la contraseña de sudo para la cuenta de usuario con la cual se conectará el dispositivo.

      Utilice el comando `sudo visudo` en la Terminal para abrir el archivo de configuración de sudoers. En el archivo que abrió, en la entrada `Especificación de privilegios de usuario`, especifique lo siguiente: `username ALL = (ALL) NOPASSWD: ALL`. En este caso, `username` representa la cuenta de usuario que se utilizará para la conexión del dispositivo mediante SSH.

   c. Guarde el archivo sudoers y, luego, ciérrelo.

   d. Conéctese nuevamente al dispositivo a través de SSH y asegúrese de que el servicio Sudo no le solicite que ingrese una contraseña; puede hacerlo usando el comando `sudo whoami`.
3. Descargue y cree un paquete de instalación:
   a. Use uno de estos métodos para obtener el paquete de instalación del Agente de red:
      - Con la interfaz de la aplicación.
      - Descargue la versión relevante del Agente de red del sitio web de Soporte técnico, https://support.kaspersky.com/mx/.
      - Solicite el paquete de instalación a nuestros especialistas del servicio de soporte técnico.

b. Para crear un paquete de instalación remota, use los archivos siguientes:

- klnagent.kud
- install.sh
- klnagentmac.dmg

4. Cree una tarea de instalación remota con la configuración siguiente:

- En la página **Configuración** del Asistente para crear nueva tarea, seleccione la casilla **Con los recursos del sistema operativo a través del Servidor de administración**. Quite la selección a todo.
- En la página **Seleccione una cuenta con la que ejecutar la tarea**, para ejecutar la tarea, especifique la configuración de la cuenta de usuario que se utiliza para conectar el dispositivo mediante SSH.

El dispositivo cliente está listo para la instalación remota del Agente de red a través de la tarea correspondiente que ha creado.

Infraestructura virtual

Kaspersky Security Center Linux admite el uso de máquinas virtuales. Puede instalar el Agente de red y una aplicación de seguridad en cada máquina virtual; también puede proteger todas las máquinas virtuales a nivel hipervisor. En el primer caso, las máquinas pueden protegerse con cualquier aplicación de seguridad estándar o con Kaspersky Security for Virtualization Light Agent. En el segundo caso, puede usar Kaspersky Security for Virtualization Agentless.

Kaspersky Security Center Linux está preparado para operar con máquinas virtuales que puedan revertir su estado a un punto anterior.

Sugerencias sobre la reducción de la carga en máquinas virtuales

Al instalar el Agente de red en una máquina virtual, le aconsejan que considere la deshabilitación de algunas funciones de Kaspersky Security Center Linux que parecen ser de poco uso para máquinas virtuales.

Al instalar el Agente de red en una máquina virtual o en una plantilla querida para la generación de máquinas virtuales, recomendamos realizar las siguientes acciones:

- Si está ejecutando una instalación remota, en la ventana de propiedades del paquete de instalación del Agente de red, en la sección **Avanzado**, seleccione la opción **Optimizar la configuración para VDI**.
- Si está ejecutando una instalación interactiva a través de un Asistente, en la ventana Asistente, seleccione la opción **Optimizar la configuración del Agente de red para la infraestructura virtual**.

Seleccionar esas opciones cambia la configuración del Agente de red de modo que las funciones siguientes permanezcan desactivadas de forma predeterminada (antes de aplicar una directiva):

- Recopilación de información acerca del software instalado
- Recopilación de información acerca del hardware

- Recopilación de información acerca de las vulnerabilidades detectadas
- Recopilación de información acerca de las actualizaciones necesarias

Por lo general, esas funciones no son necesarias en máquinas virtuales porque usan el software uniforme y el hardware virtual.

La deshabilitación de las funciones es irreversible. Si alguna de las funciones desactivadas se requiere, la puede habilitar a través de la directiva del Agente de red, o a través de la configuración local del Agente de red. La configuración local del Agente de red está disponible a través del menú contextual del dispositivo relevante en Kaspersky Security Center Web Console.

Compatibilidad con máquinas virtuales dinámicas

Kaspersky Security Center Linux es compatible con las máquinas virtuales dinámicas. Si existe una infraestructura virtual en la red de la organización, las máquinas virtuales dinámicas (temporales) se pueden utilizar en ciertos casos. Las máquinas virtuales dinámicas se crean con nombres únicos según una plantilla que preparada por el administrador. El usuario trabaja en la máquina virtual un tiempo, luego, después de apagarse, esta máquina virtual se eliminará de la infraestructura virtual. Si se ha desplegado Kaspersky Security Center Linux en la red de la organización, se agregará una máquina virtual con el Agente de red instalado a la base de datos del Servidor de administración. Después de que desactive una máquina virtual, la entrada correspondiente también se debe eliminar de la base de datos de Servidor de administración.

Para hacer funcional la función de eliminación automática de entradas en máquinas virtuales, al instalar un Agente de red en una plantilla para máquinas virtuales dinámicas, seleccione la opción **Habilitar modo dinámico para VDI**:

- Para la instalación remota: En la ventana de propiedades del paquete de instalación del Agente de red (Sección **Avanzado**)
- Para la instalación interactiva: en el Asistente de instalación del Agente de red

> Evite seleccionar la opción **Habilitar modo dinámico para VDI** al instalar el Agente de red en dispositivos físicos.

Si desea que los eventos de las máquinas virtuales dinámicas se almacenen en el Servidor de administración durante un tiempo después de eliminar esas máquinas virtuales, en la ventana de propiedades del Servidor de administración, en la sección **Repositorio de eventos**, marque la opción **Almacenar los eventos de los dispositivos eliminados** y especifique el plazo de almacenamiento máximo para los eventos (en días).

> No recomendamos habilitar el cifrado de unidades en máquinas virtuales dinámicas.

Soporte de copia de máquinas virtuales

Copiar una máquina virtual que tiene el Agente de red instalado y crear una máquina virtual a partir de una plantilla que tiene el Agente de red instalado son procedimientos idénticos al de capturar y copiar una imagen de disco duro como método para desplegar el Agente de red. Por ello, en general, si copia una máquina virtual, deberá realizar las mismas acciones que si hubiera copiado una imagen de disco para desplegar el Agente de red.

Sin embargo, los dos casos que se describen a continuación muestran el Agente de red que detecta la copia automáticamente. Debido a los motivos indicados anteriormente, no tiene que realizar las operaciones sofisticadas descritas en la sección "Despliegue con una imagen de disco duro capturada de un dispositivo":

- La opción **Habilitar modo dinámico para VDI** se seleccionó cuando el Agente de red se instaló: después de cada reinicio del sistema operativo, esta máquina virtual se reconocerá como un dispositivo nuevo, sin tener en cuenta si se ha copiado.
- Uno de los siguientes hipervisores está en uso: VMware™, HyperV® o Xen®: Agente de red detecta la copia de la máquina virtual mediante los id. modificados del hardware virtual.

El análisis de cambios en el hardware virtual no es absolutamente fiable. Antes de aplicar este método extensamente, lo debe probar en un pequeño grupo de máquinas virtuales para la versión del hipervisor actualmente usado en su organización.

Definir ajustes para instalaciones remotas en dispositivos Unix

Si va a utilizar una tarea de instalación remota para instalar una aplicación en un dispositivo Unix, puede definir ajustes específicos para Unix en la configuración de esa tarea. Una vez que cree la tarea, encontrará esos ajustes en las propiedades de la misma.

Para definir ajustes específicos para Unix en una tarea de instalación remota:

1. En el menú principal, vaya a **Tareas**.
2. Haga clic en el nombre de la tarea de instalación remota que contendrá los ajustes específicos para Unix.

   Se abrirá la ventana de propiedades de la tarea.
3. Vaya a **Configuración de la aplicación** → **Ajustes específicos de Unix**.
4. Configure los siguientes ajustes:

   Definir una contraseña para la cuenta root (solo para despliegues a través de SSH)

   Si el comando `sudo` no se puede utilizar en el dispositivo de destino sin especificar la contraseña, seleccione esta opción y luego especifique la contraseña para la cuenta root. Kaspersky Security Center Linux transmitirá la contraseña de forma cifrada al dispositivo de destino, la descifrará y, finalmente, la utilizará para iniciar el procedimiento de instalación en nombre de la cuenta root.

   Kaspersky Security Center Linux no usará la cuenta ni la contraseña especificada para crear una conexión SSH.

   Especificar la ruta a una carpeta temporal con permisos de ejecución en el dispositivo de destino (solo para despliegues a través de SSH)

Si el directorio /tmp del dispositivo de destino no tiene permiso de ejecución, seleccione esta opción y, a continuación, especifique la ruta a un directorio que sí tenga permiso de ejecución. Kaspersky Security Center Linux utiliza el directorio especificado como directorio temporal para el acceso a través de SSH. La aplicación pondrá el paquete de instalación en este directorio e iniciará el procedimiento de instalación.

5. Haga clic en el botón **Guardar**.

Se guardan los ajustes especificados en la tarea.

Supervisión del despliegue

Para supervisar la implementación de Kaspersky Security Center Linux y asegurarse de que una aplicación de seguridad y un Agente de red estén instalados en los dispositivos administrados, use la función de monitoreo e informes:

- Utilice el widget de despliegue del panel para supervisar el despliegue en tiempo real.
- Utilice informes para obtener información detallada.

Iniciar y detener aplicaciones de Kaspersky

Puede usar la tarea *Iniciar o detener aplicación* para iniciar y detener aplicaciones de Kaspersky en los dispositivos administrados.

Para crear la tarea Iniciar o detener aplicación:

1. En el menú principal, vaya a **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.
3. En la lista desplegable **Aplicación**, seleccione la aplicación para la que desea crear la tarea.

   Las aplicaciones de Kaspersky aparecen en la lista si ya ha agregado complementos web de administración para ellas.
4. En la lista **Tipo de tarea**, seleccione la tarea **Activación de la aplicación**.
5. En el campo **Nombre de la tarea**, ingrese el nombre de la tarea nueva.

   El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).
6. Seleccione los dispositivos a los que se asignará la tarea.
7. En la ventana **Aplicaciones**, haga lo siguiente:
   - Marque las casillas junto a los nombres de las aplicaciones para las que desee crear la tarea.
   - Seleccione la opción **Iniciar la aplicación** o **Detener la aplicación**.

8. Si desea modificar la configuración predeterminada de la tarea, active la opción **Abrir los detalles de la tarea cuando se complete la creación** en el paso **Finalizar la creación de la tarea**. Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Puede cambiar la configuración por defecto más tarde, en cualquier momento.

9. Haga clic en el botón **Finalizar**.

   Se crea la tarea y se la agrega a la lista de tareas.

10. Haga clic en el nombre de la nueva tarea para abrir la ventana de propiedades de la tarea.

11. En la ventana de propiedades de la tarea, defina los ajustes generales de la tarea que se adapten a sus necesidades y luego guárdelos.

La tarea queda creada y configurada.

Para ejecutar la tarea, selecciónela en la lista de tareas y haga clic en el botón **Iniciar**.

Reemplazo de aplicaciones de seguridad de terceros

Antes de instalar una aplicación de seguridad de Kaspersky a través de Kaspersky Security Center Linux, posiblemente deba eliminar aquellas aplicaciones de terceros que no sean compatibles con esa aplicación. Kaspersky Security Center Linux permite eliminar las aplicaciones de terceros de varias maneras.

Eliminar aplicaciones incompatibles al configurar la instalación remota de una aplicación

Cuando esté configurando la instalación remota de una aplicación de seguridad, puede habilitar la opción **Desinstalar aplicaciones incompatibles automáticamente** en el Asistente de despliegue de la protección. Si habilita esta opción, Kaspersky Security Center Linux eliminará las aplicaciones incompatibles antes de instalar la aplicación de seguridad en el dispositivo administrado.

Eliminar aplicaciones incompatibles a través de una tarea dedicada

Para eliminar aplicaciones incompatibles a través de una tarea, use la tarea *Desinstalar aplicación de forma remota*. Esta tarea se debe ejecutar en los dispositivos antes que la tarea para instalar la aplicación de seguridad. Por ejemplo, en la tarea de instalación, puede seleccionar **Al completarse otra tarea** como tipo de programación, en el que la otra tarea es *Desinstalar aplicación de forma remota*.

Este método de desinstalación es útil cuando el instalador de la aplicación de seguridad no puede eliminar correctamente una aplicación incompatible.

Eliminación de aplicaciones o actualizaciones de software de forma remota

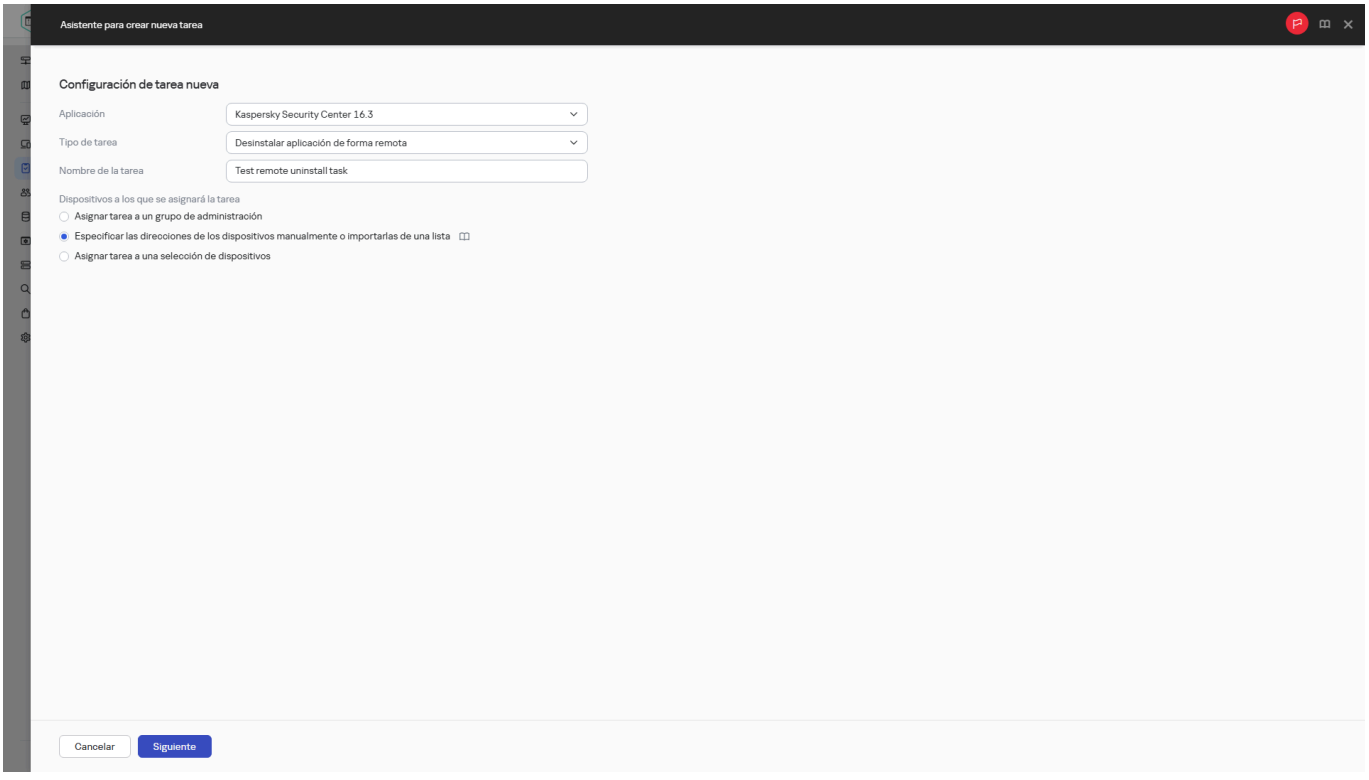
Puede eliminar aplicaciones o actualizaciones de software en dispositivos administrados que ejecutan Linux de forma remota solo mediante el Agente de red.

Para eliminar aplicaciones o actualizaciones de software de forma remota desde dispositivos seleccionados:

1. En el menú principal, vaya a **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.
3. En la lista desplegable **Aplicación**, seleccione Kaspersky Security Center Linux.
4. En la lista **Tipo de tarea**, seleccione el tipo de tarea **Desinstalar aplicación de forma remota**.
5. En el campo **Nombre de la tarea**, ingrese el nombre de la tarea nueva.

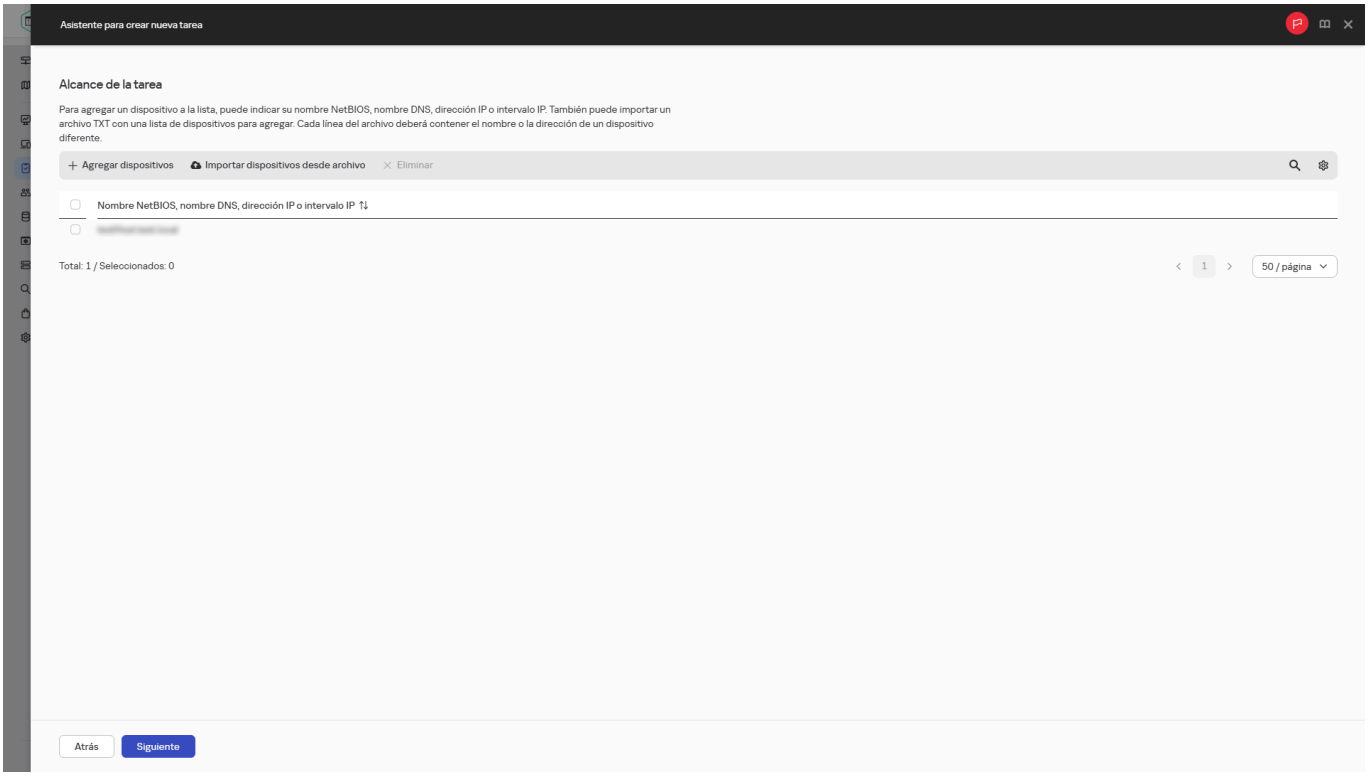
   El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).



Crear la tarea Desinstalar aplicación de forma remota

6. Seleccione los dispositivos a los que se asignará la tarea.

Avance al siguiente paso del asistente.



Especificar el alcance de la tarea

7. Seleccione qué tipo de software desea eliminar y luego seleccione aplicaciones, actualizaciones o parches específicos que desee eliminar:

   Desinstalar la aplicación administrada

   Se muestra una lista de aplicaciones de Kaspersky. Seleccione la aplicación que desee eliminar.

   Desinstalar la aplicación incompatible

   Se muestra una lista de aplicaciones incompatibles con las aplicaciones de seguridad de Kaspersky o con Kaspersky Security Center Linux. marque las casillas ubicadas al lado de las aplicaciones que desea eliminar.

   Desinstalar la aplicación del Registro de aplicaciones

   De forma predeterminada, los Agentes de red envían información al Servidor de administración sobre las aplicaciones instaladas en los dispositivos administrados. La lista de aplicaciones instaladas se almacena en el registro de aplicaciones.

   Para seleccionar una aplicación del registro de aplicaciones:

   a. Haga clic en el campo **Aplicación para desinstalar** y, luego, seleccione la aplicación que desea eliminar.

   Si selecciona Agente de red de Kaspersky Security Center al ejecutar la tarea, el estado *Completada correctamente* indica que se inició el proceso de eliminación. Si se elimina el Agente de red de Kaspersky Security Center, el estado no cambia. Si la tarea falla, el estado cambia a *Error*.

b. Especifique las opciones de desinstalación:

- **Modo de desinstalación**

  Seleccione cómo desea eliminar la aplicación:

  - **Definir el comando de desinstalación automáticamente**

    Si la aplicación tiene un comando de desinstalación definido por el proveedor de la misma, Kaspersky Security Center Linux usará ese comando. Le recomendamos que seleccione esta opción.

  - **Especificar el comando de desinstalación**

    Seleccione esta opción si desea especificar su propio comando para la desinstalación de la aplicación.

    > Le recomendamos que primero intente eliminar la aplicación utilizando la opción **Definir el comando de desinstalación automáticamente**. Si se produce un error durante la desinstalación mediante el comando definido automáticamente, utilice su propio comando.

    Escriba un comando de instalación en el campo y, luego, especifique la siguiente opción:

    Desinstalar con este comando solo si el comando predeterminado no se detectó automáticamente

    Kaspersky Security Center Linux comprueba si la aplicación seleccionada tiene o no un comando de desinstalación definido por su proveedor. Si se encuentra tal comando, Kaspersky Security Center Linux lo usará en lugar del comando especificado en el campo **Comando para desinstalar la aplicación**.

    Le recomendamos que habilite esta opción.

- **Reiniciar luego de que la aplicación se desinstale correctamente**

  Si la aplicación requiere que se reinicie el sistema operativo en el dispositivo administrado después de una desinstalación exitosa, el sistema operativo se reinicia automáticamente.

Desinstalar el parche, la actualización de software o la aplicación de terceros que especifique

Se muestra una lista de actualizaciones, parches y aplicaciones de terceros. Seleccione el elemento que desee eliminar.

La lista que se muestra es una lista general de aplicaciones y actualizaciones, y no corresponde a las aplicaciones y actualizaciones instaladas en los dispositivos administrados. Antes de seleccionar un elemento, le recomendamos que se asegure de que la aplicación o actualización esté instalada en los dispositivos definidos en el alcance de la tarea. Puede ver la lista de dispositivos en los que está instalada la aplicación o actualización, a través de la ventana de propiedades.

Para ver la lista de dispositivos:

a. Haga clic en el nombre de la aplicación o actualización.

   Se abre la ventana de propiedades.

b. Abra la sección **Dispositivos**.

   También puede ver la lista de aplicaciones instaladas y actualizaciones en la ventana de propiedades del dispositivo.

8. Especifique cómo los dispositivos cliente descargarán la utilidad de desinstalación:

Con el Agente de red

Los archivos se entregan a los dispositivos cliente mediante el Agente de red instalado en esos dispositivos cliente.

Si esta opción está deshabilitada, los archivos se entregan mediante las herramientas de Linux.

Recomendamos habilitar esta opción si la tarea está asignada a dispositivos que tienen instalado el Agente de red.

Con los recursos del sistema operativo a través del Servidor de administración

La opción es obsoleta. Utilizar la opción **Con el Agente de red** o **Con los recursos del sistema operativo a través de los puntos de distribución** en su lugar.

Los archivos se transmiten a los dispositivos cliente mediante las herramientas del sistema operativo del Servidor de administración. Puede habilitar esta opción si no hay ningún Agente de red instalado en el dispositivo cliente, pero el dispositivo cliente está en la misma red que el Servidor de administración.

Con los recursos del sistema operativo a través de los puntos de distribución

Los archivos se transmiten a los dispositivos cliente mediante el uso de herramientas del sistema operativo a través de puntos de distribución. Puede habilitar esta opción si existe al menos un punto de distribución en la red.

Si se habilita la opción **Con el Agente de red**, los archivos se entregan utilizando las herramientas del sistema operativo solo si las herramientas del Agente de red no están disponibles.

N.° máximo de descargas simultáneas

El número máximo permitido de dispositivos cliente a los que el Servidor de administración puede transmitir simultáneamente los archivos. Cuanto mayor sea este número, más rápido se desinstalará la aplicación, pero la carga en el Servidor de administración será mayor.

N.° máximo de intentos de desinstalación

Si, al ejecutar la tarea *Desinstalar aplicación de forma remota*, Kaspersky Security Center Linux no puede desinstalar la aplicación en un dispositivo administrado dentro del número de ejecuciones del instalador especificado por este parámetro, Kaspersky Security Center Linux deja de entregar la utilidad de desinstalación a ese dispositivo administrado y ya no inicia el instalador en el dispositivo.

El parámetro **N.° máximo de intentos de desinstalación** permite que guarde los recursos del dispositivo administrado, así como reducir el tráfico (desinstalación, ejecución de archivos MSI y mensajes de error).

Los intentos de inicio de tareas recurrentes pueden indicar un problema en el dispositivo que impide la desinstalación. El administrador debe resolver el problema dentro del número especificado de intentos de desinstalación y, luego, debe reiniciar la tarea (manualmente o según una programación).

Si finalmente no se logra la desinstalación, el problema se considera no resuelto y cualquier inicio de tarea adicional se considera costoso en términos de consumo innecesario de recursos y tráfico.

Cuando se crea la tarea, el contador de intentos se establece en `0`. Cada ejecución del instalador que devuelve un error en el dispositivo incrementa la lectura del contador.

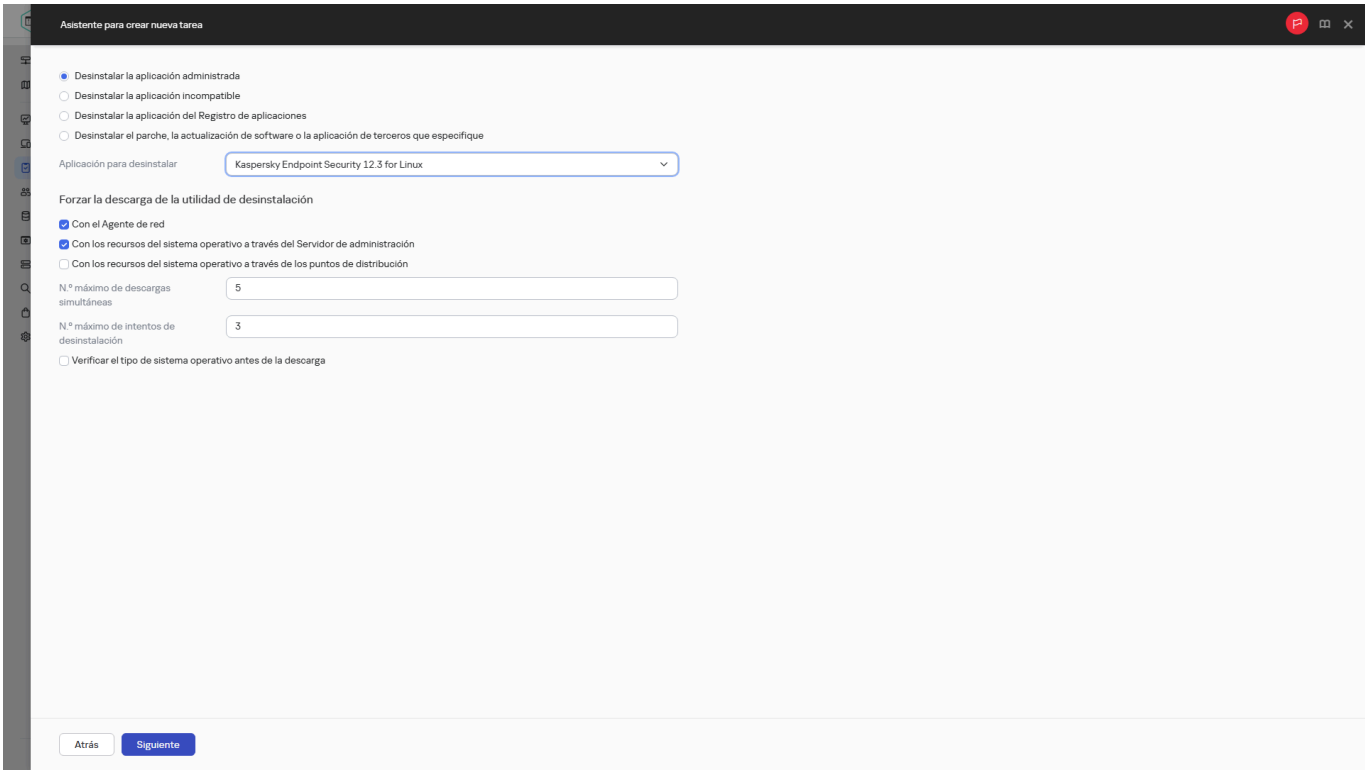
Si se superó el número de intentos especificado en el parámetro y el dispositivo está listo para la desinstalación de la aplicación, puede aumentar el valor del parámetro **N.° máximo de intentos de desinstalación** e iniciar la tarea para desinstalar la aplicación. Alternativamente, puede crear una nueva tarea *Desinstalar aplicación de forma remota*.

Verificar el tipo de sistema operativo antes de la descarga

Antes de transmitir los archivos a los dispositivos cliente, Kaspersky Security Center Linux verificará si los ajustes de la utilidad de desinstalación son adecuados para el sistema operativo del dispositivo cliente. Si no lo son, Kaspersky Security Center Linux no transmitirá los archivos y no tratará de instalar la aplicación. A modo de ejemplo, si necesita instalar una aplicación en los dispositivos de un grupo de administración que contenga dispositivos con sistemas operativos diferentes, puede asignar la tarea de instalación al grupo de administración y habilitar esta opción para que la tarea no afecte a aquellos dispositivos que no tengan el sistema operativo pertinente.

Cuando instala el Agente de red de forma remota en dispositivos no asignados, Kaspersky Security Center Linux o un punto de distribución determina automáticamente el tipo de sistema operativo del dispositivo, independientemente de la configuración **Verificar el tipo de sistema operativo antes de la descarga**.

Avance al siguiente paso del asistente.



Especificar la configuración de la tarea

9. Defina las opciones de reinicio del sistema operativo:

No reiniciar el dispositivo

Cuando termine la operación, los dispositivos cliente no se reiniciarán automáticamente. Para que la operación se complete, deberá reiniciar los dispositivos en forma manual o mediante, por ejemplo, una tarea de administración de dispositivos. Los resultados de la tarea y el estado de cada dispositivo darán cuenta de que hay un reinicio pendiente. Esta opción es útil cuando la tarea va a ejecutarse en servidores y dispositivos que deben operar continuamente.

Reiniciar el dispositivo

Los dispositivos cliente se reiniciarán automáticamente siempre que resulte necesario para completar la operación. Esta opción es útil cuando la tarea se realiza en dispositivos que admiten una breve interrupción para apagarse o reiniciarse.

Solicitar al usuario una acción

A través de un recordatorio en pantalla, se le pedirá a cada usuario que reinicie su dispositivo manualmente. Puede configurar algunos ajustes avanzados para esta opción: el texto del mensaje que se le muestra al usuario, la frecuencia con la que se muestra este mensaje y el tiempo que se espera antes de reiniciar el dispositivo por la fuerza (sin que el usuario confirme el reinicio). Esta opción es la más adecuada para estaciones de trabajo en las que los usuarios deben poder seleccionar el momento más conveniente para reiniciar.

Esta opción está seleccionada de forma predeterminada.

- **Repetir solicitud cada (min)**
- **Reiniciar después de (min)**

Forzar el cierre de aplicaciones en sesiones bloqueadas

Las aplicaciones abiertas en el dispositivo cliente podrían impedir que se lo reinicie. Si el usuario está editando un documento en un procesador de textos, por ejemplo, y no ha guardado el archivo, el procesador de textos no permitirá que el dispositivo se reinicie.

Si habilita esta opción, las aplicaciones que se estén ejecutando en un dispositivo bloqueado se cerrarán por la fuerza y, tras ello, el dispositivo se reiniciará. Los usuarios podrían perder los cambios que no hayan guardado.

Si no habilita esta opción, los dispositivos bloqueados no se reiniciarán. El estado de la tarea en tales dispositivos indicará que hay un reinicio pendiente. Los usuarios tendrán que cerrar manualmente todas las aplicaciones abiertas para luego reiniciar sus dispositivos.

Esta opción está deshabilitada de forma predeterminada.

Avance al siguiente paso del asistente.

10. Si es necesario, agregue las cuentas que se utilizarán para iniciar la tarea de desinstalación remota:

    No se necesita una cuenta (el Agente de red está instalado)

    Si selecciona esta opción, no necesitará especificar la cuenta con la que se ejecutará el instalador de la aplicación. Para ejecutar la tarea, se usará la cuenta con la que se haya iniciado el servicio del Servidor de administración.

    Esta opción no está disponible si el Agente de red no se ha instalado en los dispositivos cliente.

    Se necesita una cuenta (no se utiliza el Agente de red)

    Seleccione esta opción si el Agente de red no está instalado en los dispositivos a los que está asignando la tarea *Desinstalar aplicación de forma remota*. En este caso, puede especificar una cuenta de usuario o un certificado SSH para desinstalar la aplicación.

    - **Cuenta local o de dominio**. Si se selecciona esta opción, especifique la cuenta bajo la que se ejecutará el instalador de aplicación. Haga clic en el botón **Agregar**, seleccione **Cuenta local o de dominio** y, a continuación, especifique las credenciales de la cuenta de usuario.

      Puede especificar varias cuentas de usuario si, por ejemplo, ninguna de ellas tiene todos los derechos requeridos en todos los dispositivos a los que asigne esta tarea. En este caso, todas las cuentas añadidas se utilizan para ejecutar la tarea, en orden consecutivo de arriba abajo.

    - **Certificado de SSH**. Si desea desinstalar una aplicación de un dispositivo cliente basado en Linux, puede especificar un certificado SSH en lugar de una cuenta de usuario. Haga clic en el botón **Agregar**, seleccione **Certificado de SSH** y, a continuación, especifique las claves pública y privada del certificado.

      Para generar una clave privada, puede utilizar la utilidad ssh-keygen. Tenga en cuenta que Kaspersky Security Center Linux espera que la clave privada esté en formato PEM, pero, de manera predeterminada, la utilidad ssh-keygen genera claves SSH en formato OPENSSH. Kaspersky Security Center Linux no admite el formato OPENSSH. Para crear una clave privada en el formato PEM admitido, agregue la opción -m PEM en el comando ssh-keygen.

      Por ejemplo:

```
ssh-keygen -m PEM -t rsa -b 4096 -C "<correo electrónico del usuario>"
```

11. Si en el paso **Finalizar la creación de la tarea** del asistente habilita la opción **Abrir los detalles de la tarea cuando se complete la creación**, puede modificar la configuración predeterminada de la tarea.

    Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Podrá modificarla más adelante.

12. Haga clic en el botón **Finalizar**.

    El asistente creará la tarea. Si habilitó la opción **Abrir los detalles de la tarea cuando se complete la creación**, se abrirá automáticamente la ventana de propiedades de la tarea. En esta ventana, puede especificar la configuración general de la tarea y, si es necesario, cambiar la configuración especificada durante la creación de la tarea.

    > También puede abrir la ventana de propiedades de la tarea haciendo clic en el nombre de la tarea creada en la lista de tareas.

    La tarea se crea, configura y muestra en la lista de tareas en **Tareas**.

13. Para ejecutar la tarea, selecciónela en la lista de tareas y haga clic en el botón **Iniciar**.

    También puede programar el inicio de la tarea en la pestaña **Programación**, en la ventana de propiedades de la tarea.

    Para obtener una descripción detallada de la configuración de inicio programado, vea la configuración general de la tarea.

Cuando se complete la tarea, la aplicación seleccionada se eliminará de los dispositivos seleccionados.

Problemas de desinstalación remota

En ocasiones, la desinstalación remota de aplicaciones de terceros puede finalizar con la siguiente advertencia: "La eliminación remota ha finalizado en este dispositivo con advertencias: la aplicación que se quería eliminar no está instalada". Este problema ocurre cuando la aplicación que se pretende desinstalar ya fue desinstalada o se la instaló solo para un usuario individual. Las aplicaciones instaladas para un usuario individual (también denominadas aplicaciones por usuario) se vuelven invisibles y no se pueden desinstalar de forma remota si el usuario no inició sesión.

Este comportamiento es diferente al de las aplicaciones diseñadas para ser utilizadas por múltiples usuarios en el mismo dispositivo (también denominadas aplicaciones por dispositivo). Las aplicaciones por dispositivo son visibles y accesibles para todos los usuarios del dispositivo.

Por lo tanto, las aplicaciones por usuario deben desinstalarse solo cuando el usuario inicia sesión.

Orígenes de la información acerca de aplicaciones instaladas

El Agente de red recupera de las siguientes claves de registro información sobre el software instalado en los dispositivos Windows:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

  Contiene información sobre las aplicaciones instaladas para todos los usuarios.

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

  Contiene información sobre las aplicaciones instaladas para todos los usuarios.

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

  Contiene información sobre las aplicaciones que el usuario actual tiene instaladas.

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

  Contiene información sobre las aplicaciones instaladas para usuarios específicos.

Preparar un dispositivo Windows para la instalación remota

Es posible que la instalación remota de la aplicación en el dispositivo cliente se complete con un error por los siguientes motivos:

- La tarea ya se ha ejecutado correctamente en este dispositivo.

  En este caso, no es necesario volver a realizar la tarea.

- El dispositivo se apaga al iniciarse una tarea.

  En ese caso, encienda el dispositivo y vuelva a iniciar la tarea.

- No hay conexión entre el Servidor de administración y el Agente de red instalado en el dispositivo cliente.

  Para determinar la causa del problema, use la utilidad diseñada para realizar diagnósticos remotos en los dispositivos cliente (klactgui).

- Si no hay un Agente de red instalado en el dispositivo, pueden ocurrir los siguientes problemas durante la instalación remota:

  - El dispositivo cliente tiene la opción **Deshabilitar el uso compartido simple de archivos** de archivos habilitado.

  - El servicio del servidor no se está ejecutando en el dispositivo cliente.

  - Los puertos requeridos están cerrados en el dispositivo cliente.

  - La cuenta utilizada para ejecutar la tarea no cuenta con los privilegios suficientes.

Para evitar problemas que puedan ocurrir durante la instalación de la aplicación en un dispositivo cliente sin Agente de red instalado, debe proceder como se describe en el despliegue forzado a través de la tarea de instalación remota de Kaspersky Security Center Linux.

Antes se usaba la utilidad riprep a fin de preparar un dispositivo de Windows para la instalación remota. Ahora se trata de un método obsoleto para configurar sistemas operativos. No se recomienda el uso de la utilidad riprep en sistemas operativos más nuevos que Windows XP y Windows Server 2003 R2.

Crear la tarea Ejecución remota de scripts

Puede crear una tarea *Ejecutar scripts de forma remota* para ejecutar un paquete de instalación en un dispositivo cliente e instalar una aplicación de forma remota.

Un paquete de instalación contiene un archivo ZIP con un conjunto de scripts diseñados para ejecutarse en los dispositivos cliente y un archivo manifest.json. Encontrará más información para crear este tipo de paquete de instalación en este artículo.

Esta tarea debe iniciarse solo en dispositivos con el Agente de red para Linux.

Para iniciar una tarea Ejecutar scripts de forma remota:

1. Vaya al **Asistente para crear nueva tarea** y seleccione el tipo de tarea **Ejecutar scripts de forma remota**.
2. Ingrese el nombre de la tarea y seleccione los dispositivos a los que se la asignará. Haga clic en **Siguiente**.
3. Seleccione un paquete de instalación que esté basado en un archivo ZIP y contenga un archivo manifest.json para ejecución remota.

   Si no desea volver a ejecutar la tarea en dispositivos en los que ya se haya completado, seleccione la opción **No iniciar esta tarea en los dispositivos en los que ya se completó**.
4. Seleccione una cuenta con la que ejecutar la tarea.

   Si selecciona la cuenta predeterminada, el Agente de red (cuenta root) realizará la tarea.

   Una vez que se ha iniciado la tarea *Ejecutar scripts de forma remota*, la cuenta asignada no se puede cambiar. Para cambiar la cuenta asignada a la tarea, detenga la tarea a través de sus ajustes y vuelva a crear la tarea con los datos de la cuenta correcta.
5. Si desea modificar la configuración predeterminada de la tarea, habilite la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de la tarea**. Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Puede cambiar la configuración por defecto más tarde, en cualquier momento.

6. Haga clic en el botón **Finalizar**.

   Se crea la tarea *Ejecución remota de scripts* y se la agrega a la lista de tareas.

Después de recibir datos de la tarea *Ejecución remota de scripts*, el Agente de red limita el acceso a los datos recibidos para todos los usuarios, excepto el administrador y el usuario especificado en la configuración de la tarea.

Crear un paquete de instalación basado en un archivo de manifiesto

Para crear un paquete de instalación basado en un archivo de manifiesto:

1. En el menú principal, vaya a **Administración de software → Paquetes de instalación**.

   Se muestra una lista de paquetes de instalación disponibles en el Servidor de administración.

2. Haga clic en **Agregar**.

   Se inicia el Asistente de nuevo paquete. Avance por el asistente utilizando el botón **Siguiente**.

3. Seleccione **Crear un paquete de instalación para la tarea Ejecutar scripts de forma remota en función de un archivo ZIP con el archivo manifest.json**.

4. Escriba el nombre del paquete y haga clic en el botón **Examinar**.

   En la ventana que se abre, elija un archivo para crear el paquete de instalación.

5. Seleccione un archivo de almacenamiento en alguna de las unidades disponibles. Encontrará información sobre cómo preparar un archivo para esta tarea en este artículo.

   El archivo comienza a cargarse en el Servidor de administración de Kaspersky Security Center Linux.

   Se inicia el proceso para crear el paquete de instalación.

   El asistente le informará cuando finalice el proceso.

   Si no se crea el paquete de instalación, se muestra el mensaje pertinente.

6. Haga clic en el botón **Finalizar** para cerrar el asistente.

El paquete de instalación que ha creado se descarga en la subcarpeta Paquetes de la carpeta compartida del Servidor de administración. Al concluir la descarga, el paquete de instalación aparecerá en la lista de paquetes de instalación.

En la lista de paquetes de instalación disponibles en el Servidor de administración, al hacer clic en el vínculo con el nombre de un paquete de instalación personalizado, puede hacer lo siguiente:

- Ver las siguientes propiedades del paquete de instalación:
  - **Nombre.** Nombre del paquete de instalación personalizado.
  - **Origen.** Nombre del proveedor de la aplicación.
  - **Versión.** Versión de la aplicación.

- **Creado.** Fecha de creación del paquete de instalación.
- **Modificado.** Fecha de modificación del paquete de instalación.
- **Ruta.** Ruta al paquete de instalación personalizado en el Servidor de administración.

- Cambiar el nombre del paquete y los parámetros de la línea de comandos. Esta función solo está disponible para paquetes que no se han creado para aplicaciones de Kaspersky.

Preparar un archivo para la tarea Ejecución remota de scripts

A continuación, se enumeran los requisitos con los que debe cumplir un archivo basado en un archivo manifest.json que vaya a usarse para la tarea *Ejecutar scripts de forma remota*:

- Formato de archivo: ZIP.
- Tamaño total: no más de 1 GB.
- La cantidad de archivos y carpetas que contenga es ilimitada.
- El archivo de manifiesto en el que se base el archivo debe respetar el siguiente esquema y debe llamarse manifest.json. El esquema se valida solo durante la ejecución de la tarea en un dispositivo.

  Esquema JSON del archivo de manifiesto y descripción de las matrices

  Esquema JSON

```
{
 "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "Schema for execute scripts task",
   "type": "object",
    "properties": {
        "version": {
            "type": "integer",
            "enum": [1]
        },
        "actions":{
            "type": "array",
            "items": {
                "type": "object",
                "properties": {
                    "type": {
                        "type": "string",
                        "enum": ["execute"]
                    },
                    "path": {
                        "type": "string"
                    },
                    "args": {
                        "type": "string"
                    },
                    "results":{
                        "type": "array",
```

```
                        "items": {
                            "type": "object",
                            "properties": {
                                "code": {
                                    "type": "integer",
                                    "minimum": -255,
                                    "maximum": 255
                                },
                                "next":{
                                    "type": "string",
                                    "enum": ["break", "continue"]
                                }
                            },
                            "required": [
                                "code",
                                "next"
                            ]
                        }
                    },
                    "default_next":{
                        "type": "string",
                        "enum": ["break", "continue"]
                    }
                },
                "required": [
                    "type",
                    "path",
                    "default_next"
                ]
            }
        }
    },
    "required": [
        "version",
        "actions"
    ]
}
```

Ejemplo de archivo de manifiesto

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "scripts/run1.cmd",
      "args": "testArg",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run2.cmd",
      "results": [
```

```
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run3.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

- El archivo debe tener la siguiente estructura:

  ```
  manifest.json
  <file1>
  <file2>
  <folder1>/<file3>
  <folder2>/<folder3>/<file4>
  ...
  <fileX>
  ```

  `manifest.json` es el archivo de manifiesto de la tarea.

  `<file1>`, ..., `<fileX>` es el conjunto de archivos con scripts que se ejecutarán.

Instalar aplicaciones en dispositivos a distancia con la tarea Ejecución remota de scripts

La tarea *Ejecutar scripts de forma remota* puede usarse para instalar una aplicación en un dispositivo cliente remoto mediante la creación de un paquete de instalación personalizado.

Encontrará información sobre cómo preparar un archivo para esta tarea en este artículo.

Si desea crear un paquete de instalación que le permita instalar una aplicación en un dispositivo cliente remoto, asegúrese de que el archivo que vaya a cargar para la tarea contenga los siguientes archivos:

- `<nombre del paquete>.deb`
- **install.sh**

  ```
  sudo apt-get install <nombre del paquete>.deb
  ```

- **manifest.json**

Esquema JSON para la instalación remota de una aplicación

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "install.sh",
      "args": "<Ingrese los argumentos, si es necesario>",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

Descripción de las matrices

1. `version`: versión del archivo de manifiesto y de la tarea.

   En este momento, el único valor aceptable es 1.

2. Los elementos de la matriz `actions` determinan la composición y el orden de los scripts que se ejecutan en la tarea.

   El orden de ejecución del script corresponde con el índice (ubicación) de un elemento en la matriz.

3. Para cada elemento de la matriz `actions`, se definen los siguientes elementos.

   a. `type`: tipo de comando ejecutable a partir de los scripts. En este momento, el valor siempre es `execute`.

   b. `path`: ruta al archivo de script en el archivo comprimido.

   c. `args`: argumentos que se pasan al script como parte del comando ejecutable.

   d. `results`: matriz que define las acciones posteriores en función del resultado de la tarea.

      1. `code`: valor que devuelve el script.

      2. `next`: acción que se completará a continuación. La acción `continue` continúa con la ejecución del siguiente script (elemento de la matriz `actions`). La acción `break` detiene la tarea.

   e. `default_next`: acción que se realiza si un script devuelve un valor que no está presente en `results`.

Cuando se inicie la tarea *Ejecutar scripts de forma remota*, el Agente de red cargará el paquete de instalación con la aplicación en el dispositivo cliente. Cuando el dispositivo cliente reciba el paquete de instalación, el Agente de red de dicho dispositivo analizará el archivo manifest.json, definirá el orden de ejecución de los scripts y las acciones que deberá llevar a cabo según los resultados y, finalmente, llevará a cabo la ejecución.

Cuando se complete la tarea *Ejecutar scripts de forma remota*, la aplicación quedará instalada en el dispositivo cliente.

Configurar notificaciones y supervisar la tarea Ejecución remota de scripts

Puede configurar la supervisión, el comportamiento de guardado de eventos y las notificaciones de la tarea *Ejecutar scripts de forma remota*.

Para ver el estado de Ejecutar scripts de forma remota:

1. En el menú principal, vaya a **Tareas**.

   Se muestra la lista de tareas.

2. Seleccione la tarea y haga clic en **Historial del dispositivo**.

   Se muestra el progreso de la tarea.

Para configurar el comportamiento de guardado de eventos:

1. En la lista de tareas, haga clic en la tarea y vaya a la pestaña **Configuración**.
2. En la sección **Notificaciones**, haga clic en el botón **Configuración**.
3. Seleccione una de las siguientes opciones sobre cómo se comportará la aplicación al completarse la tarea:

   - **Guardar todos los eventos**.
   - **Guardar eventos relacionados con el progreso de la tarea**.
   - **Guardar solo los resultados de la ejecución de la tarea**.

     Los eventos se guardan en **Historial del dispositivo** y en **Repositorio de eventos**.

     De forma predeterminada, solo se guardan los resultados de la ejecución de la tarea.

     > Si selecciona **Guardar todos los eventos**, solo se guardarán los resultados de la ejecución de la tarea.

4. Si desea conservar los eventos en la base de datos del Servidor de administración, en el registro de eventos del Servidor de administración o en el dispositivo, active la opción correspondiente.

Obtenga más información sobre cómo configurar las notificaciones en este artículo.

Licencias

Esta sección proporciona la siguiente información:

- Conceptos generales relacionados con las licencias de Kaspersky Security Center Linux
- Instrucciones sobre la gestión de licencias de aplicaciones Kaspersky administradas

Licencias de Kaspersky Security Center Linux

Esta sección describe conceptos generales relacionados con la licencia de Kaspersky Security Center Linux.

Acerca del Contrato de licencia de usuario final

El *Contrato de licencia de usuario final* (Contrato de licencia o EULA) es un acuerdo obligatorio entre AO Kaspersky Lab y usted que estipula los términos según los cuales puede utilizar la aplicación.

Lea detenidamente el Contrato de licencia antes de comenzar a utilizar la aplicación.

Kaspersky Security Center Linux y sus componentes, por ejemplo, el Agente de red, tienen su propio EULA.

Puede ver los términos del Contrato de licencia de usuario final para Kaspersky Security Center Linux de distintas maneras:

- Durante la instalación de Kaspersky Security Center.
- Leyendo el documento license.txt incluido en el kit de distribución de Kaspersky Security Center.
- Leyendo el documento license.txt en la carpeta de instalación de Kaspersky Security Center.
- puede descargar el archivo license.txt desde el sitio web de Kaspersky.

Puede ver los términos del Contrato de licencia de usuario final para el Agente de red para Linux a través de los siguientes métodos:

- Durante la descarga del paquete de distribución del Agente de red desde los servidores web de Kaspersky.
- Durante la instalación del Agente de red para Linux.
- Al leer el documento license.txt incluido en el paquete de distribución del Agente de red para Linux.
- Leyendo el documento license.txt en la carpeta de instalación del Agente de red para Linux.
- puede descargar el archivo license.txt desde el sitio web de Kaspersky.

Acepta los términos del Contrato de licencia de usuario final al confirmar que está de acuerdo con el Contrato de licencia de usuario final al instalar la aplicación. Si no acepta los términos del Contrato de licencia, cancele la instalación de la aplicación y no la utilice.

Acerca de la licencia

Una *licencia* otorga el derecho a usar Kaspersky Security Center por un tiempo limitado según las condiciones del Contrato de licencia firmado (Contrato de licencia de usuario final).

El alcance de los servicios y el período de validez dependen del tipo de licencia con el que se utiliza la aplicación.

Se proporcionan los siguientes tipos de licencia:

- *Prueba*

  Una licencia gratuita diseñada para probar la aplicación. Usualmente, una licencia de prueba tiene un plazo de vigencia breve.

  Cuando vence la licencia de prueba, todas las características de Kaspersky Security Center Linux se deshabilitan. Para seguir usando la aplicación, se debe adquirir una licencia comercial.

  Puede usar la aplicación con una licencia de prueba solo durante un período de prueba.

- *Comercial*

  Una licencia pagada.

  Cuando caduca una licencia comercial, se deshabilitan las principales características de la aplicación. Para que Kaspersky Security Center siga funcionando, se debe renovar la licencia comercial. Una vez que caduque la licencia, ya no podrá usar la aplicación y deberá eliminarla del dispositivo.

  Se recomienda renovar la licencia antes de que caduque para garantizar una protección ininterrumpida contra las amenazas a la seguridad.

Acerca del certificado de licencia

Un *certificado de licencia* es un documento que se le proporciona junto con un archivo de clave o código de activación.

El certificado de licencia contiene la siguiente información sobre la licencia otorgada:

- Id. de la licencia o número de orden
- Información sobre el usuario que recibe la licencia
- Información sobre la aplicación que se puede activar con la licencia otorgada
- Límite al número de unidades con licencia (por ejemplo, el número de dispositivos en los que la licencia otorgada permite usar la aplicación)
- Fecha de inicio del periodo de vigencia de la licencia
- Fecha de caducidad de la licencia o periodo de vigencia de la licencia
- Tipo de licencia

Acerca de la clave de licencia

La *clave de licencia* es una secuencia de bits que se puede aplicar para activar y utilizar la aplicación de acuerdo con el Contrato de licencia de usuario final. Las claves de licencia son generadas por los especialistas de Kaspersky.

Puede agregar una clave de licencia a la aplicación mediante uno de los siguientes métodos: aplicando el *archivo de clave* o ingresando un *código de activación*. La clave de licencia se muestra en la interfaz de la aplicación como una secuencia alfanumérica única después de que la agrega a la aplicación.

Kaspersky puede bloquear la clave de licencia en caso de que se hayan infringido los términos del Contrato de licencia. Si la clave de licencia se ha bloqueado, debe agregar otra clave si desea usar la aplicación.

Una clave de licencia puede ser activa o adicional (de reserva).

Una *clave de licencia activa* es la clave que la aplicación está utilizando. Se puede agregar una clave de licencia activa para una licencia de prueba o comercial. La aplicación no puede tener más de una clave de licencia activa.

Una *clave de licencia adicional (o de reserva)* es una clave de licencia que le brinda a una persona el derecho a usar la aplicación, pero que no está activa en un momento dado. Una clave de licencia adicional se activa de forma automática cuando caduca la licencia asociada con la clave de licencia activa actual. Se puede agregar una clave de licencia adicional únicamente si ya se ha agregado una clave de licencia activa.

Se puede agregar una clave de licencia para la licencia de prueba como una clave de licencia activa. No se puede agregar una clave de licencia para la licencia de prueba como una clave de licencia adicional.

Ver la Política de privacidad

La Política de privacidad está disponible en línea en https://latam.kaspersky.com/products-and-services-privacy-policy.

La Política de privacidad también está disponible sin conexión:

- Puede leer la Política de privacidad antes de instalar Kaspersky Security Center Linux.
- Encontrará el texto de la Política de privacidad en el archivo license.txt, disponible en la carpeta de instalación de Kaspersky Security Center Linux.
- El archivo privacy_policy.txt está disponible en un dispositivo administrado, en la carpeta de instalación del Agente de red.
- Puede desempaquetar el archivo privacy_policy.txt del paquete de distribución del Agente de red.

Opciones de licencias de Kaspersky Security Center

Kaspersky Security Center puede funcionar en los siguientes modos:

- **Funcionalidad básica de la Consola de administración**

  Kaspersky Security Center funciona en este modo antes de que se active la aplicación o después de que caduca la licencia comercial. Kaspersky Security Center con el soporte de la funcionalidad básica de la Consola de administración se entrega como una parte de las aplicaciones de Kaspersky para la protección de redes corporativas. También se puede descargar desde el sitio web de Kaspersky.

- **Licencia comercial**

  Si necesita una funcionalidad adicional que no esté incluida en la funcionalidad básica de la Consola de administración, debe comprar una licencia comercial.

  Cuando agregue una clave de licencia en la ventana de propiedades del Servidor de administración, verifique que esta le permita utilizar Kaspersky Security Center Linux. Encontrará información a tal efecto en el sitio web de Kaspersky. La página web de cada solución contiene una lista de las aplicaciones que incluye. El Servidor de administración puede aceptar claves de licencia no admitidas (por ejemplo, una clave de licencia para Kaspersky Endpoint Security Cloud), pero esas claves de licencia no proporcionan nuevas funciones además de la funcionalidad básica de la Consola de administración.

Característica o propiedad	Modo de funcionamiento de Kaspersky Security Center Linux	
	Falta la licencia	Licencia comercial
Funcionalidad básica de la Consola de administración Están disponibles las siguientes funciones: • Creación de Servidores de administración virtuales para administrar una red de oficinas remotas u organizaciones cliente. • Creación de una jerarquía de grupos de administración para administrar dispositivos específicos como una única entidad. • Instalación remota de aplicaciones. • La configuración centralizada de aplicaciones instaladas en dispositivos cliente. • Control del estado de la seguridad antivirus de una organización. • Administración de roles de usuario. • Estadísticas e informes sobre el funcionamiento de la aplicación, así como notificaciones sobre eventos críticos. • Operaciones centralizadas con archivos que se movieron a la cuarentena o copia de seguridad y archivos cuyo procesamiento se ha pospuesto. • Administración de la protección y el cifrado de datos. • Visualización y edición manual de la lista de componentes de hardware que detectó el sondeo de la red. • Visualización de la lista de imágenes de sistema operativo disponibles para la instalación remota.	✓	✓

Característica o propiedad	Modo de funcionamiento de Kaspersky Security Center Linux	
	Falta la licencia	Licencia comercial
Administración de vulnerabilidades y parches: funcionalidad básica Las siguientes tareas no requieren una licencia comercial: • La tarea *Buscar vulnerabilidades y actualizaciones requeridas* Mediante esta tarea, Kaspersky Security Center Linux recibe las listas de las vulnerabilidades detectadas y las actualizaciones necesarias para el software de terceros instalado en los dispositivos administrados. • La tarea *Reparar vulnerabilidades* La tarea *Reparar vulnerabilidades* utiliza las actualizaciones recomendadas para el software de Microsoft y las actualizaciones indicadas por el usuario para el software de terceros. Para usar esta tarea, debe especificar manualmente las correcciones de usuario para las vulnerabilidades en la configuración de la tarea.	✓	✓
Administración de vulnerabilidades y parches: funcionalidad avanzada Puede definir las reglas para la instalación remota automática de actualizaciones de software y la reparación automática de vulnerabilidades.	—	✓
Administración de sistemas Están disponibles las siguientes funciones: • Permiso remoto de conexión a dispositivos cliente a través de un componente de Microsoft® Windows® llamado Conexión a escritorio remoto. • Conexión remota con dispositivos cliente mediante Windows Desktop Sharing.	—	✓
Exportar eventos a un sistema SIEM a través del protocolo Syslog. Usando el protocolo de Syslog, puede transmitir cualquier evento que ocurra en el Servidor de administración de Kaspersky Security Center y en Aplicaciones de Kaspersky instaladas en dispositivos administrados. El protocolo de Syslog es un protocolo de registro de mensajes estándares. Puede utilizarlo para exportar eventos a cualquier sistema SIEM.	✓	✓
Agrupación de alertas y realización de acciones de respuesta a través de Active Directory, KASAP y Kaspersky TIP Sandbox	—	✓

Acerca del archivo de clave

El *archivo de clave* es un archivo con la extensión .key que le proporciona Kaspersky. Los archivos de claves están diseñados para activar la aplicación agregando una clave de licencia.

Recibirá un archivo de clave en la dirección de correo electrónico que proporcionó al comprar Kaspersky Security Center o al solicitar la versión de prueba de Kaspersky Security Center.

No es necesario conectarse a los servidores de activación de Kaspersky para activar la aplicación con un archivo de clave.

Si el archivo de clave se eliminó accidentalmente, puede restaurarlo. Es posible que necesite un archivo de clave, por ejemplo, para registrarse en Kaspersky CompanyAccount.

Para restaurar el archivo de clave, realice una de las siguientes acciones:

- Póngase en contacto con el vendedor de la licencia.
- Obtenga un archivo de clave en el sitio web de Kaspersky con el código de activación disponible.

Sobre la provisión de datos

Datos proporcionados a terceros

Al usar la función Administración de dispositivos móviles del Software, con el fin de hacer llegar oportunamente a través del mecanismo de notificación automática los comandos a los dispositivos que ejecutan el sistema operativo Android, se utiliza Google Firebase Cloud Messaging. Si el Usuario ha configurado el uso de Google Firebase Cloud Messaging, el Usuario acepta proporcionar la siguiente información al servicio de mensajería de nube Google Firebase Cloud Messaging en modo automático:

- Id. de la instancia
- Id. del software en el servicio de mensajería en la nube de Google Firebase
- Versión del software instalado
- Versión completa del Software
- Versión de Google Play
- Nombre del paquete de distribución del software
- Versión del esquema de los datos proporcionados
- Versión del sistema operativo
- Id. del software

Para que no se intercambie información con el servicio Google Firebase Cloud Messaging, el usuario debe revertir la configuración de uso del servicio Google Firebase Cloud Messaging.

Cuando se usa la función Administración de dispositivos móviles del software, se usa también el servicio Apple Push Notification Service (APNs) con el fin de que los comandos que se transmitan a través del mecanismo de notificación push lleguen sin dilaciones a los dispositivos que ejecutan el sistema operativo iOS. Si el usuario ha instalado un certificado de APNs en un servidor de MDM para iOS, ha creado un perfil de MDM para iOS con una colección de ajustes para conectar dispositivos móviles iOS al software y ha instalado dicho perfil en sus dispositivos móviles, el usuario acepta proporcionar la siguiente información a APNs en modo automático:

- Token: token del dispositivo para notificaciones push. El servidor usa este token cuando envía notificaciones push al dispositivo.
- PushMagic: cadena que debe incluirse en la notificación push. El valor de la cadena es generado por el dispositivo.

Datos transferidos a AO Kaspersky Lab

Si la funcionalidad de Kaspersky Extended Detection and Response Optimum está disponible para el usuario, Kaspersky Security Center Linux transfiere datos en los siguientes casos:

- Para asignar un curso de capacitación a un empleado, Kaspersky Security Center Linux transfiere los siguientes datos a Kaspersky Automated Security Awareness Platform (KASAP): correo electrónico del usuario, correo electrónico del usuario alternativo (si está disponible), Id. de usuario en KASAP, Id. del grupo de capacitación.

- Para ejecutar automáticamente un archivo mediante Kaspersky Cloud Sandbox, la aplicación administrada transfiere los archivos en cuarentena desde el Servidor de administración mediante el Agente de red y, luego, mediante Kaspersky Security Center Web Console, a Kaspersky Cloud Sandbox. Kaspersky Cloud Sandbox analiza el archivo y cualquier otro archivo que pueda crearse durante su ejecución.

Datos procesados localmente

Kaspersky Security Center Linux está diseñado para ejecutar tareas de administración y mantenimiento básicas en la red de una organización de forma centralizada. Kaspersky Security Center Linux le brinda al administrador acceso a información detallada sobre el nivel de seguridad de la red de la organización y le permite configurar todos los componentes de un sistema de protección basado en las aplicaciones de Kaspersky. Estas son las principales funciones que se pueden realizar a través de Kaspersky Security Center Linux:

- Detectar dispositivos, y a los usuarios de esos dispositivos, en la red de la organización
- Crear una jerarquía de grupos de administración para la administración de dispositivos
- Instalar aplicaciones de Kaspersky en los dispositivos
- Administrar la configuración y las tareas de las aplicaciones instaladas
- Administrar actualizaciones para las aplicaciones desarrolladas por Kaspersky y por otras empresas, así como encontrar y reparar vulnerabilidades
- Activar las aplicaciones de Kaspersky en los dispositivos
- Administrar cuentas de usuario
- Ver información sobre el funcionamiento de las aplicaciones de Kaspersky en los dispositivos
- Ver informes
- Habilitar la integración con los servicios de Kaspersky

Para realizar sus funciones principales, Kaspersky Security Center Linux puede recibir, almacenar y procesar la siguiente información:

- Información sobre los dispositivos en la red de la organización recibida mediante el análisis de controladores de dominio (Active Directory, Samba, FreeIPA y ALD Pro) o mediante el análisis de intervalos de IP. El Servidor de administración recaba datos de forma independiente o recibe información del Agente de red.

- Información de los controladores de dominio (Active Directory, Samba, FreeIPA y ALD Pro) sobre las unidades organizativas, los dominios, los usuarios y los grupos. El Servidor de administración obtiene datos por sí mismo o recibe datos del Agente de red asignado para funcionar como punto de distribución.

- Detalles de los dispositivos administrados. El Agente de red transfiere los datos que se muestran a continuación de los dispositivos al Servidor de administración. El nombre y la descripción del dispositivo son introducidos por el usuario en la interfaz de Kaspersky Security Center Web Console:

  - Especificaciones técnicas del dispositivo administrado y de sus componentes necesarias para identificar el dispositivo: nombre para mostrar y descripción del dispositivo, nombre y tipo de dominio de Windows (para dispositivos pertenecientes a un dominio de Windows), nombre del dispositivo en el entorno de Windows (para dispositivos pertenecientes a un dominio de Windows), dominio DNS y nombre del DNS, dirección IPv4, dirección IPv6, localización de red, dirección MAC, número de serie, tipo de sistema operativo, indicación de si el dispositivo es una máquina virtual y tipo de hipervisor e indicación de si el dispositivo es una máquina virtual dinámica que forma parte de una VDI.

  - Otras especificaciones de los dispositivos administrados y sus componentes, necesarias para la auditoría de dispositivos administrados y para decidir si son aplicables determinados parches y actualizaciones: arquitectura del sistema operativo, proveedor del sistema operativo, número de compilación del sistema operativo, ID de versión del sistema operativo, carpeta de ubicación del sistema operativo, el tipo de máquina virtual (si el dispositivo es una máquina virtual) y el nombre del Servidor de administración virtual que se utiliza para administrar el dispositivo.

  - Detalles de acciones realizadas en los dispositivos administrados: fecha y hora de la última actualización; hora en que el dispositivo estuvo visible por última vez en la red; estado de espera de reinicio; hora en que se encendió el dispositivo.

  - Detalles de las cuentas de usuario del dispositivo y de sus sesiones de trabajo.

- Datos recibidos al ejecutar diagnósticos remotos en un dispositivo administrado: archivos de seguimiento, información del sistema, detalles de las aplicaciones de Kaspersky instaladas en el dispositivo, archivos de volcado, registros de eventos, los resultados de la ejecución de los scripts de diagnóstico recibidos del Servicio de soporte técnico de Kaspersky.

- Estadísticas de funcionamiento del punto de distribución, si el dispositivo es un punto de distribución. El Agente de red transfiere datos del dispositivo al Servidor de administración.

- Configuración del punto de distribución especificada por el usuario en Kaspersky Security Center Web Console.

- Datos necesarios para conectar dispositivos móviles al Servidor de administración: certificado, puerto de conexión móvil, dirección de conexión del Servidor de administración. El usuario ingresa los datos en la interfaz de Kaspersky Security Center Web Console.

- Información sobre dispositivos móviles transferida usando el protocolo móvil. Los datos detallados a continuación se transfieren del dispositivo móvil al Servidor de administración:

  - Información sobre la aplicación: nombre de la aplicación, versión completa de la aplicación, fecha y hora de instalación de la aplicación, estado de protección en tiempo real del dispositivo, id. de sesión.

  - Información sobre las claves de licencia utilizadas por la aplicación: número de serie de la clave de licencia y tipo de licencia, estado de la clave de licencia, período de validez de la clave de licencia en días, fechas de generación y caducidad de la clave de licencia, nombre de la empresa a la que se proporcionó la licencia, información adicional en caso de uso de suscripción (indicador de suscripción, fecha de vencimiento y número de días disponibles para la renovación de la suscripción, dirección web del proveedor de la suscripción y estado actual de la suscripción y motivo para obtener este estado), fecha y hora en que se activó la aplicación en el dispositivo, fecha y hora en la que caduca la licencia del dispositivo.

  - Información sobre el dispositivo administrado: nombre del dispositivo, id. del dispositivo, tipo de dispositivo, IMEI del dispositivo (si está disponible), número de serie del dispositivo (si está disponible), fabricante del dispositivo, nombre de la familia de la CPU del dispositivo, huella digital del certificado del propietario del dispositivo, tipo de SO, versión del SO, SO nombre, espacio total en disco en el dispositivo, nombre del servidor al que pertenece el dispositivo, dirección IP del dispositivo, nombre del grupo de dispositivos, nombre distintivo del usuario, nombre distintivo del dominio, contraseña de un solo uso o contraseña de dominio.

  - Información sobre el resultado de la ejecución de comandos personalizados: id. del comando, estado de ejecución del comando, resultado de la ejecución del comando; para el comando de localización del dispositivo: latitud, longitud, altitud y velocidad de movimiento del dispositivo; para el comando mugshot: fotos tomadas por la cámara frontal del dispositivo móvil al intentar desbloquearlo.

  - Información sobre el análisis del dispositivo: fecha y hora del último análisis del dispositivo; ruta completa en el sistema de archivos desde el que se inició el análisis; número de objeto escaneado; número de objetos maliciosos detectados; número de objetos bloqueados, eliminados y desinfectados; número de objetos que no se pudieron desinfectar; número de errores de validación; número de procesos terminados.

  - Información sobre el funcionamiento de cada componente de la aplicación y sobre el rendimiento de cada tarea presentada como evento:

    - Id. del evento

    - Gravedad

    - Nombre y tipo del evento.

    - Descripción de la causa del evento.

    - Fecha y hora en que ocurrió el evento.

    - Información sobre los eventos de la operación del componente Antirrobo (código de desbloqueo del dispositivo, coordenadas del dispositivo, método de entrega del comando, lista de datos eliminados).

    - Resultados del procesamiento del objeto o acción detectados (nombre del archivo en el dispositivo; nombre de la aplicación; nombre de la amenaza; tipo de amenaza; tipo de acción realizada sobre el archivo; resultado de la acción; código del error, en caso de que ocurra).

    - Información sobre la regla de cumplimiento activada (criterio de la regla; acción aplicada; descripción del error ocurrido al aplicar la acción, en caso de que ocurra).

    - Información sobre el error de funcionamiento de la aplicación (versión de la aplicación, versión del sistema operativo, nombre del dispositivo, descripción del error).

- Información sobre el error de Samsung KNOX (código de error, URL desde la que no se pudo descargar el archivo).
- Información sobre los permisos otorgados a la aplicación.
- Información sobre cada una de las aplicaciones instaladas en el dispositivo administrado (nombre de la aplicación, estado de instalación).
- Información sobre la aceptación global del Contrato de licencia de usuario final (EULA): id. del EULA, marca de tiempo del EULA, texto del EULA.
- Configuración de Google Firebase Cloud Messaging: id. del remitente, id. de registro del dispositivo.

- Información sobre la dirección IP pública del dispositivo.
- Valores de la configuración del usuario. El administrador gestiona la configuración en Kaspersky Security Center Web Console, mientras que el usuario la gestiona en la app móvil.

- Detalles de los dispositivos móviles transferidos mediante el protocolo de MDM para iOS. Los datos detallados a continuación se transfieren del dispositivo móvil al Servidor de administración:
  - Especificaciones técnicas del dispositivo móvil y de sus componentes necesarias para identificar el dispositivo: nombre del dispositivo; modelo; nombre, versión y número de compilación del sistema operativo; número de modelo del dispositivo; número de IMEI; número de teléfono; UDID; MEID; número de serie; cantidad de memoria total y disponible; versión del firmware del módem; dirección MAC de Bluetooth; dirección MAC de Wi-Fi; detalles de la tarjeta SIM (el ICCID, como parte del id. de la tarjeta SIM).
  - Detalles de la red móvil utilizada por el dispositivo administrado: tipo de red móvil, nombre de la red móvil que se está utilizando, nombre de la red móvil doméstica, versión de la configuración del operador de red móvil, estado del roaming de voz, estado del roaming de datos, código de país de la red doméstica, código del país de residencia, código de la red que se está utilizando y nivel de cifrado.
  - Configuración de seguridad del dispositivo móvil: uso de una contraseña y su cumplimiento con la configuración de la directiva, lista de certificados, aplicaciones y perfiles de configuración instalados.
  - Fecha y hora de la última sincronización con el Servidor de administración y estado de administración del dispositivo.
- Detalles de los datos del dispositivo móvil transferidos mediante el protocolo WebRTC: imagen de la pantalla del dispositivo.
- Detalles de los archivos marcados para su transferencia a dispositivos móviles. El usuario ingresa datos en la interfaz de Kaspersky Security Center Web Console.

- Detalles de las aplicaciones de Kaspersky instaladas en el dispositivo. La aplicación administrada transfiere datos del dispositivo al Servidor de administración a través del Agente de red:
  - Configuración de las aplicaciones de Kaspersky instaladas en el dispositivo administrado: nombre y versión de la aplicación de Kaspersky; estado; estado de la protección en tiempo real; fecha y hora del último análisis del dispositivo; número de amenazas detectadas; número de objetos que no se pudieron desinfectar; disponibilidad y estado de los componentes de la aplicación; versión de las bases de datos antivirus y hora en que se actualizaron por última vez; detalles de la configuración y las tareas de las aplicaciones de Kaspersky; información sobre las claves de licencia activa y de reserva; id. y fecha de instalación de la aplicación.
  - Estadísticas de funcionamiento de cada aplicación: eventos relacionados con los cambios en el estado de los componentes de la aplicación de Kaspersky en el dispositivo administrado y con el desempeño de las tareas iniciadas por los componentes de la aplicación.
  - Estado del dispositivo definido por la aplicación de Kaspersky.
  - Etiquetas asignadas por la aplicación de Kaspersky.
- Datos contenidos en los eventos de los componentes de Kaspersky Security Center Linux y en los de las aplicaciones de Kaspersky administradas. El Agente de red transfiere datos del dispositivo al Servidor de administración.
- Datos necesarios para la integración de Kaspersky Security Center Linux con un sistema SIEM para la exportación de eventos. El usuario ingresa los datos en la interfaz de Kaspersky Security Center Web Console.
- Datos necesarios para integrar Kaspersky Security Center Linux con controladores de dominio (Active Directory, Samba, FreeIPA y ALD Pro). El usuario ingresa los datos en la interfaz de Kaspersky Security Center Web Console.
- Archivos keytab de la conexión del inicio de sesión único (SSO) de Kerberos. El usuario ingresa los datos en la interfaz de Kaspersky Security Center Web Console.
- Datos necesarios para configurar la conexión al servidor proxy para la conexión a Internet. El usuario ingresa los datos en la interfaz de Kaspersky Security Center Web Console.
- Configuración de los componentes de Kaspersky Security Center Linux y de las aplicaciones de Kaspersky administradas definidas en las directivas y en los perfiles de las directivas. El usuario ingresa datos en la interfaz de Kaspersky Security Center Web Console.
- Configuración de las tareas para los componentes de Kaspersky Security Center Linux y para las aplicaciones de Kaspersky administradas. El usuario ingresa datos en la interfaz de Kaspersky Security Center Web Console.
- Datos procesados por la función de administración de sistemas. El Agente de red transfiere la siguiente información del dispositivo al Servidor de administración:
  - Información sobre el hardware detectado en los dispositivos administrados (Registro de hardware).

    Si el Agente de red está instalado en un dispositivo con Windows, envía al Servidor de administración la siguiente información sobre el hardware del dispositivo:
    - RAM
    - Dispositivos de almacenamiento
    - Placa madre

- CPU
- Adaptadores de red
- Monitores
- Adaptador de video
- Tarjeta de sonido

Si el Agente de red está instalado en un dispositivo con Linux o macOS, envía al Servidor de administración la siguiente información sobre el hardware del dispositivo, si el sistema operativo la proporciona:

- Volumen total de la RAM
- Volumen total de los dispositivos de almacenamiento masivo
- Placa madre
- CPU
- Adaptadores de red

- Detalles de las aplicaciones y de los parches instalados en los dispositivos administrados (Registro de aplicaciones). El software se puede comparar con la información sobre los archivos ejecutables detectados en los dispositivos por la función Control de aplicaciones.
- Detalles de las vulnerabilidades presentes en el software de terceros detectado en los dispositivos administrados.
- Detalles de las actualizaciones disponibles para las aplicaciones de terceros instaladas en los dispositivos administrados.

- Datos necesarios para descargar actualizaciones en un Servidor de administración aislado a fin de reparar vulnerabilidades en el software de terceros instalado en los dispositivos administrados. El usuario introduce y transmite datos mediante la utilidad klscflag del Servidor de administración.
- Categorías de aplicaciones creadas por el usuario. El usuario ingresa datos en la interfaz de Kaspersky Security Center Web Console.
- Detalles de los archivos ejecutables detectados por la función Control de aplicaciones en los dispositivos administrados. La aplicación administrada transfiere datos del dispositivo al Servidor de administración a través del Agente de red. Encontrará una lista con todos los datos en los archivos de ayuda de la aplicación correspondiente.
- Detalles de los archivos almacenados en Copia de seguridad. La aplicación administrada transfiere datos del dispositivo al Servidor de administración a través del Agente de red. Encontrará una lista con todos los datos en los archivos de ayuda de la aplicación correspondiente.
- Detalles de los archivos puestos en cuarentena. La aplicación administrada transfiere datos del dispositivo al Servidor de administración a través del Agente de red. Encontrará una lista con todos los datos en los archivos de ayuda de la aplicación correspondiente.
- Detalles de los archivos solicitados por los especialistas de Kaspersky para un análisis detallado. La aplicación administrada transfiere datos del dispositivo al Servidor de administración a través del Agente de red. Encontrará una lista con todos los datos en los archivos de ayuda de la aplicación correspondiente.

- Detalles del estado y la activación de las reglas del Control de anomalías adaptativo. La aplicación administrada transfiere datos del dispositivo al Servidor de administración a través del Agente de red. Encontrará una lista con todos los datos en los archivos de ayuda de la aplicación correspondiente.

- Información sobre los dispositivos (unidades de memoria, herramientas de transferencia de información, herramientas para copias de información impresas y buses de conexión) que se han instalado en el dispositivo administrado o que se han conectado a este y que fueron detectados por la función Control de dispositivos. La aplicación administrada transfiere datos del dispositivo al Servidor de administración a través del Agente de red. Encontrará una lista con todos los datos en los archivos de ayuda de la aplicación correspondiente.

- Información sobre los dispositivos Windows cifrados y sobre el estado de cifrado. La aplicación administrada transfiere datos del dispositivo al Servidor de administración a través del Agente de red.

- Información sobre los errores de cifrado de datos ocurridos en los dispositivos. El cifrado lo realiza la función de cifrado de datos de las aplicaciones de Kaspersky. La aplicación administrada transfiere datos del dispositivo al Servidor de administración a través del Agente de red. Encontrará una lista con todos los datos en los archivos de ayuda de la aplicación correspondiente.

- Lista de los controladores de lógica programable (PLC) administrados. La aplicación administrada transfiere datos del dispositivo al Servidor de administración a través del Agente de red. Encontrará una lista con todos los datos en los archivos de ayuda de la aplicación correspondiente.

- Datos necesarios para la creación de una cadena de desarrollo de amenazas. La aplicación administrada transfiere datos del dispositivo al Servidor de administración a través del Agente de red. Encontrará una lista con todos los datos en los archivos de ayuda de la aplicación correspondiente.

- Información sobre los intentos de los empleados de una organización de acceder a los servicios en la nube. La aplicación administrada transfiere datos del dispositivo al Servidor de administración a través del Agente de red. Encontrará una lista con todos los datos en los archivos de ayuda de la aplicación correspondiente.

- Datos necesarios para la integración de Kaspersky Security Center con el servicio Kaspersky Managed Detection and Response (en Kaspersky Security Center Web Console, debe instalarse un complemento dedicado): token de inicio de integración, token de integración y token de sesión de usuario. El usuario ingresa el token de inicio de integración en la interfaz de Kaspersky Security Center Web Console. El servicio Kaspersky MDR transfiere el token de integración y el token de sesión de usuario a través del complemento dedicado.

- Datos necesarios para integrar Kaspersky Security Center Linux con Kaspersky Cloud Sandbox y Kaspersky Threat Intelligence Portal (requiere la instalación del complemento adecuado para Kaspersky Security Center Web Console): un token de integración, un token de autorización. El usuario ingresa un token para la integración en la interfaz de Kaspersky Security Center Web Console. Kaspersky Security Center Web Console transfiere un token de autorización en una solicitud a la API de Kaspersky Cloud Sandbox.

- Datos necesarios para integrar Kaspersky Security Center Linux con el servicio Kaspersky Automated Security Awareness Platform (KASAP): token de API para acceder a KASAP Open API, URL (un vínculo para acceder a KASAP a través de Open API).

- Detalles de los códigos de activación ingresados y de los archivos de clave. El usuario ingresa datos en la interfaz de Kaspersky Security Center Web Console.

- Cuentas de usuario: nombre, descripción, nombre completo, dirección de correo electrónico, número de teléfono principal, contraseña, clave secreta generada por el Servidor de administración y contraseña de un solo uso para la autenticación de dos factores. El usuario ingresa datos en la interfaz de Kaspersky Security Center Web Console.

- Historial de revisiones de los objetos de administración. El usuario ingresa datos en la interfaz de Kaspersky Security Center Web Console.

- Dirección IP del dispositivo en el que un usuario creó una revisión. El Servidor de administración define la dirección IP automáticamente.
- Registro de objetos de administración eliminados. El usuario ingresa datos en la interfaz de Kaspersky Security Center Web Console.
- Paquetes de instalación creados a partir del archivo y ajustes de instalación. El usuario ingresa datos en la interfaz de Kaspersky Security Center Web Console.
- Datos necesarios para mostrar comunicaciones emitidas por Kaspersky en Kaspersky Security Center Web Console. El usuario ingresa datos en la interfaz de Kaspersky Security Center Web Console.
- Datos que se necesitan para el funcionamiento de los complementos de las aplicaciones administradas en Kaspersky Security Center Web Console y que han sido almacenados por estos complementos en la base de datos del Servidor de administración como parte de sus operaciones de rutina. Encontrará una descripción de los datos y los modos de proporcionarlos en los archivos de ayuda de la aplicación correspondiente.
- Ajustes definidos por el usuario en Kaspersky Security Center Web Console: idioma de localización y tema de la interfaz; ajustes de visualización del panel Supervisión; información sobre el estado de las notificaciones (Leídas / Por leer); estado de las columnas en las hojas de cálculo (Mostrar/Ocultar); progreso en el modo de capacitación. El usuario ingresa datos en la interfaz de Kaspersky Security Center Web Console.
- Certificado utilizado para establecer una conexión segura entre los dispositivos administrados y los componentes de Kaspersky Security Center Linux. El usuario ingresa y transmite datos mediante la utilidad klsetsrvcert del Servidor de administración.
- Certificados para establecer la confianza en los recursos web internos de la organización. El usuario ingresa datos en la interfaz de Kaspersky Security Center Web Console.
- Información sobre la aceptación por parte del usuario de los términos y condiciones de los contratos legales con Kaspersky.
- Los datos del Servidor de administración que el usuario ingresa en Kaspersky Security Center Web Console o en la interfaz OpenAPI de Kaspersky Security Center.
- Cualquier dato que el usuario ingresa en la interfaz de Kaspersky Security Center Web Console.

Los datos detallados arriba pueden estar presentes en Kaspersky Security Center Linux si se aplica uno de los siguientes métodos:

- El usuario ingresa datos en la interfaz de Kaspersky Security Center Web Console.
- El Agente de red recibe los datos automáticamente desde el dispositivo y los transfiere al Servidor de administración.
- El Agente de red recibe los datos recuperados por la aplicación de Kaspersky administrada y los transfiere al Servidor de administración. Encontrará las listas de datos procesados por las aplicaciones de Kaspersky administradas en los archivos de ayuda de las aplicaciones correspondientes.
- El Servidor de administración obtiene la información sobre los dispositivos en red por sí mismo o recibe datos del Agente de red asignado para funcionar como punto de distribución.
- Los datos se transfieren del dispositivo móvil al Servidor de administración mediante el protocolo MDM de iOS.

Los datos detallados se almacenan en la base de datos del Servidor de administración. Los hashes de contraseñas se almacenan en forma cifrada.

Todos los datos procesados localmente pueden transferirse a Kaspersky solo a través de archivos de volcado, archivos de seguimiento o archivos de registro de los componentes de Kaspersky Security Center Linux (entre estos, archivos de registro creados por utilidades o programas de instalación).

Los archivos de volcado, los archivos de seguimiento y los archivos de registro de los componentes de Kaspersky Security Center Linux contienen datos arbitrarios del Servidor de administración, del Agente de red y de Kaspersky Security Center Web Console. Los archivos pueden contener datos personales o confidenciales. Los archivos de volcado, los archivos de seguimiento y los archivos de registro se almacenan en los dispositivos en un formato no cifrado. Los archivos de volcado, los archivos de seguimiento y los archivos de registro no se transfieren a Kaspersky automáticamente, pero el administrador puede transferirlos manualmente a Kaspersky si el servicio de soporte técnico los solicita para resolver problemas con el rendimiento de Kaspersky Security Center Linux.

La información obtenida está protegida por Kaspersky Lab de conformidad con los requisitos establecidos por la ley y las normas vigentes de Kaspersky Lab. Los datos se transmiten a través de canales de comunicación seguros.

Al seguir los enlaces de la Consola de administración o de Kaspersky Security Center Web Console, el usuario da su consentimiento para la transmisión automática de los siguientes datos:

- Código de Kaspersky Security Center Linux
- Versión de Kaspersky Security Center Linux
- Ubicación de Kaspersky Security Center Linux
- Id. de la licencia
- Tipo de licencia
- Indicación de si la licencia se compró a través de un socio

La lista de datos que se proporcionan a través de cada vínculo depende de la finalidad y la ubicación del vínculo.

Kaspersky utiliza los datos recopilados en forma anónima y solo con fines estadísticos generales. Las estadísticas de resumen se generan automáticamente a partir de los datos sin procesar recibidos y no contienen información personal ni otro tipo de información confidencial. A medida que se acumulan nuevos datos, los datos más antiguos se eliminan (una vez al año). Las estadísticas de resumen se almacenan indefinidamente.

Acerca de la suscripción

Suscripción a Kaspersky Security Center Linux es una solicitud para usar la aplicación con las opciones seleccionadas (fecha de vencimiento de la suscripción, número de dispositivos protegidos). Puede registrar su suscripción a Kaspersky Security Center Linux con su proveedor de servicios (por ejemplo, su proveedor de Internet). Una suscripción se puede renovar manualmente o automáticamente; también se puede cancelar.

Una suscripción puede ser limitada (puede tener un límite de un año, por ejemplo) o puede ser ilimitada, en cuyo caso no tendrá fecha de caducidad. Para continuar usando Kaspersky Security Center tras el vencimiento de una suscripción limitada, debe renovar la suscripción. Una suscripción ilimitada se renueva automáticamente si el proveedor de servicios ha recibido a término y por adelantado el pago correspondiente.

Cuando una suscripción limitada caduca, la aplicación puede seguir funcionando por un tiempo adicional, durante un período de gracia. Este período puede aprovecharse para renovar la suscripción. El proveedor de servicios define la disponibilidad y la duración del período de gracia.

Para usar Kaspersky Security Center Linux con suscripción, debe aplicar el código de activación que le envía el proveedor de servicios.

Puede aplicar otro código de activación para Kaspersky Security Center Linux únicamente después del vencimiento de la suscripción o cuando la cancela.

El conjunto de acciones disponibles para administrar una suscripción puede variar según el proveedor de servicios. Su proveedor de servicios podría no ofrecerle un período de gracia para renovar la suscripción; en tal caso, la aplicación dejará de funcionar.

Los códigos de activación adquiridos por suscripción no se pueden usar para activar versiones anteriores de Kaspersky Security Center.

Al usar la aplicación con suscripción, Kaspersky Security Center Linux automáticamente intenta acceder al servidor de activación en los intervalos de tiempo especificados hasta el vencimiento de la suscripción. Si los servidores DNS configurados en el sistema no permiten acceder al servidor de Kaspersky, la aplicación utiliza servidores DNS públicos. Si necesita renovar su suscripción, puede hacerlo en el sitio web de su proveedor de servicios.

Activación de Kaspersky Security Center Linux

Puede activar Kaspersky Security Center Linux para usar su funcionalidad adicional. Hay dos formas de realizar esta tarea: utilizar el Asistente de inicio rápido del Servidor de administración o las propiedades del Servidor de administración.

Para activar Kaspersky Security Center Linux, haga lo quiere:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, vaya a la sección **Claves de licencia**.

3. En **Licencia actual**, haga clic en el botón **Seleccionar**.

4. En la ventana que se abre, seleccione la clave de licencia que desea usar para activar Kaspersky Security Center Linux. Si la clave de licencia no está en la lista, haga clic en el botón **Agregar nueva clave de licencia** y, luego, especifique una nueva clave de licencia.

5. Si es necesario, también puede agregar una clave de licencia de reserva. Para hacer esto, en **Clave de licencia de reserva**, haga clic en el botón **Seleccionar** y, luego, seleccione una clave de licencia existente o agregue una nueva. Tenga en cuenta que no puede agregar una clave de licencia de reserva si no hay una clave de licencia activa.

6. Haga clic en el botón **Guardar**.

Licencias de aplicaciones administradas de Kaspersky

Esta sección describe las funciones de Kaspersky Security Center relacionadas con el manejo de claves de licencia de las aplicaciones administradas de Kaspersky.

Kaspersky Security Center Linux le permite realizar una distribución centralizada de las claves de licencia de las aplicaciones de Kaspersky en dispositivos cliente, supervisar su uso y renovar las licencias.

Al agregar una clave de licencia mediante Kaspersky Security Center, las propiedades de la clave de licencia se guardan en el Servidor de administración. Los parámetros definidos en las propiedades de las claves de licencia permiten que la aplicación genere un informe sobre el uso de las claves de licencia, mantenga al administrador al tanto de la caducidad de las licencias y le informe si se infringe una restricción dispuesta por una licencia. Puede configurar notificaciones sobre el uso de las claves de licencia en los ajustes del Servidor de administración.

Licencias de aplicaciones administradas

Las aplicaciones de Kaspersky instaladas en los dispositivos administrados se deben licenciar aplicando un archivo de clave o código de activación a cada una de las aplicaciones. Los archivos de clave o códigos de activación se pueden desplegar de las siguientes formas:

- Despliegue automático
- Usar el paquete de instalación de la aplicación administrada
- La tarea Agregar clave de licencia para una aplicación administrada
- Activar la aplicación administrada manualmente

Puede agregar una nueva clave de licencia activa o de reserva mediante cualquiera de los métodos enumerados anteriormente. Una aplicación de Kaspersky utiliza una clave activa en el momento actual y almacena una clave de reserva para aplicar después de que caduque la clave activa. La aplicación para la que agrega una clave de licencia define si la clave está activa o si es de reserva. La definición de la clave no depende del método que utilice para agregar una nueva clave de licencia.

Despliegue automático

Si usa diferentes aplicaciones administradas y tiene que desplegar un archivo de clave o un código de activación específicos en los dispositivos, opte por otras formas de desplegar ese código de activación o archivo de clave.

Kaspersky Security Center le permite desplegar las claves de licencia disponibles a los dispositivos automáticamente. Suponga, por ejemplo, que tiene tres claves de licencia en el repositorio del Servidor de administración. Habilitó la opción **Clave de licencia distribuida automáticamente** para las tres claves de licencia. Los dispositivos de su organización tienen instalada una aplicación de seguridad de Kaspersky (por ejemplo, Kaspersky Endpoint Security for Linux). Se detecta un nuevo dispositivo al que se debe desplegar una clave de licencia. La aplicación determina, por ejemplo, que dos de las claves de licencia del repositorio se pueden aplicar al dispositivo: una clave de licencia llamada *Key_1* y una clave de licencia llamada *Key_2*. Una de estas claves de licencia se despliega al dispositivo. En este caso, no se puede predecir cuál de las dos claves de licencia se desplegará en el dispositivo porque el despliegue automático de claves de licencia no proporciona ninguna actividad de administrador.

Cuando se despliega una clave de licencia, los dispositivos se vuelven a contar para esa clave de licencia. Debe asegurarse de que la cantidad de dispositivos a los que se desplegó la clave de licencia no exceda el límite de la licencia. Si la cantidad de dispositivos excede el límite de la licencia, a todos los dispositivos que no estaban cubiertos por la licencia se les asignará el estado *Crítico*.

Antes del despliegue, se deben agregar el archivo de clave o el código de activación al repositorio del Servidor de administración.

Instrucciones:

- Agregar una clave de licencia al repositorio del Servidor de administración
- Distribución automática de una clave de licencia

Tenga en cuenta que una clave de licencia distribuida automáticamente podría no aparecer en el repositorio del Servidor de administración virtual en los siguientes casos:

- La clave de licencia no es válida para la aplicación.
- El Servidor de administración virtual no tiene ningún dispositivo administrado.
- La clave de licencia ya ha sido utilizada para dispositivos administrados asociados a otro Servidor de administración virtual y se ha alcanzado el límite a la cantidad de dispositivos.

Adición de un archivo de clave o un código de activación al paquete de instalación de una aplicación administrada

Por motivos de seguridad, no se recomienda utilizar esta opción. El archivo de clave o el código de activación añadidos a un paquete de instalación pueden verse comprometidos.

Si instala una aplicación administrada con un paquete de instalación, puede especificar un código de activación o un archivo de clave en este paquete de instalación o en la directiva de la aplicación. En ese caso, la clave de licencia se desplegará a los dispositivos administrados cuando estos se sincronicen nuevamente con el Servidor de administración.

Instrucciones: Agregar una clave de licencia a un paquete de instalación

Despliegue con la tarea "Agregar clave de licencia" para una aplicación administrada

Si opta por usar la tarea "Agregar clave de licencia" para una aplicación administrada, seleccione la clave que quiera desplegar a los dispositivos y, luego, elija los dispositivos utilizando cualquier método que le resulte conveniente (por ejemplo, elija un grupo de administración o una selección de dispositivos).

Antes del despliegue, se deben agregar el archivo de clave o el código de activación al repositorio del Servidor de administración.

Instrucciones:

- Agregar una clave de licencia al repositorio del Servidor de administración
- Distribución de claves de licencia a dispositivos cliente

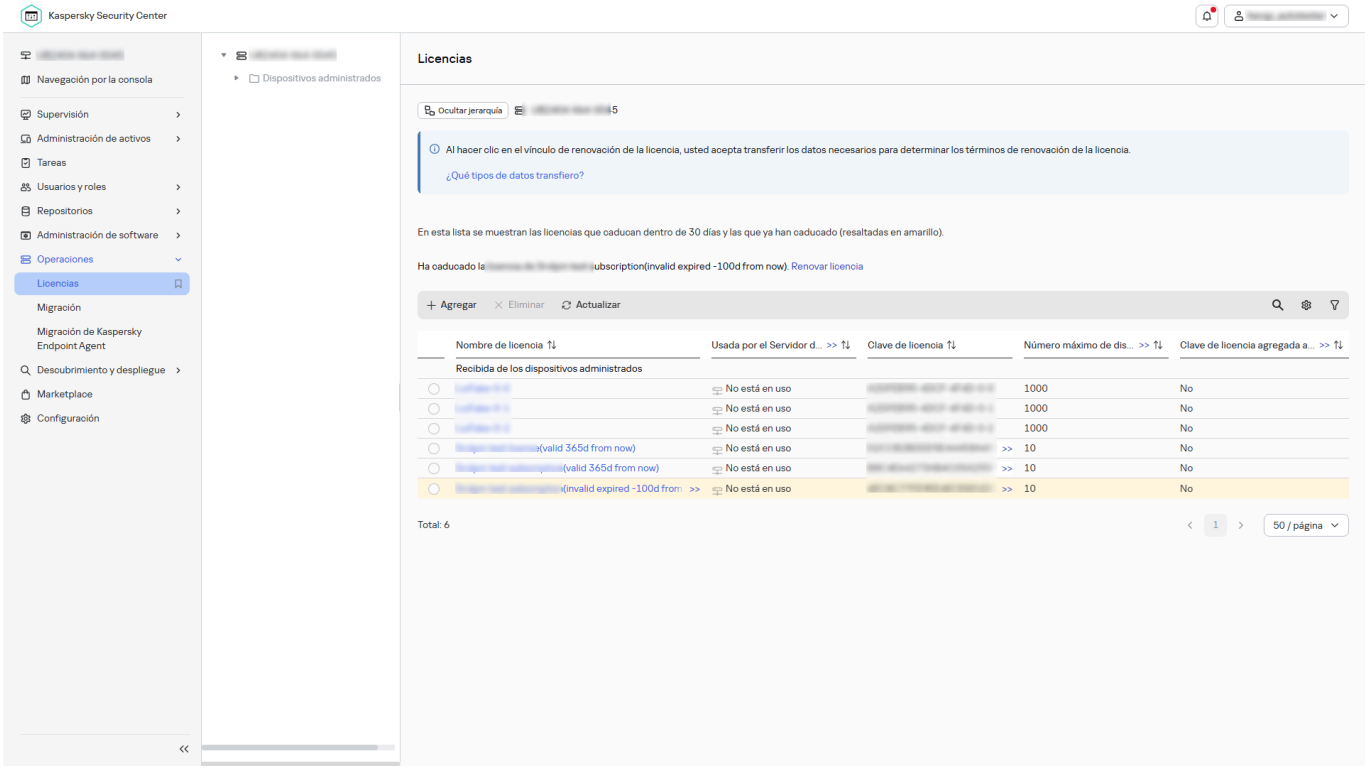
Agregar un código de activación o un archivo de clave en los dispositivos manualmente

Puede activar la aplicación de Kaspersky en forma local, usando las herramientas disponibles en la interfaz de la aplicación. Consulte la documentación de la aplicación instalada.

Agregar una clave de licencia al repositorio del Servidor de administración

Para agregar una clave de licencia al repositorio del Servidor de administración:

1. En el menú principal, vaya a **Operaciones** → **Licencias**.



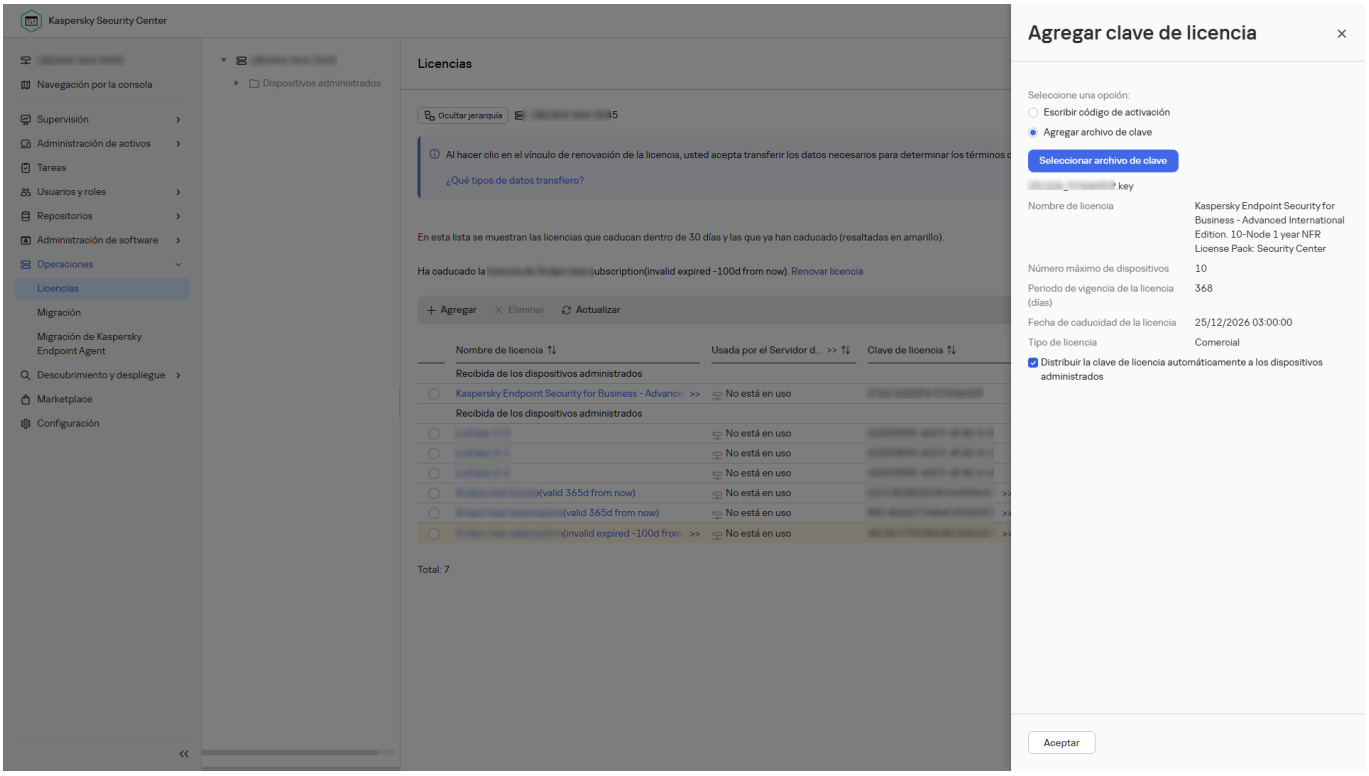
Lista de claves de licencia de Kaspersky agregadas

2. Haga clic en **Agregar**.

3. Elija lo que quiera agregar:

- **Agregar archivo de clave**

  Haga clic en el botón **Seleccionar archivo de clave** y vaya al archivo de clave que desea agregar.



Agregar una clave de licencia aplicando un archivo de clave

- **Escribir código de activación**

  Introduzca el código de activación en el campo de texto y haga clic en el botón **Enviar**.

4. Haga clic en el botón **Cerrar**.

Se agrega la clave de licencia (o las claves de licencia) al repositorio del Servidor de administración.

Distribución de claves de licencia a dispositivos cliente

Kaspersky Security Center Web Console permite distribuir una clave de licencia a los dispositivos cliente automáticamente o mediante la tarea de **Activación de la aplicación**. Con la tarea, puede distribuir claves a un grupo de dispositivos específico. Durante la distribución de una clave de licencia mediante una tarea, no se tiene en cuenta el límite de obtención de licencias en el número de dispositivos. Use la distribución automática de claves para detener la distribución de una clave de licencia automáticamente cuando se alcance el límite de obtención de licencias.

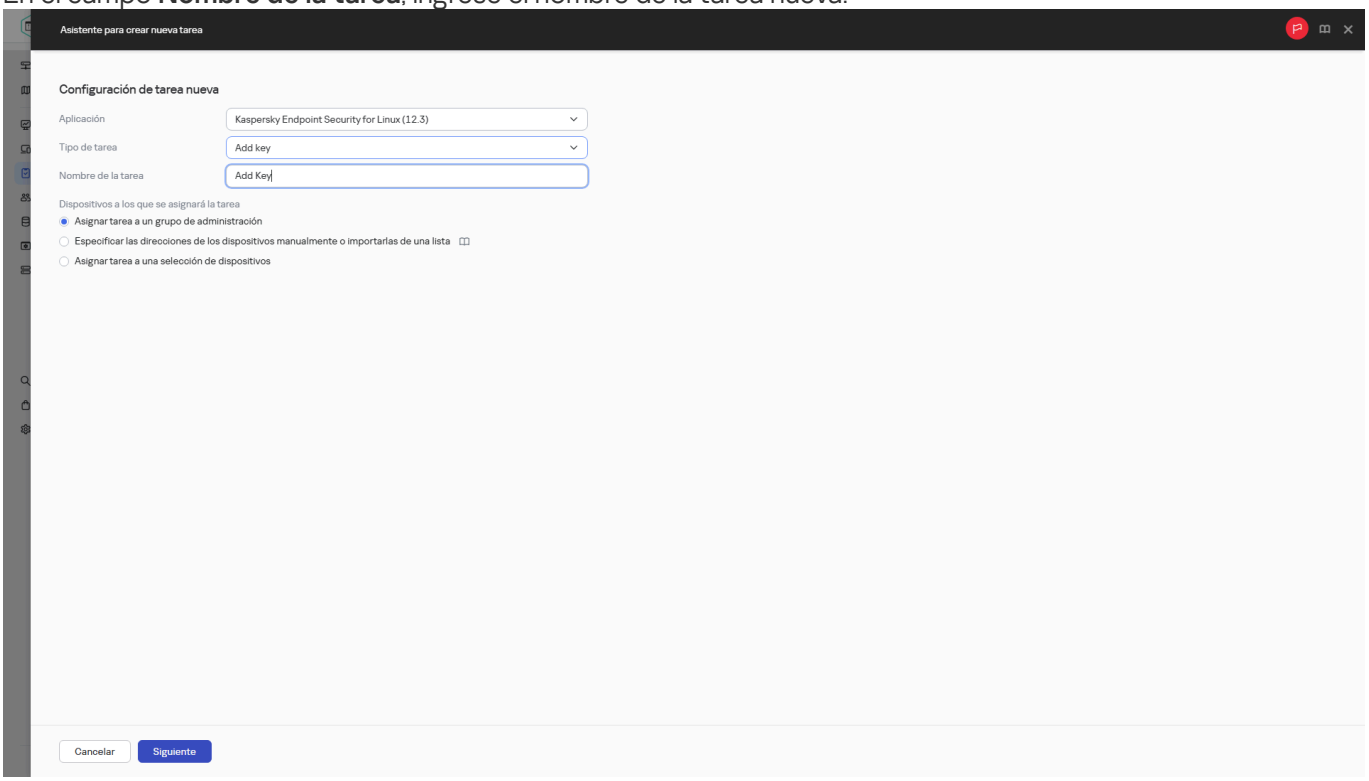
Si habilita la opción Distribución automática de una clave de licencia, no cree una tarea de **Activación de la aplicación** para distribuir la clave a los dispositivos cliente. De lo contrario, la carga en el Servidor de administración aumentará debido a la frecuencia de la sincronización.

Antes de realizar la distribución, agregue la clave de licencia al repositorio del Servidor de administración.

*Para distribuir una clave de licencia a los dispositivos cliente con la tarea de **Activación de la aplicación**:*

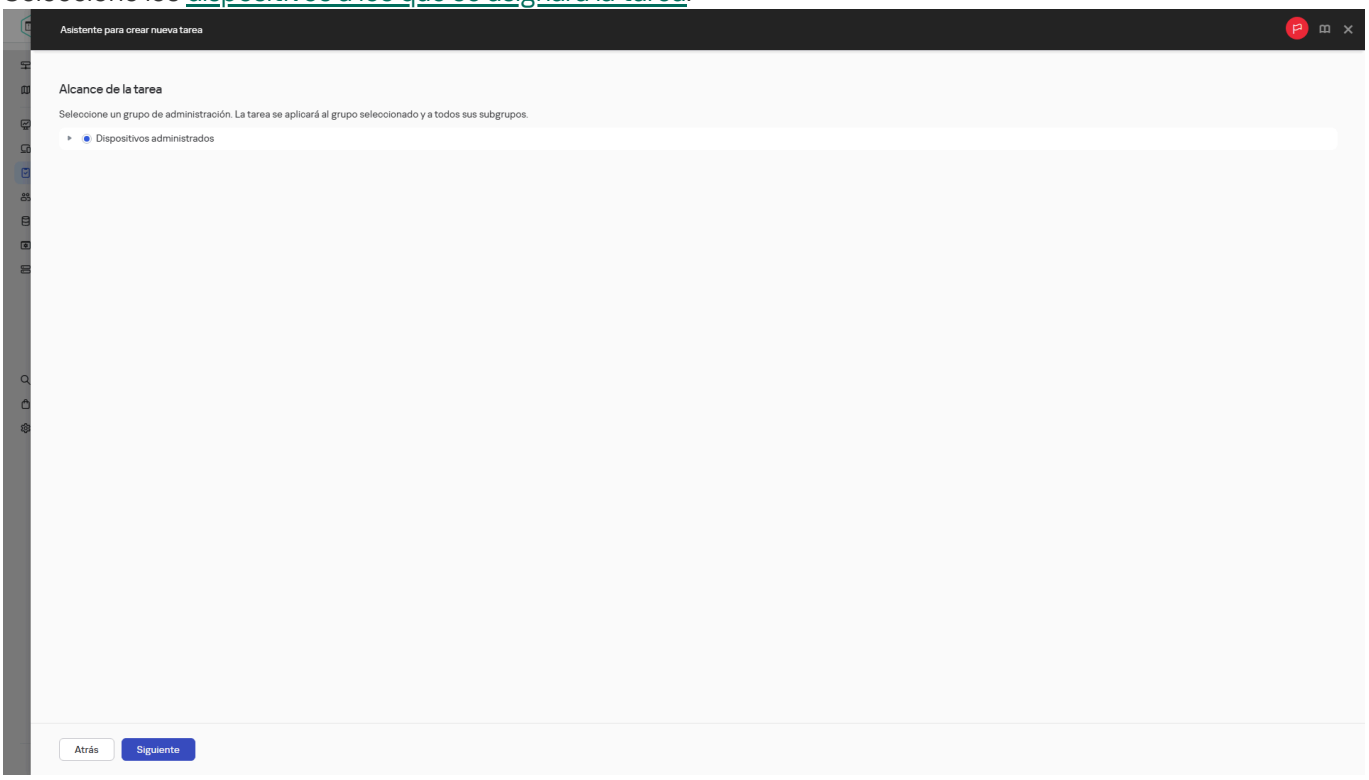
1. En el menú principal, vaya a **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el **Asistente para crear nueva tarea**. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.
3. En la lista desplegable **Aplicación**, seleccione la aplicación para la que desee agregar una clave de licencia.
4. En la lista **Tipo de tarea**, seleccione la tarea de **Activación de la aplicación**.
5. En el campo **Nombre de la tarea**, ingrese el nombre de la tarea nueva.



Creación de una tarea Agregar clave

6. Seleccione los dispositivos a los que se asignará la tarea.



Especificar el alcance de la tarea

7. En el paso **Seleccionar una clave de licencia** del asistente, haga clic en el vínculo **Agregar clave** para agregar la clave de licencia.

8. En el panel para agregar claves, agregue la clave de licencia mediante una de las siguientes opciones:

> Debe agregar la clave de licencia solo si no la agregó al repositorio del Servidor de administración antes de crear la tarea de **Activación de la aplicación**.

- Seleccione la opción **Escribir código de activación** para ingresar un código de activación y luego haga lo siguiente:

  a. Especifique el código de activación y haga clic en el botón **Enviar**.

  La información sobre la clave de licencia aparece en el panel para agregar claves.

  b. Haga clic en el botón **Guardar**.

  > Si desea distribuir la clave de licencia a los dispositivos administrados de forma automática, habilite la opción **Distribuir la clave de licencia automáticamente a los dispositivos administrados**.

  Se cerrará el panel para agregar claves.

- Seleccione la opción **Agregar archivo de clave** para agregar un archivo de clave y luego haga lo siguiente:

  a. Haga clic en el botón **Seleccionar archivo de clave**.

  b. En la ventana que se abre, seleccione un archivo de clave y haga clic en el botón **Abrir**.

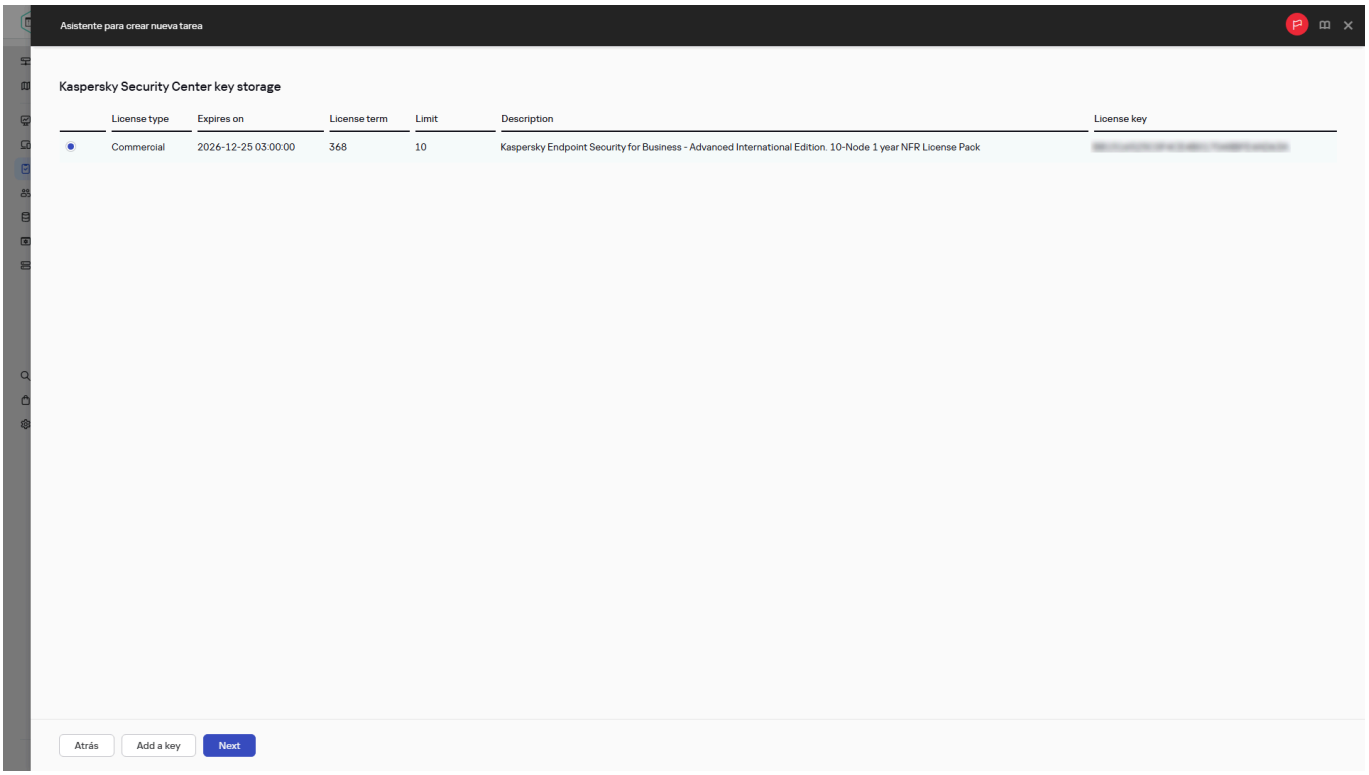
  La información sobre la clave de licencia aparecerá en el panel para agregar claves de licencia.

c. Haga clic en el botón **Guardar**.

> Si desea distribuir la clave de licencia a los dispositivos administrados de forma automática, habilite la opción **Distribuir la clave de licencia automáticamente a los dispositivos administrados**.

Se cerrará el panel para agregar claves.

9. Seleccione la clave de licencia desde la tabla de claves.

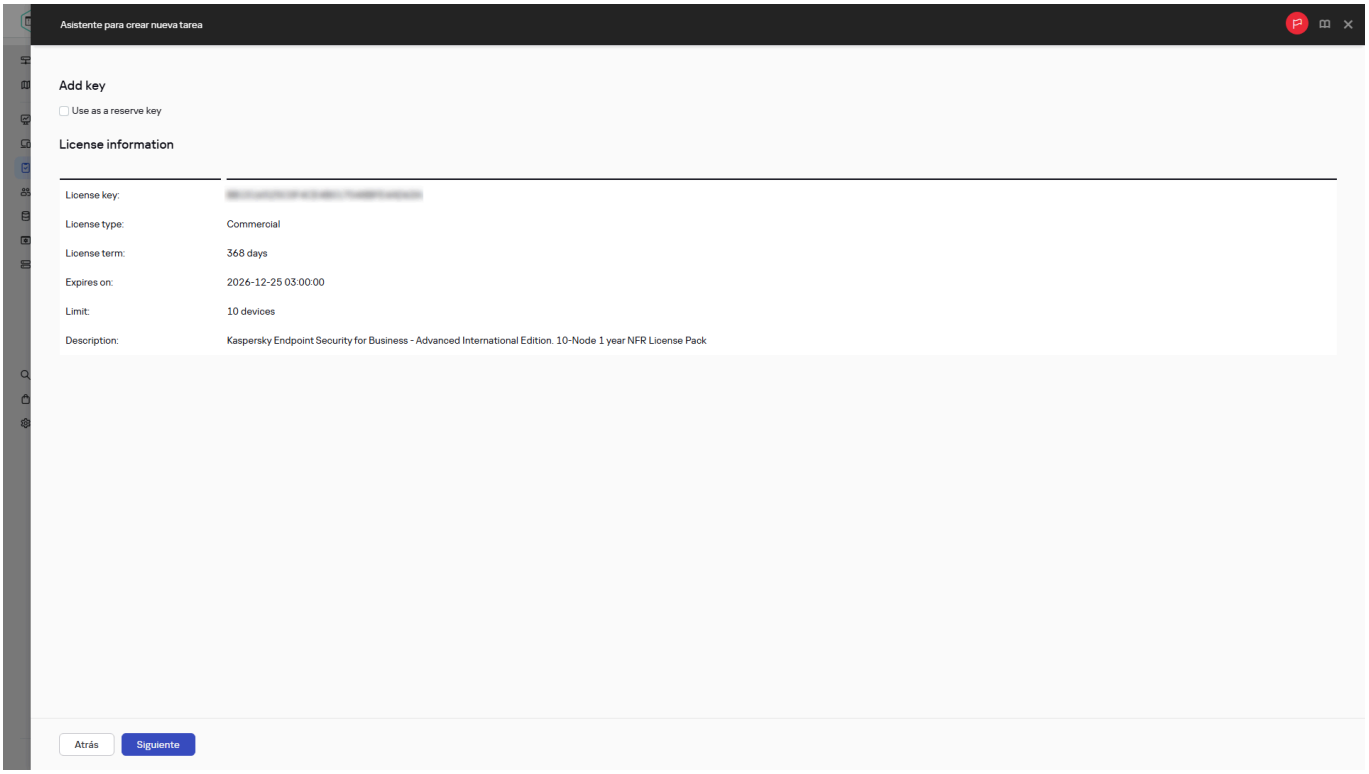


Seleccionar la clave de licencia

10. En el paso **Información de licencia** del asistente, desmarque la casilla **Usar como clave de reserva** predeterminada si desea reemplazar la clave de licencia activa.

    Por ejemplo, puede ser necesario cuando la organización cambia y se necesita la clave de otra organización en el dispositivo o si la clave se volvió a emitir y la nueva licencia caduca antes que la licencia actual. Para evitar errores, debe desmarcar la casilla **Usar como clave de reserva**.

Si desea obtener más información sobre las cuestiones que pueden surgir al agregar una clave de licencia a Kaspersky Security Center y cómo resolverlas, consulte la Base de conocimientos de Kaspersky Security Center.



Especificar la clave de licencia de reserva

11. En el paso **Finalizar la creación de la tarea** del asistente, habilite la opción **Abrir los detalles de la tarea cuando se complete la creación** para modificar la configuración predeterminada de la tarea.

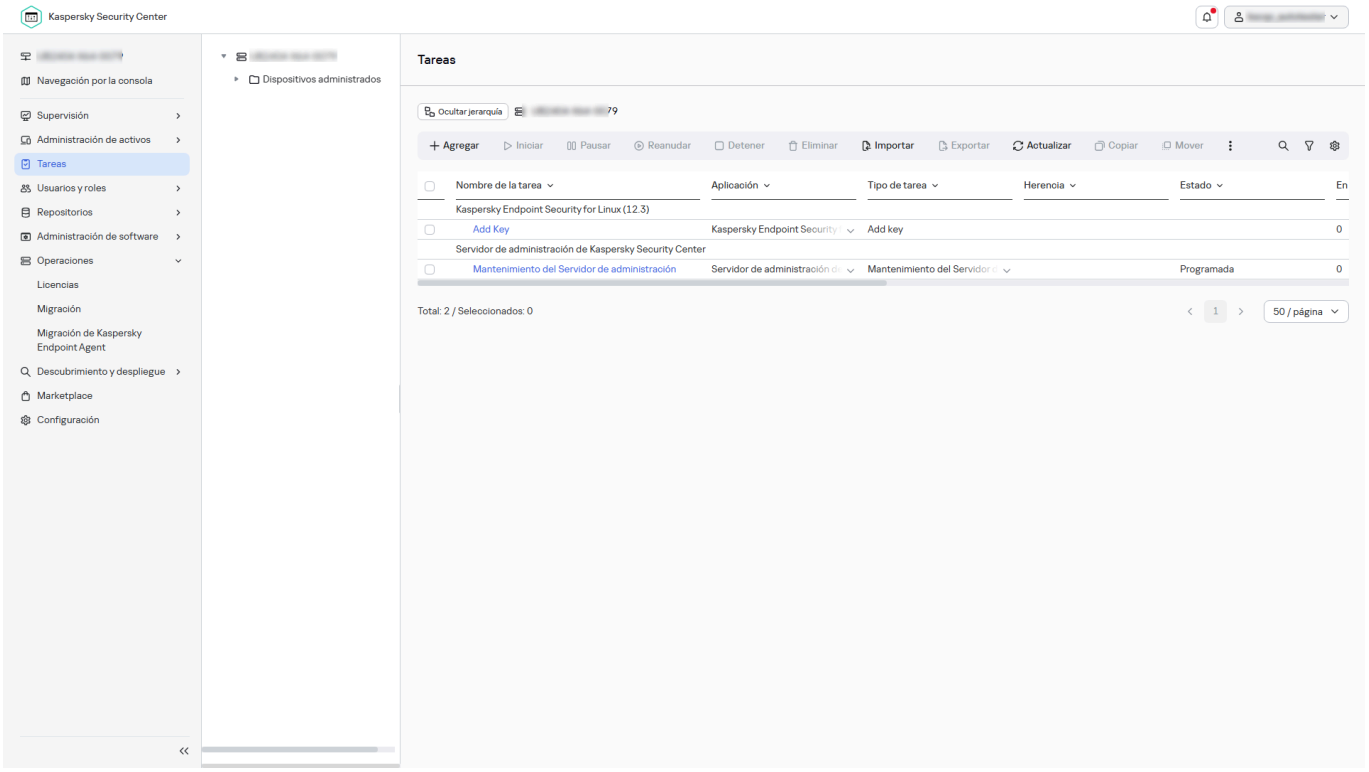
    Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Podrá modificarla más adelante.

12. Haga clic en el botón **Finalizar**.

    El asistente creará la tarea. Si habilitó la opción **Abrir los detalles de la tarea cuando se complete la creación**, se abrirá automáticamente la ventana de propiedades de la tarea. En esta ventana, puede definir la configuración general de la tarea y, si es necesario, cambiar los ajustes establecidos durante la creación de la tarea.

    También puede abrir la ventana de propiedades de la tarea haciendo clic en el nombre de la tarea creada en la lista de tareas.

La tarea se creará, configurará y se mostrará en la lista de tareas.



La lista de tareas

13. Para ejecutar la tarea, selecciónela en la lista de tareas y haga clic en el botón **Iniciar**.

    También puede programar el inicio de la tarea en la pestaña **Programación**, en la ventana de propiedades de la tarea.

    Para obtener una descripción detallada de la configuración de inicio programado, consulte la configuración general de la tarea.

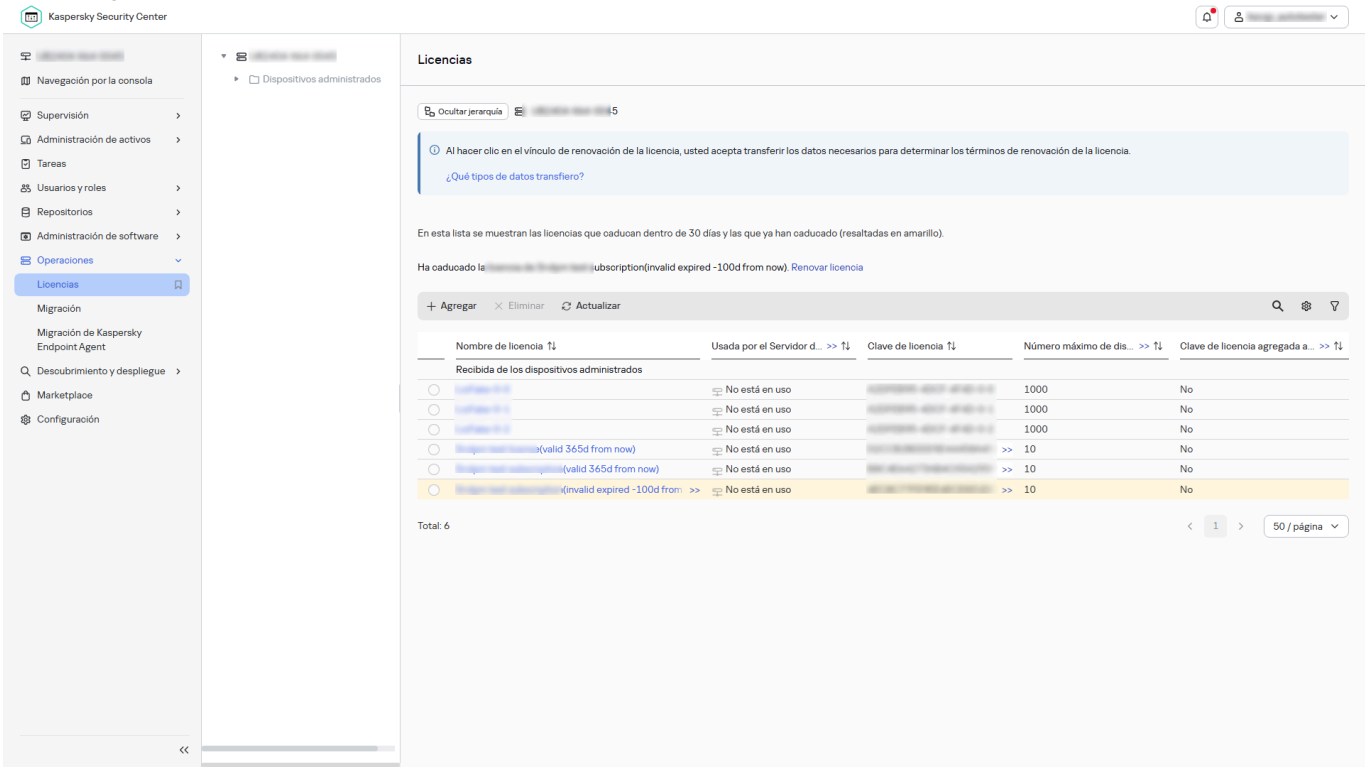
Cuando se complete la tarea, la clave de licencia se desplegará a los dispositivos seleccionados.

Distribución automática de una clave de licencia

Kaspersky Security Center Linux permite la distribución automática de claves de licencia a dispositivos administrados si están ubicadas en el repositorio de claves de licencia del Servidor de administración.

Para distribuir una clave de licencia en forma automática a los dispositivos administrados:

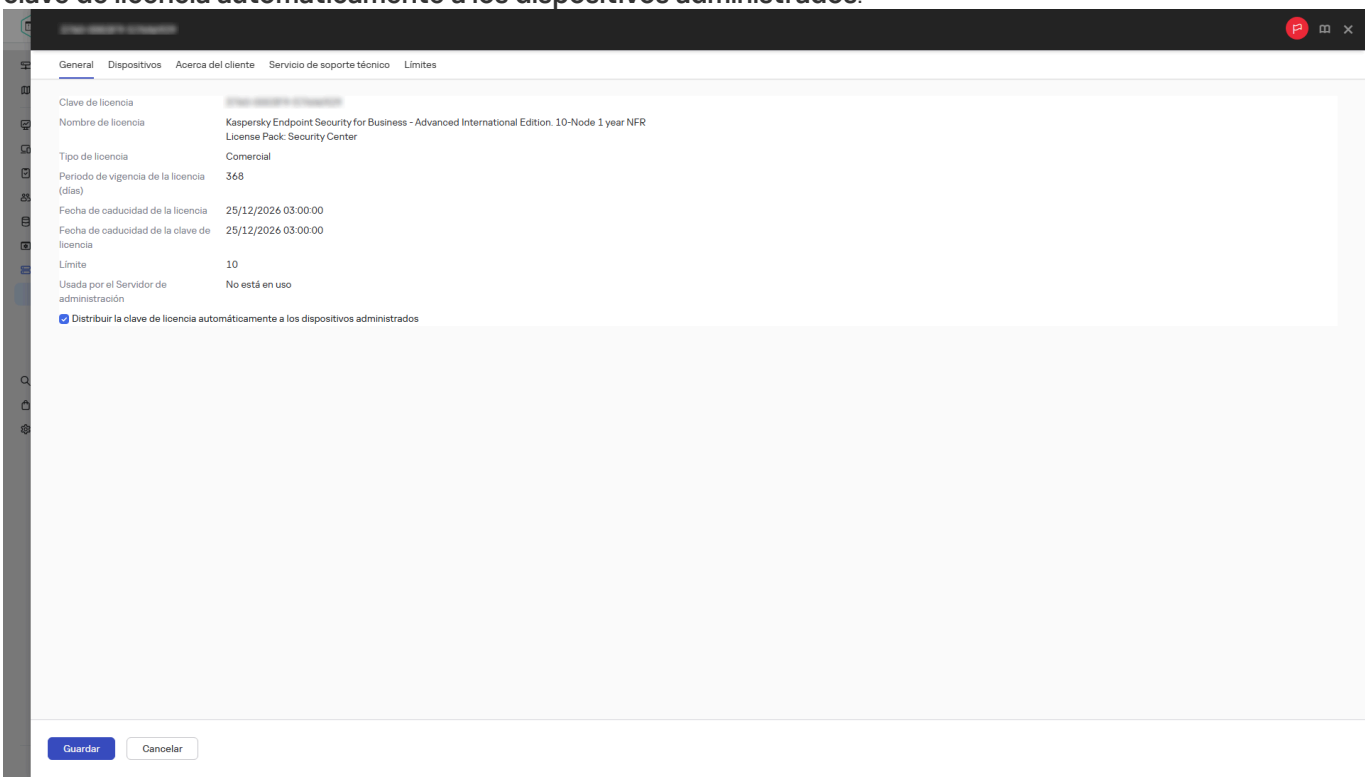
1. Vaya a **Operaciones → Licencias → Licencias**.



La lista de licencias

2. Haga clic en el nombre de la clave de licencia que quiera que se distribuya a los dispositivos automáticamente.

3. En la ventana de propiedades de la clave de licencia que se abre, active la casilla de verificación **Distribuir la clave de licencia automáticamente a los dispositivos administrados**.



La ventana de propiedades de la clave de licencia

4. Haga clic en el botón **Guardar**.

La clave de licencia se distribuirá automáticamente a todos los dispositivos compatibles.

La distribución de claves de licencia se realiza a través del Agente de red. No se crean tareas de distribución de clave de licencia para la aplicación.

Durante la distribución automática de una clave de licencia se tiene en cuenta el límite de obtención de licencias en el número de dispositivos. El límite está definido en las propiedades de la clave de licencia. Cuando se llega al límite de dispositivos, el proceso de distribución de esta clave de licencia en dispositivos se detiene automáticamente.

Tenga en cuenta que una clave de licencia distribuida automáticamente podría no aparecer en el repositorio del Servidor de administración virtual en los siguientes casos:

- La clave de licencia no es válida para la aplicación.
- El Servidor de administración virtual no tiene ningún dispositivo administrado.
- La clave de licencia ya ha sido utilizada para dispositivos administrados asociados a otro Servidor de administración virtual y se ha alcanzado el límite a la cantidad de dispositivos.

El Servidor de administración virtual distribuye automáticamente las claves de licencia desde su repositorio y desde el repositorio del Servidor de administración. Le sugerimos que atienda a las siguientes recomendaciones:

- Use la tarea *Agregar clave de licencia* para seleccionar la clave de licencia que se debe distribuir a los dispositivos.
- Evite deshabilitar la opción **Permitir el despliegue automático de claves de licencia de este Servidor de administración virtual a sus dispositivos** en la configuración del Servidor de administración virtual. De lo contrario, el Servidor de administración virtual no distribuirá claves de licencia a los dispositivos, incluidas las claves de licencia del repositorio del Servidor de administración.

Si selecciona la casilla de verificación **Distribuir la clave de licencia automáticamente a los dispositivos administrados** en la ventana de propiedades de la clave de licencia, se distribuye una clave de licencia en su red inmediatamente. Si no selecciona esta opción, puede distribuir una clave de licencia manualmente más adelante con una tarea.

La distribución automática de las claves de licencia configuradas en el Servidor de administración principal no se extiende a los dispositivos administrados por Servidores de administración secundarios no virtuales.

Visualización de información sobre las claves de licencia en uso

Para ver la lista de las claves de licencia agregadas al repositorio del Servidor de administración:

Vaya a **Operaciones** → **Licencias** → **Licencias**.

Se mostrará una lista con los archivos de clave y los códigos de activación que se hayan agregado al repositorio del Servidor de administración.

Para ver información detallada sobre una clave de licencia:

1. Vaya a **Operaciones** → **Licencias** → **Licencias**.
2. Haga clic en el nombre de la clave de licencia de su interés.

Se abre una ventana con las propiedades de la clave de licencia. En la ventana, puede ver lo siguiente:

- En la pestaña **General**, los datos generales de la clave de licencia.
- En la pestaña **Dispositivos**, la lista de dispositivos cliente en los que la clave de licencia se utilizó para activar la aplicación de Kaspersky instalada.
- En la pestaña **Límites**, la lista de límites de la licencia.

  Si activó el Servidor de administración con la licencia de Kaspersky Next XDR Optimum, la pestaña **Límites** muestra el campo **XDR-O** con el valor **Habilitado**.

Para ver qué claves de licencia se despliegan en un dispositivo cliente específico:

1. En el menú principal, vaya a **Administración de activos** → **Dispositivos administrados**.
2. Haga clic en el nombre del dispositivo pertinente.
3. En la ventana que se abre, que contendrá las propiedades del dispositivo, elija la pestaña **Aplicaciones**.

4. Haga clic en el nombre de la aplicación para la que desea ver la información sobre la clave de licencia.

5. En la ventana de propiedades de la aplicación que se abre, seleccione la pestaña **General** y, luego, abra la sección **Licencia**.

Se muestra la información principal sobre las claves de licencia de reserva y activas.

Para definir la configuración actualizada de las claves de licencia del Servidor de administración virtual, este envía una solicitud a los servidores de activación de Kaspersky como mínimo una vez al día. Si los servidores DNS configurados en el sistema no permiten acceder a los servidores de Kaspersky, la aplicación utiliza servidores DNS públicos.

Eventos sobre límites de licencia superados

Kaspersky Security Center Linux le permite obtener información sobre eventos cuando las aplicaciones de Kaspersky instaladas en dispositivos cliente superan ciertos límites de licencia.

El nivel de importancia de estos eventos cuando se supera un límite de licencia se define según las siguientes reglas:

- Cuando se ha utilizado entre un 90 % y un 100 % del número total de unidades cubiertas por la licencia, el evento se publica con el nivel de importancia **Información**.
- Cuando se ha utilizado entre un 100 % y un 110 % del número total de unidades cubiertas por la licencia, el evento se publica con el nivel de importancia **Advertencia**.
- Cuando se ha utilizado más de un 110 % del número total de unidades cubiertas por la licencia, el evento se publica con el nivel de importancia **Evento crítico**.

Eliminar una clave de licencia del repositorio

Cuando elimina la clave de licencia activa desplegada en un dispositivo administrado, la aplicación continúa trabajando en el dispositivo administrado.

Para eliminar un archivo de clave o un código de activación del repositorio del Servidor de administración:

1. Verifique que el Servidor de administración no esté utilizando el archivo de clave o el código de activación que desee eliminar. Si el Servidor de administración está utilizando ese archivo o código, no lo podrá eliminar. Para ejecutar la prueba:

   a. En el menú principal, haga clic en el nombre del Servidor de administración.

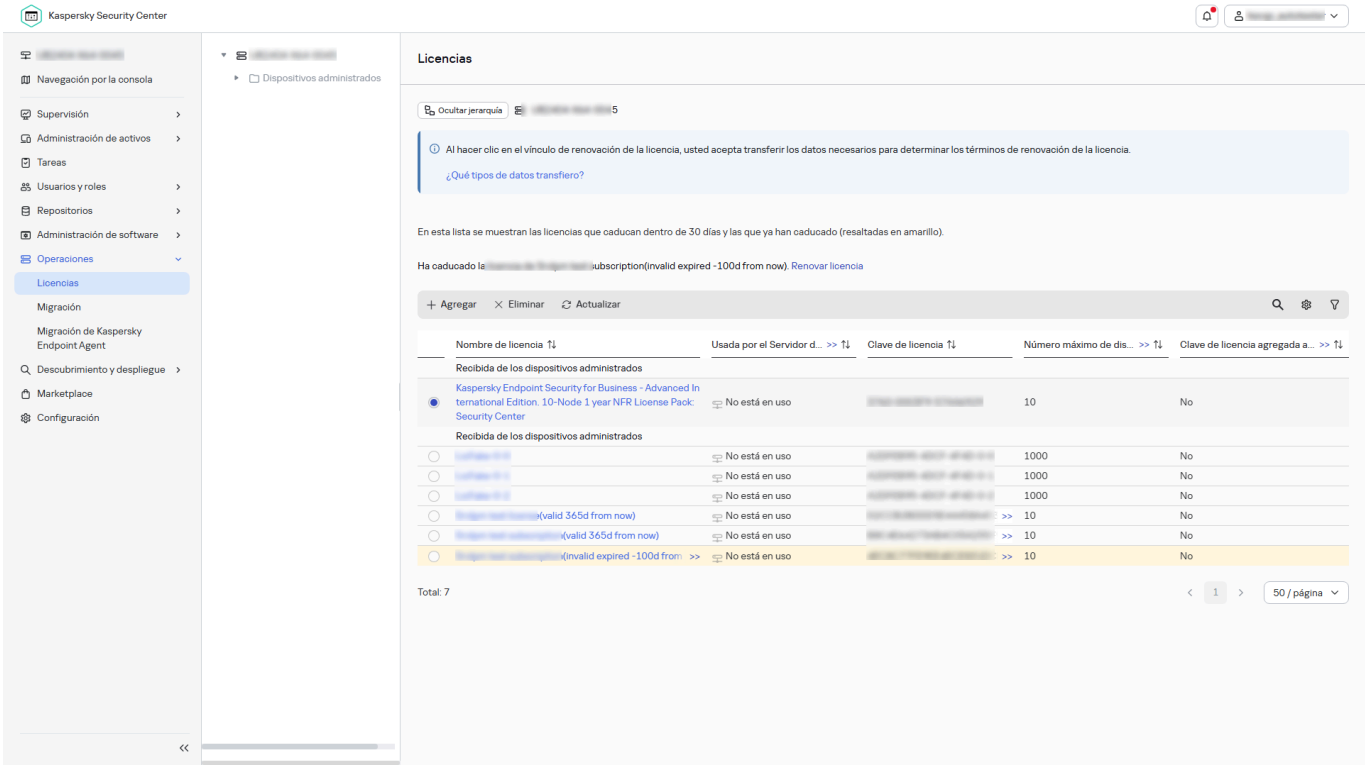
      Se abre la ventana Propiedades del Servidor de administración.

b. En la pestaña **General**, vaya a la sección **Claves de licencia**.

c. Si ve el archivo de clave o el código de activación que desea eliminar en esta sección, haga clic en el botón **Eliminar clave de licencia activa** y confirme la operación. El Servidor de administración dejará de utilizar la clave de licencia eliminada, pero no se la borrará del repositorio del Servidor de administración. Si el archivo de clave o el código de activación que desea eliminar no aparecen en esta sección, sabrá que no son el archivo o código utilizados por el Servidor de administración.

2. En el menú principal, vaya a **Operaciones** → **Licencias** → **Licencias**.

3. Seleccione el archivo de clave o el código de activación pertinentes y haga clic en el botón **Eliminar**.



La lista de licencias

El archivo de clave o el código de activación que haya seleccionado se eliminará del repositorio.

Puede agregar nuevamente la clave de licencia eliminada o puede agregar una nueva.

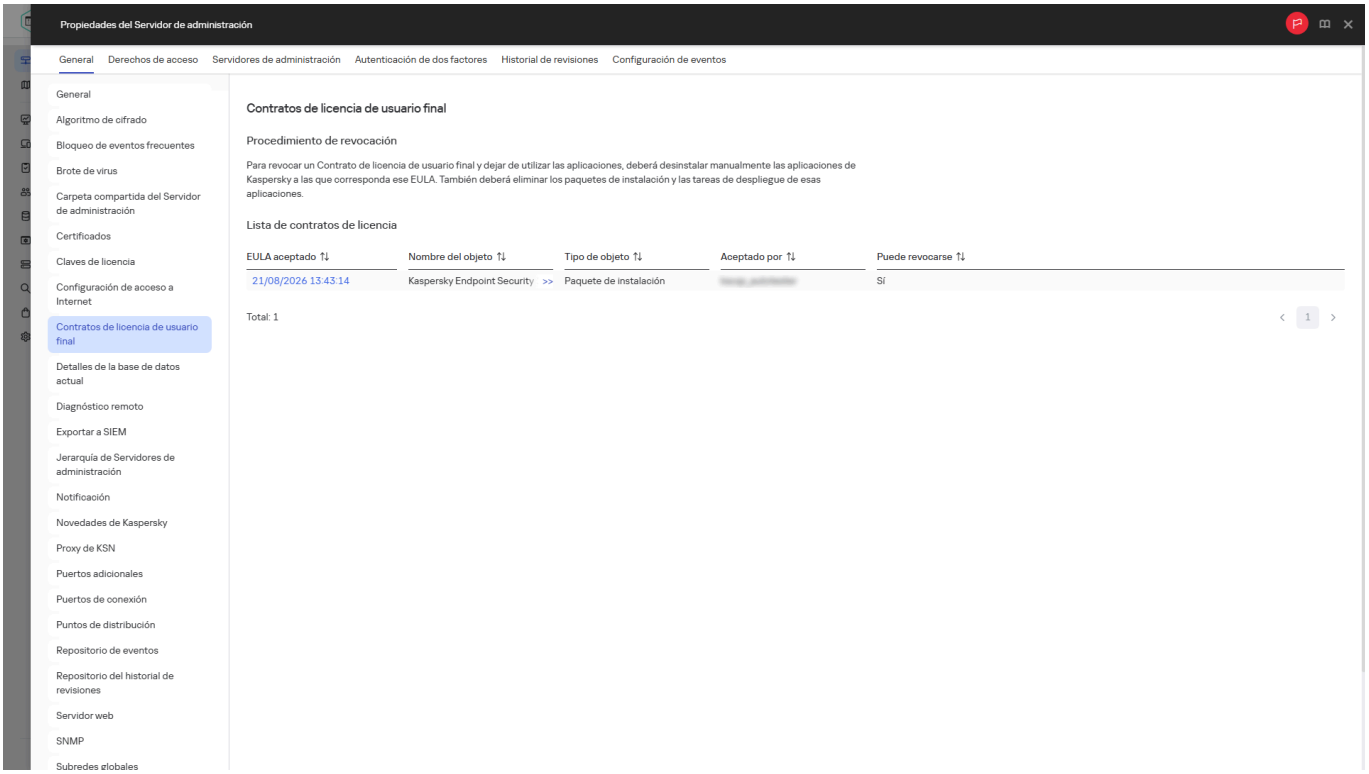
Revocar la aceptación de un Contrato de licencia de usuario final

Si ya no necesita proteger un dispositivo cliente, puede revocar el Contrato de licencia de usuario final (EULA) vinculado a la aplicación de Kaspersky administrada que ese dispositivo tenga instalada. Antes de revocar un EULA, deberá desinstalar la aplicación a la que el contrato esté asociado.

Para revocar un EULA vinculado a una aplicación de Kaspersky administrada:

1. Abra la ventana de propiedades del Servidor de administración y, en la pestaña **General**, seleccione la sección **Contratos de licencia de usuario final**.

Se muestra una lista con los EULA aceptados tras la creación de paquetes de instalación, la instalación sin problemas de actualizaciones o el despliegue de Kaspersky Security para dispositivos móviles.



La lista de los EULA

2. En la lista, seleccione el EULA que desee revocar.

   Puede ver las siguientes propiedades del EULA:

   - La fecha en la que se aceptó el EULA.
   - El nombre del usuario que aceptó el EULA.

3. Haga clic en la fecha de aceptación de un EULA para abrir una ventana de propiedades con la siguiente información:

   - El nombre del usuario que aceptó el EULA.
   - La fecha en la que se aceptó el EULA.
   - El identificador único (UID) del EULA.
   - El texto completo del EULA.
   - La lista de objetos vinculados al EULA (paquetes de instalación, actualizaciones transparentes, apps móviles). Junto al nombre de cada objeto, verá de qué tipo de objeto se trata.

4. En la parte izquierda de la ventana de propiedades del EULA, haga clic en el botón **Revocar el Contrato de licencia**.

   De existir algún objeto que impida revocar el EULA (algún paquete de instalación con su respectiva tarea), verá una notificación. No podrá revocar el contrato hasta que haya eliminado el objeto problemático.

En la ventana que se abre, se le informa que primero debe desinstalar la aplicación de Kaspersky correspondiente al EULA.

5. Haga clic en el botón para confirmar la revocación.

Se revoca el EULA. En la lista de la sección **Contratos de licencia de usuario final**, desaparece la entrada correspondiente al contrato. La ventana de propiedades del EULA se cierra; la aplicación ya no está instalada.

Renovación de licencias para aplicaciones de Kaspersky

Puede renovar la licencia de una aplicación de Kaspersky que ya haya caducado o que esté próxima a caducar (que caduque en menos de treinta días).

Para renovar una licencia caducada o una licencia que está a punto de caducar:

1. Realice una de las siguientes acciones:

   - En el menú principal, vaya a **Operaciones** → **Licencias** → **Licencias**.
   - En el menú principal, vaya a **Supervisión** → **Panel** y, luego, haga clic en el vínculo **Ver licencias por caducar** junto a una notificación.

   Se abre la ventana **Licencias**, donde puede ver y renovar las licencias.

2. Haga clic en el enlace **Renovar licencia** ubicado junto a la licencia pertinente.

   Al hacer clic en un enlace de renovación de licencia, acepta transferir a Kaspersky la siguiente información sobre Kaspersky Security Center Linux: la versión, la localización utilizada, el id. de la licencia del software (es decir, el id. de la licencia que se está renovando) y una indicación de si la licencia se compró a través de una empresa asociada o no.

3. Se abrirá una ventana del servicio de renovación de licencias. Siga las instrucciones para renovar la licencia.

   Se renueva la licencia.

Cuando una licencia esté próxima a caducar, Kaspersky Security Center Web Console mostrará una notificación siguiendo este esquema:

- 30 días antes de la caducidad
- 7 días antes de la caducidad
- 3 días antes de la caducidad
- 24 horas antes de la caducidad
- Cuando la licencia haya caducado

Utilizar Kaspersky Marketplace para elegir soluciones empresariales de Kaspersky

Marketplace es una sección del menú principal en la que puede ver el catálogo completo de soluciones empresariales de Kaspersky, seleccionar las soluciones que necesita y adquirir esos productos en el sitio web de Kaspersky. Puede utilizar filtros para ver solo las soluciones que resulten adecuadas para su organización y para los requisitos de su sistema de seguridad de la información. Cuando elija una solución, Kaspersky Security Center Linux abrirá una página del sitio web de Kaspersky en la que encontrará más información sobre esa solución. Allí podrá proceder con la compra o ver instrucciones sobre el proceso de compra.

Puede usar los siguientes criterios para filtrar las soluciones de Kaspersky que se muestran en la sección **Marketplace**:

- Número de dispositivos (endpoints, servidores y otros tipos de activos) que desea proteger:
  - 50–250
  - 250-1000
  - Más de 1000
- Nivel de madurez del equipo de seguridad de la información de su organización:
  - **Foundations**

    Este es el nivel típico de las empresas que solo tienen un equipo de TI. Se bloqueará la mayor cantidad de amenazas posible en forma automática.
  - **Optimum**

    Este es el nivel típico de las empresas que, dentro de su equipo de TI, tienen personal específicamente a cargo de la seguridad informática. En este nivel, las empresas necesitan soluciones que les permitan contrarrestar tanto amenazas básicas como amenazas que puedan eludir sus mecanismos de prevención existentes.
  - **Expert**

    Este es el nivel típico de las empresas que tienen entornos de TI complejos y distribuidos. Estas empresas tienen un equipo de seguridad informática experimentado o un centro de operaciones de seguridad (SOC). En este nivel, las empresas necesitan soluciones que les permitan contrarrestar amenazas complejas y ataques dirigidos.
- Tipos de activos que desea proteger:
  - **Endpoints**: estaciones de trabajo utilizadas por los empleados, máquinas físicas y virtuales, sistemas integrados
  - **Servidores**: servidores físicos y virtuales
  - **Nube**: entornos de nube pública, privada o híbrida; servicios en la nube
  - **Red**: red de área local, infraestructura de TI
  - **Servicios**: servicios relacionados con la seguridad proporcionados por Kaspersky

Para buscar y comprar una solución empresarial de Kaspersky:

1. En el menú principal, vaya a **Marketplace**.

   De forma predeterminada, la sección muestra todas las soluciones empresariales de Kaspersky disponibles.

2. Para ver solo aquellas soluciones que sean adecuadas para su organización, seleccione los valores pertinentes en los filtros.

3. Haga clic en la solución que desee comprar o investigar en más detalle.

Será redirigido a la página web de la solución. Puede seguir las instrucciones en pantalla para proceder con la compra.

Configuración de las aplicaciones de Kaspersky

En esta sección, encontrará información sobre la configuración manual de tareas y directivas, sobre los roles de usuario y sobre la creación de una jerarquía de tareas y una estructura de grupos de administración.

Procedimiento: Configurar la protección de la red

El asistente de inicio rápido crea directivas y tareas con la configuración predeterminada. Esta configuración podría ser subóptima o incluso inadmisible para su organización. Por este motivo, recomendamos que modifique estas directivas y tareas predeterminadas y que, de ser necesario, cree otras directivas y tareas para su red.

Requisitos previos

Antes de comenzar, compruebe que hizo lo siguiente:

- Instaló el Servidor de administración de Kaspersky Security Center Linux
- Instaló Kaspersky Security Center Web Console
- Completó todos los pasos del escenario de instalación principal de Kaspersky Security Center Linux
- Completó todos los pasos del asistente de inicio rápido o creó manualmente las siguientes directivas y tareas en el grupo de administración **Dispositivos administrados**:
  - Directiva de Kaspersky Endpoint Security
  - Tarea de grupo para actualizar Kaspersky Endpoint Security
  - Directiva del Agente de red
  - Tarea *Buscar vulnerabilidades y actualizaciones requeridas*

Etapas

El proceso para configurar la protección de la red se divide en etapas:

1. **Configurar y propagar directivas y perfiles de directivas para las aplicaciones de Kaspersky**

   Para configurar y propagar la configuración de las aplicaciones Kaspersky instaladas en los dispositivos administrados, puede utilizar dos enfoques de la gestión de la seguridad diferentes: centrada en el dispositivo o centrada en el usuario. Estos dos enfoques también se pueden combinar.

2. **Configurar tareas para administrar las aplicaciones de Kaspersky en forma remota**

Revise las tareas creadas con el asistente de inicio rápido y modifique sus ajustes según corresponda.

Instrucciones: Configurar la tarea de grupo para actualizar Kaspersky Endpoint Security, Crear la tarea Buscar vulnerabilidades y actualizaciones requeridas.

De ser necesario, cree tareas adicionales para administrar las aplicaciones de Kaspersky instaladas en los dispositivos cliente.

3. **Evaluar y limitar el impacto de los eventos en la base de datos**

   Se transfiere la información sobre eventos que ocurren durante el funcionamiento de aplicaciones administradas de un dispositivo cliente y se registra en la base de datos del Servidor de administración. Para reducir la carga del Servidor de administración, evalúe y limite la cantidad de eventos que se guardan como máximo en la base de datos.

   Instrucciones prácticas: Configurar el número máximo de eventos

Resultados

Al concluir este escenario, su red estará protegida a través de la configuración de las aplicaciones de Kaspersky, de las distintas tareas y de los eventos recibidos por el Servidor de administración:

- Las aplicaciones de Kaspersky tendrán la configuración definida en las directivas y en los perfiles de directivas.
- Las aplicaciones se administrarán a través de un grupo de tareas.
- Habrá un límite a la cantidad de eventos almacenados en la base de datos.

Una vez que termine de configurar la protección para su red, asegúrese de que las bases de datos y las aplicaciones de Kaspersky se actualicen en forma periódica.

Acerca de la administración de la seguridad centrada en el dispositivo y centrada en el usuario

Puede administrar los ajustes de seguridad utilizando dos enfoques o perspectivas diferentes. Uno de estos enfoques pone el eje en las características de los dispositivos; el otro, en los roles de los usuarios. El primer enfoque se denomina *administración de la seguridad centrada en el dispositivo*, mientras que el segundo recibe el nombre de *administración de la seguridad centrada en el usuario*. Puede usar cualquiera de estos métodos, o ambos a la vez, para configurar sus aplicaciones de maneras diferentes en dispositivos diferentes.

El enfoque centrado en el dispositivo permite que la configuración de una aplicación de seguridad varíe según las características del dispositivo administrado en el que se encuentra instalada. Es posible, por ejemplo, definir ajustes de configuración diferentes para dispositivos asignados a grupos de administración diferentes.

El enfoque centrado en el usuario permite configurar las aplicaciones de seguridad de maneras diferentes para roles de usuario diferentes. Puede crear una serie de roles de usuario, asignarlos a sus usuarios según las funciones que desempeñen en la empresa y luego crear configuraciones diferentes, que se apliquen a uno u otro dispositivo según el rol asignado al propietario del dispositivo. Imagine, por ejemplo, que una aplicación de Kaspersky debe estar configurada de un modo diferente si se encuentra instalada en el dispositivo de un contador o en el dispositivo de un especialista en RR. HH. Al implementar la administración de la seguridad centrada en el usuario, puede hacer que cada departamento (el de Contabilidad y el de Recursos Humanos) tenga su propio "juego de ajustes" para esa aplicación. El juego de ajustes determina qué valores de configuración pueden ser modificados por los usuarios y cuáles se imponen por la fuerza y solamente pueden ser modificados por el administrador.

El enfoque centrado en el usuario también permite configurar una aplicación de un modo específico para un usuario específico. Esto puede ser útil si hay un empleado con un rol único en la empresa o si se quieren supervisar los problemas de seguridad asociados a los dispositivos de una persona en particular. El rol de este empleado en particular podría determinar si la persona tendrá más o menos derechos para modificar los ajustes de la aplicación. Un administrador de sistemas que tenga a su cargo los dispositivos cliente de una oficina local podría necesitar más derechos que otros usuarios.

El enfoque centrado en el dispositivo y el enfoque centrado en el usuario pueden combinarse. Podría, por ejemplo, configurar una directiva de aplicación específica para cada uno de sus grupos de administración y, luego, podría crear perfiles de directivas que se apliquen a uno o más de los roles de usuario definidos en su empresa. En este caso, las directivas y los perfiles de directiva se aplican en el siguiente orden:

1. Se aplicarán las directivas creadas en el marco del enfoque centrado en el dispositivo.
2. Los perfiles modificarán las directivas siguiendo el orden de prioridad definido para los perfiles de directivas.
3. Los perfiles de directivas vinculados a los roles de usuario modificarán las directivas.

Configuración y propagación de directivas: enfoque centrado en el dispositivo

Cuando complete este proceso, las aplicaciones de sus dispositivos administrados estarán configuradas a través de las directivas y los perfiles de directiva que usted defina.

Requisitos previos

Antes de comenzar, asegúrese de haber instalado el Servidor de administración de Kaspersky Security Center Linux y Kaspersky Security Center Web Console. Considere también la posibilidad de administrar la seguridad utilizando un enfoque centrado en el usuario en reemplazo o como complemento del enfoque centrado en el dispositivo. Más información sobre dos enfoques de administración.

Etapas

El proceso para administrar las aplicaciones de Kaspersky utilizando un enfoque centrado en el dispositivo se divide en los siguientes pasos:

1. **Configurar directivas para las aplicaciones**

   Cree y configure una directiva para cada aplicación de Kaspersky que se encuentre instalada en los dispositivos administrados. Estas directivas se propagarán a los dispositivos cliente.

   Cuando se utiliza el asistente de inicio rápido para configurar la protección de la red, Kaspersky Security Center Linux crea una directiva predeterminada para las siguientes aplicaciones:

   - Kaspersky Endpoint Security for Linux (para dispositivos cliente con Linux)
   - Kaspersky Endpoint Security para Windows (para dispositivos cliente con Windows)

Si completó el proceso de configuración utilizando este asistente, no es necesario que cree una nueva directiva para esta aplicación.

Si tiene una estructura jerárquica de varios Servidores de administración o grupos de administración, los Servidores de administración secundarios y los grupos de administración secundarios heredan las directivas del Servidor de administración principal de forma predeterminada. Puede forzar la herencia de los grupos secundarios y los Servidores de administración secundarios para prohibir cualquier modificación de los ajustes configurados en la directiva ascendente. Si desea que solo algunos de los ajustes se hereden por la fuerza, bloquee esos ajustes en la directiva de nivel superior. El resto de configuraciones desbloqueadas estarán disponibles para modificación en las directivas posteriores. La jerarquía de directivas resultante le será de gran utilidad para gestionar los dispositivos de los grupos de administración.

Instrucciones: Crear una directiva

2. **Crear perfiles de directivas (opcional)**

   Si desea que los dispositivos de un mismo grupo de administración estén sujetos a distintos ajustes de directivas, puede crear perfiles de directivas para esos dispositivos. Un perfil de directiva es un subconjunto nominado de los valores de configuración definidos en una directiva. Este subconjunto de valores, que se distribuye a los dispositivos de destino junto con la propia directiva, entra en vigor cuando se presenta una condición específica, llamada *condición de activación del perfil*. Un perfil contiene solamente los valores de configuración que difieren de los de la directiva "básica" que se encuentra activa en el dispositivo administrado.

   Al utilizar las condiciones de activación del perfil, puede aplicar diferentes perfiles de directivas, por ejemplo, a los dispositivos con una configuración de hardware específica o marcados con etiquetas específicas. Puede usar las etiquetas para filtrar dispositivos que reúnen criterios específicos. Por ejemplo, puede crear una etiqueta llamada *CentOS*, marcar todos los dispositivos que ejecutan el sistema operativo CentOS con esta etiqueta y luego especificar esta etiqueta como condición de activación para un perfil de directiva. Como resultado, las aplicaciones de Kaspersky instaladas en todos los dispositivos que ejecutan CentOS serán administradas por su propio perfil de directivas.

   Instrucciones:

   - Crear un perfil de directiva
   - Crear una regla de activación para un perfil de directiva

3. **Propagar las directivas y los perfiles de directivas a los dispositivos administrados**

   De forma predeterminada, el Servidor de administración se sincroniza automáticamente con los dispositivos administrados cada 15 minutos. Las directivas nuevas o con cambios y los perfiles de directivas se propagan a los dispositivos administrados durante la sincronización. Puede evitar la sincronización automática y ejecutar la sincronización manualmente utilizando el comando Forzar sincronización. Una vez que se completa la sincronización, las directivas y los perfiles de directivas se entregan y aplican a las aplicaciones de Kaspersky instaladas.

   Puede verificar si las directivas y los perfiles de directivas se entregaron a un dispositivo. Kaspersky Security Center Linux indica la fecha y la hora de entrega en las propiedades del dispositivo.

   Instrucciones: Sincronización forzada

Resultados

Al concluir este proceso, las aplicaciones de Kaspersky tendrán la configuración especificada y propagada a través de la jerarquía de directivas.

Las directivas y los perfiles de directivas configurados para las aplicaciones se aplicarán automáticamente a los nuevos dispositivos que se agreguen a los grupos de administración.

Configuración y propagación de directivas: enfoque centrado en el usuario

En esta sección se describe un proceso para configurar, de manera centralizada y tomando como eje a los usuarios, los ajustes de las aplicaciones de Kaspersky instaladas en los dispositivos administrados. Cuando complete este proceso, las aplicaciones de sus dispositivos administrados estarán configuradas a través de las directivas y los perfiles de directiva que usted defina.

Requisitos previos

Antes de comenzar, asegúrese de haber instalado correctamente el Servidor de administración de Kaspersky Security Center Linux y Kaspersky Security Center Web Console. También debe haber completado el escenario de despliegue principal. Para administrar la seguridad, considere también utilizar un enfoque centrado en el dispositivo, ya sea en reemplazo o como complemento de este enfoque centrado en el usuario. Más información sobre dos enfoques de administración.

Proceso

El proceso para administrar las aplicaciones de Kaspersky utilizando un enfoque centrado en el usuario se divide en los siguientes pasos:

1. **Configurar directivas para las aplicaciones**

   Cree y configure una directiva para cada aplicación de Kaspersky que se encuentre instalada en los dispositivos administrados. Estas directivas se propagarán a los dispositivos cliente.

   Si utiliza el asistente de inicio rápido para configurar la protección de la red, Kaspersky Security Center Linux creará la directiva predeterminada para Kaspersky Endpoint Security. Si completó el proceso de configuración utilizando este asistente, no es necesario que cree una nueva directiva para esta aplicación.

   Si tiene una estructura jerárquica de varios Servidores de administración o grupos de administración, los Servidores de administración secundarios y los grupos de administración secundarios heredan las directivas del Servidor de administración principal de forma predeterminada. Puede forzar la herencia de los grupos secundarios y los Servidores de administración secundarios para prohibir cualquier modificación de los ajustes configurados en la directiva ascendente. Si desea que solo algunos de los ajustes se hereden por la fuerza, bloquee esos ajustes en la directiva de nivel superior. El resto de configuraciones desbloqueadas estarán disponibles para modificación en las directivas posteriores. La jerarquía de directivas resultante le será de gran utilidad para gestionar los dispositivos de los grupos de administración.

   Instrucciones: Crear una directiva

2. **Designar los propietarios de los dispositivos**

   Asigne los dispositivos administrados a los usuarios correspondientes.

   Instrucciones: Designación de un usuario como propietario de un dispositivo

3. **Definir los roles de usuario más usuales en la empresa**

   Piense en las clases de labores que suele realizar el personal de su empresa. Debe dividir a los empleados basándose en las funciones o roles que cumplen. Puede hacer la división por departamento, profesión o cargo, por ejemplo. Tras hacer esta división, deberá crear un rol de usuario para cada grupo. Tenga en cuenta que cada rol de usuario tendrá su propio perfil de directiva, con ajustes de software que serán específicos para ese rol.

4. **Crear roles de usuario**

   Cree y configure una función de usuario para cada grupo de empleados que definió en el paso anterior o use las funciones de usuario predefinidos. Los roles de usuario contienen un conjunto de derechos que regulan el acceso a las funciones de las aplicaciones.

   Instrucciones: Creación de roles de usuario

5. **Definir el alcance de cada rol de usuario**

   Defina los usuarios, grupos de seguridad o grupos de administración de cada uno de los roles de usuario que haya creado. Los ajustes asociados a un rol de usuario se aplican únicamente a los dispositivos que pertenecen a los usuarios que tienen ese rol, y solo cuando esos dispositivos pertenecen a grupos y subgrupos asociados al rol en cuestión.

   Instrucciones: Editar el alcance de un rol de usuario

6. **Crear perfiles de directiva**

   Cree un perfil de directiva para cada rol de usuario que exista en su empresa. Los perfiles de directivas determinan qué ajustes de configuración corresponde utilizar en las aplicaciones instaladas en los dispositivos de los usuarios, tomando como parámetro el rol de cada usuario.

   Instrucciones: Crear un perfil de directiva

7. **Asociar los perfiles de directivas con los roles de usuario**

   Asocie los perfiles de directivas que haya creado con los distintos roles de usuario. De este modo, logrará que cada perfil de directiva se activará para los usuarios que tengan el rol especificado. Los ajustes configurados en cada perfil de directiva se implementarán en las aplicaciones de Kaspersky instaladas en los dispositivos de cada usuario.

   Instrucciones: Asociación de perfiles de directivas con roles

8. **Propagar las directivas y los perfiles de directivas a los dispositivos administrados**

   De manera predeterminada, Kaspersky Security Center Linux sincroniza automáticamente el Servidor de administración con los dispositivos administrados cada quince minutos. Las directivas nuevas o con cambios y los perfiles de directivas se propagan a los dispositivos administrados durante la sincronización. Puede saltear la sincronización automática y realizar una sincronización manual a través del comando "Forzar sincronización". Una vez que se completa la sincronización, las directivas y los perfiles de directivas se entregan y aplican a las aplicaciones de Kaspersky instaladas.

   Puede verificar si las directivas y los perfiles de directivas se entregaron a un dispositivo. Kaspersky Security Center Linux indica la fecha y la hora de entrega en las propiedades del dispositivo.

   Instrucciones: Sincronización forzada

Resultados

Al concluir este proceso, las aplicaciones de Kaspersky tendrán la configuración especificada y propagada a través de la jerarquía de directivas y perfiles de directivas.

Cuando necesite sumar un nuevo usuario, cree una cuenta nueva para esa persona y asígnele los dispositivos que usará y uno de los roles de usuario que haya creado. Las directivas y los perfiles de directivas que haya configurado para las aplicaciones se aplicarán automáticamente a los dispositivos del nuevo usuario.

Directivas y perfiles de directivas

En Kaspersky Security Center Web Console, puede crear directivas para las aplicaciones de Kaspersky. En esta sección se explica qué son, cómo se crean y cómo se modifican las directivas y los perfiles de directivas.

Acerca de las directivas y perfiles de directivas

Una *directiva* es un conjunto de valores de configuración de la aplicación de Kaspersky que se aplica a un grupo de administración y sus subgrupos. Puede instalar varias aplicaciones de Kaspersky en los dispositivos de un grupo de administración. Con Kaspersky Security Center, puede crear una única directiva para cada aplicación de Kaspersky disponible en un grupo de administración. Cada directiva puede tener uno de los siguientes estados:

Estado de la directiva

Estado	Descripción
Activa	La directiva que se encuentra vigente en un dispositivo. Solo puede haber una directiva activa para cada aplicación de Kaspersky en cada grupo de administración. Los dispositivos aplican los valores configurados en la directiva activa a la aplicación de Kaspersky.
Inactiva	Una directiva que no se encuentra vigente en un dispositivo.
Fuera de la oficina	Una directiva "fuera de la oficina" entra en vigor (es decir, se activa) cuando el dispositivo sale de la red corporativa.

Las directivas funcionan de acuerdo con las siguientes reglas:

- Es posible configurar más de una directiva, con distintos valores, para una misma aplicación.
- Solo puede haber una directiva activa para la aplicación actual.
- Una directiva puede tener directivas secundarias.

En general, puede usar las directivas como preparativos para situaciones de emergencia, como un ataque de virus. Si sufriera un ataque a través de unidades USB, por ejemplo, podría activar una directiva que bloqueara el acceso a ese tipo de unidades. Al hacerlo, la directiva que se encontrara activa hasta ese momento se desactivaría automáticamente.

Para poder hacer frente a distintas situaciones sin tener que mantener un grupo de directivas que difieran entre sí en unos pocos valores de configuración, puede usar perfiles de directivas.

Un *perfil* de *directiva* es un subconjunto de valores de configuración que se agrupan bajo un nombre y reemplazan los valores de configuración de una directiva. Un perfil de directiva afecta la constitución de los ajustes vigentes de un dispositivo administrado. Los *ajustes vigentes* de un dispositivo son aquellos que se encuentran en vigor en el mismo en un momento dado como resultado de aplicar la directiva, el perfil de directiva y la configuración local de una aplicación.

Los perfiles de directivas funcionan de acuerdo con las siguientes reglas:

- Un perfil de directiva entra en vigor cuando se cumple una condición de activación específica.
- Los perfiles de directivas contienen valores de configuración que difieren de los especificados en la directiva.
- La activación de un perfil de directiva modifica los ajustes vigentes del dispositivo administrado.
- Una directiva puede tener un máximo de 100 perfiles de directiva.

Acerca del candado y el bloqueo de ajustes

Cada ajuste de configuración disponible en una directiva tiene un interruptor de bloqueo acompañado de un candado de ícono (🔒). En la siguiente tabla, se muestran los estados que puede tener el interruptor de bloqueo.

Estados del interruptor de bloqueo

Estado	Descripción
Sin definir	Cuando un ajuste tiene un candado abierto a su lado y el interruptor de bloqueo está desactivado, el valor de dicho ajuste no se especifica a través de la directiva. El usuario puede modificar el valor del ajuste mediante la interfaz de la aplicación administrada. Estos ajustes se consideran *desbloqueados*.
Imponer	Cuando un ajuste tiene un candado cerrado a su lado y el interruptor de bloqueo está activado, el valor definido para ese ajuste es el que se aplica en los dispositivos sujetos a la directiva. El usuario no puede modificar el valor del ajuste mediante la interfaz de la aplicación administrada. Estos ajustes se consideran *bloqueados*.

Recomendamos encarecidamente que cierre los bloqueos para la configuración de la directiva que desea aplicar en los dispositivos administrados. La configuración de la directiva desbloqueada se puede reasignar mediante la configuración de la aplicación Kaspersky en un dispositivo administrado.

Puede utilizar el interruptor de bloqueo para lo siguiente:

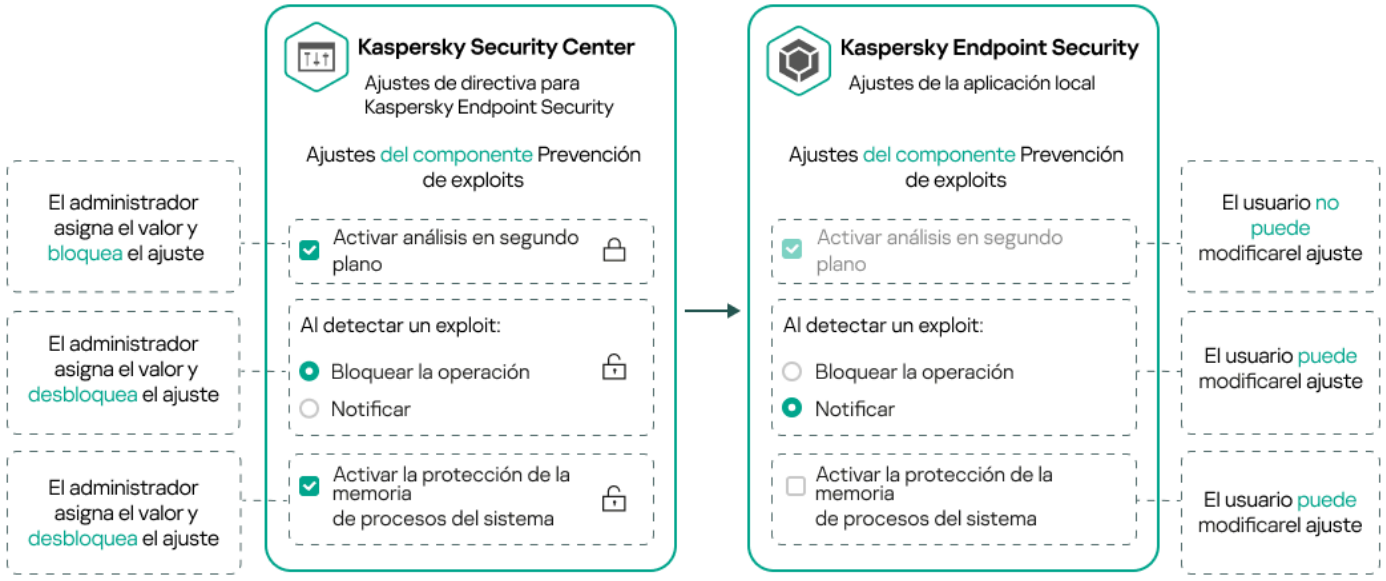
- Bloquear ajustes en la directiva de un subgrupo de administración
- Bloquear los ajustes de una aplicación de Kaspersky instalada en un dispositivo administrado

De este modo, un ajuste bloqueado se utiliza para formar y aplicar los ajustes vigentes de un dispositivo administrado.

El proceso para formar y aplicar los ajustes vigentes consta de las siguientes acciones:

- El dispositivo administrado aplica los valores de configuración definidos localmente en la aplicación de Kaspersky.
- El dispositivo administrado aplica los valores de configuración que se encuentran bloqueados en la directiva.

La directiva contiene los mismos ajustes que la aplicación de Kaspersky administrada. Cuando se modifican los ajustes dentro de una directiva, se modifican los ajustes en la aplicación de Kaspersky instalada en el dispositivo administrado. Los ajustes bloqueados no se pueden modificar en el dispositivo administrado (vea la siguiente imagen):



Candados y configuración de una aplicación de Kaspersky

Herencia en las directivas y los perfiles de directivas

En esta sección, se brinda información sobre la jerarquía y la herencia en el ámbito de las directivas y los perfiles de directivas.

Jerarquía de directivas

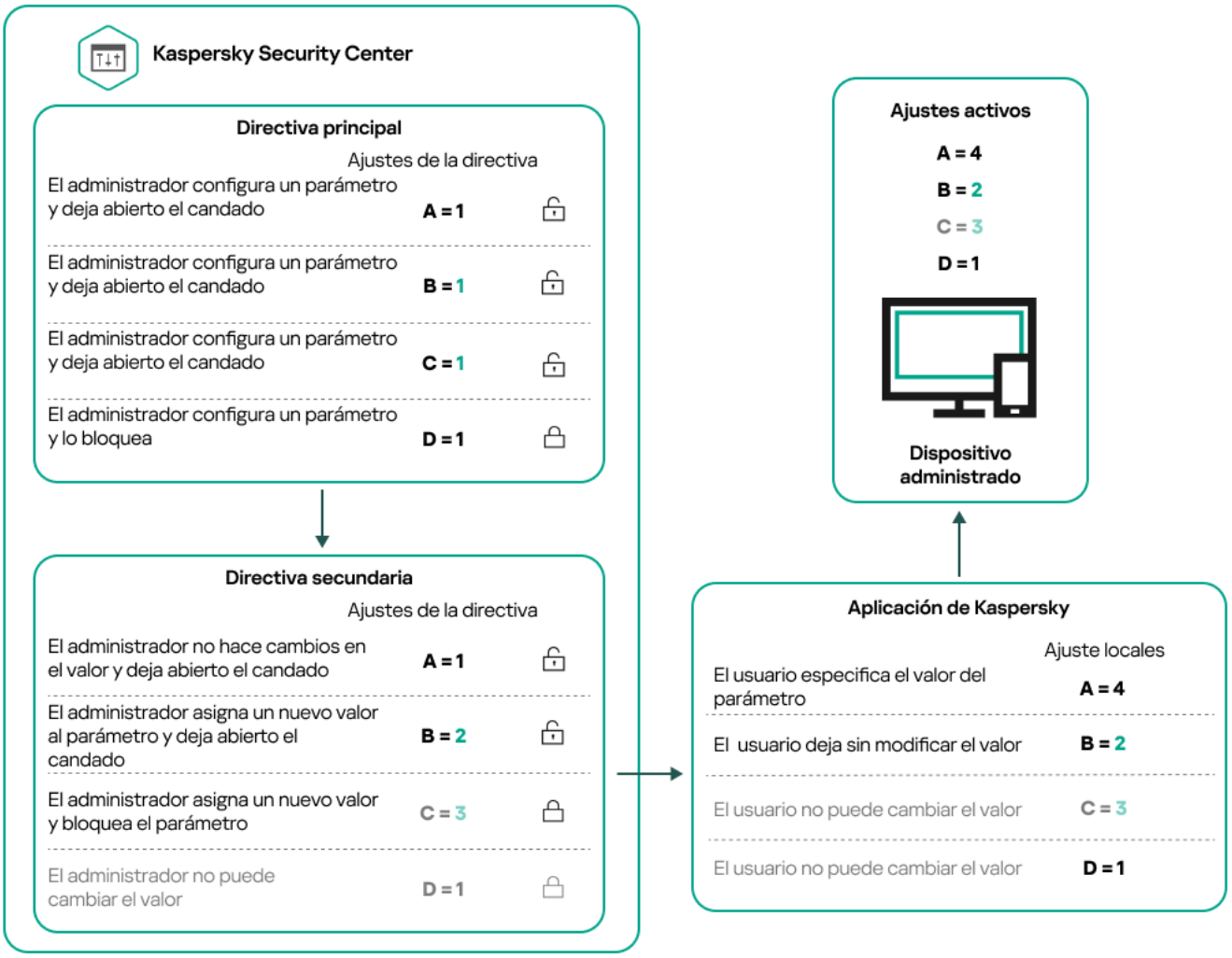
Si distintos dispositivos necesitan diferentes configuraciones, puede organizar los dispositivos en grupos de administración.

Puede especificar una directiva para un solo grupo de administración. La configuración de la directiva se puede *heredar*. La herencia hace que un subgrupo o grupo secundario de un grupo primario (un grupo de administración ubicado en un nivel superior) reciba valores de configuración de una directiva definida para ese grupo primario.

En lo sucesivo, se usará el término *directiva primaria* para hacer referencia a una directiva definida para un grupo primario. Una directiva para un subgrupo o grupo secundario se denominará *directiva secundaria*.

De forma predeterminada, existe al menos un grupo de dispositivos administrados en el Servidor de administración. Si crea grupos personalizados, se los creará como subgrupos o grupos secundarios de este grupo de dispositivos administrados.

Las directivas de una misma aplicación se afectan las unas a las otras siguiendo el orden jerárquico de los grupos de administración. Los ajustes que se bloquean en una directiva de un grupo de administración primario (de nivel superior) sobrescriben los valores de configuración en la directiva de un subgrupo (vea la siguiente imagen).



Jerarquía de directivas

Perfiles de directivas en una jerarquía de directivas

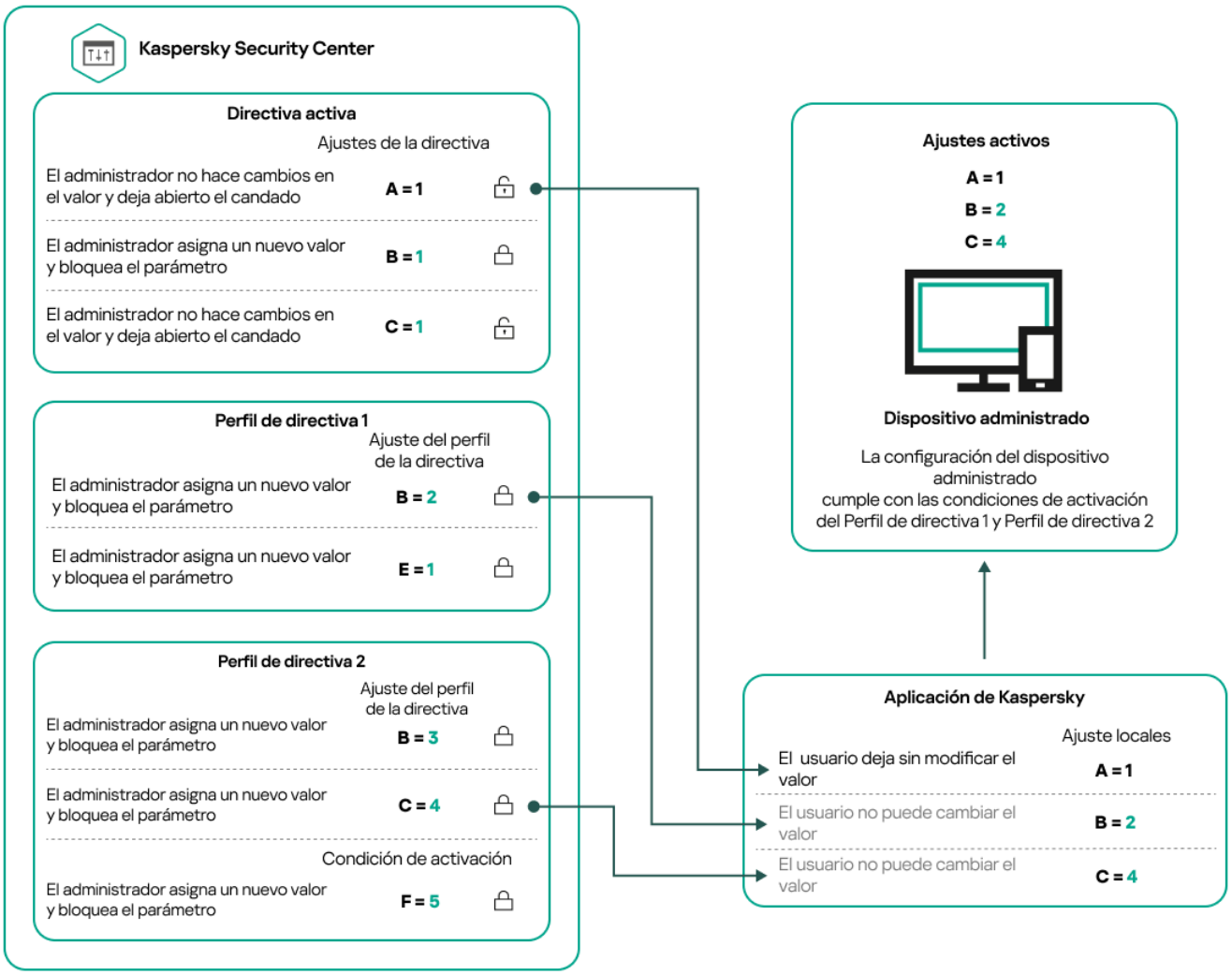
Los perfiles de directivas tienen las siguientes condiciones de asignación de prioridad:

- La posición de un perfil en una lista de perfiles indica su prioridad. La prioridad de un perfil puede modificarse. La posición más alta en la lista representa la prioridad más alta (vea la siguiente imagen).



Definición de la prioridad de un perfil de directiva

- Las condiciones de activación de los perfiles de directivas no son interdependientes. Varios perfiles pueden activarse al mismo tiempo. Cuando un mismo ajuste de configuración se ve afectado por más de un perfil, el dispositivo toma el valor de configuración indicado en el perfil de directiva de mayor prioridad (vea la siguiente imagen).

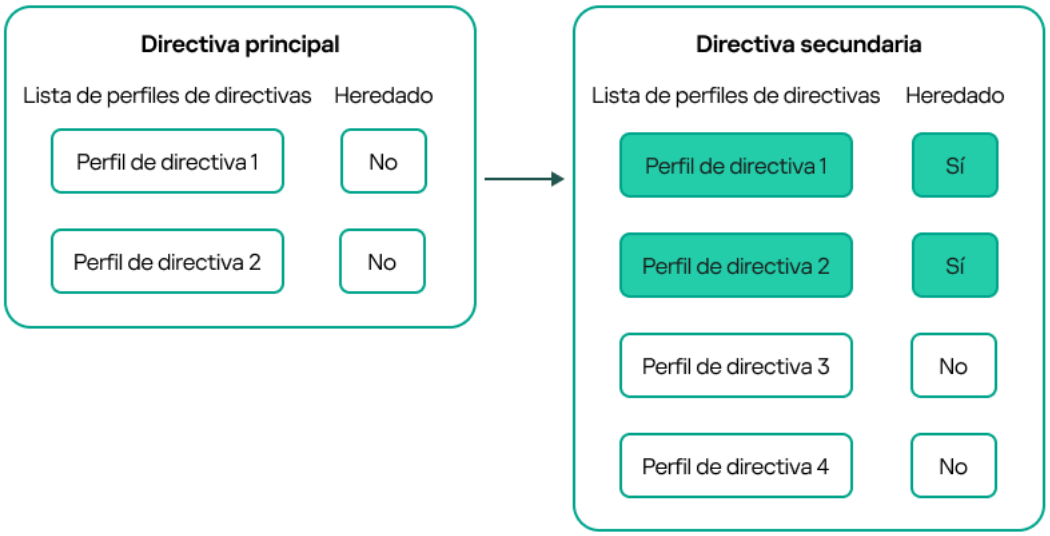


La configuración del dispositivo administrado cumple las condiciones de activación de varios perfiles de directiva

Perfiles de directivas en una jerarquía de herencia

Los perfiles de directivas definidos para directivas de distintos niveles jerárquicos se rigen por estas condiciones:

- Una directiva de nivel inferior hereda los perfiles de una directiva de nivel superior. Un perfil de directiva que se ha heredado de una directiva de nivel superior obtiene mayor prioridad que el nivel del perfil de directiva original.
- No se puede cambiar la prioridad de un perfil de directiva heredado (vea la siguiente imagen).



Herencia de perfiles de directivas

Perfiles de directivas con el mismo nombre

Cuando existen dos directivas con el mismo nombre en niveles jerárquicos diferentes, esas directivas funcionan de acuerdo con las siguientes reglas:

- Los ajustes de configuración bloqueados y la condición de activación del perfil de directiva ubicado en el nivel superior cambian los ajustes y la condición de activación del perfil de directiva ubicado en el nivel inferior (vea la siguiente imagen).



El perfil secundario hereda los valores de configuración del perfil de directiva primario

- Los ajustes de configuración desbloqueados y la condición de activación del perfil de directiva ubicado en el nivel superior no cambian ni los ajustes ni la condición de activación del perfil de directiva ubicado en el nivel inferior.

Cómo se implementan los valores de configuración en un dispositivo administrado

La implementación de los valores de configuración vigentes en un dispositivo administrado puede describirse de la siguiente manera:

- Todos los valores de configuración que no se bloquearon se toman de la directiva.
- Luego, estos valores se reemplazan con los valores configurados en la aplicación administrada.
- Finalmente, se aplican los valores de configuración que se encuentran bloqueados en la directiva en vigor. Los valores bloqueados sustituyen los valores de los ajustes vigentes que no estaban bloqueados.

Administración de directivas

Esta sección trata sobre la administración de las directivas. Encontrará instrucciones para ver la lista de directivas; crear, copiar, modificar, mover o eliminar directivas; realizar una sincronización forzada, y ver un gráfico para conocer el estado de distribución de una directiva.

Ver la lista de directivas

Puede ver listas con las directivas creadas para el Servidor de administración o para cualquier grupo de administración.

Para ver una lista de directivas:

1. En el menú principal, vaya a **Administración de activos** → **Jerarquía de grupos**.
2. En la estructura de grupos de administración, seleccione el grupo de administración al que corresponda la lista de directivas que desee ver.

   Aparece la lista de directivas en formato tabular. Si no hay ninguna directiva, la tabla estará vacía. Puede mostrar, ocultar y reorganizar las columnas de la tabla, utilizar la función de búsqueda o ver solo las líneas que contengan un valor especificado.

Crear una nueva directiva

Puede crear directivas nuevas y modificar o eliminar las directivas existentes.

Para crear una directiva:

1. En el menú principal, vaya a **Administración de activos** → **Directivas**.
2. Seleccione el grupo de administración relacionado con la directiva:
   - Para el grupo root:

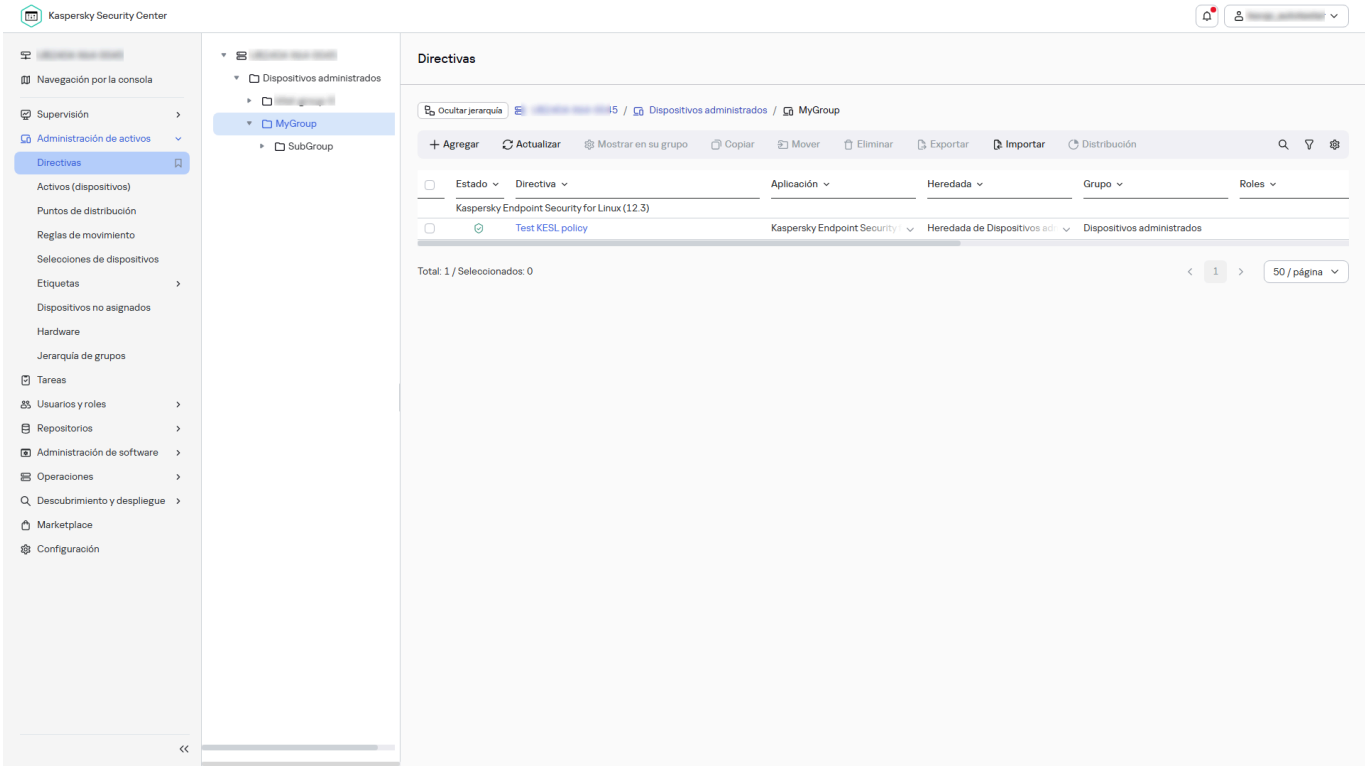
     En este caso, puede avanzar al próximo paso.
   - Para un subgrupo:

     a. Haga clic en el botón **Mostrar jerarquía** en la parte superior de la página.

     El nombre del botón cambia a **Ocultar jerarquía**.

     b. En la ventana que se abre, haga clic en el nombre del subgrupo requerido.

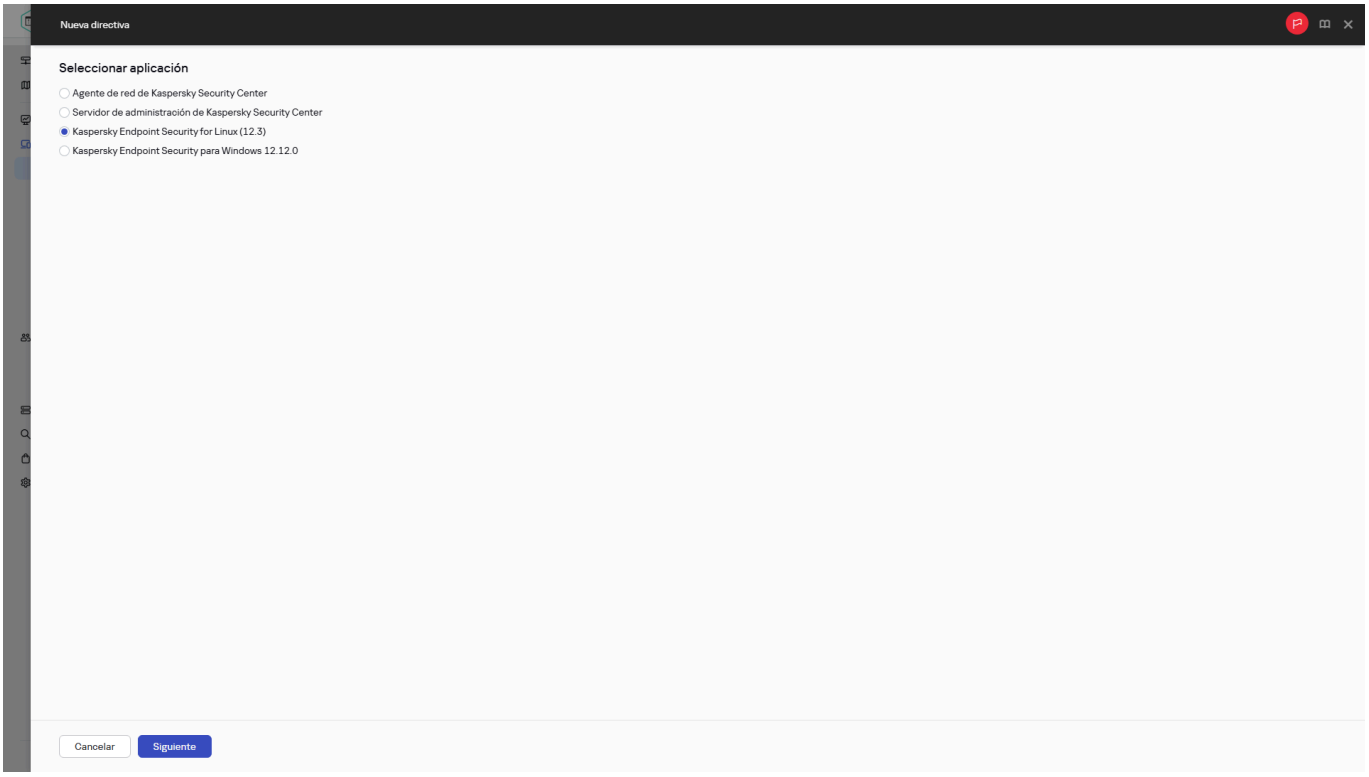
Verá la ruta al grupo seleccionado en la parte superior de la página. Si es necesario, puede hacer clic en un vínculo con el nombre del grupo de administración para ir al grupo. De forma predeterminada, el último vínculo de la ruta se encuentra inactivo. Además, puede cerrar la ventana de jerarquía si hace clic en el botón **Ocultar jerarquía**.



La lista de directivas

3. Haga clic en **Agregar**.

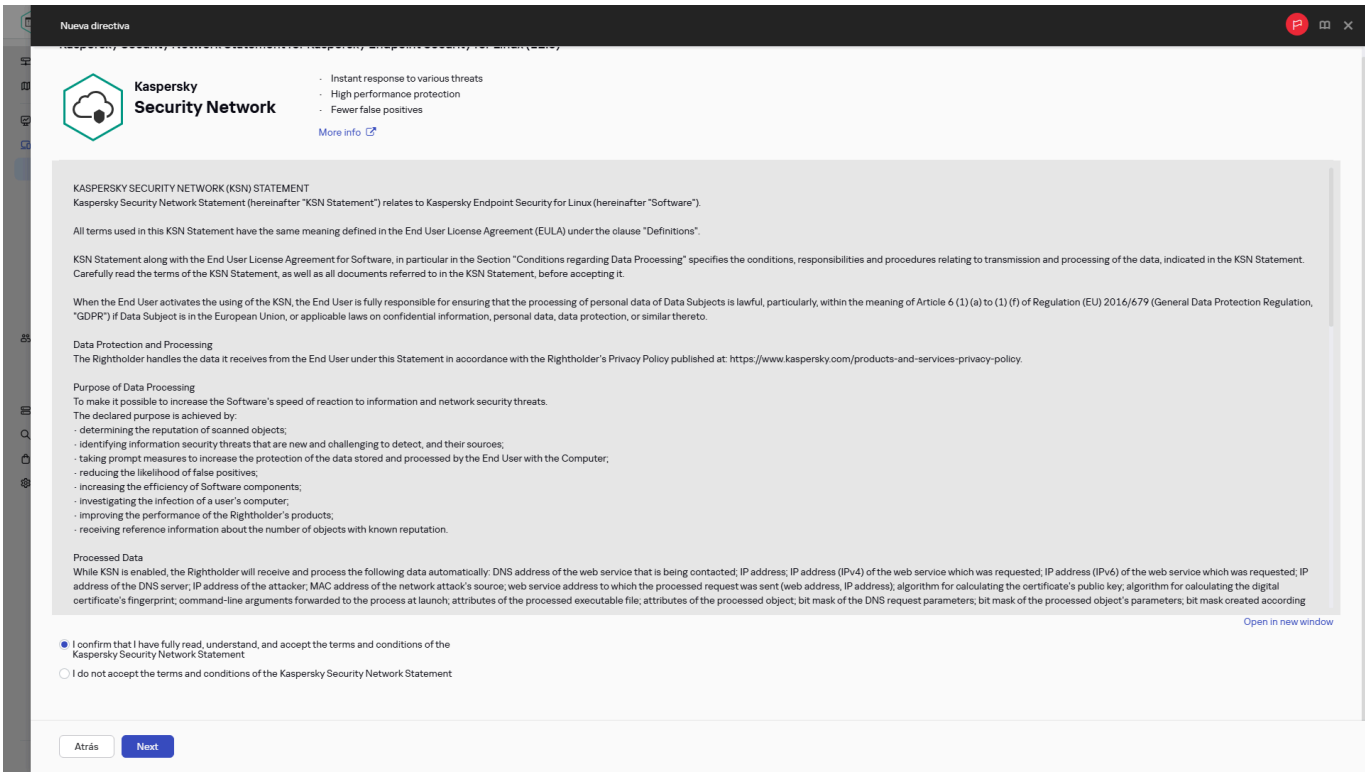
   Se abre la ventana **Seleccionar aplicación**.



Crear una nueva directiva

4. Seleccione la aplicación para la que desee crear la directiva.

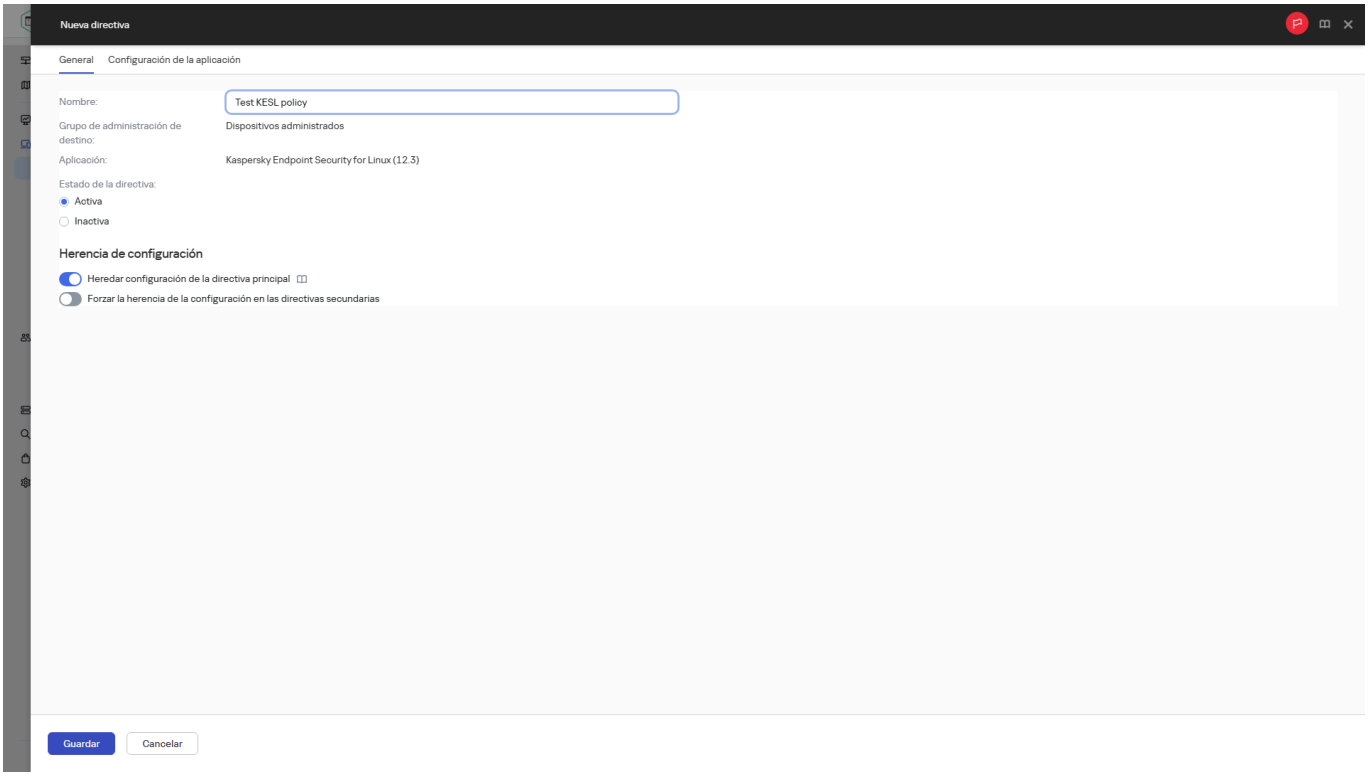
5. Si Kaspersky Security Network es compatible con la aplicación de Kaspersky, para la cual está creando una directiva, se le pedirá que acepte la Declaración de KSN. Si desea utilizar Kaspersky Security Network, acepte la Declaración de KSN.



Aceptar la Declaración de KSN

6. Haga clic en **Siguiente**.

   Se abre la ventana de configuración de la nueva directiva, con la pestaña **General** seleccionada. Si lo desea, cambie el nombre predeterminado, el estado predeterminado y las opciones de directiva predeterminadas.



La ventana de configuración de la nueva directiva

7. Seleccione la pestaña **Configuración de la aplicación**.

O, si lo prefiere, haga clic en **Guardar** y salga de la ventana. La directiva se mostrará en la lista de directivas y podrá editar su configuración en otro momento.

8. En la pestaña **Configuración de la aplicación**, en el panel izquierdo, seleccione una categoría de su interés. En el panel de resultados de la derecha, modifique la configuración de la directiva. Puede editar los ajustes de configuración disponibles en cada categoría (sección).

   El conjunto de configuraciones depende de la aplicación para el que crea una directiva. Para más detalles, consulte los siguientes recursos:

   - Configuración del Servidor de administración
   - Ajustes de la directiva del Agente de red
   - Ayuda de Kaspersky Endpoint Security para Linux
   - Ayuda de Kaspersky Endpoint Security para Windows

   Para obtener detalles sobre la configuración de otras aplicaciones de seguridad, consulte la documentación de la aplicación correspondiente.

   Al editar la configuración, puede hacer clic en **Cancelar** para cancelar la última operación.

9. Haga clic en **Guardar** para guardar la directiva.

   Se muestra una notificación con el siguiente mensaje: **La directiva se está guardando y distribuyendo por la jerarquía de los Servidores de administración**.

   Si la directiva se valida correctamente, se muestra la siguiente notificación: **La directiva se guardó**.

   Si la directiva no se valida, se muestra la siguiente notificación: **No se pudo guardar y distribuir la directiva por la jerarquía de los Servidores de administración. Comuníquese con Soporte técnico**. Puede revisar y modificar la configuración de la directiva y, luego, volver a intentarlo. Si el problema persiste, comuníquese con el servicio de Soporte técnico.

La directiva aparecerá en la lista de directivas. Una vez creada la directiva, los eventos de cambio de la directiva se exportan al sistema SIEM si esta opción está habilitada.

Ajustes generales de una directiva

General

En la pestaña **General**, puede modificar el estado de la directiva y especificar la herencia de la configuración de la directiva:

- A través del bloque **Estado de la directiva**, puede seleccionar uno de los modos posibles para la directiva:

  Activa

  Si se selecciona esta opción, se activa la directiva.

  Esta opción está seleccionada de forma predeterminada.

  Fuera de la oficina

  Una directiva "fuera de la oficina" entra en vigor (es decir, se activa) cuando el dispositivo sale de la red corporativa.

Inactiva

Si selecciona esta opción, la directiva estará inactiva, pero quedará guardada en la carpeta **Directivas**. Podrá activarla cuando resulte necesario.

- En el grupo de ajustes **Herencia de configuración**, puede configurar las opciones de directiva:

  Heredar configuración de la directiva primaria

  Si habilita esta opción, la directiva heredará los valores de configuración definidos en la directiva del grupo de nivel superior. Estos valores, en consecuencia, estarán bloqueados.

  Esta opción está activada de forma predeterminada.

  Forzar la herencia de configuración en las directivas secundarias

  Si habilita esta opción, cuando modifique la directiva y se apliquen los cambios, ocurrirá lo siguiente:

  - Los valores de configuración de la directiva se propagarán a las directivas de los subgrupos de administración (es decir, a las directivas secundarias).
  - En la ventana de propiedades de cada directiva secundaria, dentro del bloque **Herencia de configuración** de la sección **General**, se habilitará automáticamente la opción **Heredar configuración de la directiva primaria**.

  Habilitar esta opción hace que los ajustes de las directivas secundarias se bloqueen.

  Esta opción está deshabilitada de forma predeterminada.

Configuración de eventos

La pestaña **Configuración de eventos** le permite configurar el registro de los eventos y las notificaciones de eventos. Los eventos están distribuidos por nivel de importancia en las siguientes pestañas:

- **Crítico**

  La sección **Crítico** no se muestra en las propiedades de la directiva del Agente de red.

- **Error funcional**
- **Advertencia**
- **Información**

Cada sección contiene una lista con los distintos tipos de eventos y la cantidad de días por la que cada evento se deja almacenado, de manera predeterminada, en el Servidor de administración. Haga clic en un tipo de evento para configurar los siguientes ajustes:

- **Registro de los eventos**

  Puede especificar cuántos días se conservará el evento y dónde se lo guardará:

  - **Exportar al sistema SIEM usando Syslog**
  - **Guardar en el registro de eventos del SO del dispositivo**
  - **Guardar en el registro de eventos del SO del Servidor de administración**

- **Notificaciones sobre los eventos**

Puede seleccionar si desea ser notificado sobre el evento en uno de estos modos:

- **Notificar por correo electrónico**
- **Notificar por SMS**
- **Notificar mediante la ejecución de un archivo ejecutable o un script**
- **Notificar por SNMP**

De forma predeterminada, se utilizan las opciones de notificación (por ejemplo, la dirección de destino) que se encuentran definidas en la pestaña de propiedades del Servidor de administración. Si desea modificar esta configuración, puede hacerlo a través de las pestañas **Correo electrónico**, **SMS** y **Archivo ejecutable para ejecutar**.

Además, la pestaña de **Configuración de eventos** mostrará una notificación cuando se agreguen nuevos tipos de eventos (por ejemplo, en una versión nueva de la aplicación) y le permitirá aplicar la configuración nueva haciendo clic en el botón **Guardar** o **Guardar y cerrar**.

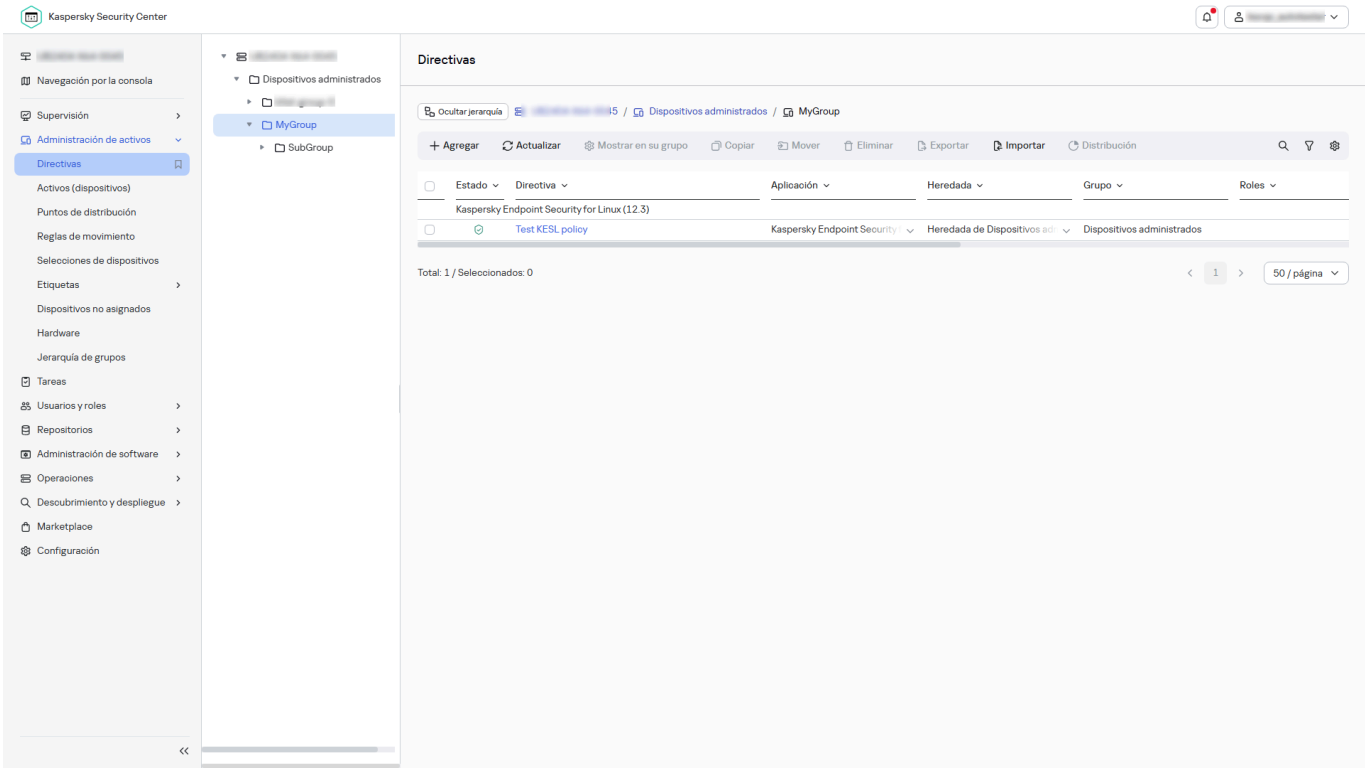
Historial de revisiones

La pestaña **Historial de revisiones** le permite ver la lista de revisiones de la directiva, comparar revisiones y revertir los cambios realizados en la directiva, si es necesario.

Modificar una directiva

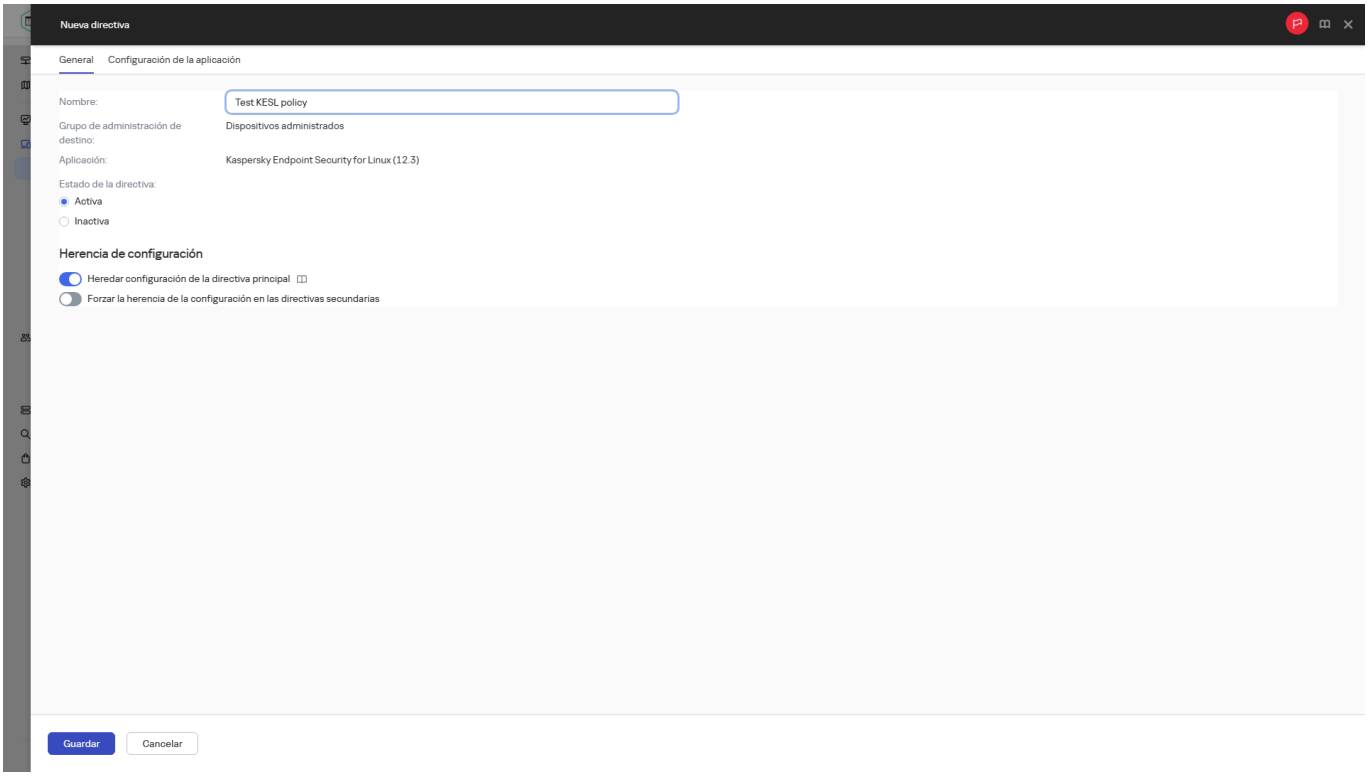
Para modificar una directiva:

1. En el menú principal, vaya a **Administración de activos** → **Directivas**.



2. Haga clic en la directiva que desee modificar.

Se abre la ventana de configuración de la directiva.



3. Especifique la configuración general y la configuración de la aplicación para la que crea una directiva. Para más detalles, consulte los siguientes recursos:

   - Configuración del Servidor de administración
   - Ajustes de la directiva del Agente de red
   - Ayuda de Kaspersky Endpoint Security para Linux
   - Ayuda de Kaspersky Endpoint Security para Windows

   Si necesita información detallada para configurar otra aplicación de seguridad, consulte la documentación de ese software.

4. Haga clic en el botón **Guardar**.

   Se muestra una notificación con el siguiente mensaje: **La directiva se está guardando y distribuyendo por la jerarquía de los Servidores de administración**.

   Si la directiva se valida correctamente, se muestra la siguiente notificación: **La directiva se guardó**.

   Si la directiva no se valida, se muestra la siguiente notificación: **No se pudo guardar y distribuir la directiva por la jerarquía de los Servidores de administración. Comuníquese con Soporte técnico**. Puede revisar y modificar la configuración de la directiva y, luego, volver a intentarlo. Si el problema persiste, comuníquese con el servicio de Soporte técnico.

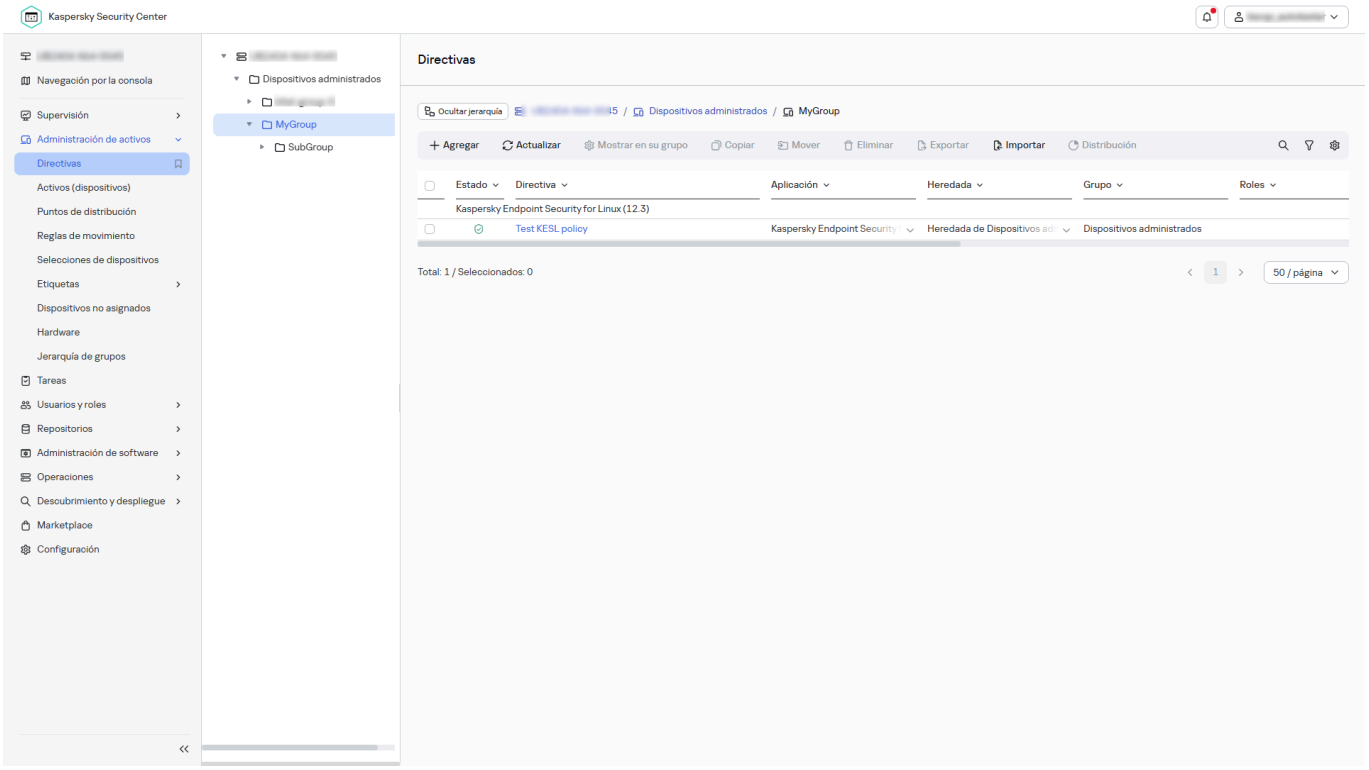
Los cambios realizados en la directiva se guardarán en las propiedades de la directiva y aparecerán en la sección **Historial de revisiones**. Una vez modificada la directiva, los eventos de cambio de directiva se exportan al sistema SIEM, si esta opción está habilitada.

Si es necesario, puede comparar las revisiones de la directiva. La opción está disponible para las directivas del Servidor de administración, el Agente de red, Kaspersky Endpoint Security para Windows (a partir de la versión 14.0 del complemento web) y Kaspersky Endpoint Security for Mac (a partir de la versión 12.2.1 Parche A del complemento web).

Habilitar y deshabilitar una opción de herencia en las directivas

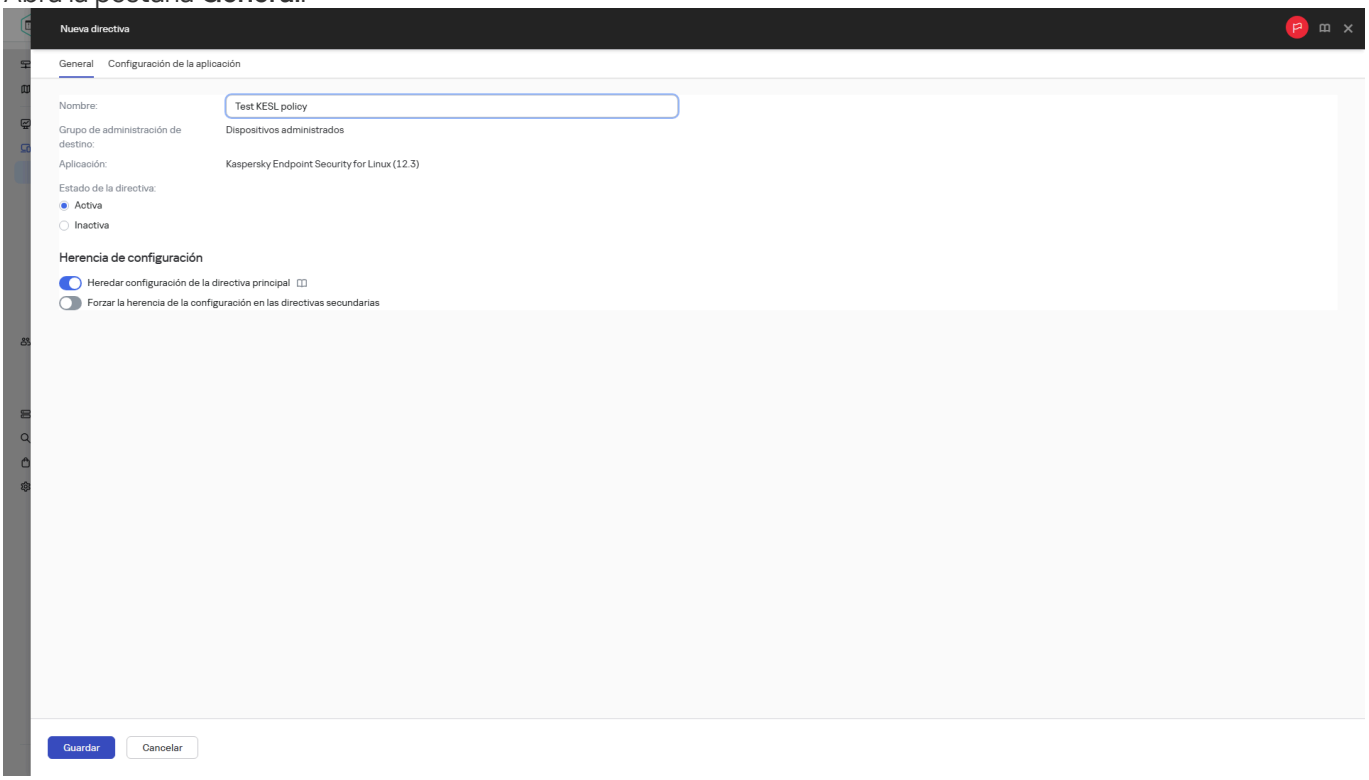
Para habilitar o deshabilitar la opción de herencia en una directiva:

1. Abra la directiva que tenga en mente.



La lista de directivas

2. Abra la pestaña **General**.



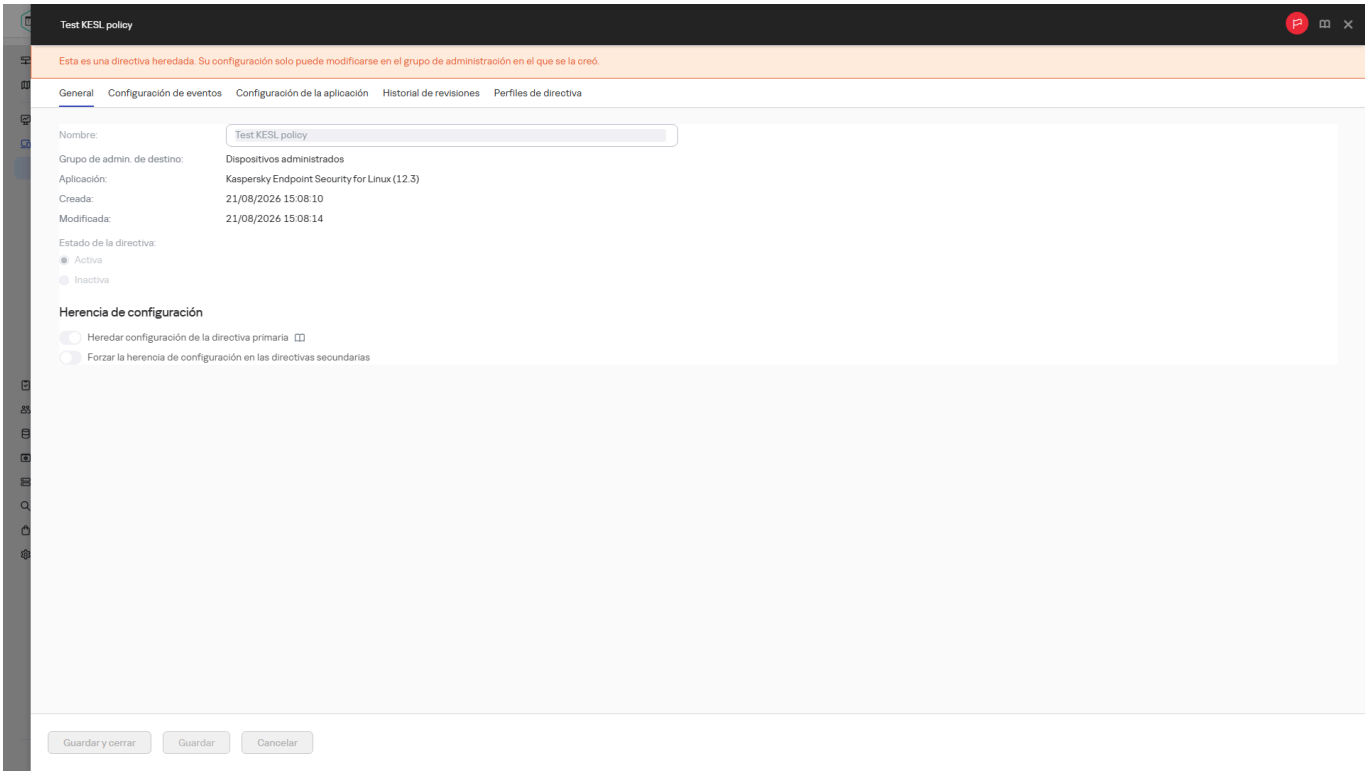
Crear una nueva directiva

3. Habilite o deshabilite la herencia en la directiva:

   - Si habilita la opción **Heredar configuración de la directiva primaria** en una directiva secundaria y un administrador bloquea algunos ajustes de configuración en la directiva primaria, no podrá cambiar esos ajustes en la directiva secundaria.

   - Si deshabilita la opción **Heredar configuración de la directiva primaria** en una directiva secundaria, podrá cambiar todos los ajustes de la directiva secundaria aunque haya ajustes bloqueados en la directiva primaria.

   - Si habilita la opción **Forzar la herencia de configuración en las directivas secundarias** en el grupo primario, se habilitará la opción **Heredar configuración de la directiva primaria** en cada directiva secundaria. No podrá deshabilitar esta opción en ninguna directiva secundaria. Los grupos secundarios heredarán por la fuerza todos los ajustes que se bloqueen en la directiva primaria; los valores de estos ajustes no se podrán modificar en los grupos secundarios.



Configuración bloqueada de la política

4. Haga clic en el botón **Guardar** para guardar los cambios o haga clic en el botón **Cancelar** para rechazar los cambios.

De manera predeterminada, la opción **Heredar configuración de la directiva primaria** está habilitada en las directivas nuevas.

Si una directiva tiene perfiles, todas las directivas secundarias los heredan.

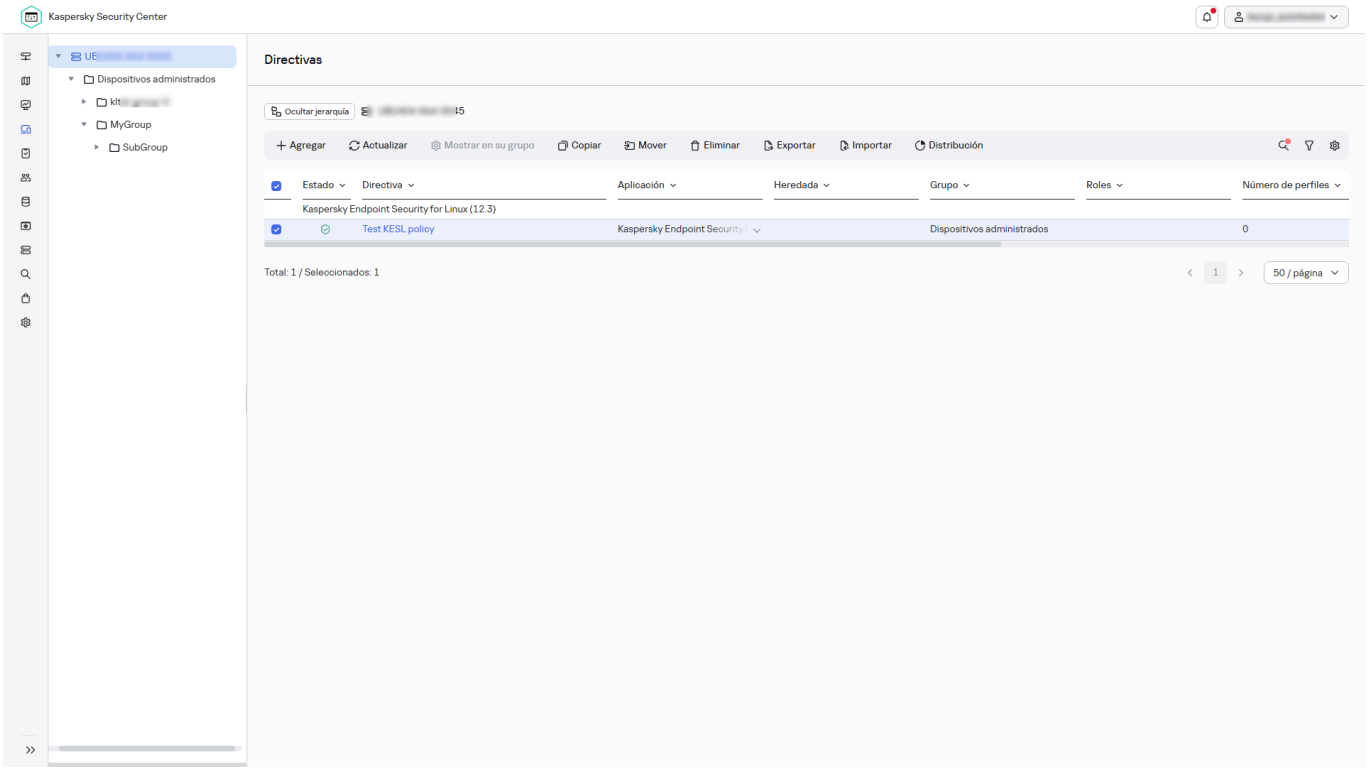
Copiar una directiva

Puede copiar directivas de un grupo de administración a otro.

Para copiar una directiva a otro grupo de administración:

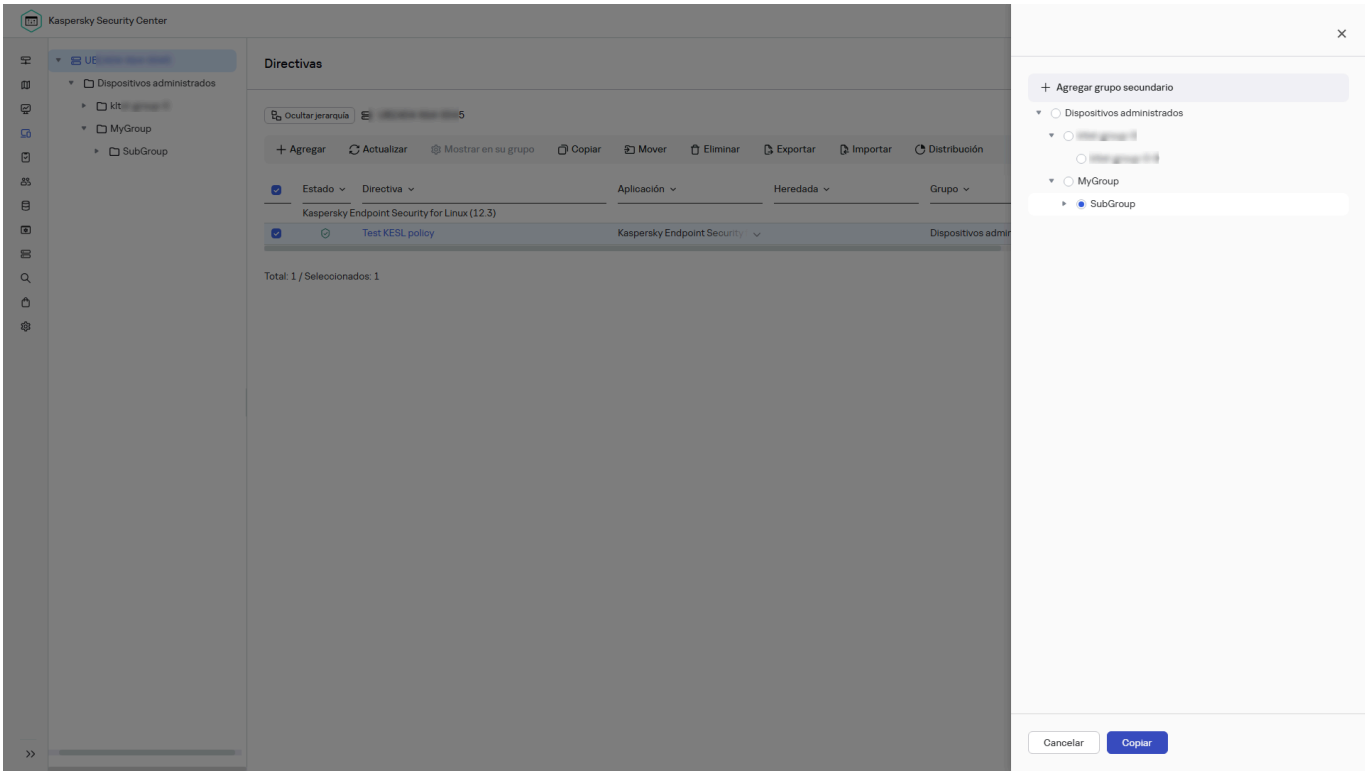
1. En el menú principal, vaya a **Administración de activos** → **Directivas**.

2. Marque la casilla ubicada junto a la directiva (o las directivas) que desee copiar.



3. Haga clic en **Copiar**.

   En el lado derecho de la pantalla, verá el árbol con los grupos de administración.



4. En el árbol, seleccione el grupo de destino (es decir, el grupo al que desee copiar la directiva o las directivas).

5. Haga clic en el botón **Copiar** que está al final de la pantalla.

6. Haga clic en **Aceptar** para confirmar la operación.

Las directivas que haya seleccionado se copiarán al grupo de destino con todos sus perfiles. El estado de estas directivas en el grupo de destino será **Inactiva**. Puede cambiar el estado a **Activa** en cualquier momento.

Si el grupo de destino contiene una directiva con el mismo nombre que la que se quiere mover, se agregará un índice secuencial —en formato (<siguiente número en la serie>), por ejemplo, (1)— al nombre de la directiva trasladada.

Mover una directiva

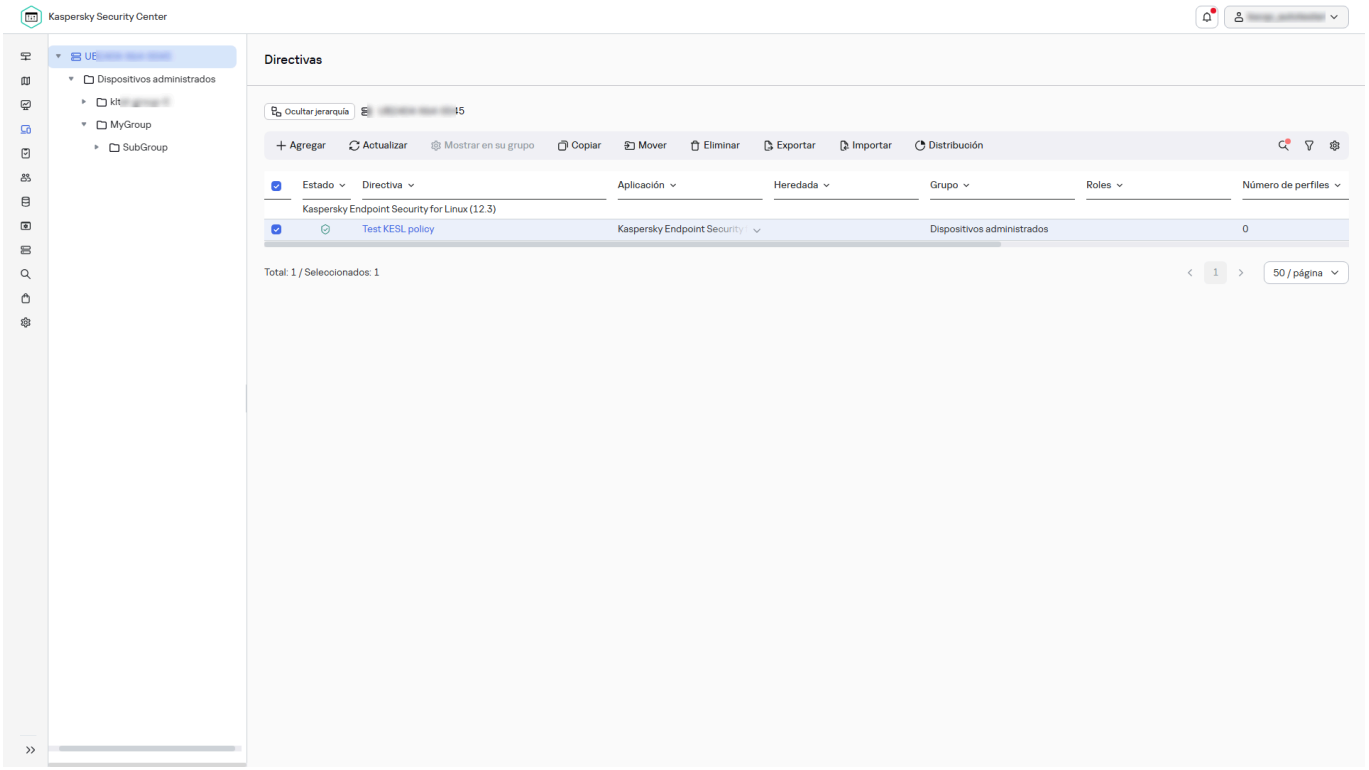
Puede mover directivas de un grupo de administración a otro. Esto puede ser útil si necesita eliminar un grupo, por ejemplo, pero quiere utilizar sus directivas para un grupo diferente. En tal caso, antes de eliminar el grupo que ya no necesita, puede mover sus directivas al nuevo grupo.

> Al mover una directiva a otro grupo de administración, se borra el historial de revisiones de la directiva. La pestaña **Historial de revisiones** solo muestra información sobre el cambio más reciente.

Para mover una directiva a otro grupo de administración:

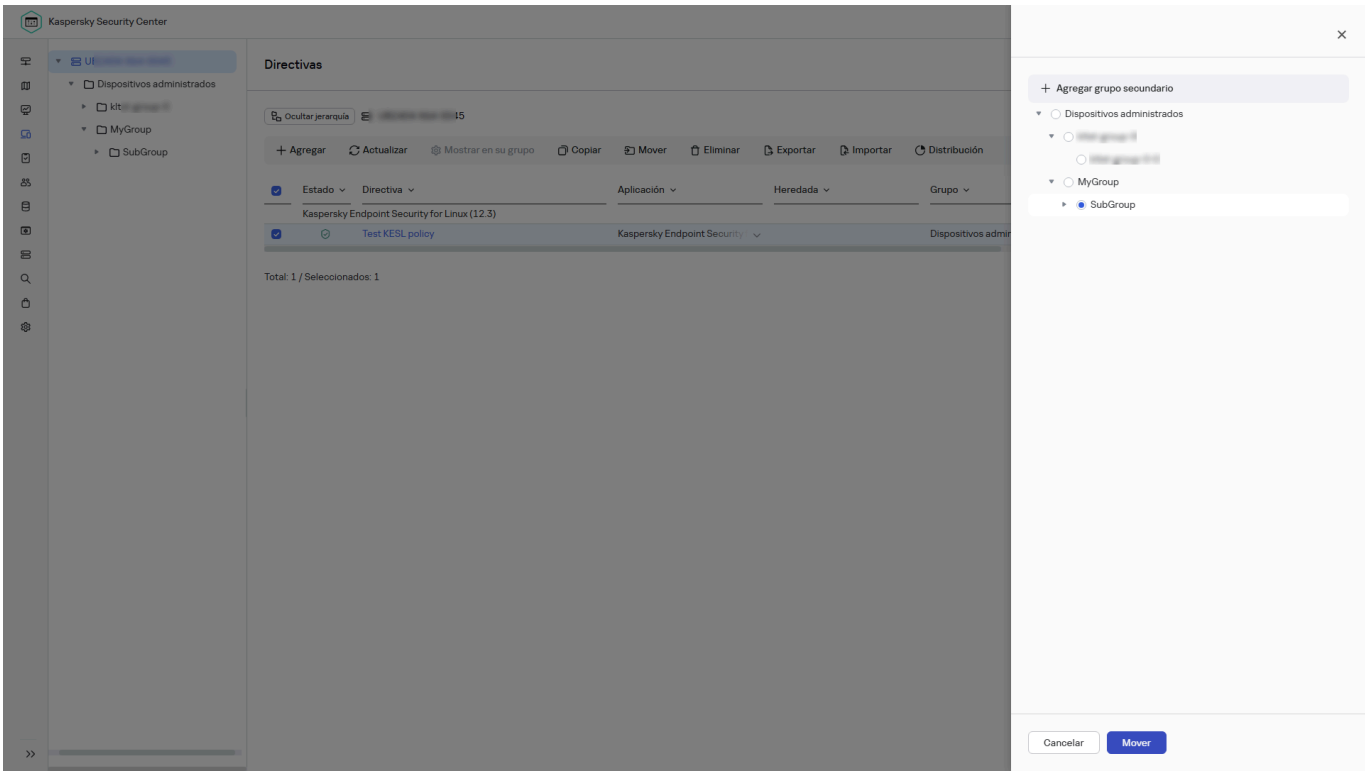
1. En el menú principal, vaya a **Administración de activos** → **Directivas**.

2. Marque la casilla ubicada junto a la directiva (o las directivas) que desee mover.



3. Haga clic en el botón **Mover**.

   En el lado derecho de la pantalla, verá el árbol con los grupos de administración.



4. En el árbol, seleccione el grupo de destino (es decir, el grupo al que desee mover la directiva o las directivas).

5. Haga clic en el botón **Mover** en la parte inferior de la pantalla.

6. Haga clic en **Aceptar** para confirmar la operación.

   Si la directiva del grupo de origen no es una directiva heredada, se la moverá al grupo de destino junto con todos sus perfiles. El estado de la directiva en el grupo de destino será **Inactiva**. Puede cambiar el estado a **Activa** en cualquier momento.

   Si la directiva del grupo de origen es una directiva heredada, permanecerá en el grupo de origen. En lugar de moverla, se la copiará al grupo de destino junto con todos sus perfiles. El estado de la directiva en el grupo de destino será **Inactiva**. Puede cambiar el estado a **Activa** en cualquier momento.

Si el grupo de destino contiene una directiva con el mismo nombre que la que se quiere mover, se agregará un índice secuencial —en formato (<siguiente número en la serie>), por ejemplo, (1)— al nombre de la directiva trasladada.

Exportación de una directiva

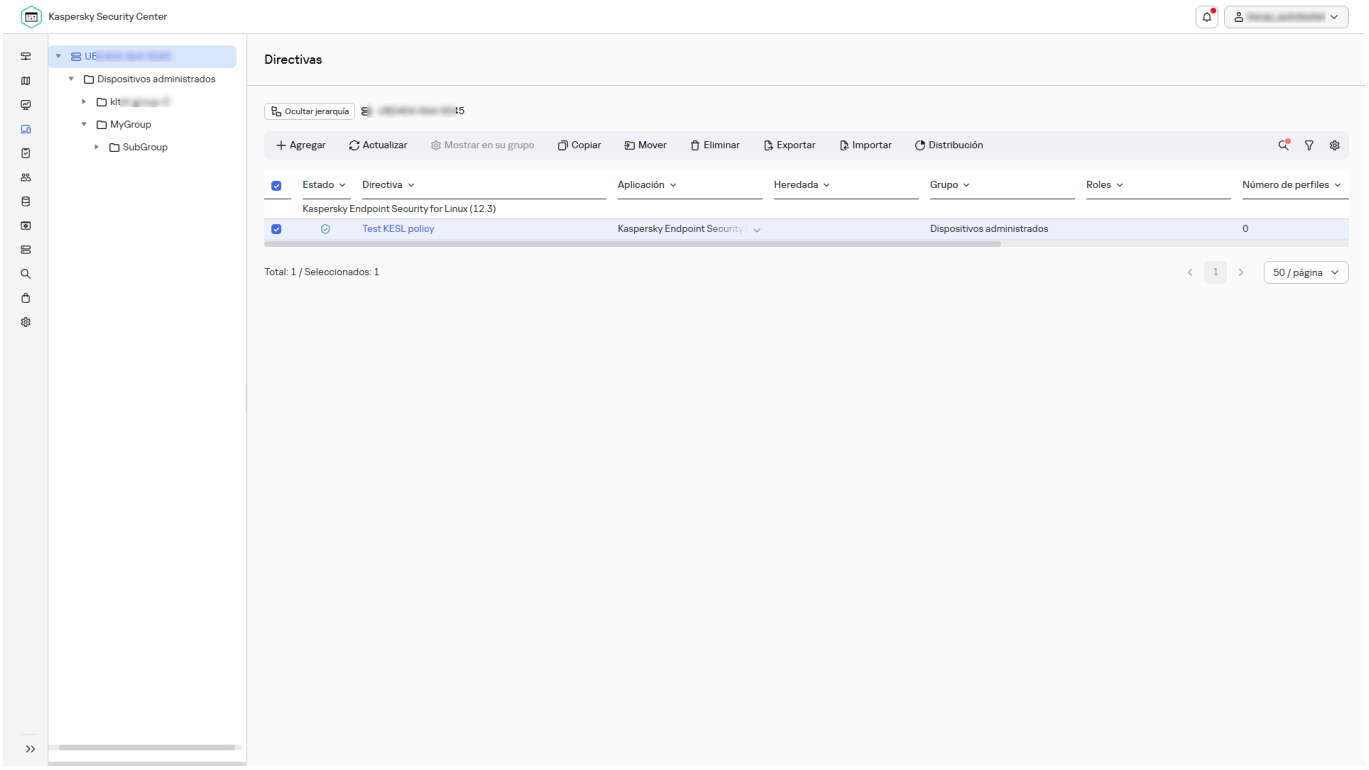
Kaspersky Security Center Linux permite guardar una directiva, su configuración y sus perfiles en un archivo KLP. El archivo KLP puede usarse para importar la directiva guardada en Kaspersky Security Center Windows o Kaspersky Security Center Linux.

Para exportar una directiva:

1. En el menú principal, vaya a **Administración de activos** → **Directivas**.

2. Marque la casilla ubicada junto a la directiva que desee exportar.

No es posible exportar más de una directiva a la vez. Si selecciona más de una directiva, el botón **Exportar** se desactivará.



Selección de una directiva para exportar

3. Haga clic en el botón **Exportar**.
4. En la ventana **Guardar como** que se abrirá, ingrese la ruta y el nombre del archivo en el que se guardará la directiva. Haga clic en el botón **Guardar**.

   La ventana **Guardar como** aparecerá solo si utiliza los navegadores Google Chrome, Microsoft Edge u Opera. Si utiliza otro navegador, el archivo de la directiva se guardará automáticamente en la carpeta **Descargas**.

Importación de una directiva

Kaspersky Security Center Linux permite importar una directiva guardada en un archivo KLP. El archivo KLP contiene la directiva exportada, su configuración y sus perfiles.

Para importar una directiva:

1. En el menú principal, vaya a **Administración de activos** → **Directivas**.
2. Haga clic en el botón **Importar**.
3. Haga clic en el botón **Examinar** para elegir el archivo de política que desee importar.
4. En la ventana que se abrirá, ingrese la ruta al archivo KLP de la directiva y haga clic en el botón **Abrir**. Tenga en cuenta que no podrá seleccionar más de un archivo de directiva.

   Comenzará a procesarse la directiva.
5. Una vez que la directiva se haya procesado, seleccione el grupo de administración al que desee aplicarla.
6. Haga clic en el botón **Completado** para finalizar la importación de políticas.

Aparecerá una notificación con los resultados de la importación. Si la tarea se importa correctamente, puede hacer clic en el vínculo **Detalles** para ver las propiedades de la misma.

Una vez que se complete la importación, la directiva aparecerá en la lista de directivas. También se importarán la configuración y los perfiles de la directiva. La directiva importada tendrá estado inactivo independientemente del estado que se haya seleccionado al exportarla. Puede cambiar el estado en las propiedades de la directiva.

Si la directiva importada tiene el mismo nombre que una directiva existente, el nombre de la directiva importada se complementará con un índice secuencial en formato **(<siguiente número secuencial>)**, por ejemplo **(1)** o **(2)**.

Sincronización forzada

En Kaspersky Security Center Linux, el estado, la configuración, las directivas y las tareas de los dispositivos administrados se sincronizan en forma automática. No obstante, en algunos casos se necesita tener la certeza de que la sincronización con un dispositivo puntual se ha realizado.

Sincronizar un solo dispositivo

Para forzar la sincronización entre el Servidor de administración y un dispositivo administrado:

1. En el menú principal, vaya a **Administración de activos** → **Dispositivos administrados**.
2. Haga clic en el nombre del dispositivo que desee sincronizar con el Servidor de administración.
   Se abrirá una ventana de propiedades con la sección **General** seleccionada.
3. Haga clic en el botón **Forzar sincronización**.

La aplicación sincronizará el dispositivo seleccionado con el Servidor de administración.

Sincronizar más de un dispositivo

Para forzar la sincronización entre el Servidor de administración y varios dispositivos administrados:

1. Abra la lista de dispositivos de un grupo de administración o una selección de dispositivos:
   - Genere una selección de dispositivos para ver la lista de dispositivos.
   - En el menú principal, vaya a **Administración de activos** → **Dispositivos administrados** y, luego, seleccione el grupo de administración que contenga los dispositivos para sincronizar:
     - Para el grupo raíz, puede continuar con el siguiente paso.
     - Para un subgrupo, haga clic en el botón **Mostrar jerarquía** en la parte superior de la página y, luego, en la ventana que se abre, haga clic en el nombre del subgrupo.

       Verá la ruta al grupo seleccionado en la parte superior de la página. Si es necesario, puede hacer clic en un vínculo con el nombre del grupo de administración para ir al grupo. De forma predeterminada, el último vínculo de la ruta se encuentra inactivo. Además, puede cerrar la ventana de jerarquía si hace clic en el botón **Ocultar jerarquía**.
2. Active las casillas de verificación ubicadas junto a los dispositivos que desee sincronizar con el Servidor de administración.
3. Haga clic en el botón de los tres puntos (...) ubicado sobre la lista de dispositivos administrados. A continuación, haga clic en el botón **Forzar sincronización**.

   La aplicación sincronizará los dispositivos seleccionados con el Servidor de administración.
4. En la lista de dispositivos, verifique a qué hora se registró la última conexión de los dispositivos seleccionados con el Servidor de administración. La hora debería haber cambiado a la actual. Si la hora no cambió, haga clic en el botón **Actualizar** para actualizar el contenido de la página.

Los dispositivos seleccionados quedan sincronizados con el Servidor de administración.

Ver la hora de entrega de una directiva

Después de cambiar una directiva para una aplicación de Kaspersky en el Servidor de administración, el administrador puede verificar si la directiva modificada se ha entregado a un dispositivo administrado específico. Una directiva se puede entregar durante una sincronización regular o una sincronización forzada.

Para ver la fecha y la hora en que la directiva de una aplicación se entregó a un dispositivo administrado:

1. En el menú principal, vaya a **Administración de activos** → **Dispositivos administrados**.
2. Haga clic en el nombre del dispositivo que desee sincronizar con el Servidor de administración.

   Se abrirá una ventana de propiedades con la sección **General** seleccionada.
3. Haga clic en la pestaña **Aplicaciones**.

4. Seleccione la aplicación para la que desee ver la fecha de sincronización de la directiva.

   Se abrirá la ventana de la directiva de la aplicación. La sección **General** estará seleccionada. Allí encontrará la fecha y la hora en que se entregó la directiva.

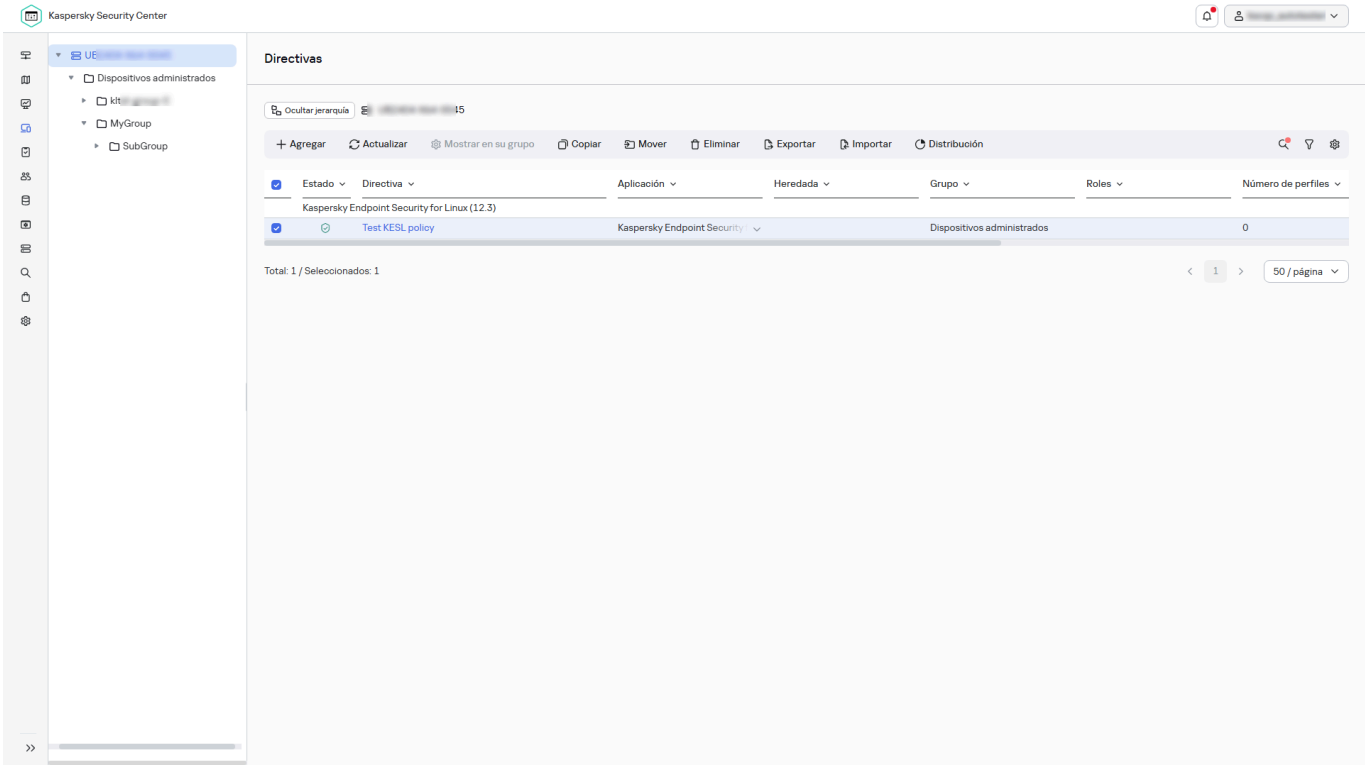
Ver el gráfico de distribución de una directiva

Kaspersky Security Center Linux permite ver el estado de aplicación de una directiva en cada dispositivo a través de un gráfico que representa el estado de distribución de la directiva.

Para ver el estado de distribución de una directiva en cada dispositivo:

1. En el menú principal, vaya a **Administración de activos** → **Directivas**.

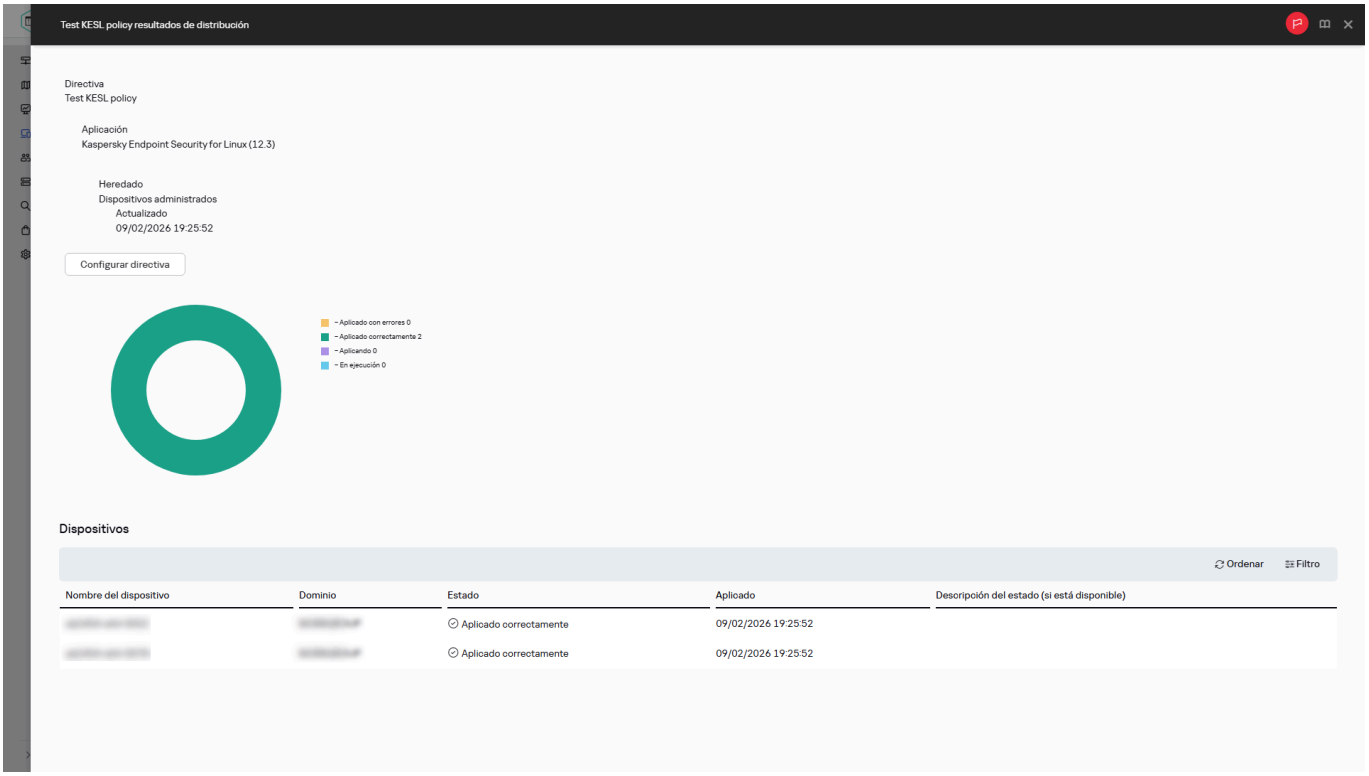
2. Marque la casilla ubicada junto a la directiva cuyo estado de distribución desee conocer.



La lista de directivas

3. En el menú que aparece, seleccione el vínculo **Distribución**.

Se abre la ventana **<Nombre de la directiva>: resultados de la distribución**.



Los resultados de la distribución de la directiva

4. En la ventana **<Nombre de la directiva>: resultados de la distribución**, encontrará la **Descripción del estado** de la directiva.

Puede cambiar la cantidad de resultados que aparecen en la lista que detalla la distribución de la directiva. El número máximo de dispositivos es 100 000.

Para cambiar la cantidad de dispositivos que se muestran en la lista con los resultados de la distribución de una directiva:

1. En el menú principal, vaya a **Configuración** → **Opciones de interfaz**.
2. En **Límite de dispositivos que se incluirán en los resultados de distribución de las directivas**, ingrese el número de dispositivos (hasta 100 000).

   De manera predeterminada, el límite es de 5000.
3. Haga clic en el botón **Guardar**.

   El cambio se aplica y se guarda.

Activar una directiva automáticamente ante un brote de virus

Para que una directiva se active automáticamente al ocurrir un evento Brote de virus, haga lo siguiente:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana de propiedades del Servidor de administración, con la pestaña **General** seleccionada.
2. Elija la sección **Brote de virus**.

3. En el panel de la derecha, haga clic en el vínculo **Configurar las directivas que se activarán ante un brote de virus**.

   Se abre la ventana **Activación de directiva**.

4. En la sección relativa al componente que detecta el brote de virus ("Antivirus para estaciones de trabajo y servidores de archivos", "Antivirus para servidores de correo" o "Antivirus para defensa del perímetro"), busque la entrada que desea, seleccione la opción adyacente a la misma y haga clic en el botón **Agregar**.

   Se abre una ventana con el grupo de administración **Dispositivos administrados**.

5. Haga clic en el ícono (›) ubicado junto a **Dispositivos administrados**.

   Se muestra una jerarquía de grupos de administración y sus directivas.

6. En la jerarquía de grupos de administración y directivas, haga clic en el nombre de la directiva que se activará cuando se detecte un brote de virus. Puede seleccionar más de una directiva.

   Para seleccionar todas las directivas incluidas en el grupo o en la lista, marque la casilla ubicada junto al nombre pertinente.

7. Haga clic en el botón **Guardar**.

   Se cierra la ventana con la jerarquía de grupos de administración y directivas.

Las directivas seleccionadas se agregan a la lista de directivas que se activarán cuando se detecte un brote de virus. Estas directivas se activarán independientemente del estado que tengan antes del brote de virus (activa o inactiva).

Si se activó una directiva en el evento de Brote de virus, solo puede volver a la directiva anterior utilizando el modo manual.

Eliminar una directiva

Puede eliminar una directiva si ya no la necesita. Puede eliminar directivas que el grupo de administración especificado no haya heredado. Una directiva heredada solo se puede eliminar en el grupo de administración de nivel superior para el que fue creada.

Para eliminar una directiva:

1. En el menú principal, vaya a **Administración de activos** → **Directivas**.

2. Marque la casilla ubicada junto a la directiva que desee eliminar y haga clic en **Eliminar**.

   El botón **Eliminar** no estará disponible (estará atenuado) si se ha seleccionado una directiva heredada.

3. Haga clic en **Aceptar** para confirmar la operación.

La directiva se elimina junto con todos sus perfiles. Una vez eliminada la directiva, los eventos de cambio de directiva se exportan al sistema SIEM si esta opción está habilitada.

Administración de perfiles de directivas

Esta sección trata sobre la administración de perfiles de directivas. Encontrará instrucciones para ver los perfiles de una directiva; cambiar la prioridad de un perfil de directiva; crear un perfil de directiva; copiar un perfil de directiva; crear una regla de activación para un perfil de directiva; y eliminar, exportar e importar un perfil de directiva.

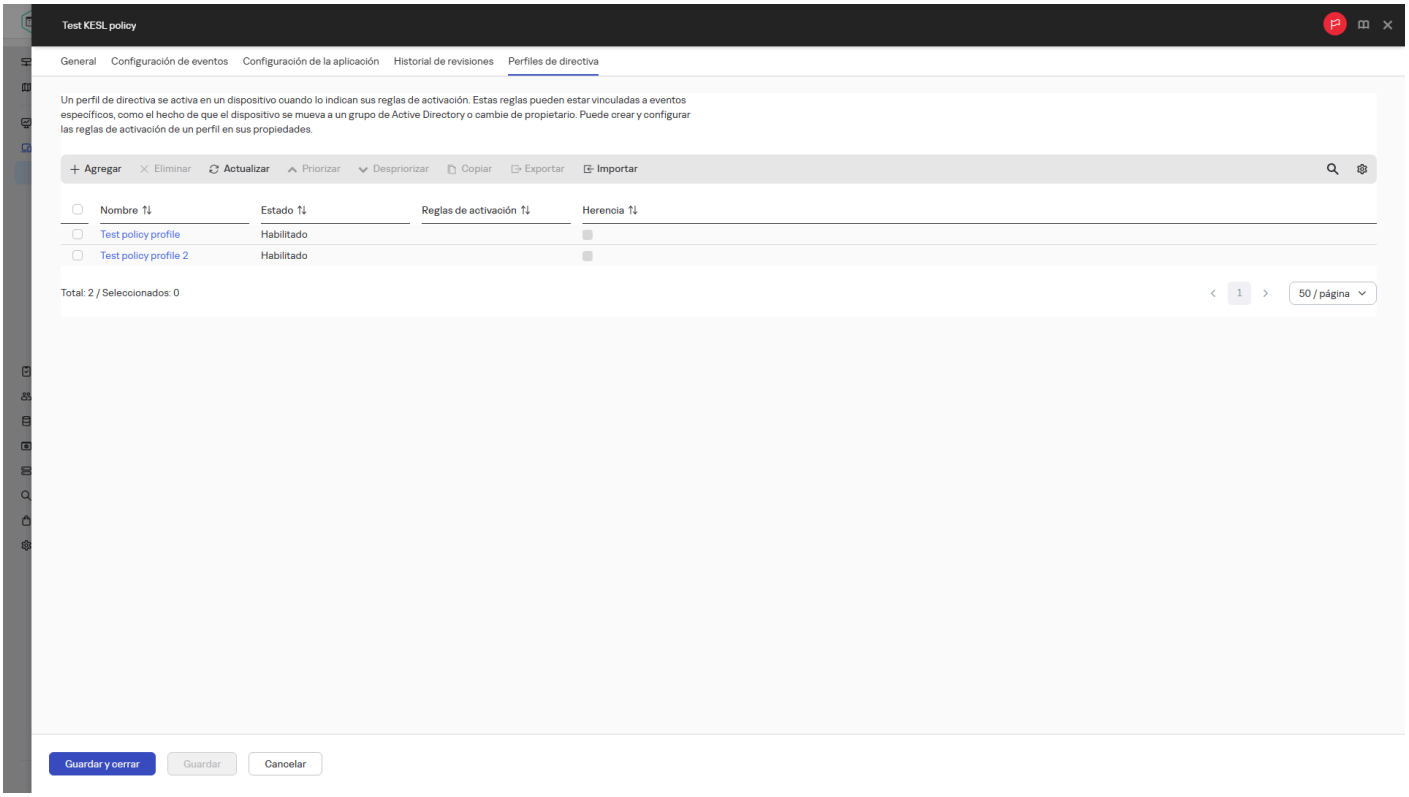
Ver los perfiles de una directiva

Para ver los perfiles de una directiva:

1. En el menú principal, vaya a **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva cuyos perfiles desee ver.

   Se abre la ventana de propiedades de la directiva, con la pestaña **General** seleccionada.
3. Abra la pestaña **Perfiles de directiva**.

Aparece la lista de perfiles de directiva en formato tabular. Si la directiva no tiene perfiles, verá una tabla vacía.



La lista de perfiles de la directiva

Cambiar la prioridad de un perfil de directiva

Para cambiar la prioridad de un perfil de directiva:

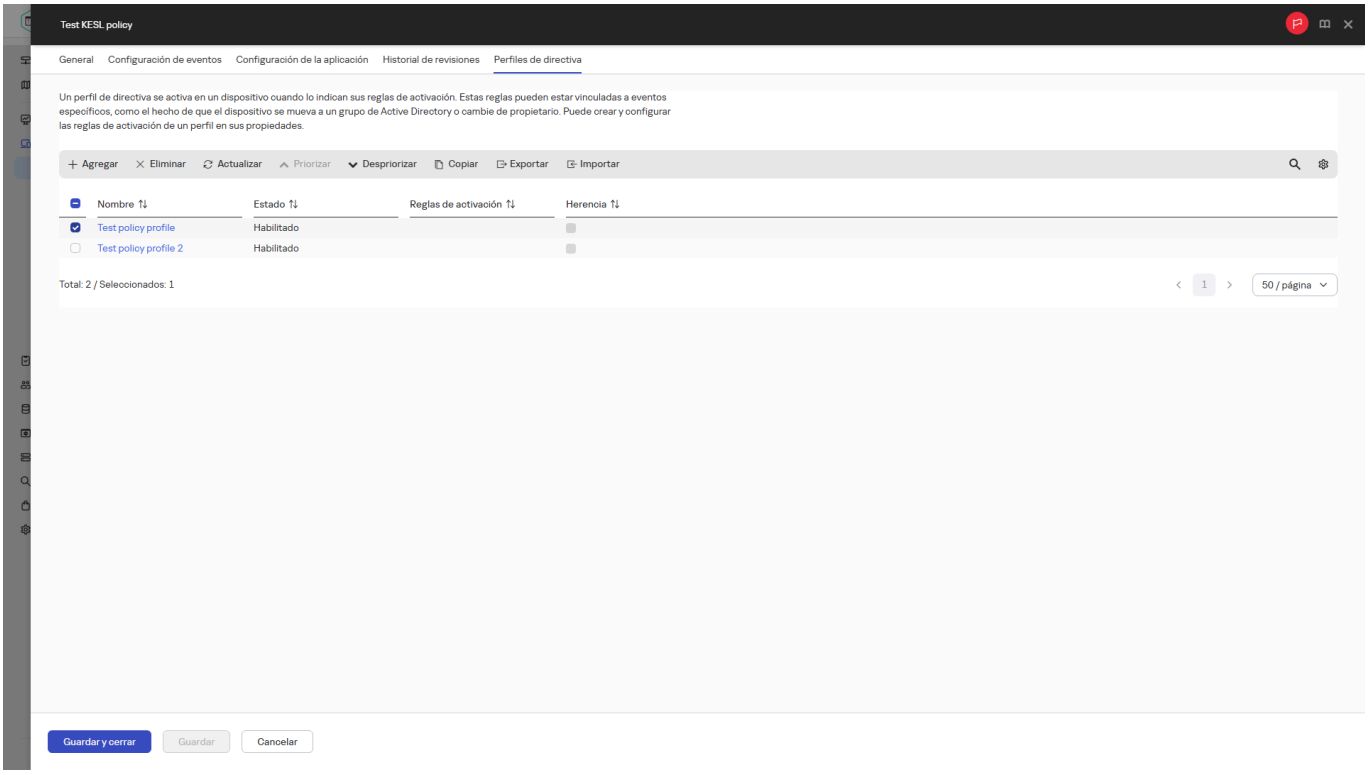
1. Abra la lista de perfiles de la directiva pertinente.

   Se abre la lista de perfiles de la directiva.

2. En la pestaña **Perfiles de directiva**, marque la casilla correspondiente al perfil de directiva que cambiará de prioridad.

3. Cambie la posición del perfil de directiva en la lista haciendo clic en los botones **Priorizar** o **Despriorizar**.

   Cuanto más arriba en la lista se encuentre el perfil de directiva, mayor será su prioridad.



4. Haga clic en el botón **Guardar**.

Se aplica la nueva prioridad del perfil de directiva seleccionado.

Crear un perfil de directiva

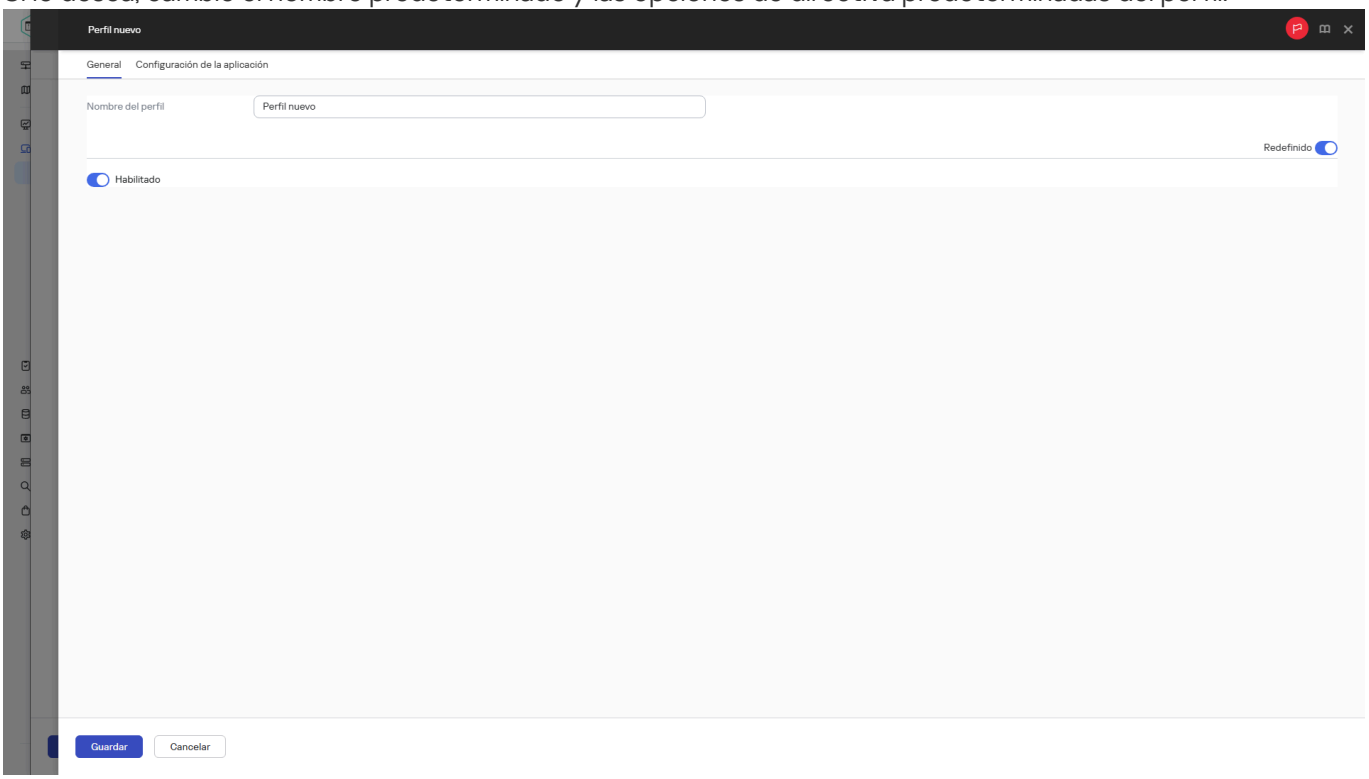
Para crear un perfil de directiva:

1. Abra la lista de perfiles de la directiva pertinente.

   Se abre la lista de perfiles de la directiva. Si la directiva no tiene perfiles, verá una tabla vacía.

2. Haga clic en **Agregar**.

3. Si lo desea, cambie el nombre predeterminado y las opciones de directiva predeterminadas del perfil.



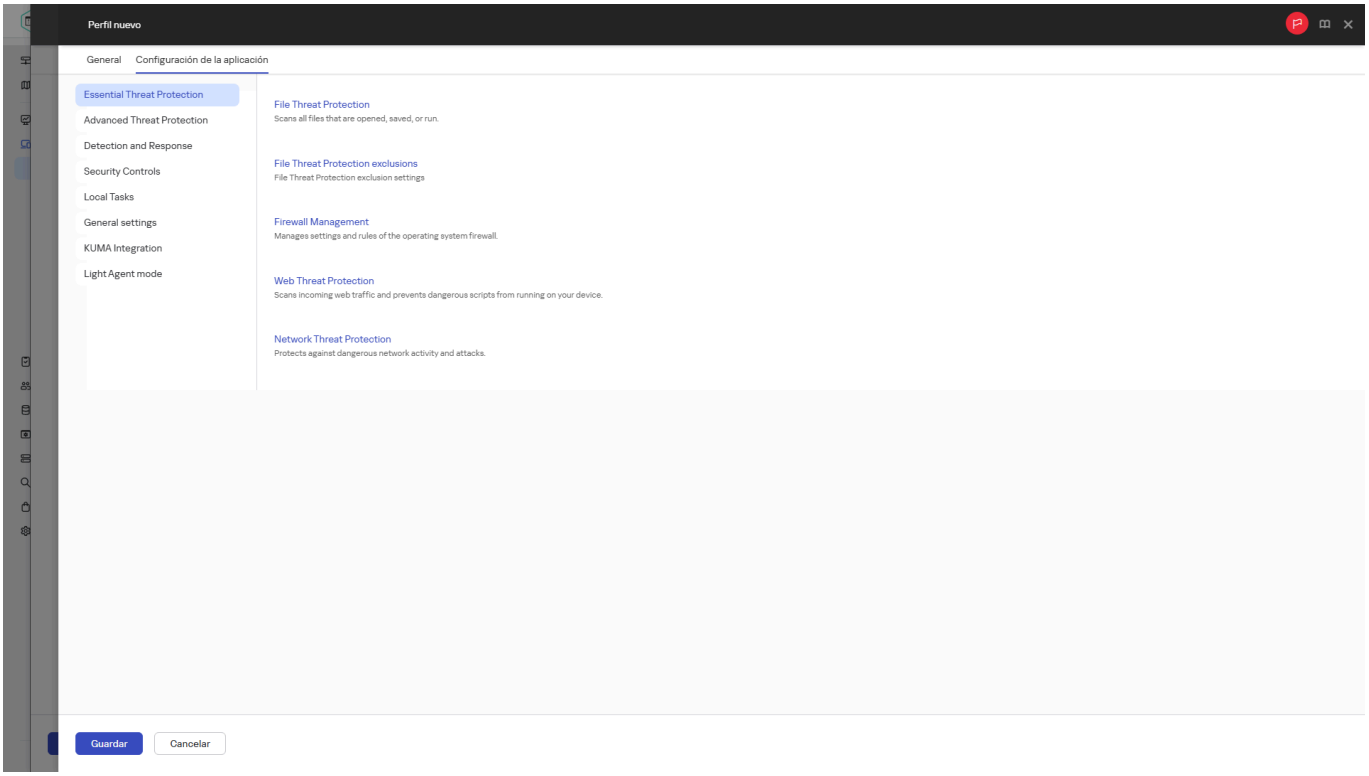
Crear un perfil de directiva

4. Seleccione la pestaña **Configuración de la aplicación**.

   O, si lo prefiere, puede hacer clic en **Guardar** y salir. El perfil que creó aparece en la lista de perfiles de directivas y podrá editar su configuración más adelante.

5. En la pestaña **Configuración de la aplicación**, en el panel izquierdo, seleccione la categoría que desea y, en el panel de resultados de la derecha, edite la configuración del perfil. Puede editar los ajustes disponibles en cada categoría (sección) para el perfil de directiva.

Al editar la configuración, puede hacer clic en **Cancelar** para cancelar la última operación.



Especificar la configuración del perfil de directiva

6. Haga clic en **Guardar** para guardar el perfil.

   El perfil aparecerá en la lista de perfiles de directiva.

Copiar un perfil de directiva

Puede copiar un perfil de directiva a la directiva actual o a otra si, por ejemplo, quiere tener perfiles idénticos para directivas diferentes. También puede copiar un perfil si necesita tener dos o más perfiles que se diferencien solo en un pequeño número de ajustes.

Para copiar un perfil de directiva:

1. Abra la lista de perfiles de la directiva pertinente.

   Se abre la lista de perfiles de la directiva. Si la directiva no tiene perfiles, verá una tabla vacía.

2. En la pestaña **Perfiles de directiva**, seleccione el perfil de directiva que desee copiar.

3. Haga clic en **Copiar**.

4. En la ventana que se abre, seleccione la directiva a la que desee copiar el perfil.

   Puede copiar un perfil de directiva en la misma directiva o en una directiva que especifique.

5. Haga clic en **Copiar**.

El perfil de directiva se copia a la directiva seleccionada. La copia del perfil obtiene la prioridad más baja. Cuando un perfil se copia a su misma directiva de origen, se agrega un índice numérico entre paréntesis al nombre de la copia (por ejemplo: (1), (2), etc.).

Más adelante, podrá cambiar la configuración del perfil de directiva, incluidos el nombre y la prioridad. En este caso, el perfil de directiva original no cambia.

Crear una regla de activación para un perfil de directiva

Para crear una regla de activación para un perfil de directiva:

1. Abra la lista de perfiles de la directiva pertinente.

   Se abre la lista de perfiles de la directiva.

2. En la pestaña **Perfiles de directiva**, haga clic en el perfil de directiva para el que desee crear la regla de activación.

   Si la lista de perfiles de la directiva está vacía, puede crear un perfil de directiva.

3. En la pestaña **Reglas de activación**, haga clic en el botón **Agregar**.

   Se abre la ventana con las reglas de activación del perfil de directiva.

4. Escriba un nombre para la regla.

5. Active las casillas de verificación ubicadas junto a las condiciones que afectarán la activación del nuevo perfil de directiva:

   Reglas generales para la activación del perfil de directiva

   Marque esta casilla para configurar reglas que hagan que el perfil de directiva se active en un dispositivo dependiendo del estado del modo sin conexión de ese dispositivo, de las reglas de conexión con el Servidor de administración o de las etiquetas que el dispositivo tenga asignadas.

   Si elige esta opción, defina esto en el paso siguiente:

   Estado del dispositivo

   Define la condición relativa a la presencia del dispositivo en la red:

   - **En línea**: el dispositivo está en la red, lo que significa que el Servidor de administración está disponible.
   - **Sin conexión**: el dispositivo está en una red externa, lo que significa que el Servidor de administración no está disponible.
   - **N/D**: no se aplica este criterio.

   Ubicación de red del dispositivo

   Elija la condición de activación del perfil de directiva (el hecho de que la regla se ejecute o no) y seleccione el nombre de la regla.

   La regla define la ubicación de red del dispositivo para la conexión con el Servidor de administración. Las condiciones de esta regla se deben cumplir (o no se deben cumplir) para que se active el perfil de directiva.

   Puede crear o configurar una descripción de ubicación de red de dispositivos para la conexión con un Servidor de administración en una regla de cambio de Agente de red.

   - **Reglas para un propietario del dispositivo específico**

     Si elige esta opción, defina esto en el paso siguiente:

     Propietario del dispositivo

Habilite esta opción para configurar y habilitar una regla que haga que el perfil se active en un dispositivo dependiendo de quién sea el propietario del mismo. En la lista desplegable bajo la casilla, seleccione el criterio que determinará la activación del perfil:

- El dispositivo pertenece al propietario especificado (signo "=").
- El dispositivo no pertenece al propietario especificado (signo "#").

  Si habilita esta opción, el perfil se activará en el dispositivo siguiendo el criterio configurado. Podrá señalar al propietario del dispositivo una vez que habilite la opción. Si no habilita esta opción, no se usará este criterio para regular la activación del perfil. Esta opción está deshabilitada de forma predeterminada.

El propietario del dispositivo está incluido en un grupo de seguridad interno

Habilite esta opción para configurar y habilitar una regla que haga que el perfil se active en un dispositivo dependiendo de si su propietario pertenece a un grupo de seguridad interno de Kaspersky Security Center Linux. En la lista desplegable bajo la casilla, seleccione el criterio que determinará la activación del perfil:

- El propietario del dispositivo es miembro del grupo de seguridad especificado (signo "=").
- El propietario del dispositivo no es miembro del grupo de seguridad especificado (signo "#").

  Si habilita esta opción, el perfil se activará en el dispositivo siguiendo el criterio configurado. Podrá especificar el nombre de un grupo de seguridad de Kaspersky Security Center Linux. Si no habilita esta opción, no se usará este criterio para regular la activación del perfil. Esta opción está deshabilitada de forma predeterminada.

- **Reglas para las especificaciones del hardware**

  Marque esta casilla para configurar reglas que hagan que el perfil de directiva se active en un dispositivo dependiendo de la cantidad de memoria y del número de procesadores lógicos que el dispositivo tenga.

  Si elige esta opción, defina esto en el paso siguiente:

  Tamaño de RAM, en MB

  Habilite esta opción para configurar y habilitar una regla que haga que el perfil se active en un dispositivo en función de la cantidad de RAM que este posea. En la lista desplegable bajo la casilla, seleccione el criterio que determinará la activación del perfil:

  - El tamaño de la RAM del dispositivo está por debajo del valor especificado (signo "<").
  - El tamaño de la RAM del dispositivo está por encima del valor especificado (signo ">").

  Si habilita esta opción, el perfil se activará en el dispositivo siguiendo el criterio configurado. Podrá especificar la cantidad de RAM con la que deberá contar el dispositivo. Si no habilita esta opción, no se usará este criterio para regular la activación del perfil. Esta opción está deshabilitada de forma predeterminada.

  Número de procesadores lógicos

  Habilite esta opción para configurar y habilitar una regla que haga que el perfil se active en un dispositivo en función del número de procesadores lógicos que este tenga. En la lista desplegable bajo la casilla, seleccione el criterio que determinará la activación del perfil:

  - El número de procesadores lógicos del dispositivo es menor o igual que el valor especificado (signo "<").
  - El número de procesadores lógicos del dispositivo es mayor o igual que el valor especificado (signo ">").

  Si habilita esta opción, el perfil se activará en el dispositivo siguiendo el criterio configurado. Podrá especificar la cantidad de procesadores lógicos con los que deberá contar el dispositivo. Si no habilita esta opción, no se usará este criterio para regular la activación del perfil. Esta opción está deshabilitada de forma predeterminada.

- **Reglas para la asignación de roles**

  Si elige esta opción, defina esto en el paso siguiente:

  Activar el perfil de directiva según el rol específico del propietario del dispositivo

  Seleccione esta opción para configurar y habilitar una regla que haga que el perfil se active en un dispositivo dependiendo del rol asignado al propietario del mismo. Utilice la lista de roles existentes para agregar el rol en forma manual.

  Si habilita esta opción, el perfil se activará en el dispositivo siguiendo el criterio configurado.

- **Reglas para el uso de la etiqueta**

  Marque esta casilla para configurar reglas que hagan que el perfil de directiva se active en un dispositivo dependiendo de las etiquetas asignadas al mismo. El perfil de directiva podrá activarse en dispositivos que tengan las etiquetas seleccionadas o que no tengan esas etiquetas.

  Si elige esta opción, defina esto en el paso siguiente:

  Lista de etiquetas

  En la lista de etiquetas, configure la regla que hará que los dispositivos que tengan ciertas etiquetas se incluyan en el perfil de directiva. Para configurar esta regla, active las casillas ubicadas junto a las etiquetas pertinentes.

  Si necesita agregar etiquetas nuevas, introdúzcalas en el campo que se encuentra sobre la lista y haga clic en el botón **Agregar**.

  El perfil de directiva incluirá aquellos dispositivos que, en su descripción, contengan todas las etiquetas seleccionadas. Si no activa estas casillas, no se aplicará este criterio. Estas casillas están desactivadas de manera predeterminada.

  Aplicar a los dispositivos que no tengan las etiquetas especificadas

  Habilite esta opción si tiene que invertir la selección de etiquetas.

  Si habilita esta opción, el perfil de directiva incluirá aquellos dispositivos que no tengan, en su descripción, ninguna de las etiquetas seleccionadas. Si deshabilita esta opción, no se aplicará el criterio.

  Esta opción está deshabilitada de forma predeterminada.

- **Reglas para el uso de Active Directory**

  Marque esta casilla para configurar reglas que hagan que el perfil de directiva se active en un dispositivo si el mismo pertenece a una unidad organizativa de Active Directory en particular o si el dispositivo o su propietario son miembros de un grupo de seguridad de Active Directory.

  Si elige esta opción, defina esto en el paso siguiente:

  Membrecía del propietario del dispositivo en un grupo de seguridad de Active Directory

  Si habilita esta opción, el perfil de directiva se activará en un dispositivo si su propietario es miembro del grupo de seguridad especificado. Si no habilita esta opción, no se usará este criterio para regular la activación del perfil. Esta opción está deshabilitada de forma predeterminada.

  Membrecía del dispositivo en un grupo de seguridad de Active Directory

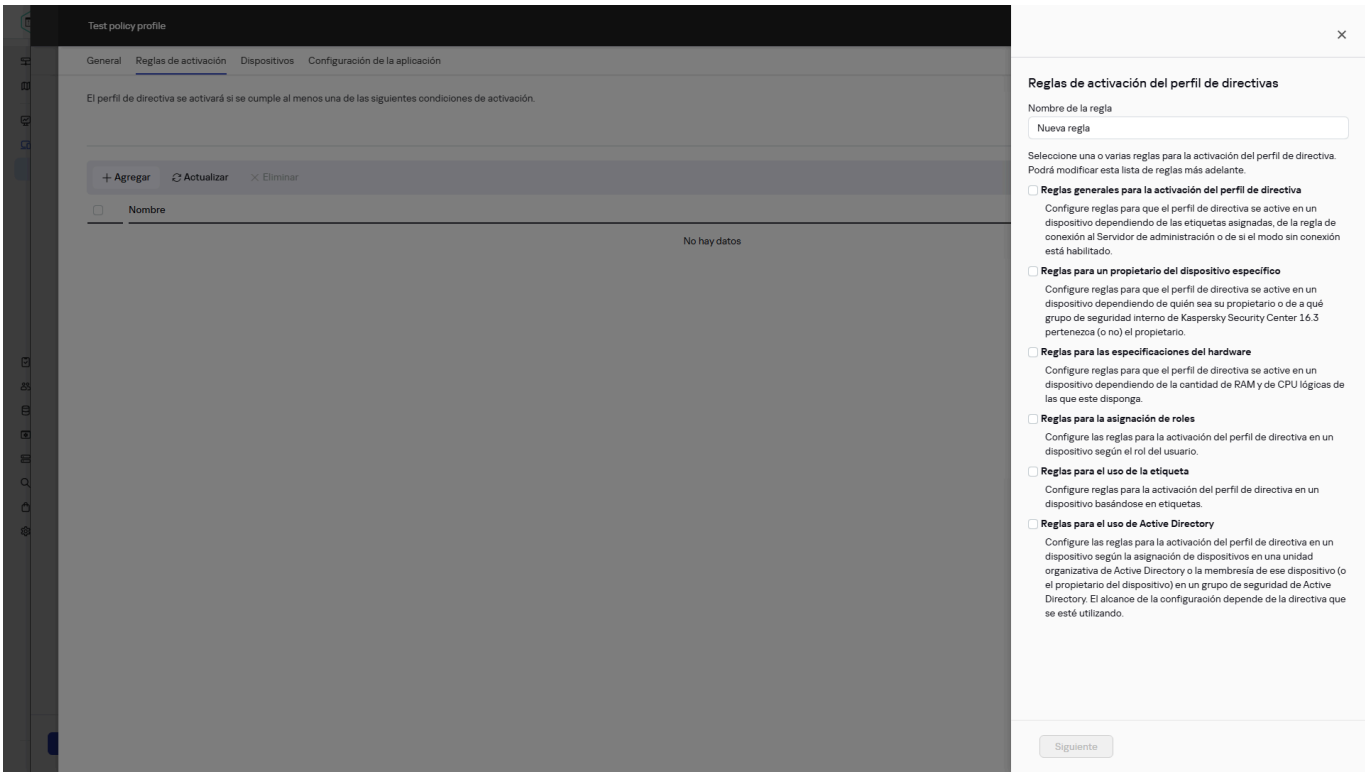
  Si habilita esta opción, el perfil de directiva se activará en el dispositivo. Si no habilita esta opción, no se usará este criterio para regular la activación del perfil. Esta opción está deshabilitada de forma predeterminada.

  Asignación de dispositivos en la unidad organizativa de Active Directory

Si habilita esta opción, el perfil de directiva se activará en un dispositivo si el mismo está incluido en la unidad organizativa de Active Directory especificada. Si no habilita esta opción, no se usará este criterio para regular la activación del perfil.

Esta opción está deshabilitada de forma predeterminada.

El número de páginas adicionales del asistente dependerá de las opciones que haya elegido en el primer paso. Podrá modificar las reglas de activación del perfil de directiva más adelante.



Crear una regla de activación para un perfil de directiva

6. Revise la lista de parámetros configurados. Si no hay errores en la lista, haga clic en **Crear**.

Se guardará el perfil. El perfil se activará en el dispositivo cuando se desencadenen las reglas de activación.

Las reglas de activación creadas para un perfil de directiva se muestran en las propiedades del perfil, dentro de la pestaña **Reglas de activación**. Puede modificar o eliminar cualquiera de las reglas de activación del perfil de directiva.

Existe la posibilidad de que varias reglas de activación se desencadenen simultáneamente.

Eliminar un perfil de directiva

Para eliminar un perfil de directiva:

1. Abra la lista de perfiles de la directiva pertinente.

Se abre la lista de perfiles de la directiva.

2. En la pestaña **Perfiles de directiva**, marque la casilla ubicada junto al perfil de directiva que desee eliminar y haga clic en **Eliminar**.

3. En la ventana que se abre, haga clic de nuevo en **Eliminar**.

   El perfil de directiva se elimina. Si la directiva es heredada por un grupo de nivel inferior, el perfil permanece en ese grupo pero se convierte en el perfil de la directiva de ese grupo. De este modo, se evitan cambios radicales en la configuración de las aplicaciones administradas que se encuentran instaladas en los dispositivos de los grupos de nivel inferior.

Exportación e importación de un perfil de directiva

Puede guardar un perfil de directiva en un archivo KLPROF sin exportar una directiva y luego usar este archivo KLPROF para importar el perfil guardado a la directiva.

Esto le permite restaurar la configuración de la directiva de perfil rápidamente, en lugar de volver a configurarla.

Un perfil de directiva se importa a la directiva de la misma versión de la aplicación desde la cual exportó el perfil. Para aplicaciones que admiten la compatibilidad con versiones anteriores de directivas (por ejemplo, Kaspersky Endpoint Security para Windows), puede importar perfiles de directiva a diferentes versiones de la directiva.

Para exportar un perfil de directiva:

1. Abra la lista de perfiles de la directiva pertinente.

   Se abre la lista de perfiles de la directiva.

2. En la pestaña **Perfiles de directiva**, haga clic en el perfil de directiva que desee exportar.

3. En la barra de herramientas, haga clic en el botón **Exportar**.

4. En la ventana que se abre, especifique el directorio en el que desea guardar el archivo con el perfil de la directiva.

   Puede cambiar el nombre del archivo, si es necesario.

5. Haga clic en el botón **Guardar**.

   Si la operación se completa con éxito, se muestra el mensaje correspondiente en la pantalla. De lo contrario, se muestra un mensaje de error.

Para importar un perfil de directiva:

1. Abra la lista de perfiles de la directiva pertinente.

   Se abre la lista de perfiles de la directiva.

2. En la barra de herramientas, haga clic en el botón **Importar**.

3. En la ventana que se abre, seleccione el archivo KLPROF con el perfil de directiva requerido y luego haga clic en el botón **Abrir**.

   El tamaño máximo del archivo importado es de 4 MB.

Si la operación se completa con éxito, se muestra el mensaje correspondiente en la pantalla. De lo contrario, se muestra un mensaje de error.

El perfil de directiva se importa con el nombre que tenía cuando lo exportó, no con el nombre del archivo KLPROF.
El archivo se importa con el estado **Deshabilitado** y la prioridad más baja, independientemente de la prioridad que tenía el perfil de directiva antes de la exportación.

No puede realizar la importación:

- si la directiva ya tiene un perfil con el mismo nombre;
- si la cantidad de perfiles en la directiva es 100.

Ajustes de la directiva del Agente de red

Para configurar la directiva del Agente de red:

1. En el menú principal de la aplicación, vaya a **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva del Agente de red.

   Se abre la ventana de propiedades de la directiva del Agente de red. La ventana de propiedades contiene las pestañas y los ajustes que se describen a continuación.

Consulte la tabla comparativa que detalla cómo se aplican las configuraciones a continuación, según el tipo de sistema operativo utilizado.

General

En esta pestaña, puede cambiar el nombre y el estado de la directiva, así como modificar los ajustes que controlan la herencia de sus valores de configuración:

- En el campo **Nombre**, puede modificar el nombre de la directiva.
- A través del bloque **Estado de la directiva**, puede seleccionar uno de los modos posibles para la directiva:

  Activa

  Si se selecciona esta opción, se activa la directiva.

  Esta opción está seleccionada de forma predeterminada.

  Inactiva

Si selecciona esta opción, la directiva estará inactiva, pero quedará guardada en la carpeta **Directivas**. Podrá activarla cuando resulte necesario.

- En el grupo de ajustes **Herencia de configuración**, puede configurar las opciones de directiva:

  Heredar configuración de la directiva primaria

  Si habilita esta opción, la directiva heredará los valores de configuración definidos en la directiva del grupo de nivel superior. Estos valores, en consecuencia, estarán bloqueados.

  Esta opción está activada de forma predeterminada.

  Forzar la herencia de configuración en las directivas secundarias

  Si habilita esta opción, cuando modifique la directiva y se apliquen los cambios, ocurrirá lo siguiente:

  - Los valores de configuración de la directiva se propagarán a las directivas de los subgrupos de administración (es decir, a las directivas secundarias).
  - En la ventana de propiedades de cada directiva secundaria, dentro del bloque **Herencia de configuración** de la sección **General**, se habilitará automáticamente la opción **Heredar configuración de la directiva primaria**.

  Habilitar esta opción hace que los ajustes de las directivas secundarias se bloqueen.

  Esta opción está deshabilitada de forma predeterminada.

Configuración de eventos

En esta pestaña, puede configurar el registro de eventos y las notificaciones de eventos. Los eventos se organizan por nivel de importancia en estas secciones:

- **Error funcional**
- **Advertencia**
- **Información**

Cada sección contiene una lista con los distintos tipos de eventos y la cantidad de días por la que cada evento se deja almacenado, de manera predeterminada, en el Servidor de administración. Cuando hace clic en un tipo de evento, puede especificar el registro de eventos y las notificaciones relativas a los eventos seleccionados en la lista. De manera predeterminada, la configuración de notificación general especificada para todo el Servidor de administración se utiliza para todos los tipos de eventos. Sin embargo, puede cambiar configuraciones específicas para los tipos de eventos requeridos.

Por ejemplo, en la sección **Advertencia**, puede configurar el tipo de evento **Ocurrió un problema de seguridad**. Tales eventos pueden ocurrir, por ejemplo, cuando el espacio libre en el disco de un punto de distribución es inferior a 2 GB (se requieren al menos 4 GB para instalar aplicaciones y descargar actualizaciones de forma remota). Para configurar el evento **Ocurrió un problema de seguridad**, haga clic en este y especifique dónde almacenar los eventos ocurridos y cómo notificarlos.

> Si el Agente de red detecta un problema de seguridad, puede administrar este problema utilizando la configuración de un dispositivo administrado.

Configuración

En la sección **Configuración**, puede configurar la directiva del Agente de red:

Distribuir archivos solo a través de los puntos de distribución

Si se habilita esta opción, los Agentes de red en los dispositivos administrados recuperarán las actualizaciones solo de los puntos de distribución.

Si se deshabilita esta opción, los Agentes de red en los dispositivos administrados recuperarán las actualizaciones de los puntos de distribución o del Servidor de administración.

> Tenga en cuenta que las aplicaciones de seguridad en los dispositivos administrados recuperan las actualizaciones del conjunto de origen de la tarea de actualización para cada aplicación de seguridad. Si habilita la opción **Distribuir archivos solo a través de los puntos de distribución**, asegúrese de que Kaspersky Security Center Linux esté configurado como origen de actualizaciones en las tareas de actualización.

Esta opción está deshabilitada de forma predeterminada.

Tamaño máximo de la cola de eventos, en MB

En este campo se puede especificar el espacio máximo que puede ocupar una cola de evento en la unidad.

La configuración predeterminada es 2 MB.

La aplicación podrá obtener información adicional sobre la directiva en el dispositivo

La aplicación de seguridad de un dispositivo administrado (por ejemplo, Kaspersky Endpoint Security for Linux) recibe, del Agente de red instalado en el mismo dispositivo, información sobre la directiva aplicada para ella. Si lo desea, puede ver esta información en la interfaz de la aplicación de seguridad.

El Agente de red le brinda los siguientes datos a la aplicación:

- Hora en que la directiva se entregó en el dispositivo administrado.
- Nombre de la directiva activa que se encontraba vigente cuando la directiva se entregó en el dispositivo administrado.
- Nombre de la directiva fuera de la oficina que se encontraba vigente cuando la directiva se entregó en el dispositivo administrado (no disponible en el Agente de red para Linux).
- Nombre y ruta completa al grupo de administración en el que se encontraba el dispositivo administrado cuando la directiva se entregó en el dispositivo administrado.
- Lista de perfiles de directivas activas que se encontraban vigentes cuando la directiva se entregó en el dispositivo administrado, con sus nombres y prioridades.

Puede utilizar esta información para solucionar problemas o verificar que la directiva aplicada al dispositivo sea la esperada. Esta opción está deshabilitada de forma predeterminada.

Evitar que el servicio del Agente de red se detenga o se elimine sin autorización e impedir cambios en su configuración

Cuando esta opción está habilitada, una vez que el Agente de red se encuentre instalado en un dispositivo administrado, no se lo podrá eliminar ni reconfigurar a menos que se tengan los privilegios necesarios. El servicio del Agente de red no se podrá detener. Esta opción no tiene efecto en los controladores de dominio.

Habilite esta opción para proteger el Agente de red en estaciones de trabajo operadas con derechos de administrador local.

Esta opción está deshabilitada de forma predeterminada.

Utilizar contraseña de desinstalación

Si activa esta opción y hace clic en el botón **Modificar**, podrá especificar la contraseña para la utilidad klmover y la desinstalación remota del Agente de red en dispositivos Windows.

Esta opción está deshabilitada de forma predeterminada.

Repositorios

En la sección **Repositorios**, puede seleccionar los tipos de objetos acerca de los cuales el Agente de red enviará detalles al Servidor de administración:

Detalles de las aplicaciones instaladas

Si se habilita esta opción, la información sobre las aplicaciones instaladas en los dispositivos cliente se enviará al Servidor de administración.

Esta opción está activada de forma predeterminada.

Incluir información sobre parches

Se enviará información al Servidor de administración sobre los parches de las aplicaciones instaladas en los dispositivos clientes. Si habilita esta opción, podría aumentar la carga del Servidor de administración y del sistema de administración de bases de datos (DBMS). También podría aumentar el volumen de la base de datos.

Esta opción está activada de forma predeterminada. Está disponible solo para Windows.

Detalles de las actualizaciones de Windows Update

Si esta opción está habilitada, se enviará información al Servidor de administración sobre las actualizaciones de Microsoft Windows Update que deban instalarse en los dispositivos cliente.

Esta opción está activada de forma predeterminada. Está disponible solo para Windows.

La información sobre las actualizaciones opcionales de Microsoft Windows no se envía al Servidor de administración.

Detalles de vulnerabilidades de software y actualizaciones correspondientes

Si esta opción está habilitada, se enviará información al Servidor de administración sobre las vulnerabilidades que se detecten en las aplicaciones de terceros instaladas en los dispositivos administrados (incluidas las aplicaciones de Microsoft) y sobre las actualizaciones disponibles para reparar vulnerabilidades en aplicaciones de terceros (excluidas, en este caso, las aplicaciones de Microsoft).

Si habilita la opción **Detalles de las vulnerabilidades de software y las actualizaciones correspondientes**, aumentarán la carga en la red, la carga en el disco del Servidor de administración y el uso de recursos del Agente de red.

Esta opción está activada de forma predeterminada. Está disponible solo para Windows.

Para administrar las actualizaciones de software de Microsoft, use la opción **Detalles de las actualizaciones de Windows Update**.

Detalles del registro de hardware

Cuando el Agente de red está instalado en un dispositivo, envía información acerca del hardware de dicho dispositivo al Servidor de administración. Puede ver los detalles del hardware en las propiedades del dispositivo.

Asegúrese de que la utilidad lshw esté instalada en los dispositivos Linux desde los que desea obtener detalles del hardware. Los detalles de hardware obtenidos de las máquinas virtuales pueden estar incompletos según el hipervisor que se utilice.

La directiva del Agente de red podría impedirle modificar algunos ajustes de esta sección.

Actualizaciones y vulnerabilidades de software

En la sección **Actualizaciones y vulnerabilidades de software**, puede activar el análisis de archivos ejecutables en busca de vulnerabilidades:

Analizar los archivos ejecutables en busca de vulnerabilidades al iniciarlos

Si habilita esta opción, cuando se inicie un archivo ejecutable, se lo analizará en busca de vulnerabilidades.

Esta opción está activada de forma predeterminada.

Opciones de reinicio

En la sección **Opciones de reinicio**, puede indicar qué acción se llevará a cabo cuando se necesite reiniciar el sistema operativo de un dispositivo administrado para que una aplicación pueda instalarse, desinstalarse o utilizarse correctamente.

No reiniciar el sistema operativo

Cuando termine la operación, los dispositivos cliente no se reiniciarán automáticamente. Para que la operación se complete, deberá reiniciar los dispositivos en forma manual o mediante, por ejemplo, una tarea de administración de dispositivos. Los resultados de la tarea y el estado de cada dispositivo darán cuenta de que hay un reinicio pendiente. Esta opción es útil cuando la tarea va a ejecutarse en servidores y dispositivos que deben operar continuamente.

Reiniciar el sistema operativo automáticamente, de ser necesario

Los dispositivos cliente se reiniciarán automáticamente siempre que resulte necesario para completar la operación. Esta opción es útil cuando la tarea se realiza en dispositivos que admiten una breve interrupción para apagarse o reiniciarse.

Solicitar al usuario una acción

A través de un recordatorio en pantalla, se le pedirá a cada usuario que reinicie su dispositivo manualmente. Puede configurar algunos ajustes avanzados para esta opción: el texto del mensaje que se le muestra al usuario, la frecuencia con la que se muestra este mensaje y el tiempo que se espera antes de reiniciar el dispositivo por la fuerza (sin que el usuario confirme el reinicio). Esta opción es la más adecuada para estaciones de trabajo en las que los usuarios deben poder seleccionar el momento más conveniente para reiniciar.

Esta opción está seleccionada de forma predeterminada.

Repetir la solicitud cada (min)

Si habilita esta opción, la aplicación le solicitará al usuario que reinicie su sistema operativo con la frecuencia especificada.

Esta opción está activada de forma predeterminada. El intervalo por defecto es de 5 minutos. Los valores disponibles van de 1 a 1440 minutos.

Si no habilita esta opción, la solicitud se mostrará una sola vez.

Forzar reinicio después de (min)

Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

Esta opción está activada de forma predeterminada. El tiempo de espera por defecto es de 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

Forzar el cierre de aplicaciones en sesiones bloqueadas

Las aplicaciones abiertas en el dispositivo cliente podrían impedir que se lo reinicie. Si el usuario está editando un documento en un procesador de textos, por ejemplo, y no ha guardado el archivo, el procesador de textos no permitirá que el dispositivo se reinicie.

Si habilita esta opción, las aplicaciones que se estén ejecutando en un dispositivo bloqueado se cerrarán por la fuerza y, tras ello, el dispositivo se reiniciará. Los usuarios podrían perder los cambios que no hayan guardado.

Si no habilita esta opción, los dispositivos bloqueados no se reiniciarán. El estado de la tarea en tales dispositivos indicará que hay un reinicio pendiente. Los usuarios tendrán que cerrar manualmente todas las aplicaciones abiertas para luego reiniciar sus dispositivos.

Esta opción está deshabilitada de forma predeterminada.

Administrar parches y actualizaciones

En la sección Administrar parches y actualizaciones, puede configurar la descarga y la distribución de actualizaciones, así como la instalación de parches en los dispositivos administrados:

Instalar automáticamente las actualizaciones y parches de estado Sin definir que estén disponibles para los componentes

Si esta opción está habilitada, los parches de Kaspersky con el estado de aprobación *Sin definir* se instalan automáticamente en los dispositivos administrados inmediatamente después de que se descargan de los servidores de actualizaciones.

Si deshabilita esta opción, los parches de Kaspersky que se descarguen y que tengan el estado *Sin definir* se instalarán únicamente si cambia su estado a *Aprobada*.

Esta opción está activada de forma predeterminada.

Descargar actualizaciones y bases de datos antivirus del Servidor de administración con anticipación (recomendado)

Si esta opción está habilitada, las actualizaciones se descargan utilizando el modelo sin conexión. Cuando el Servidor de administración recibe actualizaciones, notifica al Agente de red (en los dispositivos donde está instalado) las actualizaciones que serán necesarias para las aplicaciones administradas. Cuando el Agente de red recibe la información sobre las actualizaciones, descarga por anticipado los archivos relevantes desde el Servidor de administración. En la primera conexión con un Agente de red, el Servidor de administración inicia una descarga de actualizaciones. Después de que Agente de red descarga todas las actualizaciones a un dispositivo cliente, las actualizaciones quedan disponibles para las aplicaciones en ese dispositivo.

Cuando una aplicación administrada de un dispositivo cliente intenta acceder al Agente de red para descargar actualizaciones, el Agente de red comprueba si tiene todas las actualizaciones necesarias. Si las actualizaciones se reciben desde el Servidor de administración no más de 25 horas antes de que la aplicación administrada las solicite, el Agente de red no se conecta al Servidor de administración, sino que proporciona actualizaciones desde el caché local a la aplicación administrada. Es posible que la conexión con el Servidor de administración no se establezca cuando el Agente de red proporciona actualizaciones para las aplicaciones en los dispositivos cliente, pero no se requiere conexión para la actualización.

Deshabilite esta opción si prefiere no utilizar el modelo de descarga de actualizaciones sin conexión. Las actualizaciones se distribuirán siguiendo la programación de la tarea de descarga de actualizaciones.

Esta opción está activada de forma predeterminada.

Conectividad

La sección **Conectividad** incluye tres subsecciones:

- **Red**
- **Perfiles de conexión**
- **Programación de conexiones**

En la subsección **Red**, puede configurar la conexión al Servidor de administración, habilitar el uso de un puerto UDP y especificar el número de ese puerto UDP.

- En el grupo de configuraciones **Conexión con el Servidor de administración**, puede configurar la conexión con el Servidor de administración y especificar el intervalo de tiempo para la sincronización entre dispositivos cliente y el Servidor de administración.

  Intervalo de sincronización (min)

  El Agente de red se encarga de sincronizar el dispositivo administrado con el Servidor de administración. Recomendamos que el intervalo de sincronización (también llamado latido) se fije en 15 minutos por cada 10 000 dispositivos administrados.

  Comprimir tráfico de red

  Si esta opción está habilitada, se reducirá el volumen de datos transferido. En consecuencia, el Agente de red podrá transmitir información a mayor velocidad y el Servidor de administración deberá soportar menos carga.

  > El uso de la CPU del equipo cliente podría aumentar.

  Esta casilla está activada de manera predeterminada.

Abrir puertos del Agente de red en el Firewall de Microsoft Windows

Cuando se habilita esta opción, se agregan los puertos que el Agente de red necesita para funcionar a la lista de exclusiones del Firewall de Microsoft Windows.

Esta opción está activada de forma predeterminada.

Usar conexión SSL

Si se habilita esta opción, la conexión al Servidor de administración se establecerá a través de un puerto seguro utilizando el protocolo SSL.

Esta opción está activada de forma predeterminada.

Utilizar la puerta de enlace de conexión del punto de distribución (si está disponible) con la configuración de conexión predeterminada

Si esta opción está habilitada, la puerta de enlace de conexión del punto de distribución se usará con la configuración especificada en las propiedades del grupo de administración.

Esta opción está activada de forma predeterminada.

- **Usar puerto UDP**

  Si necesita que el Agente de red se conecte al Servidor de administración a través de un puerto UDP, habilite la opción **Usar puerto UDP** y especifique un **número de puerto UDP**. Esta opción está activada de forma predeterminada. El puerto UDP predeterminado para conectarse al Servidor de administración es 15000.

- **Número de puerto UDP**

  En este campo, puede indicar el número del puerto UDP. El número de puerto predeterminado es 15000.

  El sistema decimal se usa para los registros.

- **Usar punto de distribución para forzar la conexión con el Servidor de administración**

  Seleccione esta opción si seleccionó **Utilizar este punto de distribución como servidor push** en la ventana de configuración del punto de distribución. De lo contrario, el punto de distribución no funcionará como un servidor push.

En la subsección **Perfiles de conexión**, puede especificar la configuración de las ubicaciones de red y habilitar el modo fuera de la oficina cuando el Servidor de administración no esté disponible:

Configuración de ubicación de red

La configuración de una ubicación de red define las características de la red con la cual está conectado el dispositivo cliente y especifica las reglas que hacen que el Agente de red cambie de un perfil de conexión de Servidor de administración a otro en respuesta a un cambio en las características de la red.

Perfiles de conexión al Servidor de administración

Puede ver y crear los perfiles que rigen la conexión entre el Agente de red y el Servidor de administración. Desde aquí también puede crear reglas para que el Agente de red cambie a un Servidor de administración diferente cuando ocurren los siguientes eventos:

- Cuando el dispositivo cliente se conecta a otra red local
- Cuando el dispositivo pierde la conexión con la red local de la organización
- Cuando se modifican la dirección de la puerta de enlace de conexión o la dirección del servidor DNS

Habilitar el modo de fuera de la oficina cuando el Servidor de administración no esté disponible

Si se habilita esta opción, en caso de que se establezca la conexión mediante este perfil, las aplicaciones instaladas en el dispositivo cliente utilizarán perfiles de directiva para dispositivos en modo fuera de la oficina, así como directivas fuera de la oficina. Si no hay una directiva fuera de la oficina definida para la aplicación, se utilizará la directiva activa.

Si se deshabilita esta opción, las aplicaciones utilizarán directivas activas.

Esta opción está deshabilitada de forma predeterminada.

En la subsección **Programación de conexiones**, puede especificar los intervalos de tiempo durante los cuales el Agente de red enviará datos al Servidor de administración:

Establecer conexión cuando sea necesario

Si se selecciona esta opción, la conexión se establece cuando el Agente de red debe enviar datos al Servidor de administración.

Esta opción está seleccionada de forma predeterminada.

Establecer conexión en los intervalos que especifique

Si se selecciona esta opción, el Agente de red se conecta al Servidor de administración a una hora especificada. Puede agregar varios períodos de conexión.

Sondeo de red con puntos de distribución

En la sección **Sondeo de red con puntos de distribución**, puede configurar el sondeo automático de la red. Puede utilizar las siguientes opciones para habilitar el sondeo y definir una frecuencia de sondeo:

Red de Windows

La opción está disponible solo para puntos de distribución basados en Windows.

Si se habilita esta opción, el Servidor de administración sondeará automáticamente la red de acuerdo con la programación que configuró al hacer clic en los enlaces **Establecer programación de sondeo rápido** y **Establecer programación de sondeo completo**.

Si esta opción está deshabilitada, el Servidor de administración sondeará la red con la frecuencia indicada en el campo **Frecuencia de sondeos de la red (min)**.

El intervalo de detección de dispositivos para las versiones de Agente de red se puede configurar en los campos **Frecuencia de sondeos de dominios de Windows (min)** (para el sondeo rápido de redes Windows) y **Frecuencia de sondeos de la red (min)** (para el sondeo completo de redes Windows).

Esta opción está deshabilitada de forma predeterminada.

Intervalos IP

Si se habilita esta opción, el punto de distribución sondeará automáticamente los intervalos IP siguiendo la programación que se haya configurado tras hacer clic en el botón **Configurar programación de sondeos**.

Si esta opción no está habilitada, el punto de distribución no hará sondeos de intervalos IP.

La frecuencia de sondeo de rangos IP para las versiones del Agente de red anteriores a la versión 10.2 se puede configurar en el campo **Intervalo de sondeo (min)**. El campo estará disponible si se habilita la opción.

Esta opción está deshabilitada de forma predeterminada.

Zeroconf

Si esta opción está habilitada, el punto de distribución automáticamente sondea la red con dispositivos IPv6 mediante el uso de las redes de configuración cero (también denominadas *Zeroconf*). En este caso, el sondeo de rangos de IP habilitados se ignora, porque el punto de distribución sondea toda la red.

Para empezar a usar Zeroconf, se deben cumplir las siguientes condiciones:

- El punto de distribución debe ejecutar Linux.
- Debe instalar la utilidad avahi-browse en el punto de distribución.

Si esta opción está habilitada, el punto de distribución no sondea las redes con dispositivos IPv6.

Esta opción está deshabilitada de forma predeterminada.

Controladores de dominio

Si se habilita esta opción, el punto de distribución sondeará automáticamente los controladores de dominio de acuerdo con la programación que configuró al hacer clic en el botón **Configurar programación de sondeos**.

Si esta opción no está habilitada, el punto de distribución no hará sondeos de controladores de dominio.

La frecuencia de sondeo de controladores de dominio para las versiones del Agente de red anteriores a la versión 10.2 se puede configurar en el campo **Intervalo de sondeo (min)**. El campo estará disponible si se habilita esta opción.

Esta opción está deshabilitada de forma predeterminada.

Configuración de red para puntos de distribución

En la sección **Configuración de red para puntos de distribución**, puede configurar los ajustes de acceso a Internet:

- **Usar servidor proxy**

  Si esta opción está habilitada, se usa un servidor proxy de Internet para conectar los puntos de distribución a los servidores de actualización de Kaspersky.

- **Dirección**

- **Número de puerto**

- **No usar el servidor proxy para direcciones locales**

  Si habilita esta opción, no se usará un servidor proxy para establecer conexión con los dispositivos de la red local.

  Esta opción está deshabilitada de forma predeterminada.

- **Autenticación del servidor proxy**

  Si se selecciona esta casilla, en los campos de entrada se podrán especificar las credenciales para la autenticación del servidor proxy.

  Esta casilla está desactivada por defecto.

Proxy de KSN (puntos de distribución)

En la sección **Proxy de KSN (puntos de distribución)**, puede hacer que la aplicación utilice el punto de distribución para reenviar las solicitudes para Kaspersky Security Network (KSN) de los dispositivos administrados:

Habilitar el proxy de KSN en el lado del punto de distribución

El servicio de proxy de KSN se ejecuta en el dispositivo que se utiliza como punto de distribución. Utilice esta función para redistribuir y optimizar el tráfico de la red.

El punto de distribución enviará a Kaspersky las estadísticas de KSN que se enumeran en la declaración de Kaspersky Security Network.

Esta opción está deshabilitada de forma predeterminada. Esta opción solo se activa si las opciones **Usar Servidor de administración como servidor proxy** y **Acepto utilizar Kaspersky Security Network** están habilitadas en la ventana de propiedades del Servidor de administración.

Puede asignar un nodo de un clúster activo-pasivo a un punto de distribución y habilitar el servidor proxy de KSN en ese nodo.

Transmitir las solicitudes para KSN al Servidor de administración

El punto de distribución envía las solicitudes KSN desde los dispositivos administrados al Servidor de administración.

Esta opción está activada de forma predeterminada.

Acceder a KSN Cloud/KPSN directamente a través de Internet

El punto de distribución envía las solicitudes KSN desde los dispositivos administrados a KSN Cloud o a KPSN. Las solicitudes de KSN generadas en el punto de distribución mismo también se envían directamente a la nube de KSN Cloud o a KPSN.

Puerto TCP

El número del puerto de TCP que los dispositivos administrados utilizarán para conectarse al Servidor proxy de KSN. El número de puerto predeterminado es 13111.

Puerto UDP

Si necesita que el Agente de red se conecte al Servidor de administración a través de un puerto UDP, habilite la opción **Usar puerto UDP** y especifique un **número de puerto UDP**. Esta opción está activada de forma predeterminada. El puerto UDP predeterminado para conectarse al Servidor de administración es 15000.

Puerto HTTPS

Si necesita que los dispositivos administrados se conecten al servidor proxy de KSN a través de un puerto HTTPS, habilite la opción **Usar HTTPS** y, luego, especifique un número de puerto en el campo **Puerto HTTPS**. Esta opción está deshabilitada de forma predeterminada. El puerto HTTPS predeterminado de conexión al servidor proxy de KSN es 17111.

Actualizaciones (puntos de distribución)

En la sección **Actualizaciones (puntos de distribución)**, puede habilitar la función de descarga de archivos diff, para que los puntos de distribución reciban actualizaciones en forma de archivos diff desde los servidores de actualización de Kaspersky.

Administración de cuenta local (solo Linux)

La sección **Administración de cuenta local (solo Linux)** incluye tres subsecciones:

- **Administración de certificados de usuario**
- **Agregar o editar grupos de administradores locales vigentes**
- **Carga de archivo de referencia para proteger frente a la modificación del archivo de sudoers en el dispositivo del usuario**

En la subsección **Administración de certificados de usuario**, puede especificar qué certificados raíz instalar. Estos certificados se pueden utilizar, por ejemplo, para verificar la autenticidad de sitios web o servidores web.

Instalar certificados raíz

Si esta opción está habilitada, los certificados agregados a la tabla se instalarán en los dispositivos especificados.

Si esta opción está deshabilitada, no se instalarán certificados en los dispositivos especificados.

Esta opción está deshabilitada de forma predeterminada.

Agregar

Al hacer clic en este botón, se abre una ventana en la que puede agregar un certificado.

El certificado debe ser inferior a 10 MB.

Kaspersky Security Center admite certificados con extensiones CER, CRT, CERT, PEM y KEY.

En la subsección **Agregar o editar grupos de administradores locales vigentes**, puede administrar grupos de administradores locales. Estos grupos se utilizan, por ejemplo, al revocar los derechos de administrador local. También puede consultar la lista de cuentas de usuarios con privilegios mediante **Informe sobre usuarios privilegiados en el dispositivo (solo Linux)**.

Agregar

Al hacer clic en este botón, se abre una ventana en la que puede agregar un grupo de administradores locales.

Editar

Al hacer clic en este botón, se abre una ventana en la que puede editar el grupo de administradores locales.

Este botón está disponible si se selecciona la casilla junto al grupo de administradores locales.

Eliminar

Al hacer clic en este botón, se elimina de la tabla el grupo de administradores locales seleccionado.

Este botón está disponible si se selecciona la casilla junto al grupo de administradores locales.

En la subsección **Carga de archivo de referencia para proteger frente a la modificación del archivo de sudoers en el dispositivo del usuario**, puede configurar el control del archivo sudoers. Los grupos con privilegios y los usuarios del dispositivo se definen mediante el archivo sudoers en el dispositivo. El archivo sudoers se encuentra en `/etc/sudoers`. Puede cargar un archivo sudoers de referencia para proteger el archivo sudoers contra cambios. Esto evitará cambios no deseados en el archivo sudoers.

Un archivo sudoers de referencia no válido puede hacer que el dispositivo del usuario no funcione correctamente.

Controlar archivo de sudoers

Si esta opción está habilitada, el archivo sudoers será reemplazado por el archivo sudoers de referencia actual.

Si esta opción está deshabilitada, el archivo sudoers permanecerá sin cambios.

Esta opción está deshabilitada de forma predeterminada.

Archivo de referencia de sudoers

Este campo muestra el nombre del archivo sudoers de referencia cargado.

Cargar

Al hacer clic en este botón, se abre una ventana en la que puede cargar un archivo sudoers de referencia.

Archivo de referencia de sudoers actual

Al hacer clic en este botón, se muestra el contenido del archivo sudoers actual.

Historial de revisiones

En la pestaña **Historial de revisiones**, puede:

- Ver y guardar el historial de revisiones de directivas.
- Anular la revisión de una directiva.
- Agregar y editar las descripciones de las revisiones de directivas.
- Compare revisiones de la directiva.

Uso del Agente de red para Windows, Linux y macOS: comparación

El uso del Agente de red varía según el sistema operativo del dispositivo. Los ajustes de la directiva y del paquete de instalación del Agente de red también difieren según el sistema operativo. La tabla de abajo compara las características del Agente de red y los escenarios de uso disponibles para los sistemas operativos Windows, Linux y macOS.

Función del Agente de red	Windows	Linux	macOS
Instalación			
Instalación con una imagen clónica del disco duro del administrador, que contenga un sistema operativo y una copia del Agente de red y se haya generado con herramientas desarrolladas por terceros para trabajar con imágenes de disco	✓ Limitación: No es compatible con el Agente de red para Microsoft Windows en Arm.	✓	✓
Instalación con herramientas de terceros para la instalación remota de aplicaciones	✓	✓	✓
Instalación manual, ejecutando el instalador de la aplicación en los dispositivos	✓	✓	✓
Instalación del Agente de red en modo silencioso	✓	✓	✓
Conexión manual de un dispositivo cliente al Servidor de administración (utilidad klmover)	✓	✓	✓
Instalación automática de actualizaciones y parches para los componentes de Kaspersky Security Center	✓	✓	—
Distribución automática de una clave	✓	✓	✓
Sincronización forzada	✓	✓	✓ Excepción de un servidor push
Punto de distribución			
Uso como punto de distribución	✓ Limitación: No es compatible con el Agente de red para Microsoft Windows en Arm.	✓	✓
Cálculo de la cantidad de puntos de distribución y su configuración	✓ Limitación: No es compatible con el Agente de red para Microsoft Windows en Arm.	✓ Sin utilizar el reconocimiento de ubicación de red (NLA).	✓ Sin utilizar el reconocimiento de ubicación de red (NLA).
Modelo de descarga de actualizaciones sin conexión	✓ Limitación: No es compatible con el Agente de red para Microsoft Windows en Arm.	✓	✓
Sondeo de red	✓ • Sondeo de intervalos IP • Sondeo del controlador de dominio (Microsoft Active Directory) Limitación: No es compatible con el Agente de red para Microsoft Windows en Arm.	✓ Sondeo de intervalos IP Sondeo con Zeroconf Sondeo del controlador de dominio (Microsoft Active Directory, Samba 4 Active Directory, FreeIPA, ALD Pro)	—

Función del Agente de red	Windows	Linux	macOS
Ejecución del servicio de proxy de KSN en un punto de distribución	✓ Limitación: No es compatible con el Agente de red para Microsoft Windows en Arm.	✓	—
Descarga de actualizaciones a través de los servidores de actualización de Kaspersky a los repositorios de los puntos de distribución que distribuyen actualizaciones a los dispositivos administrados	✓ Limitación: No es compatible con el Agente de red para Microsoft Windows en Arm.	✓	— (Si hay uno o más dispositivos con Linux o macOS en el alcance de la tarea "Descargar actualizaciones en los repositorios de los puntos de distribución", la tarea terminará con el estado "Error" aunque se complete sin errores en todos los dispositivos con Windows).
Insertar (push) instalación de aplicaciones	✓ Limitación: No es compatible con el Agente de red para Microsoft Windows en Arm.	Restringido: no es posible realizar una instalación remota en dispositivos Windows mediante el uso de puntos de distribución Linux.	Restringido: no es posible realizar una instalación remota en dispositivos Windows mediante el uso de puntos de distribución macOS.
Uso como servidor push	✓ Limitación: No es compatible con el Agente de red para Microsoft Windows en Arm.	✓	—
Administración de aplicaciones de terceros			
Instalación remota de aplicaciones en dispositivos	✓	✓	✓ Consulte el siguiente artículo para obtener más detalles: Instalación remota de aplicaciones en dispositivos macOS.
Configuración de actualizaciones del sistema operativo en una directiva del Agente de red	✓ Limitación: No es compatible con el Agente de red para Microsoft Windows en Arm.	—	—
Consulta de información sobre las vulnerabilidades de software	✓ Limitación: No es compatible con el Agente de red para Microsoft Windows en Arm.	—	—
Análisis de aplicaciones en busca de vulnerabilidades	✓ Limitación: No es compatible con el Agente de red para Microsoft Windows en Arm.	—	—
Instalación de actualizaciones de software	✓ Limitación: No es compatible con el Agente de red para Microsoft Windows en Arm.	—	—
Inventariado del software instalado en los dispositivos	✓	✓	—
Máquinas virtuales			
Instalación del Agente de red en una máquina virtual	✓	✓	✓

Función del Agente de red	Windows	Linux	macOS
Optimización de la configuración para infraestructura de escritorio virtual (VDI)	✓ Limitación: No es compatible con el Agente de red para Microsoft Windows en Arm.	✓	✓
Compatibilidad con máquinas virtuales dinámicas	✓ Limitación: No es compatible con el Agente de red para Microsoft Windows en Arm.	✓	✓
Otro			
Acciones de auditoría en dispositivos cliente remotos mediante Windows Desktop Sharing	✓	—	—
Supervisión del estado de protección antivirus	✓	✓	✓
Administración del reinicio de los dispositivos	✓	—	—
Compatibilidad con las reversiones de estado en los sistemas de archivos	✓	✓	✓
Uso del Agente de red como puerta de enlace de conexión	✓	✓	✓
Administrador de conexiones	✓	✓	✓
Perfiles de conexión para los usuarios fuera de la oficina	✓	✓	✓
Cambio del Servidor de administración al que está conectado el Agente de red (de forma automática, según la ubicación de red)	✓	✓	✓
Comprobación de la conexión entre un dispositivo cliente y el Servidor de administración. Utilidad klnagchk	✓	✓	✓
Conexión remota al escritorio de un dispositivo cliente	✓	✓	✓ A través del sistema VNC (siglas de "Virtual Network Computing", computación virtual en red)
Descarga de un paquete de instalación independiente a través del Asistente de migración	✓	✓	✓
Ver información sobre el hardware de los dispositivos cliente	✓	✓ La información sobre el hardware de los dispositivos con Linux enviada al Servidor de administración por el Agente de red instalado en estos dispositivos se limita a la información especificada en la descripción de la configuración del dispositivo administrado.	✓ La información sobre el hardware de los dispositivos con macOS enviada al Servidor de administración por el Agente de red instalado en estos dispositivos se limita a la información especificada en la descripción de la configuración del dispositivo administrado.

Comparación de la configuración del Agente de red por sistemas operativos

La siguiente tabla muestra qué configuraciones de la directiva del Agente de red están disponibles según el sistema operativo del dispositivo administrado donde se instaló el Agente de red.

Configuración del Agente de red: comparación por sistemas operativos

Sección Configuración	Windows	Linux	macOS
General	✓	✓	✓
Configuración de eventos	✓	✓	✓
Configuración	✓	✓ Están disponibles las siguientes opciones: • **Distribuir archivos solo a través de los puntos de distribución** • **Tamaño máximo de la cola de eventos, en MB** • **La aplicación podrá obtener información adicional sobre la directiva en el dispositivo**	✓
Repositorios	✓	✓ Están disponibles las siguientes opciones: • **Detalles de las aplicaciones instaladas** • **Detalles del registro de hardware**	✓ La opción **Detalles del Registro de hardware** está disponible.
Conectividad → Red	✓	✓ Excepto la opción **Abrir puertos del Agente de red en el Firewall de Microsoft Windows**.	✓
Conectividad → Perfiles de conexión	✓	✓	✓
Conectividad → Programación de conexiones	✓	✓	✓
Sondeo de red con puntos de distribución	✓ Están disponibles las siguientes opciones: • **Red de Windows** • **Intervalos IP** • **Controladores de dominio**	✓ Están disponibles las siguientes opciones: • **Zeroconf** • **Intervalos IP** • **Controladores de dominio**	—
Configuración de red para puntos de distribución	✓	✓	✓
Proxy de KSN (puntos de distribución)	✓	✓	—
Actualizaciones (puntos de distribución)	✓	✓	—
Historial de revisiones	✓	✓	✓

Habilitar y deshabilitar el modo de bajo consumo de recursos para el Agente de red

El modo de bajo consumo de recursos permite limitar el uso de RAM del Agente de red instalado en el dispositivo cliente. El modo de bajo consumo de recursos está deshabilitado de manera predeterminada.

En el modo de bajo consumo de recursos, las siguientes prestaciones no están disponibles:

- El Agente de red no se puede designar como punto de distribución (ya sea de forma manual o automática).
- El Agente de red no registra información sobre el estado del Agente de red en un archivo de texto separado.
- El Agente de red no permite utilizar el modelo sin conexión de descarga de actualizaciones.
- Los siguientes componentes y procesos se deshabilitan:
  - Obtención de información sobre actualizaciones y vulnerabilidades de terceros.
  - Ejecución del proxy de KSN en el punto de distribución.
  - Carga de actualizaciones al repositorio del punto de distribución.
  - Anulación del bloqueo del servidor DNS.
  - Información sobre el espacio libre en disco.

Los componentes y procesos reanudan su funcionamiento cuando se deshabilita el modo de bajo consumo de recursos.

Para habilitar el modo de bajo consumo de recursos, haga lo siguiente:

1. Ejecute el siguiente comando en la línea de comandos del dispositivo cliente:

   ```
   sudo /opt/kaspersky/klnagent64/sbin/klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 1
   ```

2. Reinicie el Agente de red con el siguiente comando:

   ```
   sudo service klnagent64 restart
   ```

3. En el registro del sistema operativo, compruebe que se muestre la entrada **El Agente de red de Kaspersky Security Center está funcionando en el modo de bajo consumo de recursos**.

El modo de bajo consumo de recursos queda habilitado.

Para deshabilitar el modo de bajo consumo de recursos, haga lo siguiente:

1. Ejecute el siguiente comando en la línea de comandos del dispositivo cliente:

   ```
   sudo /opt/kaspersky/klnagent64/sbin/klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 0
   ```

2. Reinicie el Agente de red con el siguiente comando:

   ```
   sudo service klnagent64 restart
   ```

El modo de bajo consumo de recursos queda deshabilitado.

También puede habilitar el modo de bajo consumo de recursos de forma remota mediante la tarea *Ejecución remota de scripts*.

Configurar la protección de las aplicaciones administradas

Para configurar la protección de las aplicaciones de Kaspersky administradas, puede usar directivas.

Para obtener más información sobre cómo configurar las directivas de Kaspersky Endpoint Security, consulte la Ayuda correspondiente:

- Ayuda de Kaspersky Endpoint Security para Windows
- Ayuda de Kaspersky Endpoint Security for Linux
- Ayuda de Kaspersky Endpoint Security for Mac:

Configuración manual de la tarea de grupo para actualizar Kaspersky Endpoint Security

La opción de programación óptima y recomendada para Kaspersky Endpoint Security es **Al descargar nuevas actualizaciones al repositorio** cuando la casilla de verificación **Utilizar retardo aleatorio automático para el inicio de la tarea** está seleccionada.

Instalación manual de la tarea de grupo para analizar un dispositivo con Kaspersky Endpoint Security

El Asistente de inicio rápido crea una tarea de grupo para analizar un dispositivo. Si la programación especificada automáticamente de la tarea de análisis de grupo no es adecuada para su organización, debe configurar de forma manual la programación más conveniente para esta tarea según las reglas del lugar de trabajo adoptadas en la organización.

Por ejemplo, la tarea tiene asignada la programación **Ejecutar los viernes a las 7:00 p. m.** con aleatorización automática y la casilla de verificación **Ejecutar tareas no realizadas** no está marcada. Esto significa que si los dispositivos de la organización se apagan, por ejemplo, los viernes a las 6:30 p.m., la tarea de análisis de los dispositivos nunca se ejecutará. En este caso, debe configurar la tarea de análisis de grupo manualmente.

Kaspersky Security Network (KSN)

En esta sección se describe cómo usar la infraestructura de servicios en línea llamada Kaspersky Security Network (KSN). Aquí encontrará información detallada sobre KSN e instrucciones para habilitar KSN, configurar el acceso a KSN y ver las estadísticas de uso del servidor proxy de KSN.

Es posible que la funcionalidad de las actualizaciones (incluida la provisión de actualizaciones de firmas antivirus y actualizaciones de base de código) y la funcionalidad de KSN no estén disponibles en el software en los EE. UU.

Acerca de KSN

Kaspersky Security Network (KSN) es una infraestructura de servicios en línea que brinda acceso a la base de conocimientos en línea de Kaspersky, que contiene información sobre la reputación de los archivos, los recursos web y el software. El uso de los datos de Kaspersky Security Network garantiza una respuesta más rápida de las aplicaciones de Kaspersky ante las amenazas, mejora la eficacia de algunos componentes de protección y reduce el riesgo de falsos positivos. KSN permite utilizar las bases de datos de reputación de Kaspersky para obtener información sobre las aplicaciones instaladas en los dispositivos administrados.

Al participar en Kaspersky Security Network, acepta proporcionar automáticamente a Kaspersky información sobre el funcionamiento de las aplicaciones de seguridad instaladas en las computadoras y los dispositivos móviles administrados mediante Kaspersky Security Center Linux. La información se transfiere de conformidad con la configuración de acceso a KSN.

Kaspersky Security Center Linux es compatible con las siguientes soluciones de infraestructura de KSN:

- *KSN Global*. Esta solución permite intercambiar información con Kaspersky Security Network. Al participar en KSN, usted acepta enviar a Kaspersky, de manera automática, información sobre el funcionamiento de las aplicaciones de Kaspersky instaladas en los dispositivos cliente administrados mediante Kaspersky Security Center Linux. La información se transfiere de conformidad con la configuración de acceso a KSN. Los analistas de Kaspersky realizan un examen adicional de la información recibida y la suman a las bases de datos de estadísticas y de reputación de Kaspersky Security Network. Kaspersky Security Center Linux utiliza esta solución de forma predeterminada.

- *Kaspersky Private Security Network (KPSN)* es una solución que permite a los usuarios de dispositivos con aplicaciones de Kaspersky instaladas obtener acceso a bases de datos de reputación de Kaspersky Security Network y otros datos estadísticos, sin enviar datos a KSN Global desde sus propios dispositivos. KPSN diseñada para clientes corporativos que, por alguno de los siguientes motivos, no pueden participar en Kaspersky Security Network:

  - Los dispositivos de los usuarios no tienen acceso a Internet.

  - La transmisión de datos fuera del país o de la LAN corporativa está prohibida por ley o por las directivas de seguridad corporativas.

  Puede configurar los ajustes de acceso de Kaspersky Private Security Network en la sección **Proxy de KSN** de la ventana de propiedades del Servidor de administración.

La aplicación le preguntará si desea unirse a KSN cuando ejecute el asistente de inicio rápido. Una vez que comience a usar la aplicación, podrá habilitar o deshabilitar el uso de KSN en cualquier momento.

Utiliza KSN de acuerdo con la Declaración de KSN que lee y acepta cuando habilita KSN. Si se actualiza la Declaración de KSN, se le mostrará cuando actualice una versión del Servidor de administración. Puede aceptar la Declaración de KSN actualizada o rechazarla. Si la rechaza, seguirá usando KSN de acuerdo con la versión anterior de la Declaración de KSN que aceptó anteriormente.

Cuando KSN está habilitado, Kaspersky Security Center Linux verifica si se puede acceder a los servidores de KSN para asegurarse de que se mantenga el nivel de seguridad para los dispositivos administrados. Si los servidores DNS configurados en el sistema no permiten acceder a los servidores de Kaspersky, la aplicación utiliza servidores DNS públicos.

Los dispositivos cliente administrados por el Servidor de administración interactúan con KSN mediante el servidor proxy de KSN. El servidor proxy de KSN proporciona las funciones siguientes:

- Permite que los dispositivos cliente envíen solicitudes a KSN, obtengan información de KSN y transfieran información a KSN, incluso cuando no tengan acceso directo a Internet.
- El servidor proxy de KSN almacena en caché los datos procesados y reduce, de esta manera, la carga en el canal de salida y el período de tiempo que se utiliza para esperar información solicitada por un dispositivo cliente.

Puede configurar el servidor proxy de KSN en la sección **Proxy de KSN** de la ventana de propiedades del Servidor de administración.

Configurar el acceso a KSN

Puede configurar el acceso a Kaspersky Security Network (KSN) desde las propiedades del Servidor de administración, desde la directiva del Servidor de administración y desde el punto de distribución.

Para configurar el acceso del Servidor de administración a KSN desde las propiedades del Servidor de administración:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, elija la sección **Proxy de KSN**.

3. Establezca el botón de alternancia **Habilitar el proxy de KSN en el Servidor de administración** en Habilitado.

   Si esta opción está habilitada, el servidor proxy de KSN envía datos a KSN para aumentar la eficiencia de los componentes de Kaspersky Security Center y mejorar el rendimiento de las aplicaciones de Kaspersky. Los datos se envían desde los dispositivos cliente a KSN de acuerdo con la directiva de Kaspersky Endpoint Security activa en esos dispositivos. Si este botón de activación está desactivado, no se enviarán datos a KSN desde el Servidor de administración y los dispositivos cliente a través de Kaspersky Security Center Linux. Sin embargo, si la configuración de los mismos lo permite, los dispositivos cliente podrán enviar datos directamente a KSN (es decir, sin pasar por Kaspersky Security Center Linux). La directiva de Kaspersky Endpoint Security, que está activa en los dispositivos cliente, determina qué datos se enviarán de los dispositivos a KSN en forma directa (es decir, sin pasar por Kaspersky Security Center Linux).

4. Seleccione Solución de infraestructura KSN.

En la subsección **Participación en KSN**, realice una de las siguientes acciones:

- Si utiliza KSN Global, establezca el botón de alternancia **Usar Kaspersky Security Network en Habilitado**.

  Al activar esta opción, asegúrese de leer y aceptar los términos de la Declaración de KSN.

- Si utiliza KPSN, establezca el botón de alternancia **Usar Kaspersky Private Security Network** en Habilitado y haga clic en el botón **Seleccionar archivo de configuración del proxy de KSN** para cargar la configuración de KPSN (archivos con las extensiones .pkcs7 y .pem). Una vez descargada la configuración, la interfaz muestra el nombre y contactos del proveedor, así como la fecha de creación del archivo con la configuración de KPSN.

Cuando establece el botón de alternancia **Usar Kaspersky Private Security Network** en Habilitado, se muestra un mensaje con información detallada sobre KPSN.

Las siguientes aplicaciones de Kaspersky son compatibles con KPSN:

- Kaspersky Security Center Linux
- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security para Windows

Si habilita KPSN en Kaspersky Security Center Linux, se les comunicará a estas aplicaciones que el servicio utilizado es KPSN. En la ventana de configuración de la aplicación, en la subsección de **Kaspersky Security Network** de la sección **Protección avanzada contra amenazas**, se muestra la información sobre el proveedor KSN seleccionado: KSN o KPSN.

Kaspersky Security Center Linux no envía ningún dato estadístico a Kaspersky Security Network si se configura KPSN en la sección **Proxy de KSN** de la ventana de propiedades del Servidor de administración.

5. Si tiene las configuraciones del servidor proxy configuradas en las propiedades del Servidor de administración, pero su arquitectura de red requiere que use KPSN directamente, habilite la opción **No usar el servidor proxy configurado para conectarse a KPSN**. De lo contrario, las solicitudes de las aplicaciones administradas no podrán llegar a KPSN.

6. Configure la conexión del Servidor de administración al servicio del proxy de KSN:

   - En **Conexión**, en el campo **Puerto TCP**, ingrese el número del puerto TCP que se utilizará para conectarse al servidor proxy de KSN. El puerto predeterminado para conectarse al servidor proxy de KSN es el 13111.

   - Si desea que el Servidor de administración se conecte al servidor proxy de KSN a través de un puerto UDP, habilite la opción **Usar puerto UDP** e ingrese el número de puerto en el campo **Puerto UDP**. Esta opción está desactivada de forma predeterminada y se utiliza el puerto TCP. Si habilita esta opción, de forma predeterminada, se usará el puerto UDP 15111 para establecer conexión con el servidor proxy de KSN.

   - Si desea que el Servidor de administración se conecte al servidor proxy de KSN a través de un puerto HTTPS, habilite la opción **Usar HTTPS** y especifique un número de puerto para **Puerto HTTPS**. Esta opción está desactivada de forma predeterminada y se utiliza el puerto TCP. Si habilita esta opción, el puerto HTTPS predeterminado de conexión al servidor proxy de KSN es 17111.

     Si selecciona esta opción, habilite HTTPS en todos los puntos de distribución que actúen como proxy de KSN. Esto evita sobrecargar el proxy.

7. Habilite el botón de alternancia **Conectar los Servidores de administración secundarios a KSN mediante el Servidor de administración principal**.

   Cuando esta opción está habilitada, los servidores de administración secundarios utilizan el Servidor de administración principal como servidor proxy de KSN. Si esta opción está desactivada, los Servidores de administración secundarios se conectan a KSN por sus propios medios. En este caso, los dispositivos administrados usan Servidores de administración secundarios como servidores proxy de KSN.

   > Los Servidores de administración secundarios usan el Servidor de administración principal como servidor proxy si, en el panel derecho de la sección **Proxy de KSN** de las propiedades de los Servidores de administración secundarios, el botón de alternancia **Habilitar el proxy de KSN en el Servidor de administración** también está establecido en Habilitado.

8. Haga clic en el botón **Guardar**.

Se guarda la configuración de acceso a KSN.

Para configurar el acceso del Servidor de administración a KSN desde la directiva del Servidor de administración:

1. En el menú principal, vaya a **Administración de activos** → **Directivas**.
2. Seleccione una directiva del Servidor de administración.
3. En la ventana de propiedades que se abre, haga clic en la pestaña **Configuración de la aplicación**.
4. Seleccione la sección **Proxy de KSN** y siga los pasos del 3 al 8 de las instrucciones anteriores.

Se guardó la configuración de acceso a KSN.

También puede configurar el acceso de puntos de distribución a KSN, por ejemplo, si desea reducir la carga en el Servidor de administración. El punto de distribución que actúa como un servidor proxy KSN envía solicitudes de KSN desde dispositivos administrados a Kaspersky directamente, sin utilizar el Servidor de administración.

Para configurar el acceso del punto de distribución a Kaspersky Security Network (KSN):

1. Asegúrese de que el punto de distribución se asigne manualmente.
2. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.
3. En la pestaña **General**, elija la sección **Puntos de distribución**.
4. Haga clic en el nombre del punto de distribución para abrir la ventana de propiedades.

5. En la ventana de propiedades del punto de distribución, en la sección **Proxy de KSN**, habilite la opción **Habilitar el proxy de KSN en el lado del punto de distribución** y, a continuación, habilite la opción **Acceder a KSN Cloud/KPSN directamente a través de Internet**.

6. Haga clic en **Aceptar**.

El punto de distribución actuará como servidor proxy de KSN.

Tenga en cuenta que el punto de distribución no admite la autenticación de dispositivos administrados mediante el protocolo NTLM.

Habilitar y deshabilitar el uso de KSN

Pasos para habilitar el uso de KSN:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, elija la sección **Proxy de KSN**.

3. Establezca el botón de alternancia **Habilitar el proxy de KSN en el Servidor de administración** en Habilitado.

El servidor proxy de KSN está activado y envía datos a KSN para aumentar la eficiencia de los componentes de Kaspersky Next XDR Expert y mejorar el rendimiento de las aplicaciones de Kaspersky.

1. Dependiendo de la solución de infraestructura de KSN que utiliza, habilite los botones interruptores correspondientes.

   - Si utiliza KSN Global, establezca el botón de alternancia **Usar Kaspersky Security Network en Habilitado**.

     Ya está disponible el envío de datos a KSN. Al activar esta opción, asegúrese de leer y aceptar las condiciones de la Declaración de KSN.

   - Si utiliza KPSN, establezca el botón de alternancia **Usar Kaspersky Private Security Network** en Habilitado y haga clic en el botón **Seleccionar archivo de configuración del proxy de KSN** para cargar la configuración de KPSN (archivos con las extensiones .pkcs7 y .pem). Una vez descargada la configuración, la interfaz muestra el nombre y contactos del proveedor, así como la fecha de creación del archivo con la configuración de KPSN.

     Cuando establece el botón de alternancia **Usar Kaspersky Private Security Network** en Habilitado, se muestra un mensaje con información detallada sobre KPSN.

2. Haga clic en el botón **Guardar**.

Pasos para deshabilitar el uso de KSN:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, elija la sección **Proxy de KSN**.

3. Establezca el botón de alternancia **Habilitar el proxy de KSN en el Servidor de administración** en Deshabilitado para deshabilitar el servicio del proxy de KSN.

4. Haga clic en el botón **Guardar**.

Ver la Declaración de KSN aceptada

Para habilitar Kaspersky Security Network (KSN), debe leer y aceptar la Declaración de KSN. Si ya ha aceptado la Declaración de KSN y quiere verla nuevamente, puede hacerlo en cualquier momento.

Para ver la Declaración de KSN aceptada:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, elija la sección **Proxy de KSN**.

3. Haga clic en el enlace **Ver la Declaración de Kaspersky Security Network**.

En la ventana que se abre, puede ver el texto de la Declaración de KSN aceptada.

Aceptar una Declaración de KSN actualizada

Utiliza KSN de acuerdo con la Declaración de KSN que lee y acepta cuando habilita KSN. Si se actualiza la Declaración de KSN, se le mostrará cuando actualice una versión del Servidor de administración. Puede aceptar la Declaración de KSN actualizada o rechazarla. Si la rechaza, seguirá usando KSN bajo los términos estipulados en la versión que ya haya aceptado de la Declaración de KSN.

Después de actualizar una versión del Servidor de administración, la Declaración de KSN actualizada se muestra automáticamente. Si rechaza la Declaración de KSN actualizada, de todos modos podrá verla y aceptarla más adelante.

Para ver y luego aceptar o rechazar una Declaración de KSN actualizada:

1. Haga clic en el vínculo **Ver notificaciones** en la esquina superior derecha de la ventana principal de la aplicación.

   Se abre la ventana **Notificaciones**.

2. Haga clic en el enlace **Ver la Declaración de KSN actualizada**.

   Se abre la ventana **Actualización de la Declaración de Kaspersky Security Network**.

3. Lea la Declaración de KSN y haga clic en el botón que responda a su decisión:

   - **Acepto la Declaración de KSN actualizada**
   - **Utilizar KSN con la antigua Declaración**

Según su elección, KSN sigue funcionando de acuerdo con los términos de la Declaración de KSN actual o actualizada. Puede ver el texto de la Declaración de KSN aceptada en las propiedades del Servidor de administración en cualquier momento.

Verificar si el punto de distribución opera como servidor proxy de KSN

Puede habilitar el proxy de Kaspersky Security Network (KSN) en un dispositivo administrado que se haya designado como punto de distribución. Para funcionar como proxy de KSN, el dispositivo administrado debe tener activo el servicio ksnproxy. Puede verificar, activar o desactivar este servicio en el dispositivo localmente.

El dispositivo designado como punto de distribución puede utilizar Windows o Linux. El modo de llevar a cabo la verificación en el punto de distribución depende del sistema operativo instalado en el punto de distribución.

Para verificar si un punto de distribución con Linux opera como servidor proxy de KSN:

1. En el dispositivo del punto de distribución, ejecute el comando `ps aux` para mostrar la lista de procesos en ejecución.

2. Revise la lista de procesos en ejecución para verificar si se está ejecutando el proceso `/opt/kaspersky/klnagent64/sbin/ksnproxy`.

Si el servicio `/opt/kaspersky/klnagent64/sbin/ksnproxy` se está ejecutando, el Agente de red del dispositivo participa en Kaspersky Security Network y funciona como servidor proxy de KSN para los dispositivos administrados incluidos en el alcance del punto de distribución.

Para verificar si un punto de distribución con Windows opera como servidor proxy de KSN:

1. En el dispositivo de punto de distribución, en Windows, abra **Servicios** (**Todos los programas** → **Herramientas administrativas** → **Servicios**).

2. En la lista de servicios, verifique si el servicio ksnproxy se está ejecutando.

   Si el servicio ksnproxy se está ejecutando, entonces el Agente de red del dispositivo participa en Kaspersky Security Network y funciona como servidor proxy de KSN para los dispositivos administrados incluidos en el alcance del punto de distribución.

Si lo desea, puede desactivar el servicio ksnproxy. En este caso, el Agente de red del punto de distribución deja de participar en Kaspersky Security Network. Esto requiere derechos de administrador local.

Ver las estadísticas del servidor proxy de KSN

Kaspersky Security Center Web Console le permite ver las estadísticas de uso del servidor proxy KSN.

Las estadísticas incluyen los siguientes parámetros:

- Estado de la conexión a KSN
- Número de registros de caché
- Número de paquetes procesados en caché
- Número de paquetes recibidos

Si utiliza KPSN como solución de infraestructura, se mostrarán estadísticas de uso de KPSN.

Para ver las estadísticas:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, seleccione la sección **Proxy de KSN** y luego abra la pestaña **Estadísticas**.

   Esta sección muestra las estadísticas de operación reales del servidor proxy de KSN. Las estadísticas se actualizan cada 15 segundos.

Puede copiar estadísticas haciendo clic en el botón **Copiar al portapapeles**.

Administración de tareas

En esta sección, se describen las tareas utilizadas por Kaspersky Security Center Linux.

Acerca de las tareas

Para administrar las aplicaciones de seguridad de Kaspersky instaladas en los dispositivos a través de Kaspersky Security Center Linux, es necesario crear y ejecutar *tareas*. Las tareas son el medio que se utiliza para instalar, iniciar y detener aplicaciones, analizar archivos, actualizar bases de datos y módulos de software y realizar otras acciones en las aplicaciones.

Si desea utilizar Kaspersky Security Center Web Console para crear una tarea para una aplicación específica, deberá haber instalado el complemento de administración correspondiente a esa aplicación en el Servidor de Kaspersky Security Center Web Console.

Una tarea se puede ejecutar en el Servidor de administración o en un dispositivo.

Las tareas que se realizan en el Servidor de administración incluyen lo siguiente:

- Distribución automática de informes
- Descarga de actualizaciones en el repositorio
- Copia de seguridad de los datos del Servidor de administración
- Mantenimiento de la base de datos

Los siguientes tipos de tareas se ejecutan en los dispositivos:

- *Tareas locales*. Son tareas que se ejecutan en un dispositivo específico.

  Las tareas locales pueden ser modificadas por el administrador (mediante Kaspersky Security Center Web Console) o por el usuario de un dispositivo remoto (por ejemplo, mediante la interfaz de la aplicación de seguridad). Si el administrador y el usuario del dispositivo administrado modifican una tarea local al mismo tiempo, los cambios realizados por el administrador se consideran prioritarios y son los que entran en vigor.

- *Tareas de grupo*. Son tareas que se ejecutan en todos los dispositivos de un grupo específico.

  A menos que se especifique lo contrario en las propiedades de la tarea, una tarea de grupo también afecta a todos los subgrupos del grupo seleccionado. Una tarea de grupo también afecta (opcionalmente) a los dispositivos que se han conectado a Servidores de administración secundarios y virtuales incluidos en el grupo o en cualquiera de sus subgrupos.

- *Tareas globales*. Son tareas que se ejecutan en un conjunto de dispositivos que pueden o no pertenecer a un grupo.

Para cada aplicación, puede crear cualquier número de tareas de grupo, tareas globales o tareas locales.

Puede copiar, importar, exportar y eliminar tareas, consultar el progreso de su ejecución y modificar su configuración.

Para que una tarea se inicie en un dispositivo, la aplicación para la que se la ha creado debe estar en ejecución.

Los resultados de ejecución de las tareas se guardan en el registro de eventos del sistema operativo en cada dispositivo, en el registro de eventos del sistema operativo en el Servidor de administración y en la base de datos del Servidor de administración.

No incluya datos privados en la configuración de las tareas. Por ejemplo, evite especificar la contraseña del administrador del dominio.

Acerca del alcance de las tareas

El *alcance de una tarea* es el conjunto de dispositivos en los que se realiza esa tarea. Los tipos de alcance son los siguientes:

- Para una *tarea local*, el alcance es el propio dispositivo.
- Para una *tarea del Servidor de administración*, el alcance es el Servidor de administración.
- Para una *tarea de grupo*, el alcance es la lista de dispositivos incluidos en el grupo.

Al crear una *tarea global*, puede usar los siguientes métodos para especificar su alcance:

- Especificar dispositivos puntuales manualmente.

  Puede utilizar una dirección IP (o un intervalo IP) o un nombre de DNS. También puede seleccionar los dispositivos de la red que detecta el servidor de administración.

- Importar una lista de dispositivos de un archivo .txt que contenga, en líneas separadas, la dirección de cada dispositivo que se quiera agregar.

  Si importa una lista almacenada en un archivo o crea una lista manualmente y elige identificar los dispositivos por nombre, tenga en cuenta que la lista únicamente podrá incluir dispositivos sobre los que ya haya información en la base de datos del Servidor de administración. Dicha información deberá haberse cargado durante la conexión o el descubrimiento de los dispositivos.

- Especificar una selección de dispositivos.

El alcance de una tarea cambia con el tiempo, según cambia el conjunto de dispositivos incluidos en la selección. Puede generar una selección de dispositivos basada en los atributos de los dispositivos que quiera incluir (por ejemplo, el software instalado) o en las etiquetas asignadas a esos dispositivos. Una selección de dispositivos es la opción más flexible para especificar el alcance de una tarea.

Las tareas para selecciones de dispositivos siempre son ejecutadas por el Servidor de administración en forma programada. Estas tareas no se pueden ejecutar en dispositivos que carecen de conexión con el Servidor de administración. Las tareas cuyo alcance se especifica mediante otros métodos se ejecutan directamente en los dispositivos y, por lo tanto, no dependen de la conexión del dispositivo al Servidor de administración.

Las tareas para selecciones de dispositivos no se ejecutan según la hora local del dispositivo, sino según la hora local del Servidor de administración. Cuando el alcance se especifica por otros medios, la tarea se ejecuta según la hora local del dispositivo.

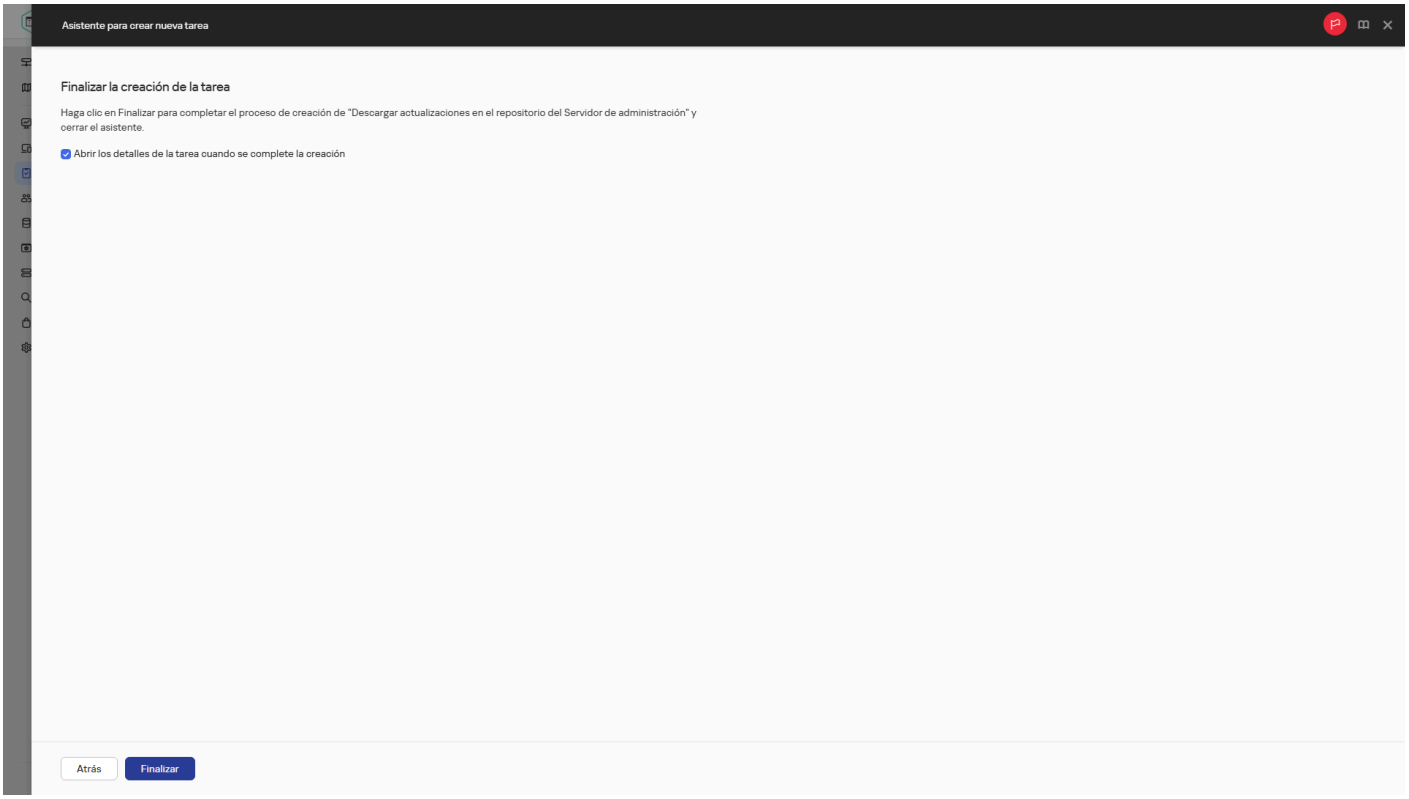
Crear una tarea

Para crear una tarea:

1. En el menú principal, vaya a **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Siga las instrucciones.
3. Si desea modificar la configuración predeterminada de la tarea, habilite la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de la tarea**. Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Puede cambiar la configuración por defecto más tarde, en cualquier momento.
4. Haga clic en el botón **Finalizar**.

Se crea la tarea y se la agrega a la lista de tareas.



Finalizar la creación de la tarea

Para crear una nueva tarea asignada a los dispositivos seleccionados:

1. En el menú principal, vaya a **Administración de activos** → **Dispositivos administrados**.

   Se muestra la lista de dispositivos administrados.

2. En la lista de dispositivos administrados, seleccione las casillas de verificación junto a los dispositivos para ejecutar la tarea para ellos. Puede utilizar las funciones de búsqueda y filtrado para encontrar los dispositivos de su interés.

3. Haga clic en el botón **Ejecutar una tarea** y, luego, seleccione **Agregar una nueva tarea**.

   Se inicia el Asistente para crear nueva tarea.

   En el primer paso del asistente, puede eliminar los dispositivos seleccionados para incluirlos en el alcance de la tarea. Siga las instrucciones del asistente.

4. Haga clic en el botón **Finalizar**.

La tarea se crea para los dispositivos seleccionados.

Iniciar una tarea manualmente

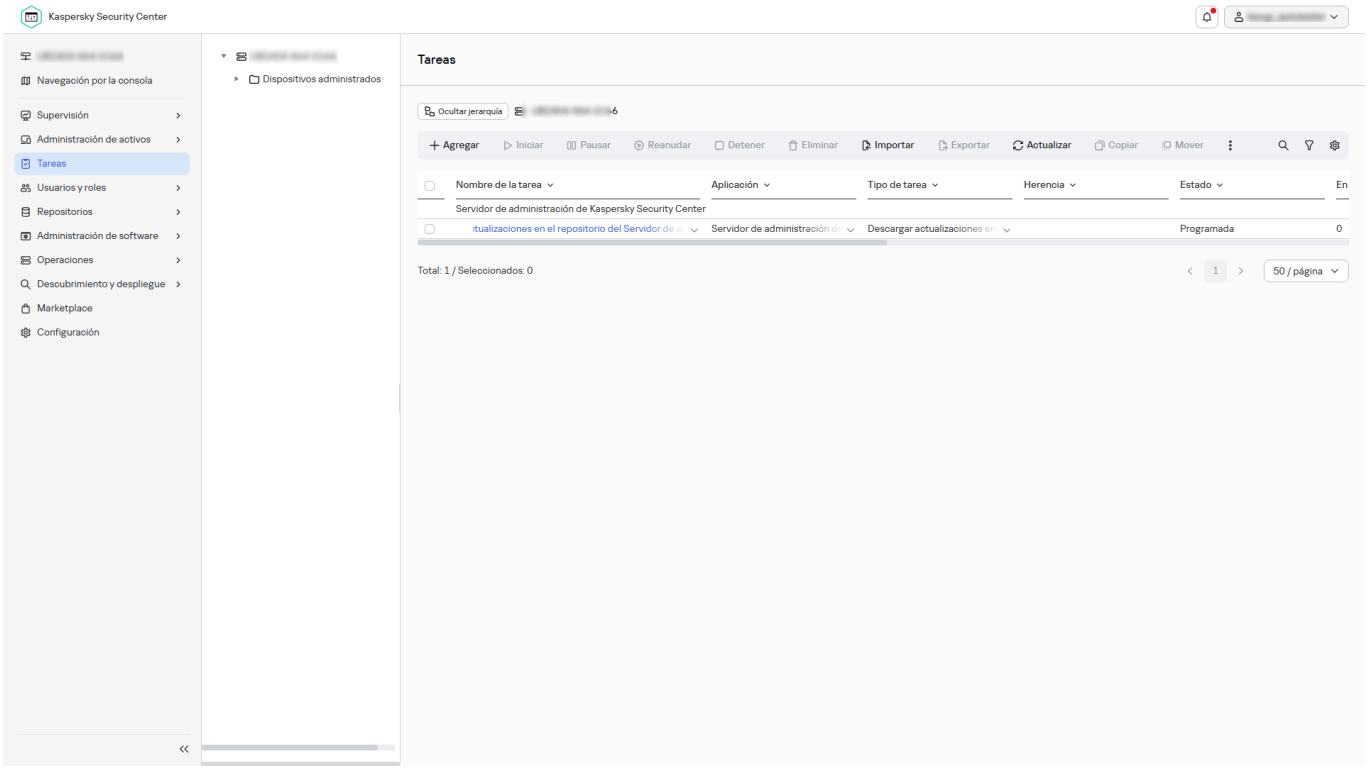
La aplicación inicia las tareas siguiendo la programación configurada en las propiedades de cada tarea. Puede iniciar una tarea de forma manual en cualquier momento desde la lista de tareas. Como alternativa, puede seleccionar dispositivos en la lista **Dispositivos administrados** y, luego, iniciar una tarea existente para ellos.

Para iniciar una tarea manualmente:

1. En el menú principal, vaya a **Tareas**.

2. En la lista de tareas, marque la casilla ubicada junto a la tarea que desee iniciar.

3. Haga clic en el botón **Iniciar**.



Iniciar una tarea desde la lista de tareas

Se inicia la tarea. Puede verificar el estado de la tarea en la columna **Estado** o haciendo clic en el botón **Resultado**.

Iniciar una tarea para dispositivos puntuales

Puede seleccionar uno o más dispositivos cliente en la lista de dispositivos y, luego, iniciar una tarea creada previamente para ellos. Esto le permite ejecutar tareas creadas anteriormente para un conjunto específico de dispositivos.

Esto cambia los dispositivos a los que se asignó la tarea a la lista de dispositivos seleccionados al ejecutar la tarea.
El ámbito de la tarea anterior se elimina y se reemplaza por el ámbito seleccionado.

Para iniciar una tarea para dispositivos puntuales:

1. En el menú principal, vaya a **Administración de activos** → **Dispositivos administrados**. Se muestra la lista de dispositivos administrados.

2. En la lista de dispositivos administrados, seleccione las casillas de los dispositivos para los que desea ejecutar la tarea. Puede utilizar las funciones de búsqueda y filtrado para encontrar los dispositivos de su interés.

3. Haga clic en el botón **Ejecutar tarea** y, luego, seleccione **Usar tarea existente**.

   Se mostrará la lista de tareas existentes.

4. Los dispositivos seleccionados se muestran arriba de la lista de tareas. Si es necesario, puede eliminar un dispositivo de esta lista. Puede eliminar todos los dispositivos menos uno.

5. Seleccione la tarea deseada en la lista. Puede usar el cuadro de búsqueda ubicado sobre la lista para buscar la tarea por nombre. Solo se puede seleccionar una única tarea.

6. Guarde los cambios haciendo clic en uno de los botones:

   - **Ejecutar y cerrar**

     La tarea se ejecuta para los dispositivos seleccionados.

   - **Ejecutar y abrir**

     La tarea se ejecuta para los dispositivos seleccionados y se muestra la ventana de propiedades de la tarea, donde puede revisar rápidamente los resultados.

La configuración de inicio programada de la tarea no se modifica.

Ver la lista de tareas

Puede ver la lista de tareas que se crean en Kaspersky Security Center Linux.

Para ver la lista de tareas:

En el menú principal, vaya a **Tareas**.

Se muestra la lista de tareas. Las tareas se agrupan en torno a los nombres de las aplicaciones con las que están relacionadas. Por ejemplo, la tarea *Instalar aplicación de forma remota* está vinculada al Servidor de administración y la tarea *Actualizar*, a Kaspersky Endpoint Security.

Para ver las propiedades de una tarea:

Haga clic en el nombre de la tarea.

Aparece la ventana de propiedades de la tarea. En ella encontrará una serie de pestañas con nombre. La pestaña llamada **General** contiene la propiedad **Tipo de tarea**, por ejemplo, y si ingresa a la pestaña **Programación**, encontrará la programación de la tarea.

Configuración general de tareas

En esta sección, se enumeran los ajustes que puede ver y configurar en la mayoría de las tareas. La lista de ajustes disponibles depende de la tarea que se está configurando.

Ajustes que se configuran al crear una tarea

A continuación, se enumeran los ajustes que puede definir al momento de crear una tarea. Algunos de estos ajustes también se pueden modificar en las propiedades de la tarea creada.

- Ajustes de reinicio del sistema operativo:

  No reiniciar el dispositivo

Cuando termine la operación, los dispositivos cliente no se reiniciarán automáticamente. Para que la operación se complete, deberá reiniciar los dispositivos en forma manual o mediante, por ejemplo, una tarea de administración de dispositivos. Los resultados de la tarea y el estado de cada dispositivo darán cuenta de que hay un reinicio pendiente. Esta opción es útil cuando la tarea va a ejecutarse en servidores y dispositivos que deben operar continuamente.

Reiniciar el dispositivo

Los dispositivos cliente se reiniciarán automáticamente siempre que resulte necesario para completar la operación. Esta opción es útil cuando la tarea se realiza en dispositivos que admiten una breve interrupción para apagarse o reiniciarse.

Forzar el cierre de aplicaciones en sesiones bloqueadas

Las aplicaciones abiertas en el dispositivo cliente podrían impedir que se lo reinicie. Si el usuario está editando un documento en un procesador de textos, por ejemplo, y no ha guardado el archivo, el procesador de textos no permitirá que el dispositivo se reinicie.

Si habilita esta opción, las aplicaciones que se estén ejecutando en un dispositivo bloqueado se cerrarán por la fuerza y, tras ello, el dispositivo se reiniciará. Los usuarios podrían perder los cambios que no hayan guardado.

Si no habilita esta opción, los dispositivos bloqueados no se reiniciarán. El estado de la tarea en tales dispositivos indicará que hay un reinicio pendiente. Los usuarios tendrán que cerrar manualmente todas las aplicaciones abiertas para luego reiniciar sus dispositivos.

Esta opción está deshabilitada de forma predeterminada.

- Programación de la tarea:

  Los tipos de programación pueden variar según la tarea.

  Es posible que algunos tipos de programación no estén disponibles para otras aplicaciones de Kaspersky.

  - **Iniciar tarea (ajuste):**

    Cada N horas

    La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la fecha y hora indicadas. Cada ejecución estará separada de la anterior por el número de horas que indique.

    De manera predeterminada, la tarea se ejecutará cada 6 horas, a partir de la fecha y hora actuales del sistema.

    Cada N días

    La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta opción permite elegir la fecha y hora de la primera ejecución. Podrá configurar estos dos ajustes si son compatibles con la aplicación para la que esté creando la tarea.

    De forma predeterminada, la tarea se ejecutará todos los días, a partir de la fecha y hora actuales del sistema.

    Cada N minutos

    La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la hora indicada en el día en que se cree la tarea. Cada ejecución estará separada de la anterior por el número de minutos que indique.

    De forma predeterminada, la tarea se ejecutará cada treinta minutos, a partir de la hora actual del sistema.

    Por días de la semana

La tarea se ejecutará periódicamente en los días de la semana y a la hora que indique.

De manera predeterminada, la tarea se ejecutará todos los viernes a las 18:00:00.

Mensual

La tarea se ejecutará periódicamente, en el día del mes y a la hora que indique.

Si el día elegido no forma parte de un mes, la tarea se ejecutará el último día de ese mes.

Por defecto, la tarea se ejecutará el primer día de cada mes, a la hora actual del sistema.

Manual

La tarea no se ejecutará automáticamente. Solo se la podrá iniciar en forma manual.

Esta opción está seleccionada de forma predeterminada.

Una vez

La tarea se ejecuta una vez, en la fecha y hora especificadas (de manera predeterminada, el día en que se creó la tarea).

Inmediatamente

La tarea se ejecuta inmediatamente después de guardar su configuración.

Mensualmente en el día de la semana seleccionado

La tarea se ejecutará periódicamente, en los días del mes y a la hora que indique.

De manera predeterminada, la hora de inicio es a las 18:00 y no se selecciona ningún día del mes.

> Tenga en cuenta que no selecciona una fecha específica en el mes, ni el número de la semana (primera, segunda semana del mes), sino el número de secuencia del día de la semana dentro de un mes. Por ejemplo, si coloca el cursor en la celda **Ma** de la **Primero** fila, significa que la tarea se ejecutará el primer martes de cada mes nuevo.

Puede seleccionar varios días de la semana.

Al descargar nuevas actualizaciones al repositorio

La tarea se ejecuta después de descargar las actualizaciones en el repositorio. Por ejemplo, es posible que desee utilizar este programa para la tarea *Actualizar*.

Al completarse otra tarea

La tarea actual se iniciará después de que se complete otra tarea. Esta opción solo funciona si ambas tareas están asignadas a los mismos dispositivos. Por ejemplo, podría ejecutar la tarea *Administrar dispositivos* con la opción **Encender el dispositivo** y hacer que, una vez completada esa tarea, se ejecute la tarea *Análisis antivirus* como una tarea desencadenante.

Debe seleccionar la tarea desencadenante de la tabla y el estado con el que esta tarea debe completarse (**Completada correctamente** o **Error**).

Si es necesario, puede buscar, ordenar y filtrar las tareas en la tabla de la siguiente manera:

- Ingrese el nombre de la tarea en el campo de búsqueda para buscar la tarea por su nombre.
- Haga clic en el ícono de ordenar para ordenar las tareas por nombre.

  De manera predeterminada, las tareas se clasifican en orden alfabético ascendente.
- Haga clic en el ícono de filtro y, en la ventana que se abre, filtre las tareas por grupo y luego haga clic en el botón **Aplicar**.

Si está creando una tarea para una aplicación administrada y la programación de la tarea se puede pausar, la tarea tiene las siguientes opciones de programación:

- **Hora de finalización**

  La programación de la tarea se detiene a las 12:00 a. m. de la fecha especificada. Si la tarea sigue en ejecución cuando llega la hora de finalización de la programación, no se interrumpe.

  Por ejemplo, suponga que una tarea se ejecuta todos los días a las 11:00 p. m. Usted especifica que la programación de esta tarea finalizará el 1 de enero. El 31 de diciembre, la tarea se inicia a las 11:00 p. m. y, el 1 de enero a las 12:00 a. m., se pausa su programación. La tarea continúa ejecutándose hasta completarse, pero después de las 11:00 p. m. del 1 de enero, la programación ya no activa la tarea.

  Esta opción está disponible para todos los tipos de programación, excepto **Manual** y **Una vez**.
- **Pausar tarea**

  Si esta opción está habilitada, puede especificar un intervalo durante el cual debe pausarse una tarea que ya se inició según la programación. Por ejemplo, de 10:00 a. m. a 11:00 a. m.

  Esto puede ser necesario durante los períodos de mayor uso del dispositivo para reducir el impacto de la aplicación administrada (por ejemplo, Kaspersky Endpoint Security) en el rendimiento.

  Esta opción está disponible para todos los tipos de programación.

- **Ejecutar tareas no realizadas**

  Esta opción determina el comportamiento de la tarea cuando la misma está por iniciarse y uno de los dispositivos cliente no está visible en la red.

  Si esta opción está habilitada, el sistema intentará iniciar la tarea la siguiente vez que la aplicación de Kaspersky se ejecute en el dispositivo cliente. Si la programación de la tarea es **Manual**, **Una vez** o **Inmediatamente**, la tarea se iniciará inmediatamente después de que el dispositivo aparezca en la red o inmediatamente después de que el dispositivo sea incluido en el alcance de la tarea.

  Si esta opción está deshabilitada, solo las tareas programadas se ejecutan en los dispositivos cliente. Para la programación **Manual**, **Una vez** e **Inmediatamente**, las tareas se ejecutan solo en los dispositivos cliente que están visibles en la red. Podría deshabilitar esta opción para, por ejemplo, una tarea que consuma muchos recursos y que solo deba ejecutarse fuera del horario laboral.

  Esta opción está activada de forma predeterminada.

- **Utilizar retardo aleatorio automático para el inicio de la tarea**

  Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo que especifique. Se realizará, de este modo, un *inicio distribuido*. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

  La hora de inicio distribuida se calcula automáticamente cuando se crea una tarea. El cálculo tiene en cuenta el número de dispositivos cliente a los que la tarea está asignada. Las ejecuciones posteriores a la inicial ocurren siempre a la hora de inicio calculada. Sin embargo, tenga en cuenta que si modifica la configuración de la tarea o inicia la tarea manualmente, la hora de inicio calculada cambiará.

Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

Esta opción está activada de forma predeterminada.

- **Utilizar el retardo aleatorio automático para el inicio de la tarea dentro de un intervalo de**

  Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo de tiempo especificado. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

  Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

  Esta opción está deshabilitada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

- Dispositivos a los que se asignará la tarea:

  Seleccionar dispositivos de la red detectados por el Servidor de administración

  La tarea se asignará a ciertos dispositivos específicos. Estos pueden ser tanto dispositivos asignados a grupos de administración como dispositivos no asignados.

  Podría usar esta opción para, por ejemplo, una tarea que instale el Agente de red en los dispositivos que no estén asignados a un grupo de administración.

  Especificar las direcciones de los dispositivos manualmente o importarlas de una lista

  Puede especificar los nombres DNS, las direcciones IP y las subredes IP de los dispositivos a los cuales desee asignar la tarea.

  Podría elegir esta opción si necesita que la tarea se ejecute en una subred específica. Esto puede ser útil si, por ejemplo, necesita instalar una aplicación solo en los dispositivos que utilizan los contadores o si quiere analizar los dispositivos de una subred puntual que probablemente esté infectada.

  Asignar tarea a una selección de dispositivos

  La tarea se asignará a los dispositivos incluidos en una selección de dispositivos. Puede elegir una selección existente.

  Esta opción puede ser útil para, por ejemplo, ejecutar una tarea en los dispositivos que tengan una versión específica de un sistema operativo.

  Asignar tarea a un grupo de administración

  La tarea se asignará a los dispositivos incluidos en un grupo de administración. Puede seleccionar un grupo existente o crear uno nuevo.

  Puede usar esta opción para, por ejemplo, ejecutar una tarea que envíe un mensaje a ciertos usuarios si el contenido atañe solamente a los dispositivos de un grupo de administración puntual.

  Si se asigna una tarea a un grupo de administración, la pestaña **Seguridad** no se muestra en la ventana de propiedades de la tarea porque las tareas de grupo están sujetas a la configuración de seguridad de los grupos a los que se aplican.

- Ajustes de cuenta:

  Cuenta predeterminada

  La tarea se ejecutará utilizando la misma cuenta que la aplicación que realizará la tarea.

  Esta opción está seleccionada de forma predeterminada.

  Especificar cuenta

Complete los campos **Cuenta** y **Contraseña** para especificar los detalles de la cuenta con la que se ejecutará la tarea. La cuenta debe tener los derechos necesarios para realizar la tarea.

Inicio de sesión.

Cuenta con la que se ejecutará la tarea.

Contraseña

Contraseña de la cuenta con la que se ejecutará la tarea.

Ajustes que se configuran tras crear una tarea

Los siguientes ajustes pueden definirse solamente cuando la tarea ya se ha creado.

- Ajustes para tareas de grupo:

  Distribuir a subgrupos

  Esta opción solo está disponible en los ajustes de tareas de grupo.

  Cuando esta opción está habilitada, el alcance de la tarea incluye lo siguiente:

  - El grupo de administración que se seleccionó al crear la tarea.
  - Los grupos de administración subordinados al grupo de administración seleccionado y ubicados en cualquier nivel de la jerarquía de grupos.

  Cuando esta opción está deshabilitada, el alcance de la tarea incluye solo el grupo de administración que se seleccionó al crear la tarea.

  Esta opción está activada de forma predeterminada.

  Distribuir a Servidores de administración secundarios y virtuales

  Cuando esta opción está habilitada, la tarea aplicada al Servidor de administración principal se aplica también a los servidores de administración secundarios (incluidos los virtuales). Si ya existe una tarea del mismo tipo en un Servidor de administración secundario, se aplican ambas tareas a ese servidor (la existente y la heredada del Servidor de administración principal).

  Esta opción solo está disponible cuando la opción **Distribuir a subgrupos** está habilitada.

  Esta opción está deshabilitada de forma predeterminada.

- Ajustes de programación avanzados:

  Encender dispositivos mediante la función Wake-on-LAN antes de iniciar la tarea

  El sistema operativo del dispositivo se iniciará a la hora especificada antes de que se ejecute la tarea. El período de tiempo predeterminado es de cinco minutos.

  Habilite esta opción si desea que la tarea se ejecute en todos los dispositivos cliente que formen parte del alcance de la tarea, incluidos aquellos que se encuentren apagados cuando la tarea esté próxima a comenzar.

  Si desea que el dispositivo se apague automáticamente una vez completada la tarea, habilite la opción **Apagar dispositivos cuando se complete la tarea**. Encontrará esta opción en la misma ventana.

  Esta opción está deshabilitada de forma predeterminada.

  Apagar los dispositivos después de completar la tarea

Esta opción puede ser útil para, por ejemplo, una tarea que actualice los dispositivos cliente todos los viernes después del horario laboral y luego los apague para que no consuman energía el fin de semana.

Esta opción está deshabilitada de forma predeterminada.

Detener la tarea si tarda más de

Una vez que transcurra el período especificado, la tarea se detendrá automáticamente, se haya completado o no.

Habilite esta opción si desea que las tareas que tarden mucho en completarse se interrumpan o se detengan.

Esta opción está deshabilitada de forma predeterminada. El tiempo de ejecución por defecto para las tareas es de 120 minutos.

- Ajustes de notificaciones:

  - Bloque **Almacenar el historial de la tarea**:

    Guardar en la base de datos del Servidor de administración por (días)

    El Servidor de administración conservará por el número de días especificado los eventos de la aplicación que estén relacionados con la ejecución de la tarea en los dispositivos cliente incluidos en el alcance de la tarea. Transcurrido este período, la información se eliminará del Servidor de administración.

    Esta opción está activada de forma predeterminada.

    Guardar en el registro de eventos del SO del dispositivo

    Los eventos de la aplicación relacionados con la ejecución de la tarea se almacenarán localmente en el registro de eventos de Syslog de cada dispositivo cliente.

    Esta opción está deshabilitada de forma predeterminada.

    Guardar en el registro de eventos del SO del Servidor de administración

    Los eventos de la aplicación que estén relacionados con la ejecución de la tarea en los dispositivos cliente incluidos en el alcance de la tarea se almacenarán centralmente, en el registro de eventos de Syslog del sistema operativo en el que esté instalado el Servidor de administración.

    Esta opción está deshabilitada de forma predeterminada.

    Guardar todos los eventos

    Si selecciona esta opción, se guardarán todos los sucesos vinculados a la tarea en los registros de eventos.

    Guardar eventos relacionados con el progreso de la tarea

    Si selecciona esta opción, se guardarán solo aquellos sucesos que estén vinculados con la ejecución de la tarea en los registros de eventos.

    Guardar solo los resultados de la ejecución de la tarea

    Si selecciona esta opción, se guardarán solo aquellos sucesos que estén vinculados con los resultados de la tarea en los registros de eventos.

  - **Notificar los resultados de ejecución de la tarea al administrador**

    Puede seleccionar los métodos que se usarán para notificar a los administradores sobre los resultados de la ejecución de la tarea. Los métodos posibles son el correo electrónico, los mensajes SMS y la ejecución de un archivo. Para configurar el mecanismo de notificación, haga clic en el vínculo **Configuración**.

De forma predeterminada, todos los métodos de notificación están deshabilitados.

- **Notificar solo acerca de los errores**

  Si esta opción está habilitada, los administradores recibirán una notificación solo si ocurre un error al ejecutar la tarea.

  Si esta opción está deshabilitada, los administradores recibirán una notificación cada vez que se complete la tarea.

  Esta opción está activada de forma predeterminada.

- Los ajustes de seguridad.
- Configuración de la cobertura de la tarea.

  Dependiendo de cómo se determine el alcance de la tarea, estarán presentes los siguientes ajustes:

  Dispositivos

  Si el alcance de la tarea está determinado por un grupo de administración, verá el nombre del grupo. No podrá hacer ningún cambio. Sin embargo, podrá configurar **Exclusiones del alcance de la tarea**.

  Si el alcance de la tarea está determinado por una lista de dispositivos, podrá agregar y eliminar dispositivos en la lista.

  Selección de dispositivos

  Podrá cambiar la selección de dispositivos a la que se aplicará la tarea.

  Exclusiones del alcance de la tarea

  Podrá definir grupos de dispositivos a los que no se aplicará la tarea. Los grupos excluidos solo pueden ser subgrupos del grupo de administración al que se aplica la tarea.

- **Historial de revisiones**.

Exportar una tarea

Kaspersky Security Center Linux permite guardar una tarea y su configuración en un archivo KLT. El archivo KLT puede usarse para importar la tarea guardada en Kaspersky Security Center Windows o Kaspersky Security Center Linux.

Para exportar una tarea:

1. En el menú principal, vaya a **Tareas**.
2. Marque la casilla ubicada junto a la tarea que desee exportar.

   No es posible exportar más de una tarea a la vez. Si selecciona más de una tarea, el botón **Exportar** se desactivará. Las tareas del Servidor de administración tampoco pueden exportarse.
3. Haga clic en el botón **Exportar**.

4. En la ventana **Guardar como** que se abrirá, ingrese la ruta y el nombre del archivo en que se guardará la tarea. Haga clic en el botón **Guardar**.

   La ventana **Guardar como** aparecerá solo si utiliza los navegadores Google Chrome, Microsoft Edge u Opera. Si utiliza otro navegador, el archivo de la tarea se guardará automáticamente en la carpeta **Descargas**.

Importar una tarea

Kaspersky Security Center Linux permite importar una tarea guardada en un archivo KLT. El archivo KLT contiene la tarea exportada y su configuración.

> Para importar correctamente la tarea de la aplicación de Kaspersky, debe instalar el complemento de administración adecuado.

Para importar una tarea:

1. En el menú principal, vaya a **Tareas**.
2. Haga clic en el botón **Importar**.
3. Haga clic en el botón **Examinar** para elegir el archivo de tareas que desee importar.
4. En la ventana que se abrirá, ingrese la ruta al archivo KLT de la tarea y haga clic en el botón **Abrir**. Tenga en cuenta que no podrá seleccionar más de un archivo de tarea.

   Comenzará a procesarse la tarea.
5. Una vez que la tarea se haya procesado, seleccione los dispositivos a los que desee asignarla. Para ello, seleccione una de las siguientes opciones:

   Asignar tarea a un grupo de administración

   La tarea se asignará a los dispositivos incluidos en un grupo de administración. Puede seleccionar un grupo existente o crear uno nuevo.

   Puede usar esta opción para, por ejemplo, ejecutar una tarea que envíe un mensaje a ciertos usuarios si el contenido atañe solamente a los dispositivos de un grupo de administración puntual.

   Si la tarea se asigna a un grupo de administración, la pestaña **Seguridad** no se mostrará en la ventana de propiedades de la tarea; esto se debe a que las tareas de grupo están sujetas a la configuración de seguridad de los grupos a los que se aplican.

   Especificar las direcciones de los dispositivos manualmente o importarlas de una lista

   Puede especificar los nombres DNS, las direcciones IP y las subredes IP de los dispositivos a los cuales desee asignar la tarea.

   Podría elegir esta opción si necesita que la tarea se ejecute en una subred específica. Esto puede ser útil si, por ejemplo, necesita instalar una aplicación solo en los dispositivos que utilizan los contadores o si quiere analizar los dispositivos de una subred puntual que probablemente esté infectada.

   Asignar tarea a una selección de dispositivos

   La tarea se asignará a los dispositivos incluidos en una selección de dispositivos. Puede elegir una selección existente.

   Esta opción puede ser útil para, por ejemplo, ejecutar una tarea en los dispositivos que tengan una versión específica de un sistema operativo.

6. Elija el alcance de la tarea.

7. Haga clic en el botón **Completado** para finalizar la importación de la tarea.

Aparecerá una notificación con los resultados de la importación. Si la tarea se importa correctamente, puede hacer clic en el vínculo **Detalles** para ver las propiedades de la misma.

Una vez que se complete la importación, la tarea aparecerá en la lista de tareas. También se importarán la configuración y la programación de la tarea. La tarea se iniciará de acuerdo con su programación.

Si la tarea importada tiene el mismo nombre que una tarea existente, el nombre de la tarea importada se complementará con un índice secuencial en formato **(<siguiente número secuencial>)**, por ejemplo **(1)** o **(2)**.

Iniciar el Asistente para cambiar contraseñas de tareas

Para una tarea no local, puede especificar una cuenta en la que se debe ejecutar la tarea. La cuenta puede definirse al momento de crear la tarea; si la tarea ya existe, puede definirse en sus propiedades. Si la cuenta especificada se usa de acuerdo con las instrucciones de seguridad de la organización, estas instrucciones pueden requerir cambiar la contraseña de la cuenta de vez en cuando. Cuando la contraseña de la cuenta caduca y usted configura una nueva, las tareas no se iniciarán hasta que especifique la nueva contraseña válida en las propiedades de la tarea.

El Asistente para cambiar contraseñas de tareas permite reemplazar automáticamente la contraseña antigua por una nueva en todas las tareas en las que se utiliza la cuenta especificada. También puede cambiar la contraseña manualmente en las propiedades de cada tarea.

Para iniciar el Asistente para cambiar contraseñas de tareas:

1. En el menú principal, vaya a **Tareas**.

2. Haga clic en **Administrar credenciales de cuentas para tareas de inicio**.

Siga los pasos del asistente.

Paso 1. Especificar credenciales

Especifique las nuevas credenciales que actualmente son válidas en su sistema. Cuando avance al siguiente paso del asistente, Kaspersky Security Center Linux verificará si el nombre de cuenta especificado coincide con el nombre de cuenta configurado en las propiedades de cada tarea no local. Si los nombres de las cuentas coinciden, la contraseña en las propiedades de la tarea se reemplazará automáticamente por la nueva.

Para especificar las nuevas credenciales, seleccione una de estas opciones:

Utilizar cuenta actual

El asistente usará el nombre de la cuenta con la que haya iniciado sesión en Kaspersky Security Center Web Console. Usted deberá escribir la contraseña de dicha cuenta en el campo **Contraseña actual para utilizar en las tareas**.

Especificar una cuenta distinta

Especifique el nombre de la cuenta con la que se iniciarán las tareas. A continuación, escriba la contraseña de dicha cuenta en el campo **Contraseña actual para utilizar en las tareas**.

Si completa el campo **Contraseña anterior (opcional, si desea sustituirla por la actual)**, Kaspersky Security Center Linux únicamente reemplazará la contraseña en aquellas tareas que contengan tanto el nombre de la cuenta como la contraseña anterior. El reemplazo se realiza automáticamente. En todos los demás casos, debe elegir una acción para realizar el siguiente paso del Asistente.

Paso 2. Seleccionar una acción para realizar

Si no especificó la contraseña anterior en el primer paso del Asistente o si la contraseña anterior especificada no coincide con las contraseñas en las propiedades de las tareas, debe elegir una acción para las tareas encontradas.

Para elegir una acción para una tarea:

1. Busque la tarea para la que necesite elegir una acción y seleccione la casilla a su lado.
2. Realice una de las siguientes acciones:
   - Si desea eliminar la contraseña de las propiedades de la tarea, haga clic en **Eliminar credenciales**.

     La tarea pasará a ejecutarse con la cuenta predeterminada.
   - Si desea reemplazar la contraseña con una nueva, haga clic en **Aplicar el cambio de contraseña incluso si la contraseña anterior no se proporcionó o es incorrecta**.
   - Si desea cancelar el cambio de contraseña, haga clic en **No se seleccionó ninguna acción**.

Las acciones que elija se aplicarán cuando avance al siguiente paso del asistente.

Paso 3. Ver los resultados

En el último paso del asistente, tendrá la oportunidad de ver los resultados de cada una de las tareas encontradas. Para finalizar el Asistente, haga clic en el botón **Finalizar**.

Ver resultados de la ejecución de tareas almacenados en el Servidor de administración

Kaspersky Security Center Linux le permite ver los resultados de la ejecución para tareas de grupos, tareas para dispositivos específicos y tareas del Servidor de administración.

Para ver los resultados de la tarea:

En la ventana de propiedades de la tarea, vaya a la pestaña **Resultados**.

Para ver los resultados de la tarea de un Servidor de administración secundario:

1. En la ventana de propiedades de la tarea, seleccione la sección **General**.
2. Haga clic en el vínculo **Resultados** para abrir la ventana **Resultados de la tarea**.
3. Haga clic en **Estadísticas de los servidores secundarios**.
4. Seleccione el servidor secundario para el que desea mostrar la ventana **Resultados de la tarea**.

Etiquetas de aplicación

En esta sección, se explica qué son las etiquetas para aplicaciones y se ofrecen instrucciones para crearlas y modificarlas, así como para etiquetar aplicaciones de terceros.

Etiquetas de aplicación

Kaspersky Security Center Linux le permite etiquetar las aplicaciones desde el registro de aplicaciones. Las etiquetas son rótulos que se asignan a las aplicaciones y que pueden utilizarse para agruparlas o encontrarlas. Asignada a una serie de aplicaciones, una etiqueta puede servir de condición para crear una selección de dispositivos.

Por ejemplo, puede crear la etiqueta `[Navegadores]` y asignarla a todos los navegadores, como Microsoft Internet Explorer, Google Chrome y Mozilla Firefox.

Creación de una etiqueta de aplicación

Para crear una etiqueta de aplicación:

1. En el menú principal, vaya a **Administración de software → Aplicaciones de terceros → Etiquetas de aplicación**.
2. Haga clic en **Agregar**.

   Se abre una ventana para crear la etiqueta.
3. Introduzca el nombre de la etiqueta.
4. Haga clic en **Aceptar** para guardar los cambios.

La nueva etiqueta aparece en la lista de etiquetas de aplicación.

Cambiar el nombre de una etiqueta de aplicación

Para cambiar el nombre de una etiqueta de aplicación:

1. En el menú principal, vaya a **Administración de software → Aplicaciones de terceros → Etiquetas de aplicación**.
2. Marque la casilla ubicada junto a la etiqueta a la que desee cambiarle el nombre y haga clic en **Editar**.

   Se abre la ventana de propiedades de la etiqueta.
3. Cambie el nombre de la etiqueta.
4. Haga clic en **Aceptar** para guardar los cambios.

La etiqueta actualizada aparece en la lista de etiquetas de aplicación.

Asignación de etiquetas a una aplicación

Para asignar una o varias etiquetas a una aplicación:

1. En el menú principal, vaya a **Administración de software → Aplicaciones de terceros → Registro de aplicaciones**.
2. Haga clic en el nombre de la aplicación a la que desee asignar las etiquetas.
3. Seleccione la pestaña **Etiquetas**.

   En la pestaña, verá todas las etiquetas de aplicación que existan en el Servidor de administración. Las etiquetas que estén asignadas a la aplicación elegida tendrán una casilla activada en la columna **Modo de asignación**.
4. Busque las etiquetas que desee asignar y active las casillas de verificación correspondientes en la columna **Modo de asignación**.
5. Haga clic en **Guardar** para guardar los cambios.

Se asignan las etiquetas a la aplicación.

Quitarle una etiqueta a una aplicación

Para quitarle una o más etiquetas a una aplicación:

1. En el menú principal, vaya a **Administración de software → Aplicaciones de terceros → Registro de aplicaciones**.
2. Haga clic en el nombre de la aplicación a la que desee quitarle etiquetas.

3. Seleccione la pestaña **Etiquetas**.

   En la pestaña, verá todas las etiquetas de aplicación que existan en el Servidor de administración. Las etiquetas que estén asignadas a la aplicación elegida tendrán una casilla activada en la columna **Modo de asignación**.

4. Busque las etiquetas que desee quitarle a la aplicación y desactive las casillas de verificación correspondientes en la columna **Modo de asignación**.

5. Haga clic en **Guardar** para guardar los cambios.

Se le quitan las etiquetas seleccionadas a la aplicación.

Las etiquetas de aplicación desasignadas no se eliminan. Si lo desea, puede eliminarlas manualmente.

Eliminación de una etiqueta de aplicación

Para eliminar una etiqueta de aplicación:

1. En el menú principal, vaya a **Administración de software → Aplicaciones de terceros → Etiquetas de aplicación**.

2. En la lista, seleccione la etiqueta de aplicación que desee eliminar.

3. A continuación, haga clic en el botón **Eliminar**.

4. En la ventana que se abre, haga clic en **Aceptar**.

   Se elimina la etiqueta de aplicación. La etiqueta eliminada se borra automáticamente de las aplicaciones a las que estaba asignada.

Usar la utilidad klscflag para abrir el puerto 13291

Puede automatizar el funcionamiento de Kaspersky Security Center Linux usando la utilidad klakaut. La utilidad klakaut y un sistema de ayuda para ello se encuentran en la carpeta de instalación de Kaspersky Security Center Linux. Si desea usar la utilidad klakaut, abra el puerto 13291 mediante la utilidad klscflag.

La utilidad cambia el valor del parámetro KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN.

Para abrir el puerto 13291:

1. Ejecute el siguiente comando en la línea de comandos:

```
/opt/kaspersky/ksc64/sbin/klscflag -ssvset -pv klserver -s 87 -n
KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -sv true -svt BOOL_T -ss "|ss_type =
\"SS_SETTINGS\";"
```

2. Reinicie el servicio del Servidor de administración de Kaspersky Security Center mediante el siguiente comando:
   ```
   sudo systemctl restart kladminserver_srv
   ```

El puerto 13291 está abierto.

Para verificar que el puerto 13291 se haya abierto:

Ejecute el siguiente comando en la línea de comandos:

```
/opt/kaspersky/ksc64/sbin/klscflag -ssvget -pv klserver -s 87 -n
KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
```

El comando dará el siguiente resultado:

```
+--- (PARAMS_T)
+---KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN = (BOOL_T)true
```

El valor `true` significa que el puerto está abierto. De lo contrario, se muestra el valor `false`.

Registro de la aplicación Kaspersky Industrial CyberSecurity for Networks en Kaspersky Security Center Web Console

Para comenzar a trabajar con la aplicación de Kaspersky Industrial CyberSecurity for Networks a través de Kaspersky Security Center Web Console, primero debe registrarlo en Kaspersky Security Center Web Console.

Para registrar la aplicación de Kaspersky Industrial CyberSecurity for Networks:

1. Asegúrese de que se cumplan estos requisitos:

   - Descargó e instaló el complemento web de Kaspersky Industrial CyberSecurity for Networks.

     Puede ocuparse de esto más adelante, mientras el servidor de Kaspersky Industrial CyberSecurity for Networks se sincroniza con el Servidor de administración. Una vez descargado e instalado el complemento, se muestra la sección **KICS para redes** en el menú principal de Kaspersky Security Center Web Console.

   - En la interfaz web de Kaspersky Industrial CyberSecurity for Networks, se configura y habilita la interacción con Kaspersky Security Center Linux. Para obtener más información, consulte la Ayuda de Kaspersky Industrial CyberSecurity for Networks.

2. Mueva el dispositivo donde está instalado Kaspersky Industrial CyberSecurity for Networks Server del grupo Dispositivos no asignados al grupo Dispositivos administrados:

   a. En el menú principal, vaya a **Administración de activos** → **Dispositivos no asignados**.

   b. Seleccione la casilla de verificación ubicada junto al dispositivo donde está instalado Kaspersky Industrial CyberSecurity for Networks Server.

   c. Haga clic en el botón **Mover a un grupo**.

d. En la jerarquía de grupos de administración, seleccione la casilla de verificación ubicada junto al grupo **Dispositivos administrados**.

e. Haga clic en el botón **Mover**.

3. Abra la ventana de propiedades del dispositivo donde está instalado Kaspersky Industrial CyberSecurity for Networks Server.

4. En la página de propiedades del dispositivo, en la sección **General**, seleccione la opción **No desconectarse del Servidor de Administración** y, a continuación, haga clic en el botón **Guardar**.

5. En la página de propiedades del dispositivo, seleccione la sección **Aplicaciones**.

6. En la sección **Aplicaciones**, seleccione el Agente de red de Kaspersky Security Center.

7. Si el estado actual de la solicitud es *Detenido*, espere hasta que cambie a *En ejecución*.

   Esto puede tardar hasta 15 minutos. Si aún no ha instalado el complemento web de Kaspersky Industrial CyberSecurity for Networks, puede hacerlo ahora.

8. Si desea ver las estadísticas de Kaspersky Industrial CyberSecurity for Networks, puede agregar widgets en el panel. Para agregar los widgets, haga lo siguiente:

   a. En el menú principal, vaya a **Supervisión → Panel**.

   b. En el panel, haga clic en el botón **Agregar o restaurar widget web**.

   c. En el menú del widget que se abre, seleccione **Otros**.

   d. Seleccione el widget que desea agregar:

      - Mapa de implementación de KICS para redes
      - Información de KICS para Servidores de Redes
      - Eventos actualizados de KICS para Redes
      - Dispositivos con problemas en KICS para Redes
      - Eventos críticos en KICS para Redes
      - Estados en KICS para Redes

9. Para acceder a la interfaz web de Kaspersky Industrial CyberSecurity for Networks, haga lo siguiente:

   a. En el menú principal, vaya a **KICS para Redes → Buscar**.

   b. Haga clic en el botón **Buscar eventos o dispositivos**.

   c. En la ventana **Parámetros de consulta** que se abrirá, haga clic en el campo **Servidor**.

   d. Seleccione el servidor Kaspersky Industrial CyberSecurity for Networks de la lista desplegable de servidores integrados con Kaspersky Security Center Linux y luego haga clic en el botón **Buscar**.

   e. Haga clic en el vínculo **Ir al servidor** junto al nombre del servidor de Kaspersky Industrial CyberSecurity for Networks.

Se muestra la página de inicio de sesión de Kaspersky Industrial CyberSecurity for Networks.

Para iniciar sesión en la interfaz web de Kaspersky Industrial CyberSecurity for Networks, debe proporcionar las credenciales de la cuenta de usuario de la aplicación.

Administración de usuarios y roles de usuarios

En esta sección se explica qué son, cómo se crean y cómo se modifican los usuarios y los roles de usuario. También se brindan instrucciones para asignar roles y grupos a los usuarios y para asociar los roles a perfiles de directivas.

Acerca de las cuentas de usuario

Kaspersky Security Center Linux le permite administrar cuentas de usuario y grupos de seguridad. La aplicación admite tres tipos de cuentas:

- Cuentas de empleados de la organización. El Servidor de administración obtiene los datos de las cuentas de estos usuarios del dominio cuando sondea el controlador de dominio de la organización.
- Cuentas de usuarios locales. Cuentas locales en dispositivos administrados, así como las cuentas locales en el dispositivo en el que está el instalador del Servidor de administración.
- Cuentas de usuarios internos de Kaspersky Security Center Linux. Puede crear cuentas de usuarios internos. Estas cuentas solamente se utilizan en Kaspersky Security Center Linux.

Las cuentas de usuario locales y el grupo local kladmins del sistema operativo Linux no se pueden utilizar para acceder a Kaspersky Security Center Web Console en Kaspersky Security Center Linux. El grupo kladmins solo puede contener cuentas que se utilizan para iniciar los servicios de Kaspersky Security Center Linux. Los empleados de la organización podrán usar sus cuentas de usuario para iniciar sesión después de configurar la autenticación de dominio.

Para ver tablas de cuentas de usuario y grupos de seguridad, haga lo siguiente:

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos**.
2. Seleccione la pestaña **Usuarios** o **Grupos**.

Se abrirá la tabla de usuarios o grupos de seguridad. Si desea ver la tabla solo con usuarios o grupos internos o solo con usuarios o grupos locales, establezca los criterios de filtro **Tipo de cuenta** en **Interno** o **Local** respectivamente.

Si la tabla de usuarios contiene más de 50 000 usuarios, solo se muestran los primeros 50 000 y no se muestran los demás.

Acerca de los roles de usuario

Un *rol de usuario* (también denominado *rol*) es un objeto que contiene un conjunto de derechos y privilegios. Un rol puede asociarse a la configuración de las aplicaciones de Kaspersky instaladas en un dispositivo de usuario. Puede asignar un rol a un conjunto de usuarios o a un conjunto de grupos de seguridad en cualquier nivel en la jerarquía de grupos de administración, Servidores de administración, o al nivel de objetos específicos.

Si administra dispositivos a través de una jerarquía de Servidores de administración que incluye servidores de administración virtuales, tenga en cuenta que puede crear, modificar o eliminar funciones de usuario sólo desde un Servidor de administración físico. Luego, puede propagar las funciones de usuario a los Servidores de administración secundarios, incluidos los virtuales.

Los roles de usuario pueden asociarse a perfiles de directivas. Cuando a un usuario se le asigna un rol, se le conceden los ajustes de seguridad que necesita para cumplir con sus funciones laborales.

Un rol de usuario puede asociarse a los usuarios que trabajan con los dispositivos de un grupo de administración específico.

Alcance de un rol de usuario

El *alcance de un rol de usuario* es una combinación de usuarios y grupos de administración. Los ajustes asociados a un rol de usuario se aplican únicamente a los dispositivos que pertenecen a los usuarios que tienen ese rol, y solo cuando esos dispositivos pertenecen a grupos y subgrupos asociados al rol en cuestión.

Ventajas de utilizar roles

Una ventaja de utilizar roles es que evita la necesidad de especificar los ajustes de seguridad de cada dispositivo administrado o de cada usuario por separado. La cantidad de usuarios y dispositivos en una empresa puede ser bastante grande, pero el número de descripciones de puestos que requieren ajustes de seguridad diferentes es considerablemente menor.

Diferencias con los perfiles de directivas

Los perfiles de directivas son propiedades de una directiva creada para cada aplicación de Kaspersky por separado. Un rol se asocia a muchos perfiles de directivas creados para aplicaciones diferentes. De ese modo, un rol es una manera de unir en un solo lugar los ajustes para un determinado tipo de usuario.

Configurar los derechos de acceso a las funciones de la aplicación. Control de acceso basado en roles

Kaspersky Security Center Linux proporciona funciones para el acceso basado en roles a las funciones de Kaspersky Security Center Linux y a las de las aplicaciones de Kaspersky administradas.

Puede configurar los derechos de acceso a las funciones de la aplicación para los usuarios de Kaspersky Security Center Linux de una de las siguientes formas:

- Configure los derechos de cada usuario o grupo de usuarios individualmente;
- puede crear roles de usuario estándares con un conjunto de derechos predefinidos y, luego, puede asignar esos roles a sus usuarios basándose en las responsabilidades de esas personas.

Aplicar roles de usuario es una manera de simplificar y agilizar la tarea rutinaria de configurar derechos de acceso a las funciones de la aplicación. Cada rol tiene asignados permisos de acceso que responden a las tareas y obligaciones con las que deben cumplir los usuarios.

Los roles de usuario pueden llevar nombres que identifiquen sus propósitos. Puede crear un número ilimitado de roles en la aplicación.

Puede utilizar roles de usuario predefinidos, que vienen configurados con un conjunto de derechos, o puede crear roles nuevos y configurar los derechos necesarios por su cuenta.

Derechos de acceso a las funciones de la aplicación

En la siguiente tabla, se muestran las funciones de Kaspersky Security Center Linux con los derechos de acceso para administrar las tareas, los informes y las configuraciones asociados y para realizar las acciones del usuario asociadas.

Para realizar las acciones de usuario que se detallan en la tabla, el usuario debe tener el derecho indicado junto a la acción.

Los derechos **Leer**, **Escribir** y **Ejecutar** son aplicables a cualquier tarea, informe o ajuste de configuración. Además de estos tres derechos, para administrar tareas, informes o ajustes en selecciones de dispositivos, el usuario debe tener el derecho **Realizar operaciones en selecciones de dispositivos**.

Todas las tareas, informes, ajustes de configuración y paquetes de instalación que no figuran en la tabla pertenecen al área funcional **Características generales: Funcionalidad básica**.

Área funcional	Derecho	Acción del usuario: derecho necesario para realizar la acción	Tarea	Informe	Otro
Características generales: **Administración de grupos de administración**	**Escribir**	• Agregar un dispositivo a un grupo de administración: **Escribir** • Eliminar un dispositivo de un grupo de administración: **Escribir** • Agregar un grupo de administración a otro grupo de administración: **Escribir** • Eliminar un grupo de administración de otro grupo de administración: **Escribir**	Ninguno	N/C	N/C

Área funcional	Derecho	Acción del usuario: derecho necesario para realizar la acción	Tarea	Informe	Otro
Características generales: **Acceder a objetos sin importar sus ACL**	**Leer**	Obtener acceso de lectura a todos los objetos: **Leer**	Ninguno	N/C	El área funcional **Características generales: Acceder a objetos sin importar sus ACL** está diseñada con fines de auditoría. Un permiso de **Leer** en esta área funcional otorga acceso completo de **Leer** a todos los objetos. Recomendamos conceder estos derechos con precaución y a un conjunto limitado de usuarios que los necesiten para realizar sus funciones oficiales. El acceso se otorga sin importar los demás derechos, incluso si se prohíbe el acceso de lectura a objetos específicos.
Características generales: **Funcionalidad básica**	• **Leer** • **Escribir** • **Ejecutar** • **Realizar operaciones en selecciones de dispositivos**	• Reglas de movimiento de dispositivos (crear, modificar o eliminar) para el Servidor virtual: **Escribir**, **Realizar operaciones en selecciones de dispositivos** • Obtener certificado personalizado del protocolo móvil (LWNGT): **Lectura** • Establecer certificado personalizado del protocolo móvil (LWNGT): **Escritura** • Obtener la lista de redes definidas por NLA: **Leer** • Agregar, modificar o eliminar la lista de redes definidas por NLA: **Escribir** • Ver la lista de control de acceso de los grupos: **Leer** • Consulte el registro del sistema operativo: **Leer** • Ver la clave de recuperación para restaurar el acceso a un disco duro cifrado con BitLocker: **Ejecutar**	• "Descargar actualizaciones en el repositorio del Servidor de administración" • "Entregar informes" • "Distribuir paquete de instalación" • "Instalar aplicación en Servidores de administración secundarios de forma remota"	• "Informe del estado de la protección" • "Informe de amenazas" • "Informe de los dispositivos más infectados" • "Informe sobre el estado de las bases de datos antivirus" • "Informe de errores" • "Informe de ataques de red" • "Informe conciso sobre las aplicaciones instaladas para la protección de sistemas de correo" • "Informe conciso sobre las aplicaciones instaladas para proteger estaciones de trabajo y servidores Windows Server" • "Informe conciso sobre las aplicaciones instaladas para la defensa del perímetro" • "Informe conciso sobre los tipos de aplicaciones instaladas" • "Informe sobre usuarios de dispositivos infectados"	Ninguno

Área funcional	Derecho	Acción del usuario: derecho necesario para realizar la acción	Tarea	Informe	Otro
				• "Informe sobre problemas de seguridad" • "Informe de eventos" • "Informe de actividad de puntos de distribución" • "Informe sobre los Servidores de administración secundarios" • "Informe sobre los eventos de Control de dispositivos" • "Informe de vulnerabilidades" • "Informe sobre aplicaciones prohibidas" • "Informe de Control web" • "Informe sobre el estado de cifrado de los dispositivos administrados" • "Informe sobre el estado de cifrado de los dispositivos de almacenamiento masivo" • "Informe sobre derechos de acceso a unidades cifradas" • "Informe sobre los errores de cifrado de archivos" • "Informe sobre el bloqueo de acceso a los archivos cifrados" • "Informe sobre permisos de usuario vigentes" • "Informe sobre derechos"	
Características generales: **Objetos eliminados**	• **Leer** • **Escribir**	• Ver objetos eliminados en la Papelera de reciclaje: **Leer** • Eliminar objetos de la Papelera de reciclaje: **Escribir**	Ninguno	N/C	N/C

Área funcional	Derecho	Acción del usuario: derecho necesario para realizar la acción	Tarea	Informe	Otro
Características generales: **Procesamiento de eventos**	• **Eliminar eventos** • **Editar la configuración de notificaciones sobre los eventos** • **Editar la configuración del registro de eventos** • **Escribir**	• Cambiar los ajustes de registro de eventos: **Editar la configuración de registro de eventos** • Cambiar los ajustes de las notificaciones sobre los eventos: **Editar configuración de notificación de eventos** • Eliminar eventos: **Eliminar eventos**	Ninguno	N/C	Configuración: • Cantidad máxima de eventos almacenados en la base de datos • Período por el que se almacenan los eventos de los dispositivos eliminados
Características generales: **Operaciones en el Servidor de administración**	• **Leer** • **Escribir** • **Ejecutar** • **Modificar ACL de objeto** • **Realizar operaciones en selecciones de dispositivos**	• Especificar los puertos del Servidor de administración para la conexión del Agente de red: **Escribir** • Especificar los puertos del proxy de activación ejecutado en el Servidor de administración: **Escribir** • Especificar los puertos del proxy de activación para dispositivos móviles ejecutado en el Servidor de administración: **Escribir** • Especificar los puertos del Servidor web para la distribución de paquetes independientes: **Escribir** • Especificar los puertos del Servidor web para la distribución de perfiles de MDM: **Escribir** • Especificar los puertos SSL del Servidor de administración para conectarse a través de Web Console: **Escribir** • Especificar los puertos del Servidor de administración para la conexión de dispositivos móviles: **Escribir** • Especificar la cantidad máxima de eventos que se pueden almacenar en la base de datos del Servidor de administración **Escribir**	• "Copia de seguridad de los datos del Servidor de administración" • "Mantenimiento de bases de datos"	Ninguno	N/C

Área funcional	Derecho	Acción del usuario: derecho necesario para realizar la acción	Tarea	Informe	Otro
		• Especificar la cantidad máxima de eventos que puede enviar el Servidor de administración: **Escribir** • Especificar el período durante el cual puede enviar eventos el Servidor de administración: **Escribir**			
Características generales: **Despliegue del software de Kaspersky**	• **Administrar parches de Kaspersky** • **Leer** • **Escribir** • **Ejecutar** • **Realizar operaciones en selecciones de dispositivos**	Aprobar o rechazar la instalación del parche: **Administrar parches de Kaspersky**	Ninguno	• "Informe sobre el uso de claves de licencia por Servidor de administración virtual" • "Informe de versiones del software de Kaspersky" • "Informe de aplicaciones incompatibles" • "Informe sobre la versión de las actualizaciones para los módulos de software de Kaspersky" • "Informe del despliegue de la protección"	Paquete de instalación: "Kaspersky"
Características generales: **Administración de claves**	• **Exportar archivo de clave** • **Escribir**	• Exportar un archivo de clave: **Exportar archivo de clave** • Modificar la configuración de la clave de licencia del Servidor de administración: **Escribir**	Ninguno	N/C	N/C
Características generales: **Administración de informes**	• **Leer** • **Escribir**	• Crear informes independientemente de sus ACL: **Escribir** • Ejecutar informes independientemente de sus ACL: **Leer**	Ninguno	N/C	N/C
Características generales: **Jerarquía de Servidores de administración**	**Configurar los parámetros de jerarquía del Servidor de administración**	• Registrar, actualizar o eliminar Servidores de administración secundarios: **Configurar la jerarquía de Servidores de administración**	Ninguno	N/C	N/C
Características generales: **Permisos de usuario**	**Modificar ACL de objeto**	• Cambiar las propiedades de seguridad de cualquier objeto: **Modificar ACL de objeto** • Administrar roles de usuario: **Modificar ACL de objeto** • Administrar usuarios internos: **Modificar ACL de objeto**	Ninguno	N/C	N/C

Área funcional	Derecho	Acción del usuario: derecho necesario para realizar la acción	Tarea	Informe	Otro
		• Administrar grupos de seguridad: **Modificar ACL de objeto** • Administrar alias: **Modificar ACL de objeto**			
Características generales: **Servidores de administración virtuales**	• **Administración de Servidores de administración virtuales** • **Leer** • **Escribir** • **Ejecutar** • **Realizar operaciones en selecciones de dispositivos**	• Obtener la lista de Servidores de administración virtuales: **Leer** • Obtener información sobre el Servidor de administración virtual: **Leer** • Crear, actualizar o eliminar un Servidor de administración virtual: **Administrar Servidores de administración virtuales** • Mover un Servidor de administración virtual a otro grupo: **Administrar Servidores de administración virtuales** • Definir los permisos de un Servidor de administración virtual: **Administrar Servidores de administración virtuales**	Ninguno	N/C	N/C

Área funcional	Derecho	Acción del usuario: derecho necesario para realizar la acción	Tarea	Informe	Otro
Características generales: Administración de claves de cifrado	**Escribir**	Importar las claves de cifrado: **Escribir**	Ninguno	N/C	N/C
Administración de dispositivos móviles: General	• **Conectar nuevos dispositivos** • **Enviar únicamente comandos de información a dispositivos móviles** • **Enviar comandos a dispositivos móviles** • **Administrar certificados** • **Leer** • **Escribir**	• Obtener datos de restauración del servicio de administración de claves: **Leer** • Eliminar certificados de usuario: **Administrar certificados** • Obtener la parte pública de un certificado de usuario: **Leer** • Comprobar si la infraestructura de claves públicas está habilitada: **Leer** • Comprobar la cuenta de la infraestructura de claves públicas: **Leer** • Obtener plantillas de la infraestructura de claves públicas: **Leer** • Obtener plantillas de la infraestructura de claves públicas mediante un certificado de uso extendido de clave: **Leer** • Comprobar si el certificado de la infraestructura de claves públicas ha sido revocado: **Leer** • Actualizar la configuración de emisión de certificados de usuario: **Administrar certificados** • Obtener la configuración de emisión de certificados de usuario: **Leer** • Obtener paquetes por nombre y versión de aplicación: **Leer** • Definir o cancelar un certificado de usuario: **Administrar certificados** • Renovar un certificado de usuario: **Administrar certificados**	Ninguno	N/C	N/C

Área funcional	Derecho	Acción del usuario: derecho necesario para realizar la acción	Tarea	Informe	Otro
		• Definir una etiqueta para un certificado de usuario: **Administrar certificados** • Ejecutar la generación del paquete de instalación de MDM; cancelar la generación del paquete de instalación de MDM: **Conectar nuevos dispositivos**			
Administración de sistemas: **Conectividad**	• **Iniciar sesiones RDP** • **Conexión a sesiones de RDP existentes** • **Iniciar la tunelización** • **Guardar los archivos de los dispositivos en la estación de trabajo del administrador** • **Leer** • **Escribir** • **Ejecutar** • **Realizar operaciones en selecciones de dispositivos**	• Crear una sesión de escritorio compartido: **Derecho para crear una sesión de escritorio compartido** • Crear una sesión de RDP: **Conexión a sesiones de RDP existentes** • Crear un túnel: **Iniciar la tunelización** • Guardar la lista de red de contenido: **Guardar archivos de los dispositivos en la estación de trabajo del administrador**	Ninguno	"Informe sobre los usuarios de los dispositivos"	Ninguno
Administración de sistemas: **Administración de vulnerabilidades y parches**	• **Leer** • **Escribir** • **Ejecutar** • **Realizar operaciones en selecciones de dispositivos**	• Ver propiedades de parches de terceros: **Leer** • Cambiar las propiedades de parches de terceros: **Escribir**	• "Reparar vulnerabilidades" • "Instalar actualizaciones requeridas y reparar vulnerabilidades"	"Informe de actualizaciones de software"	Ninguno
Administración del sistema: **Ejecución remota de scripts**	• **Leer** • **Escribir** • **Ejecutar** • **Realizar operaciones en selecciones de dispositivos**	El usuario puede ver las propiedades de la tarea: **Lectura** El usuario puede crear, eliminar o modificar un paquete de instalación: **Escritura** El usuario puede ejecutar una tarea: **Escribir**. En los dispositivos cliente Linux, los scripts se ejecutan con privilegios de raíz. El usuario puede ejecutar una tarea o programar su ejecución: **Ejecución** El usuario puede ejecutar una tarea en una selección de dispositivos: **Realizar operaciones en selecciones de dispositivos**	"Ejecución remota de scripts"	Ninguno	N/C

Roles de usuario predefinidos

Los roles de usuario asignados a los usuarios de Kaspersky Security Center Linux les proporcionan conjuntos de derechos que necesitan para acceder a las funciones de la aplicación.

A los usuarios creados en un Servidor virtual no se les puede asignar una función en el Servidor de administración.

Puede utilizar roles de usuario predefinidos, que vienen configurados con un conjunto de derechos, o puede crear roles nuevos. En este caso, debe establecer el alcance del rol y asignar los derechos de acceso a las funciones de Kaspersky Security Center Linux por su cuenta. Algunas de las funciones de usuario predefinidas disponibles en Kaspersky Security Center Linux se pueden asociar con puestos de trabajo específicos, por ejemplo, **Auditor**, **Oficial de seguridad**, **Supervisor**. Los derechos de acceso de estos roles están preconfigurados para facilitar las obligaciones y las tareas típicas de los puestos asociados. En la siguiente tabla, se muestra cómo estos roles pueden vincularse a puestos de trabajo específicos.

Ejemplos de roles para puestos de trabajo específicos

Rol	Comentario
Auditor	Permite todas las operaciones de visualización y ejecución de las tareas creadas en selecciones de dispositivos conectados al Servidor de administración a través del Agente de red con derechos de administrador local (raíz para Linux). Recomendamos asignar esta función con cuidado y a un grupo limitado de usuarios que la necesiten para desempeñar sus funciones oficiales.
Supervisor	Permite realizar cualquier operación de visualización; no permite realizar otras operaciones. Puede asignar este rol a un oficial de seguridad y a otras personas que tengan a su cargo la seguridad de TI de la organización.
Oficial de seguridad	Permite realizar cualquier operación de visualización y permite administrar los informes; también otorga permisos limitados en el área **Administración de sistemas**: **Conectividad**. Puede asignar este rol al responsable de la seguridad de TI de su organización.

En la siguiente tabla, se muestran los derechos de acceso asignados a cada rol de usuario predefinido.

Derechos de acceso de los roles de usuario predefinidos

Rol	Descripción
Administrador del Servidor de administración	Permite todas las operaciones en las siguientes áreas funcionales: • **Características generales**: • **Funcionalidad básica** • **Administración de claves de cifrado** • **Procesamiento de eventos** • **Jerarquía de Servidores de administración** • **Servidores de administración virtuales** • **Administración de sistemas**: • **Conectividad** • **Inventario de hardware** • **Inventario de software**

Rol	Descripción
Operador del Servidor de administración	Otorga los derechos **Leer** y **Ejecutar** (cuando corresponde) en las siguientes áreas funcionales: • **Características generales**: • **Funcionalidad básica** • **Administración de claves de cifrado** • **Servidores de administración virtuales** • **Administración de sistemas**: • **Conectividad** • **Inventario de hardware** • **Inventario de software**
Auditor	Permite todas las operaciones en las siguientes áreas funcionales, en **Características generales**: • **Acceder a objetos sin importar sus ACL** • **Objetos eliminados** • **Administración de informes controlada** Puede asignar este rol a la persona que realiza la auditoría de su organización.
Administrador de instalación	Permite todas las operaciones en las siguientes áreas funcionales: • **Características generales:** • **Funcionalidad básica** • **Despliegue de la aplicación Kaspersky** • **Administración de claves de licencia** • **Administración de sistemas:** • **Despliegue de sistemas operativos** • **Administración de vulnerabilidades y parches** • **Instalación remota** • **Inventario de software** Otorga los derechos **Leer** y **Ejecutar** en el área funcional **Características generales: servidores de administración virtuales**.
Operador de instalación	Otorga los derechos **Leer** y **Ejecutar** (cuando corresponde) en las siguientes áreas funcionales: • **Características generales:** • **Funcionalidad básica** • **Despliegue del software de Kaspersky** (también otorga el derecho **Administrar parches de Kaspersky Lab** en esta área) • **Servidores de administración virtuales** • **Administración de sistemas:** • **Despliegue de sistemas operativos** • **Administración de vulnerabilidades y parches** • **Instalación remota** • **Inventario de software**
Administrador de Kaspersky Endpoint Security	Permite todas las operaciones en las siguientes áreas funcionales: • **Características generales: funcionalidad básica** • **Características generales: administración de claves de cifrado** • **Área de Kaspersky Endpoint Security**, incluidas todas las funciones
Operador de Kaspersky Endpoint Security	Otorga los derechos **Leer** y **Ejecutar** (cuando corresponde) en las siguientes áreas funcionales: • **Características generales: funcionalidad básica** • **Características generales: administración de claves de cifrado** • **Área de Kaspersky Endpoint Security**, incluidas todas las funciones
Administrador general	Permite todas las operaciones en todas las áreas funcionales, *excepto* en las siguientes áreas, en **Características generales**: • **Acceder a objetos sin importar sus ACL** • **Administración de informes forzados**

Rol	Descripción
Operador principal	Otorga los derechos **Leer** y **Ejecutar** (cuando corresponde) en las siguientes áreas funcionales: • **Características generales**: • **Funcionalidad básica** • **Objetos eliminados** • **Administración de claves de cifrado** • **Operaciones con el Servidor de administración** • **Etiquetas de dispositivo** • **Despliegue de la aplicación Kaspersky** • **Integración de aplicaciones** • **Servidores de administración virtuales** • **Área de administración de dispositivos móviles**, incluidas todas las funciones • **Área de administración de sistemas**, incluidas todas las funciones • **Área de Kaspersky Endpoint Security**, incluidas todas las funciones
Administrador de Administración de dispositivos móviles	Permite todas las operaciones en las siguientes áreas funcionales: • **Características generales: funcionalidad básica** • **Área de administración de dispositivos móviles**, incluidas todas las funciones Otorga el derecho **Exportar archivo clave** en **Características generales: administración de claves de licencia**. Otorga el derecho **Lectura** en **Administración del sistema: administración de vulnerabilidades y parches**.
Operador de Administración de dispositivos móviles	Otorga los derechos **Leer** y **Ejecutar** en **Características generales: funcionalidad básica**. Otorga los derechos **Leer** y **Enviar comandos de información a dispositivos móviles** en **Administración de dispositivos móviles**: • **Común** • **Self Service Portal**
Oficial de seguridad	Permite todas las operaciones en las siguientes áreas funcionales, en **Características generales**: • **Acceder a objetos sin importar sus ACL** • **Administración de informes forzados** Otorga los siguientes derechos en el área funcional **Administración del sistema: conectividad:Leer**, **Escribir**, **Ejecutar**, **Guardar archivos desde dispositivos en la estación de trabajo del administrador** y **Realizar operaciones en selecciones de dispositivos**. Puede asignar este rol al responsable de la seguridad de TI de su organización.
Usuario de Self Service Portal	Permite todas las operaciones en el área funcional **Administración de dispositivos móviles: Self Service Portal**.
Supervisor	Otorga el derecho **Leer** en las áreas funcionales **Características generales**: **Acceder a objetos sin importar sus ACL** y **Características generales**: **Administración de informes forzados**. Puede asignar este rol a un Director de seguridad y a otras personas que tengan a su cargo la seguridad de TI de la organización.
Administrador de Administración de vulnerabilidades y parches	Permite todas las operaciones en las áreas funcionales **Características generales**: **Funcionalidad básica** y **Administración de sistemas** (se incluyen todas las funciones, *excepto* la función **Ejecución remota de scripts**).
Operador de Administración de vulnerabilidades y parches	Otorga los derechos **Leer** y **Ejecutar** (cuando corresponde) en las áreas funcionales **Características generales**: **Funcionalidad básica** y **Administración de sistemas** (se incluyen todas las funciones, *excepto* la función **Ejecución remota de scripts**).

Asignación de derechos de acceso a objetos específicos

Además de asignar derechos de acceso al nivel de servidor, puede configurar el acceso a objetos específicos, por ejemplo, a una tarea específica. La aplicación le permite especificar derechos de acceso a los siguientes tipos de objetos:

- Grupos de administración
- Tareas
- Informes
- Selecciones de dispositivos
- Selecciones de eventos

Para asignar derechos de acceso a un objeto específico:

1. Según el tipo de objeto, en el menú principal vaya a la sección correspondiente:
   - **Administración de activos → Jerarquía de grupos**
   - **Tareas**
   - **Supervisión → Informes**
   - **Administración de activos → Selecciones de dispositivos**
   - **Supervisión → Selecciones de eventos**
2. Abra las propiedades del objeto al que desea configurar los derechos de acceso.

   Para abrir la ventana de propiedades de un grupo de administración o una tarea, haga clic en el nombre del objeto. Las propiedades de otros objetos se pueden abrir usando el botón en la barra de herramientas.
3. En la ventana de propiedades, abra la sección **Derechos de acceso**.

   Se abre la lista de usuarios. Los usuarios y grupos de seguridad enumerados tienen derechos de acceso al objeto. De forma predeterminada, si utiliza una jerarquía de grupos o servidores de administración, la lista y los derechos de acceso se heredan del grupo de administración principal o del servidor principal.
4. Para poder modificar la lista, habilite la opción **Usar permisos personalizados** opción.

5. Configurar derechos de acceso:

   - Use los botones **Agregar** y **Eliminar** para modificar la lista.
   - Especifique los derechos de acceso para un usuario o grupo de seguridad. Realice una de las siguientes acciones:
     - Si desea especificar los derechos de acceso manualmente, seleccione el usuario o grupo de seguridad, haga clic en el botón **Derechos de acceso** y, a continuación, especifique los derechos de acceso.
     - Si desea asignar un rol de usuario al usuario o grupo de seguridad, seleccione el usuario o grupo de seguridad, haga clic en el botón **Roles** y, a continuación, seleccione el rol que desea asignar.

6. Haga clic en el botón **Guardar**.

Los derechos de acceso al objeto se configuran.

Asignar derechos de acceso a usuarios y grupos de seguridad

Puede asignar derechos de acceso a sus usuarios y grupos de seguridad para que puedan utilizar diferentes funciones del Servidor de administración, como Kaspersky Endpoint Security for Linux.

Para asignar derechos de acceso a un usuario o grupo de seguridad, haga lo siguiente:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Derechos de acceso**, marque la casilla ubicada junto al nombre del usuario o del grupo de seguridad al que desea asignar derechos y, luego, haga clic en el botón **Derechos de acceso**.

   No puede seleccionar varios usuarios o grupos de seguridad al mismo tiempo. Si selecciona más de un elemento, el botón **Derechos de acceso** se deshabilitará.

3. Configure el conjunto de derechos para el usuario o grupo:

   a. Amplíe el nodo con funciones del Servidor de administración o de otra aplicación de Kaspersky.

   b. Marque las casillas **Permitir** o **Denegar** ubicadas junto a la función o el derecho de acceso pertinentes.

      Ejemplo 1: Marque la casilla **Permitir** ubicada junto al nodo **Integración de aplicaciones** para otorgar a un usuario o grupo todos los derechos de acceso disponibles para la característica de integración de aplicaciones (**Lectura**, **Escritura** y **Ejecución**).

      Ejemplo 2: Expanda el nodo **Administración de claves de cifrado** y marque la casilla **Permitir** ubicada junto al permiso **Escritura** para otorgar a un usuario o grupo el derecho de acceso **Escritura** para la función de administración de claves de cifrado.

4. Después de configurar el conjunto de derechos de acceso, haga clic en **Aceptar**.

Se configurará el conjunto de derechos para el usuario o grupo de usuarios.

Los permisos del Servidor de administración (o el grupo de administración) se dividen en las siguientes áreas:

- Características generales:
  - Gestión de grupos de administración
  - Acceder a objetos sin importar sus ACL
  - Funcionalidad básica
  - Objetos eliminados
  - Administración de claves de cifrado
  - Procesamiento de eventos
  - Operaciones en el Servidor de administración (solo en la ventana de propiedades del Servidor de administración)
  - Etiquetas de dispositivos
  - Despliegue de la aplicación de Kaspersky
  - Administración de claves de licencia
  - Integración de aplicaciones
  - Administración de informes controlada
  - Jerarquía de Servidores de administración
  - Permisos de usuario
  - Servidores de administración virtuales
- Administración de dispositivos móviles:
  - General
  - Self Service Portal
- Administración de sistemas:
  - Conectividad
  - Ejecutar scripts de forma remota
  - Inventario de hardware
  - Control de acceso a la red
  - Despliegue del SO
  - Administración de vulnerabilidades y parches

- Instalación remota
- Inventario de software

Si no se selecciona **Permitir** ni **Denegar** para un permiso, el permiso se considera *indefinido*: se deniega hasta que se deniegue o permita explícitamente al usuario.

Los derechos de un usuario son la suma de lo siguiente:

- los propios derechos del usuario
- los derechos de todos los roles asignados al usuario
- los derechos de todo el grupo de seguridad al que pertenece el usuario
- los derechos de todos los roles asignados a los grupos de seguridad a los que pertenece el usuario

Si al menos uno de estos conjuntos de derechos tiene **Denegar** para un permiso, al usuario se le niega este permiso, incluso si otros conjuntos lo permiten o lo dejan sin definir.

También puede agregar usuarios y grupos de seguridad al alcance de un rol de usuario para usar diferentes funciones del Servidor de administración. Los ajustes asociados a un rol de usuario se aplican únicamente a los dispositivos que pertenecen a los usuarios que tienen ese rol, y solo cuando esos dispositivos pertenecen a grupos y subgrupos asociados al rol en cuestión.

Agregar una cuenta de un usuario interno

Si desea agregar una cuenta de usuario, asegúrese de que su cuenta tenga el derecho Modificar ACL de objeto en el área funcional Características generales: Permisos de usuario.

Para agregar una nueva cuenta de usuario interna a Kaspersky Security Center Linux:

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos** y luego seleccione la pestaña **Usuarios**.
2. Haga clic en **Agregar**.
3. En la ventana **Agregar usuario** que se abre, especifique la configuración de la nueva cuenta de usuario:
   - **Nombre**.
   - **Contraseña** para la conexión del usuario con Kaspersky Security Center Linux.
     La contraseña debe cumplir con las siguientes reglas:
     - La contraseña debe tener entre 8 y 256 caracteres.
     - La contraseña debe incluir caracteres de al menos tres de los grupos enumerados a continuación:
       - Letras mayúsculas (A–Z)
       - Letras minúsculas (a-z)

- Números (0–9)
- Caracteres especiales (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

- La contraseña no debe contener espacios en blanco, caracteres Unicode ni la combinación de "." y "@" cuando "." precede a "@".

Para ver la contraseña ingresada, haga clic en .

Puede habilitar la opción **El usuario debe cambiar la contraseña la primera vez que inicie sesión** para obligarlo a cambiar la contraseña cuando se autentique por primera vez.

4. Guarde los cambios para terminar de crear la nueva cuenta de usuario.

Se agrega una nueva cuenta de usuarios a la lista de usuarios.

Para iniciar sesión con una cuenta de usuario interno creada en Kaspersky Security Center Web Console, debe asignar una función a la cuenta. Antes de iniciar sesión, asegúrese de que se haya asignado una función a la cuenta de usuario interno. De lo contrario, se producirá un error de inicio de sesión.

Crear un grupo de seguridad

Para crear un grupo de seguridad:

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos** y luego seleccione la pestaña **Grupos**.
2. Haga clic en **Agregar**.
3. En la ventana **Crear grupo de seguridad** que se abre, especifique la siguiente configuración para el nuevo grupo de seguridad:
   - **Nombre del grupo**
   - **Descripción**
4. Haga clic en **Guardar** para guardar los cambios.

Se agrega un nuevo grupo de seguridad a la lista de grupos.

Editar una cuenta de un usuario interno

Si desea editar una cuenta de usuario, asegúrese de que su cuenta tenga el derecho Modificar ACL de objeto en el área funcional Características generales: Permisos de usuario.

Para modificar una cuenta de usuario interna en Kaspersky Security Center Linux:

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos** y luego seleccione la pestaña **Usuarios**.
2. Haga clic en el nombre de la cuenta de usuario que desee editar.
3. En la ventana de configuración de usuario que se abre, en la pestaña **General**, cambie la configuración de la cuenta de usuario:

   - **Cuenta del usuario**

     Si es necesario, cambie el botón de alternar a **Inactiva** para prohibir que el usuario se conecte a la aplicación. Puede desactivar una cuenta, por ejemplo, después de que un empleado abandone la empresa.

   - Descripción
   - **Nombre completo**
   - **Dirección de correo electrónico**
   - **Teléfono principal**
   - **Contraseña**

     Si es necesario, puede configurar una nueva contraseña para la conexión del usuario a Kaspersky Security Center Linux de la siguiente manera:

     a. Haga clic en el botón **Cambiar contraseña** y establezca la contraseña nueva de la cuenta de usuario.

     La contraseña debe cumplir con las siguientes reglas:

     - La contraseña debe tener entre 8 y 256 caracteres.
     - La contraseña debe incluir caracteres de al menos tres de los grupos enumerados a continuación:
       - Letras mayúsculas (A–Z)
       - Letras minúsculas (a-z)
       - Números (0–9)
       - Caracteres especiales (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - La contraseña no debe contener espacios en blanco, caracteres Unicode ni la combinación de "." y "@" cuando "." precede a "@".

     Para ver la contraseña ingresada, haga clic en .

     b. Si es necesario, active la opción **El usuario debe cambiar la contraseña la primera vez que inicie sesión** para forzar el cambio de contraseña la siguiente vez que el usuario se autentique.

     c. Si la cuenta de usuario está protegida contra modificaciones no autorizadas, verifique si tiene los permisos necesarios para modificarla. En la ventana **Protección de cuentas**, especifique las credenciales de la cuenta con derecho de Modificar ACL de objeto en el área funcional Características generales: Permisos de usuario.

4. En la pestaña **Autenticación de dos factores**, puede especificar la configuración de seguridad para esta cuenta.
5. En la pestaña **Grupos**, puede añadir al usuario a grupos de seguridad.
6. En la pestaña **Dispositivos**, puede asignar dispositivos al usuario.
7. En la pestaña **Roles**, puede asignar funciones al usuario.
8. Guarde los cambios para terminar de editar la cuenta de usuario.

La cuenta de usuario actualizada aparece en la lista de usuarios.

Editar un grupo de seguridad

Para editar un grupo de seguridad:

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos** y luego seleccione la pestaña **Grupos**.
2. Haga clic en el nombre del grupo de seguridad que desee editar.
3. Cuando se abra la ventana de configuración del grupo, cambie la configuración del grupo de seguridad:
   - En la pestaña **General**, puede cambiar la configuración de **Nombre** y **Descripción**. Estas configuraciones están disponibles solo para grupos de seguridad internos.
   - En la pestaña **Usuarios**, puede agregar usuarios al grupo de seguridad. Esta configuración solo está disponible para usuarios internos y grupos de seguridad internos.
   - En la pestaña **Roles**, puede asignar un rol al grupo de seguridad.
4. Haga clic en **Guardar** para guardar los cambios.

Los cambios se aplican al grupo de seguridad.

Asignación de un rol a un usuario o a un grupo de seguridad

Para asignar un rol a un usuario o grupo de seguridad, haga lo siguiente:

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos**, y luego seleccione la pestaña **Usuarios** o **Grupos**.
2. Seleccione el nombre del usuario o del grupo de seguridad a quien desea asignar un rol.

   Puede seleccionar varios nombres.
3. En la línea del menú, haga clic en el botón **Asignar rol**.

   Se inicia el asistente de asignación de roles.

4. Siga las instrucciones del asistente: seleccione el rol que desea asignar a los usuarios o grupos de seguridad seleccionados, y elija el alcance del rol.

   El *alcance de un rol de usuario* es una combinación de usuarios y grupos de administración. Los ajustes asociados a un rol de usuario se aplican únicamente a los dispositivos que pertenecen a los usuarios que tienen ese rol, y solo cuando esos dispositivos pertenecen a grupos y subgrupos asociados al rol en cuestión.

El rol con un conjunto de derechos para trabajar con el Servidor de administración se asigna al usuario (o usuarios, o al grupo de seguridad). En la lista de usuarios o grupos de seguridad, aparece una casilla en la columna **Tiene roles asignados**.

Agregar cuentas de usuario a un grupo interno de seguridad

Las únicas cuentas que se pueden agregar a un grupo interno son las de usuarios de seguridad.

Para agregar cuentas de usuario a un grupo interno de seguridad:

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos** y luego seleccione la pestaña **Usuarios**.
2. Active las casillas de verificación ubicadas junto a las cuentas de usuario que desee agregar al grupo de seguridad.
3. Haga clic en el botón **Asignar grupo**.
4. En la ventana **Asignar grupo** que se abrirá, seleccione el grupo de seguridad al que desee agregar las cuentas de usuario.
5. Haga clic en el botón **Guardar**.

Las cuentas de usuario se agregarán al grupo de seguridad. También puede agregar usuarios internos a un grupo de seguridad mediante la configuración del grupo.

Designación de un usuario como propietario de un dispositivo

Si busca información para designar a un usuario como propietario de un dispositivo móvil, consulte la Ayuda de Kaspersky Secure Mobility Management.

Para designar a un usuario como propietario de un dispositivo:

1. Si desea asignar un propietario de un dispositivo conectado a un Servidor de administración virtual, primero cambie al Servidor de administración virtual:

   a. En el menú principal, haga clic en el ícono de corchete (›) a la derecha del nombre del Servidor de administración actual.

   b. Seleccione el Servidor de administración requerido.

2. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos** y luego seleccione la pestaña **Usuarios**.

   Se abre la lista de usuarios. Si actualmente está conectado a un Servidor de administración virtual, la lista incluye usuarios del Servidor de administración virtual actual y el Servidor de administración principal.

3. Haga clic en el nombre de la cuenta de usuario que desee designar como propietario del dispositivo.

4. En la ventana que se abre con la configuración del usuario, seleccione la pestaña **Dispositivos**.

5. Haga clic en **Agregar**.

6. En la lista de dispositivos, seleccione el dispositivo que desee asignar al usuario.

7. Haga clic en **Aceptar**.

El dispositivo seleccionado se agrega a la lista de dispositivos asignados al usuario.

Como alternativa para realizar esta operación, ingrese a **Administración de activos** → **Dispositivos administrados**, haga clic en el nombre del dispositivo que desee asignar y luego haga clic en el vínculo **Administrar propietario del dispositivo**.

Designación de un usuario como propietario de un dispositivo durante la instalación del Agente de red

Para designar a un usuario como propietario de un dispositivo al instalar el Agente de red a través de un paquete de instalación, agregue las variables especificadas en la siguiente tabla a la configuración del paquete de instalación del Agente de red.

Nombre de la variable	Obligatoria	Descripción	Valores posibles
KLNAGENT_DEVICEOWNER_REGISTRATION_START	No	Permite ejecutar la utilidad para registrar al usuario como propietario del dispositivo después de que se instale el Agente de red. Si deshabilita esta función, el usuario no podrá registrarse como propietario del dispositivo.	1: la utilidad para registrar al usuario como propietario del dispositivo se iniciará después de que se instale el Agente de red. Otro valor: la utilidad no estará disponible.

KLNAGENT_DEVICEOWNER_LOGIN	No Sí, si ingresa la contraseña	Contiene el nombre de usuario de la persona que se registrará como propietario del dispositivo.	El nombre de usuario como se figura en la lista de usuarios de Kaspersky Security Center Linux.
KLNAGENT_DEVICEOWNER_PASSWORD	No Sí, si ingresa el nombre de usuario	Contiene la contraseña cifrada de la persona que se registrará como propietario del dispositivo.	La contraseña del usuario.

El Agente de red descifrará el nombre de usuario y la contraseña especificados durante la instalación de Kaspersky Security Center Linux, y el usuario será registrado como propietario del dispositivo.

Como alternativa, para designar a un usuario como propietario de un dispositivo al instalar el Agente de red en modo silencioso, puede usar un archivo de respuesta.

Para designar a un usuario como propietario de un dispositivo al instalar el Agente de red en modo silencioso con un archivo de respuesta:

1. Agregue el parámetro KLNAGENT_DEVICEOWNER_REGISTRATION_START al archivo de respuesta y establezca su valor en 1.

   La utilidad para registrar al usuario como propietario del dispositivo se iniciará después de que se instale el Agente de red.

2. Ingrese el nombre de usuario y la contraseña en la línea de comandos del dispositivo cliente.

   Se designará al usuario como propietario del dispositivo.

Si el usuario forma parte de un grupo de seguridad interno, el nombre de usuario debe ser el mismo.

Si el usuario forma parte de un grupo de seguridad de Active Directory, el nombre de usuario debe constar del nombre de usuario y el nombre de dominio.

Debe ingresar la contraseña de un solo uso basado en el tiempo (TOTP) de la app para la autenticación de dos factores.

Asignar a un usuario como propietario del dispositivo tras instalar el Agente de red

Para permitir que el usuario se registre como propietario de un dispositivo Linux:

1. En Kaspersky Security Center Web Console, vaya a **Administración de software → Paquetes de instalación**.

   Se abrirá la lista de paquetes de instalación.

2. Haga clic en el paquete de instalación del Agente de red.

   Se abrirá la ventana de propiedades del paquete de instalación.

3. En la ventana de propiedades del paquete de instalación, haga clic en **Configuración → Avanzado**.

4. En la sección **Registro de usuario como propietario de un dispositivo (solo Linux)**, active la opción **Permitir la ejecución de la utilidad de registro de usuario luego de la instalación del Agente de red** y haga clic en **Guardar**.

La utilidad para registrar al usuario como propietario del dispositivo se puede ejecutar a través de la línea de comandos en el dispositivo cliente.

Para registrar un usuario como propietario de un dispositivo Linux en el dispositivo cliente:

1. Execute the following command in the command line on the client device:
   `$ /opt/kaspersky/klnagent64/bin/nagregister -set_owner`

2. Ingrese el nombre de usuario y la contraseña, si se le solicitan estos datos.

   If the login and the password are included in the answer file or installation package of Network Agent, execute the following command in the command line on the client device:
   `$ /opt/kaspersky/klnagent64/bin/nagregister -set_owner -unattended`

Si el usuario forma parte de un grupo de seguridad interno, el nombre de usuario debe ser el mismo.

Si el usuario forma parte de un grupo de seguridad de Active Directory, el nombre de usuario debe constar del nombre de usuario y el nombre de dominio.

Debe ingresar la contraseña de un solo uso basado en el tiempo (TOTP) de la app para la autenticación de dos factores.

Se registrará al usuario como propietario del dispositivo.

Anular la designación de un usuario como propietario de un dispositivo

Para anular la designación de un usuario como propietario del dispositivo en un dispositivo cliente:

1. Ejecute el siguiente comando en la línea de comandos del dispositivo cliente:
   `$ /opt/kaspersky/klnagent64/bin/nagregister -remove_owner`

2. Ingrese el nombre de usuario y la contraseña.

Si el usuario forma parte de un grupo de seguridad interno, el nombre de usuario debe ser el mismo.

Si el usuario forma parte de un grupo de seguridad de Active Directory, el nombre de usuario debe constar del nombre de usuario y el nombre de dominio.

Debe ingresar la contraseña de un solo uso basado en el tiempo (TOTP) de la app para la autenticación de dos factores.

El usuario ya no estará designado como propietario del dispositivo.

Habilitación de la protección de una cuenta desde la modificación no autorizada

Puede habilitar una opción adicional para proteger la cuenta de un usuario contra modificaciones no autorizadas. Si esta opción está habilitada, la modificación de la configuración de la cuenta de usuario requiere la autorización del usuario con derechos de modificación.

Para habilitar o deshabilitar la protección de una cuenta desde la modificación no autorizada:

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos** y luego seleccione la pestaña **Usuarios**.
2. Haga clic en el nombre de la cuenta de usuario interna para la que desea especificar la protección de la cuenta frente a modificaciones no autorizadas.
3. En la ventana que se abre con la configuración del usuario, seleccione la pestaña **Autenticación de dos factores**.
4. En la pestaña **Autenticación de dos factores**, seleccione la opción **Solicitar autenticación para verificar el permiso para modificar cuentas de usuario** si desea solicitar credenciales y un código de seguridad de un solo uso para la autenticación de dos factores cada vez que se cambie o modifique la configuración de la cuenta. De lo contrario, seleccione la opción **Permitir que los usuarios modifiquen esta cuenta sin solicitar autenticación adicional**.
5. Guarde sus cambios.

Configuración de la autenticación de dos factores

A partir de la versión 16.1 del Servidor de administración, la autenticación de dos factores se habilita automáticamente. No se admite la opción global para deshabilitar la autenticación de dos factores. Este escenario proporciona los pasos para configurar la autenticación de dos factores en el primer inicio de sesión y configurar los ajustes de autenticación de dos factores en el Servidor de administración.

Etapas

La configuración de la autenticación de dos factores se realiza en etapas:

1. **Instalar una aplicación de autenticación en un dispositivo**

   Puede instalar cualquier aplicación que admita el algoritmo de contraseña de un solo uso basado en el tiempo (TOTP).

   Disponible en Rusia:

   - Kaspersky Password Manager para empresas (recomendado)
   - Bitrix24 OTP
   - Yandex ID
   - Avanpost Authenticator
   - Aladdin 2FA
   - Rutoken OTP

Disponible en todo el mundo (incluida Rusia):

- Google Authenticator
- Microsoft Authenticator

Para comprobar si Kaspersky Security Center Linux es compatible con la aplicación de autenticación que desea utilizar, habilite la autenticación de dos factores para todos los usuarios o para un usuario en particular.

En uno de los pasos, se sugiere indicar el código de seguridad generado por la aplicación de autenticación. Si tiene éxito, Kaspersky Security Center Linux es compatible con el autenticador seleccionado.

> No recomendamos en absoluto instalar la app de autenticación en el mismo dispositivo desde el que se administra el servidor de administración.

2. **Sincronizar la hora del dispositivo con la app de autenticación con la hora del dispositivo en el que está instalado el Servidor de administración**

   Asegúrese de que la hora del dispositivo en el que esté instalada la app de autenticación y la hora del dispositivo que contenga el Servidor de administración estén sincronizadas con UTC. Para una mayor precisión, recomendamos utilizar los mismos servidores NTP en toda su infraestructura. De lo contrario, pueden producirse errores al configurar la autenticación de dos factores.

3. **Configuración de la autenticación de dos factores para las cuentas de usuario al iniciar sesión en Web Console**

   Inicie sesión en Web Console y configure la autenticación de dos factores.

   Si la configuración de autenticación de dos factores no está disponible para usted, comuníquese con un usuario que tenga el derecho Modificar ACL de objetos en el área funcional **Características generales: Permisos de usuario** y la autenticación de dos factores configurada para agregar su cuenta la lista de permitidos para autenticación de dos factores.

4. **Configuración de la autenticación de dos factores en el Servidor de administración**

   Si configuró la autenticación de dos factores y el derecho Modificar ACL de objetos del área funcional **Características generales**: **Permisos de usuario**, puede configurar los ajustes de autenticación de dos factores en el Servidor de administración de la siguiente manera:

   1. Revisión de la lista de usuarios que pueden configurar la autenticación de dos factores al iniciar sesión:

      - Para instalar el Servidor de administración 16.1 desde cero: agregue los usuarios requeridos a la lista de permitidos para autenticación de dos factores para que puedan configurar la autenticación de dos factores en su primer inicio de sesión.
      - Para actualizar o restaurar al Servidor de administración 16.1: revise la lista de permitidos para autenticación de dos factores y elimine las cuentas que no deben tener acceso al Servidor de administración.

   2. Excluir las cuentas de usuario para las que no es necesario habilitar la autenticación de dos factores (opcional)

      Excluya las cuentas de usuario de la autenticación de dos factores para permitirles iniciar sesión en el Servidor de administración incluso si no configuraron la autenticación de dos factores. Es posible que sea necesario excluir cuentas de la autenticación de dos factores en el caso de cuentas de integración que no pueden proporcionar un código de seguridad durante la autenticación. Las cuentas de integración se utilizan para ejecutar scripts a través de OpenAPI.

3. Restablecimiento o eliminación de una clave secreta de autenticación de dos factores (opcional)

   Puede restablecer una clave secreta de autenticación de dos factores cuando un usuario pierde el acceso a su dispositivo de autenticación de dos factores o necesita configurar la autenticación de dos factores en un nuevo dispositivo. También puede restablecer una clave secreta para su propia cuenta.

   Puede eliminar una clave secreta para bloquear completamente el inicio de sesión de un usuario en Web Console y evitar que el usuario acceda al Servidor de administración.

4. Editar el nombre del emisor de un código de seguridad (opcional)

   Si tiene varios Servidores de administración con nombres similares, es posible que tenga que cambiar los nombres de los emisores de códigos de seguridad para que se reconozcan mejor los diferentes Servidores de administración.

Resultados

Una vez completado este procedimiento:

- La autenticación de dos factores está configurada para su propia cuenta y para otra cuenta de usuario que necesita acceso al Servidor de administración.
- Las cuentas de integración están excluidas de la autenticación de dos factores.

Acerca de la autenticación de dos factores para una cuenta

Kaspersky Security Center Linux ofrece un mecanismo de autenticación de dos factores para los usuarios de Kaspersky Security Center Web Console. La autenticación de dos factores se basa en el estándar RFC 6238 (TOTP: algoritmo de contraseña de un solo uso basado en el tiempo).

Cada vez que inicia sesión en Kaspersky Security Center Web Console, ingresa su nombre de usuario, contraseña y un código de seguridad de un solo uso adicional. Para recibir un código de seguridad de un solo uso, debe tener una app de autenticación en el equipo o dispositivo móvil.

> La app de autenticación puede ser cualquier software de autenticación que admita el algoritmo de contraseña de un solo uso basado en el tiempo (TOTP), por ejemplo, Google Authenticator. Para generar el código de seguridad de un solo uso, debe sincronizar la hora configurada en el dispositivo con la app de autenticación y con la hora configurada en el dispositivo del Servidor de administración. Para una mayor precisión, recomendamos utilizar los mismos servidores NTP en toda su infraestructura.

Para comprobar si Kaspersky Security Center Linux es compatible con la app de autenticación que desea utilizar, intente configurar la autenticación de dos factores con esta app de autenticación.

En uno de los pasos, se sugiere indicar el código de seguridad de un solo uso generado por la app de autenticación. Si tiene éxito, Kaspersky Security Center Linux es compatible con el autenticador seleccionado.

Generación de un código secreto mediante una app de autenticación

La aplicación de autenticación genera el código de seguridad de la siguiente manera:

1. El Servidor de administración genera una clave secreta especial y un código QR.
2. Usted le brinda la clave secreta o el código QR generados a la aplicación de autenticación.
3. La aplicación de autenticación genera un código de seguridad de un solo uso, que usted transfiere a la ventana de autenticación del Servidor de administración.

Un código de seguridad tiene un identificador denominado *nombre del emisor*. El nombre del emisor del código de seguridad se utiliza como identificador del Servidor de administración en la aplicación de autenticación. Puede cambiar el nombre del emisor del código de seguridad. El nombre del emisor del código de seguridad tiene un valor predeterminado que es el mismo que el nombre del Servidor de administración. Se asigna un nuevo nombre de emisor del código de seguridad al Servidor de administración después del siguiente inicio de sesión. Los códigos de seguridad son de un solo uso y válidos por hasta 30 segundos (el tiempo exacto puede variar).

Recomendamos que guarde la clave secreta (o el código QR) y los conserve en un lugar seguro. Con esto podrá restaurar el acceso a Kaspersky Security Center Web Console en caso de que pierda el acceso al dispositivo con la app de autenticación.

La autenticación de dos factores tiene las siguientes características:

- A partir de la versión 16.1 del Servidor de administración, la autenticación de dos factores se habilita automáticamente y la opción para configurar la autenticación de dos factores al iniciar sesión está deshabilitada de manera predeterminada. La configuración de la autenticación de dos factores al iniciar sesión solo está disponible para los usuarios que están incluidos en la lista de permitidos para autenticación de dos factores.
- Un usuario puede configurar la autenticación de dos factores solo para su cuenta.
- Un usuario puede excluir cuentas de la autenticación de dos factores. Puede ser necesario para las cuentas de integración que no pueden recibir un código de seguridad de un solo uso para la autenticación. Las cuentas de integración se utilizan para ejecutar scripts a través de OpenAPI.
- Para volver a generar una clave secreta de autenticación de dos factores, el usuario debe restablecer la clave secreta para su propia cuenta.
- Para restablecer o eliminar una clave secreta de autenticación de dos factores para la cuenta de otro usuario, el usuario debe tener una cuenta con autenticación de dos factores configurada y con el derecho Modificar ACL de objetos en el área funcional **Características generales**: **Permisos de usuario**.
- Para excluir cuentas de otros usuarios de la autenticación de dos factores o modificar la lista de permitidos para autenticación de dos factores, el usuario debe tener una cuenta con autenticación de dos factores configurada y con el derecho Modificar ACL de objetos en el área funcional **Características generales**: **Permisos de usuario**.
- Siempre debe haber al menos un usuario con la autenticación de dos factores configurada para que este usuario pueda administrar la lista de permitidos para autenticación de dos factores y la lista de exclusiones.
- La autenticación de dos factores se habilita automáticamente solo para la versión 16.1 del Servidor de administración. Si otros Servidores de administración primarios o secundarios ejecutan la versión 16 o anteriores, su configuración de autenticación de dos factores no se modificará.

- Un Servidor de administración virtual hereda la configuración de autenticación de dos factores del Servidor de administración físico, de modo que si la autenticación de dos factores está habilitada en el Servidor de administración físico, también se habilita en un Servidor de administración virtual. No puede configurar la autenticación de dos factores en un Servidor de administración virtual.
- Para que la autenticación de dos factores funcione correctamente, debe actualizar el Servidor de administración y la Web Console a la versión 16.1 o posteriores.

Para garantizar una protección integral mediante el uso de la autenticación de dos factores, es necesario proteger no solo el Servidor de administración, sino también el dispositivo en el que está instalado. Para hacer esto, tenga en cuenta las recomendaciones de la Guía para reforzar la seguridad.

Configuración de una clave secreta de autenticación de dos factores al iniciar sesión en la consola web de Kaspersky Security Center

La primera vez que inicie sesión en Kaspersky Security Center Linux 16.1 o posterior, se abre la ventana para configurar la autenticación de dos factores.

Para configurar la autenticación de dos factores para su cuenta, siga estos pasos:

1. Instale cualquier aplicación que admita el algoritmo de contraseña de un solo uso basado en el tiempo (TOTP) en el dispositivo móvil o la computadora.

   Disponible en Rusia:

   - Kaspersky Password Manager para empresas (recomendado)
   - Bitrix24 OTP
   - Yandex ID
   - Avanpost Authenticator
   - Aladdin 2FA
   - Rutoken OTP

   Disponible en todo el mundo (incluida Rusia):

   - Google Authenticator
   - Microsoft Authenticator

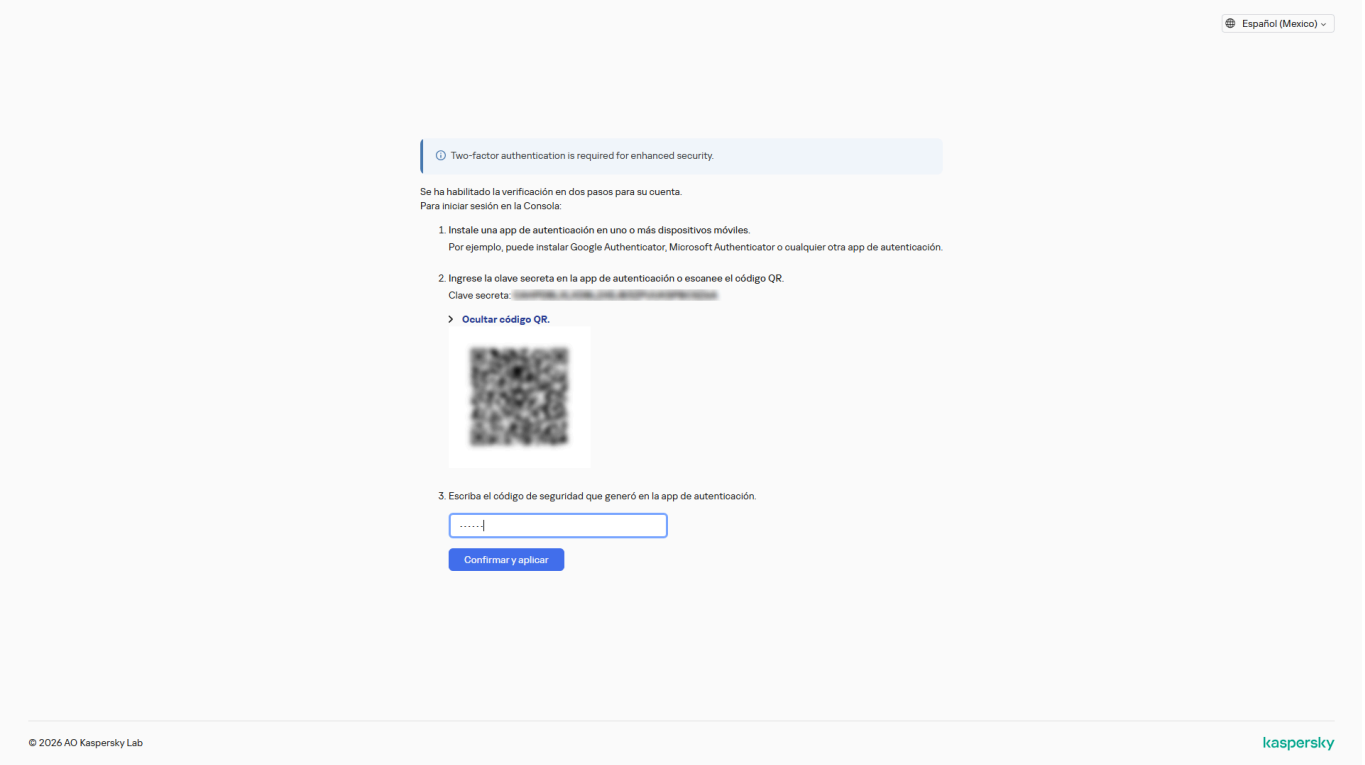
   No recomendamos en absoluto instalar la app de autenticación en el mismo dispositivo desde el que se administra el servidor de administración.

2. Asegúrese de que la hora del dispositivo en el que esté instalada la app de autenticación y la hora del dispositivo que contenga el Servidor de administración estén sincronizadas con UTC. Para una mayor precisión, recomendamos utilizar los mismos servidores NTP en toda su infraestructura.

3. Genere un código de seguridad de un solo uso mediante la app de autenticación en el dispositivo móvil o la computadora. Para hacerlo, siga uno de estos pasos:

   - Ingrese manualmente la clave secreta de autenticación de dos factores en la app de autenticación.
   - Haga clic en **Ver código QR** y escanee el código QR con la aplicación de autenticación.

   Se mostrará un código de seguridad de un solo uso de 6 dígitos en el dispositivo móvil.



Configuración de una clave secreta de autenticación de dos factores al iniciar sesión en la consola web de Kaspersky Security Center

4. En la ventana **Autenticación de dos factores**, especifique el código de seguridad de un solo uso generado por la app de autenticación y haga clic en el botón **Confirmar y aplicar**.

   Configuración de Rutoken OTP

   Si utiliza Rutoken OTP, necesita un dispositivo móvil Android con la aplicación Rutoken OTP instalada. El dispositivo móvil Android debe cumplir los siguientes requisitos:

   - Sistema operativo Android 7 o superior.
   - Módulo NFC disponible y activado.

   En la aplicación Rutoken OTP, debe configurar los siguientes parámetros:

   - Escanee el código QR que se muestra en el asistente de configuración en dos pasos.
   - Establezca el intervalo de tiempo en 30 segundos.
   - Seleccione SHA1 como algoritmo.

   Para configurar Rutoken OTP:

   1. Coloque el dispositivo Rutoken OTP junto al dispositivo móvil que tiene el módulo NFC.
   2. En la aplicación Rutoken OTP, presione **Conectar token**.

3. En la aplicación Rutoken OTP, presione **Configuración** y, a continuación, **Guardar clave secreta**.

   Si el token se conecta de forma correcta al dispositivo móvil, la aplicación Rutoken OTP muestra los siguientes mensajes de estado:

   - **El token está conectado.**
   - **La configuración está establecida.**
   - **Se guardó la clave secreta.**

4. En el dispositivo Rutoken OTP, presione el botón.

   En el dispositivo, verá un código de seguridad.

5. En Kaspersky Security Center Web Console, en la ventana de verificación en dos pasos, introduzca el código de seguridad.

La autenticación de dos factores se configura para su cuenta. Puede acceder al Servidor de administración de acuerdo con sus derechos.

Si la configuración de autenticación de dos factores no está disponible para usted, comuníquese con un usuario que tenga el derecho Modificar ACL de objetos en el área funcional **Características generales**: **Permisos de usuario** y la autenticación de dos factores configurada para agregar su cuenta a la lista de permitidos para autenticación de dos factores.

Permitir a los usuarios configurar la autenticación de dos factores

La lista de permitidos para autenticación de dos factores es una lista de usuarios que pueden configurar inicialmente la autenticación de dos factores al iniciar sesión en Web Console. Esta lista contiene cuentas de usuario sin autenticación de dos factores configurada. De manera predeterminada, las cuentas de usuario nuevas no se incluyen en la lista de permitidos para autenticación de dos factores y deben ser agregadas a la lista por un administrador. Si una cuenta nueva es una cuenta de integración utilizada para ejecutar scripts de OpenAPI, debe excluirse de la autenticación de dos factores.

Una cuenta de usuario se eliminará automáticamente de la lista de permitidos para autenticación de dos factores cuando haya configurado la autenticación de dos factores o se excluya de ella.

La modificación manual de la lista de permitidos para autenticación de dos factores está disponible para las cuentas que configuraron la autenticación de dos factores y que tienen el derecho Modificar ACL de objetos en el área funcional **Características generales**: **Permisos de usuario**.

Para agregar una cuenta de usuario a la lista de permitidos para autenticación de dos factores manualmente, siga esyos pasos:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Autenticación de dos factores** de la ventana de propiedades, en la tabla **Usuarios que tienen permitido generar claves secretas**, haga clic en el botón **Agregar**.

3. En la ventana que se abre:

   a. Seleccione la cuenta de usuario que desea agregar.

      Solo los usuarios que no están excluidos de la autenticación de dos factores y no tienen una clave secreta de autenticación de dos factores pueden agregarse a la lista de permitidos para autenticación de dos factore.

   b. Si la cuenta está protegida contra modificaciones no autorizadas, verifique si tiene los permisos necesarios para modificarla. En la ventana **Protección de cuentas**, especifique las credenciales de su propia cuenta y el código de seguridad de un solo uso para la autenticación de dos factores.

   c. Guarde sus cambios.

   La cuenta de usuario seleccionada se agrega a la lista de permitidos para autenticación de dos factores. En el próximo inicio de sesión, el usuario podrá generar una clave secreta.

Una cuenta de usuario se puede eliminar de la lista de permitidos para autenticación de dos factores hasta que se configure la autenticación de dos factores para esa cuenta.

Para eliminar manualmente las cuentas de usuario de la lista de permitidos para autenticación de dos factores, siga estos pasos:

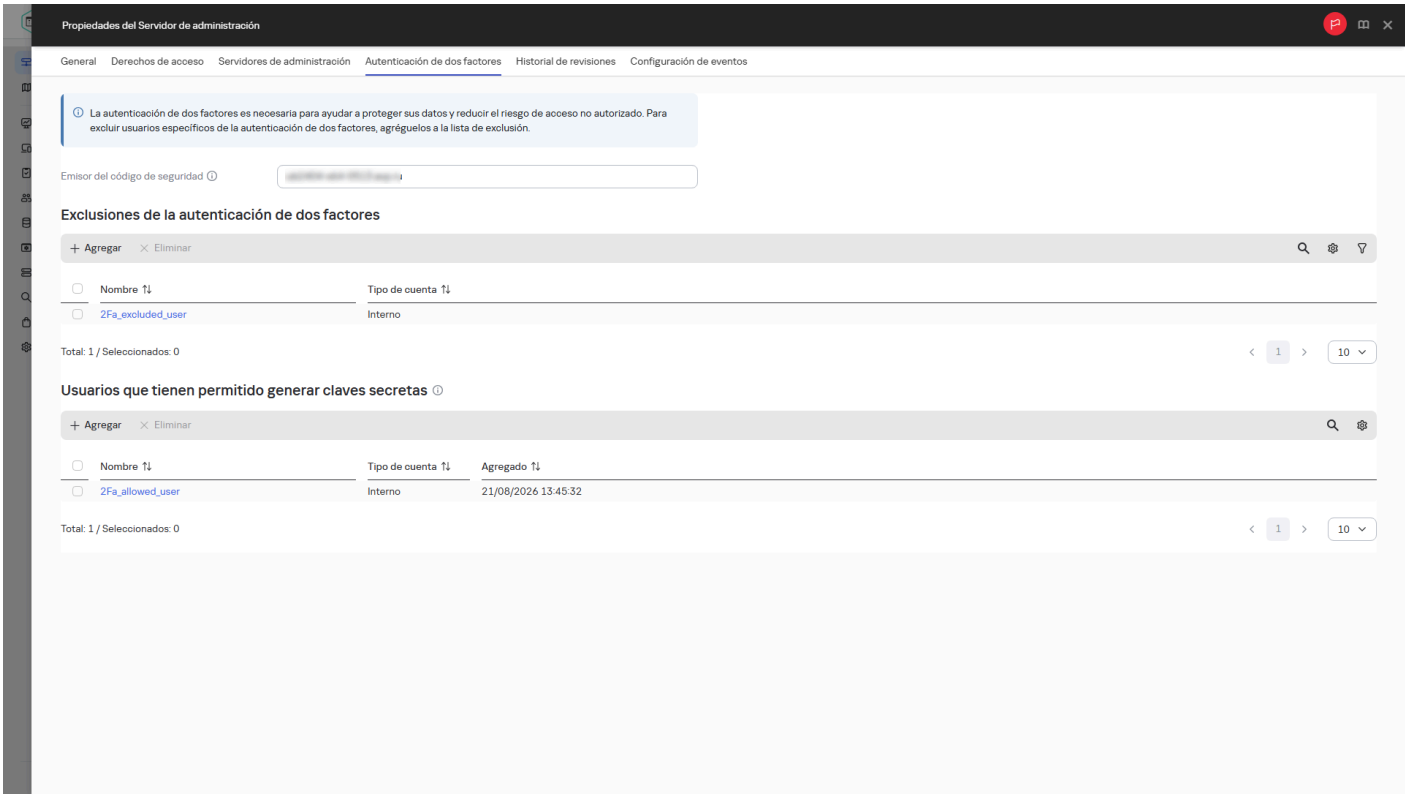
1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Autenticación de dos factores** de la ventana de propiedades, en la tabla **Usuarios que tienen permitido generar claves secretas**, seleccione las cuentas de usuario que desea eliminar y, a continuación, haga clic en **Eliminar**.

3. Si la cuenta está protegida contra modificaciones no autorizadas, verifique si tiene los permisos necesarios para modificarla. En la ventana **Protección de cuentas**, especifique las credenciales de su propia cuenta y el código de seguridad de un solo uso para la autenticación de dos factores.

Las cuentas de usuario seleccionadas se eliminan de la lista de permitidos para autenticación de dos factores.



Configuración de la lista de permitidos para autenticación de dos factores

Si, durante una sesión activa en el Servidor de administración, otro usuario elimina su clave secreta de autenticación de dos factores o si restablece la clave pero no crea una nueva, la capacidad de modificar la lista de permitidos para autenticación de dos factores se bloquea.

Las cuentas de usuario también se pueden agregar y eliminar automáticamente de la lista de permitidos para autenticación de dos factores.

Al restablecer una clave secreta de autenticación de dos factores para otras cuentas, sus cuentas se agregan automáticamente a la lista de permitidos de la autenticación de dos factores para que puedan generar una nueva clave secreta.

Al actualizar el Servidor de administración de la versión 16 o anterior a la versión 16.1 o posterior, así como cuando crea una copia de seguridad de datos en el Servidor de administración versión 16 o anterior y la restaura en el Servidor de administración versión 16.1 o posterior, las cuentas de usuario se agregarán automáticamente a la lista de permitidos de la autenticación de dos factores si se cumplen todas las condiciones siguientes:

- El usuario tiene el permiso de lectura en el área funcional *Características generales: Funcionalidad básica* asignada directamente al usuario (no a través de un grupo de seguridad). El alcance del rol de usuario con este permiso debe incluir todos los dispositivos administrados y dispositivos no asignados, y debe establecerse en el nivel del Servidor de administración.

- El usuario no está excluido de la autenticación de dos factores.

- El usuario no tiene una clave secreta de autenticación de dos factores.
- La autenticación de dos factores no estaba habilitada para todos los usuarios en el Servidor de administración de la versión anterior.

Si no se cumple alguna de las condiciones, el usuario no se agregará a la lista de permitidos de autenticación de dos factores.

Después de una actualización o restauración, recomendamos asegurarse de que la lista de permitidos para autenticación de dos factores contenga solo las cuentas de usuario que deben tener acceso al Servidor de administración. Revise la lista de permitidos para autenticación de dos factores y elimine cualquier otra cuenta de ella. Agregue las cuentas de integridad utilizadas para ejecutar scripts a través de OpenAPI a la lista de exclusión para evitar errores en los scripts.

Las cuentas de los usuarios perderán el acceso al Servidor de administración después de una actualización o restauración si se cumplen todas las condiciones siguientes:

- El usuario tiene el permiso de lectura en el área funcional *Características generales: Funcionalidad básica* asignada a través de una seguridad grupo (no directamente al usuario) o no tiene este permiso en absoluto.
- El usuario no está excluido de la autenticación de dos factores.
- El usuario no tiene una clave secreta de autenticación de dos factores.
- La autenticación de dos factores no estaba habilitada para todos los usuarios en el Servidor de administración de la versión anterior.

Estas cuentas se pueden agregar manualmente a la lista de permitidos para autenticación de dos factores si es necesario.

Restablecimiento y eliminación de una clave secreta de autenticación de dos factores

Puede restablecer una clave secreta cuando un usuario pierde el acceso a su dispositivo de autenticación de dos factores o necesita configurar la autenticación de dos factores en un nuevo dispositivo. Restablecer la clave secreta le permite al usuario iniciar sesión en Web Console nuevamente y generar una nueva clave secreta.

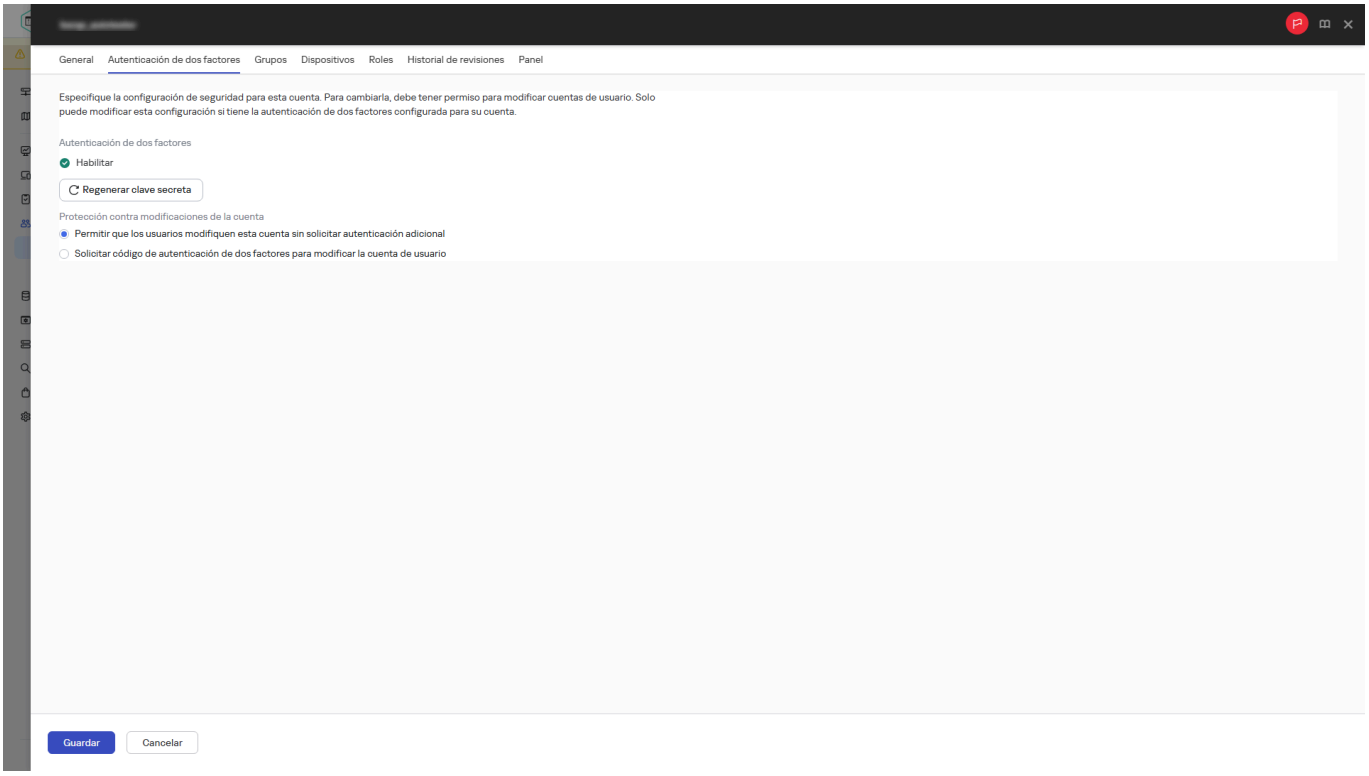
Puede restablecer o eliminar una clave secreta de autenticación de dos factores para las cuentas de otros usuarios solo si configuró la autenticación de dos factores y tiene el derecho Modificar ACL de objetos en el área funcional **Características generales**: **Permisos de usuario**. También puede regenerar su propia clave secreta.

Para restablecer una clave secreta para una cuenta, siga estos pasos:

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos** y luego seleccione la pestaña **Usuarios**.
2. Haga clic en el nombre de la cuenta de usuario para la cual desea restablecer una clave secreta.

3. Si desea restablecer una clave secreta para su cuenta, siga estos pasos:

a. En la pestaña **Autenticación de dos factores**, haga clic en el botón **Regenerar clave secreta**.

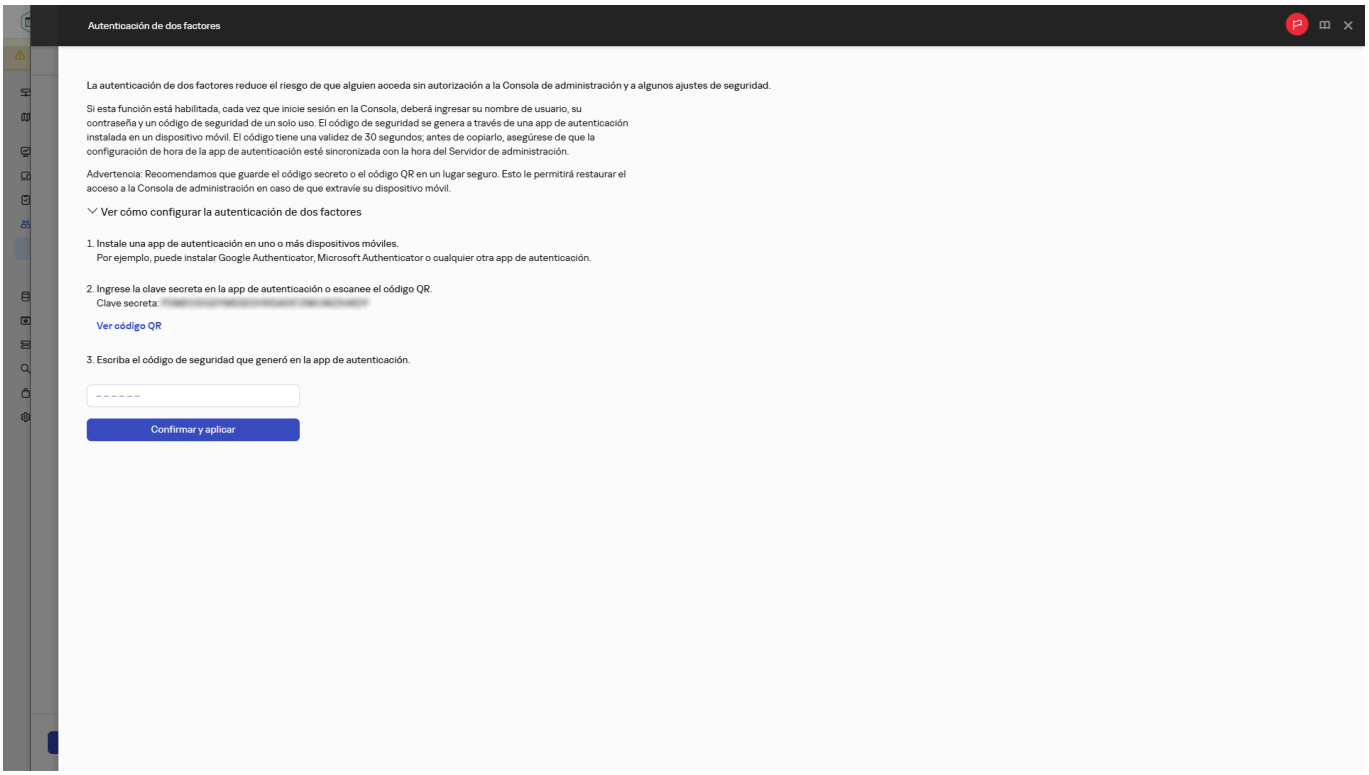


Regeneración de la clave secreta de autenticación de dos factores para la cuenta de usuario actual

a. Si su cuenta está protegida contra modificaciones no autorizadas, verifique si tiene los permisos necesarios para modificarla. En la ventana **Protección de cuentas**, especifique las credenciales de su propia cuenta y el código de autenticación de dos factores.

b. En la ventana **Autenticación de dos factores**, haga clic en **Ver cómo configurar la autenticación de dos factores** y, a continuación, haga clic en **Ver código QR**.

c. Utilice la app de autenticación en el dispositivo móvil para realizar un análisis del código QR y recibir un código de seguridad de un solo uso.



Configuración de una nueva clave secreta de autenticación de dos factores para la cuenta de usuario actual

a. En la ventana **Autenticación de dos factores**, especifique el código de seguridad de un solo uso generado por la app de autenticación, haga clic en el botón **Confirmar y aplicar** y, a continuación, guarde los cambios.

Configuración de Rutoken OTP

Si utiliza Rutoken OTP, necesita un dispositivo móvil Android con la aplicación Rutoken OTP instalada. El dispositivo móvil Android debe cumplir los siguientes requisitos:

- Sistema operativo Android 7 o superior.
- Módulo NFC disponible y activado.

En la aplicación Rutoken OTP, debe configurar los siguientes parámetros:

- Escanee el código QR que se muestra en el asistente de configuración en dos pasos.
- Establezca el intervalo de tiempo en 30 segundos.
- Seleccione SHA1 como algoritmo.

Para configurar Rutoken OTP:

1. Coloque el dispositivo Rutoken OTP junto al dispositivo móvil que tiene el módulo NFC.
2. En la aplicación Rutoken OTP, presione **Conectar token**.
3. En la aplicación Rutoken OTP, presione **Configuración** y, a continuación, **Guardar clave secreta**.

Si el token se conecta de forma correcta al dispositivo móvil, la aplicación Rutoken OTP muestra los siguientes mensajes de estado:

- **El token está conectado.**
- **La configuración está establecida.**
- **Se guardó la clave secreta.**

4. En el dispositivo Rutoken OTP, presione el botón.

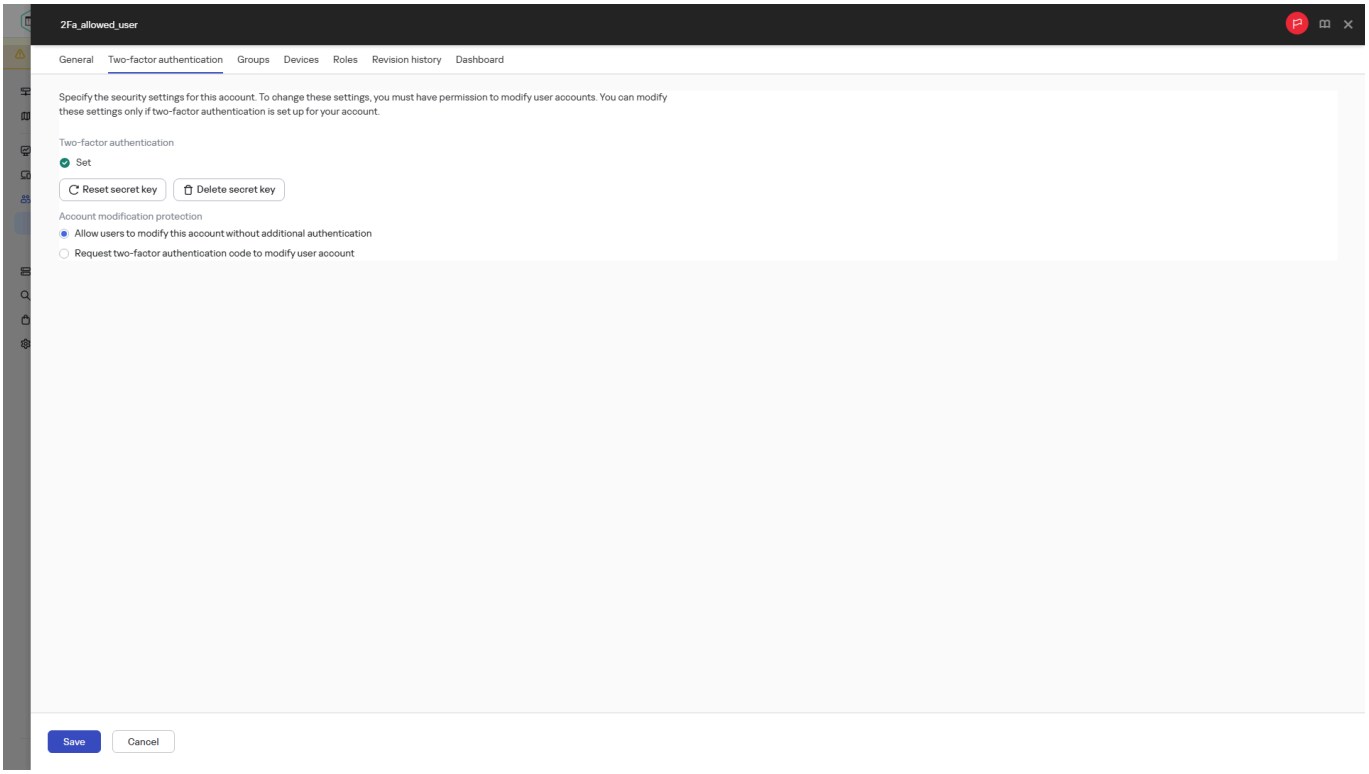
   En el dispositivo, verá un código de seguridad.

5. En Kaspersky Security Center Web Console, en la ventana de verificación en dos pasos, introduzca el código de seguridad.

Se cambia la clave secreta de su cuenta.

4. Si desea restablecer una clave secreta para otra cuenta, siga estos pasos:

   a. En la pestaña **Autenticación de dos factores**, haga clic en el botón **Restablecer clave secreta**.



Restablecimiento de la clave secreta de autenticación de dos factores para otra cuenta de usuario

   a. Si la cuenta está protegida contra modificaciones no autorizadas, verifique si tiene los permisos necesarios para modificarla. En la ventana **Protección de cuentas**, especifique las credenciales de su propia cuenta y el código de seguridad de un solo uso para la autenticación de dos factores.

   b. Confirme el restablecimiento de la clave secreta y, a continuación, guarde los cambios.

Cuando restablece una clave secreta para otra cuenta, la clave secreta existente se elimina y la cuenta de usuario se agrega a la lista de permitidos para autenticación de dos factores en las propiedades del Servidor de administración. En el próximo inicio de sesión, el usuario podrá generar una nueva clave secreta.

Se restablece la clave secreta de una cuenta de usuario.

Puede eliminar una clave secreta para bloquear completamente el inicio de sesión de un usuario en Web Console y evitar que el usuario acceda al Servidor de administración.

Para eliminar una clave secreta, siga estos pasos:

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos** y luego seleccione la pestaña **Usuarios**.
2. Haga clic en el nombre de la cuenta de usuario interna para la cual desea eliminar una clave secreta.

   No puedes eliminar una clave secreta de tu propia cuenta.

3. En la pestaña **Autenticación de dos factores**, haga clic en el botón **Eliminar clave secreta**.
4. Si la cuenta está protegida contra modificaciones no autorizadas, verifique si tiene los permisos necesarios para modificarla. En la ventana **Protección de cuentas**, especifique las credenciales de su propia cuenta y el código de seguridad de un solo uso para la autenticación de dos factores.
5. Confirme la eliminación de la clave secreta y, a continuación, guarde los cambios.

Se elimina la clave secreta de una cuenta de usuario.

Puede restaurar el acceso agregando al usuario a la lista de permitidos para autenticación de dos factores en las propiedades del Servidor de administración. En este caso, en el próximo inicio de sesión, el usuario podrá generar una nueva clave secreta.

Excluir cuentas de la autenticación de dos factores

Puede excluir las cuentas de usuario de la autenticación de dos factores para permitirles iniciar sesión en el Servidor de administración incluso si no configuraron la autenticación de dos factores. Es posible que sea necesario excluir cuentas de la autenticación de dos factores en el caso de cuentas de integración que no pueden proporcionar un código de seguridad de un solo uso durante la autenticación. Las cuentas de integración se utilizan para ejecutar scripts a través de OpenAPI.

Puede modificar la lista de exclusión si la autenticación de dos factores está configurada para su cuenta y tiene el derecho Modificar ACL de objetos en el área de funcional **Características generales**: **Permisos de usuario**.

Para excluir una cuenta de usuario de la autenticación de dos factores, siga estos pasos:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Autenticación de dos factores** de la ventana de propiedades, en la tabla **Exclusiones de la autenticación de dos factores**, haga clic en el botón **Agregar**.

3. En la ventana que se abre:

   a. Seleccione la cuenta de usuario que desea excluir.

   b. Si la cuenta está protegida contra modificaciones no autorizadas, verifique si tiene los permisos necesarios para modificarla. En la ventana **Protección de cuentas**, especifique las credenciales de su propia cuenta y el código de seguridad de un solo uso para la autenticación de dos factores.

   c. Guarde sus cambios.

   Las cuentas de usuario seleccionadas se excluyen de la autenticación de dos factores y sus claves secretas se eliminan si existen. La lista de cuentas excluidas no cambia cuando restaura una copia de seguridad en el Servidor de administración 16.1 o actualiza el Servidor de administración a la versión 16.1 o posterior. Si las cuentas de la lista de exclusión tenían secretos en la versión anterior del Servidor de administración, estas claves secretas se eliminarán en 16.1.

Puede eliminar cuentas de usuario de la lista de exclusión para evitar que los usuarios inicien sesión en Web Console y evitar que accedan al Servidor de administración.

Para eliminar cuentas de usuarios de la lista de exclusión, siga estos pasos:

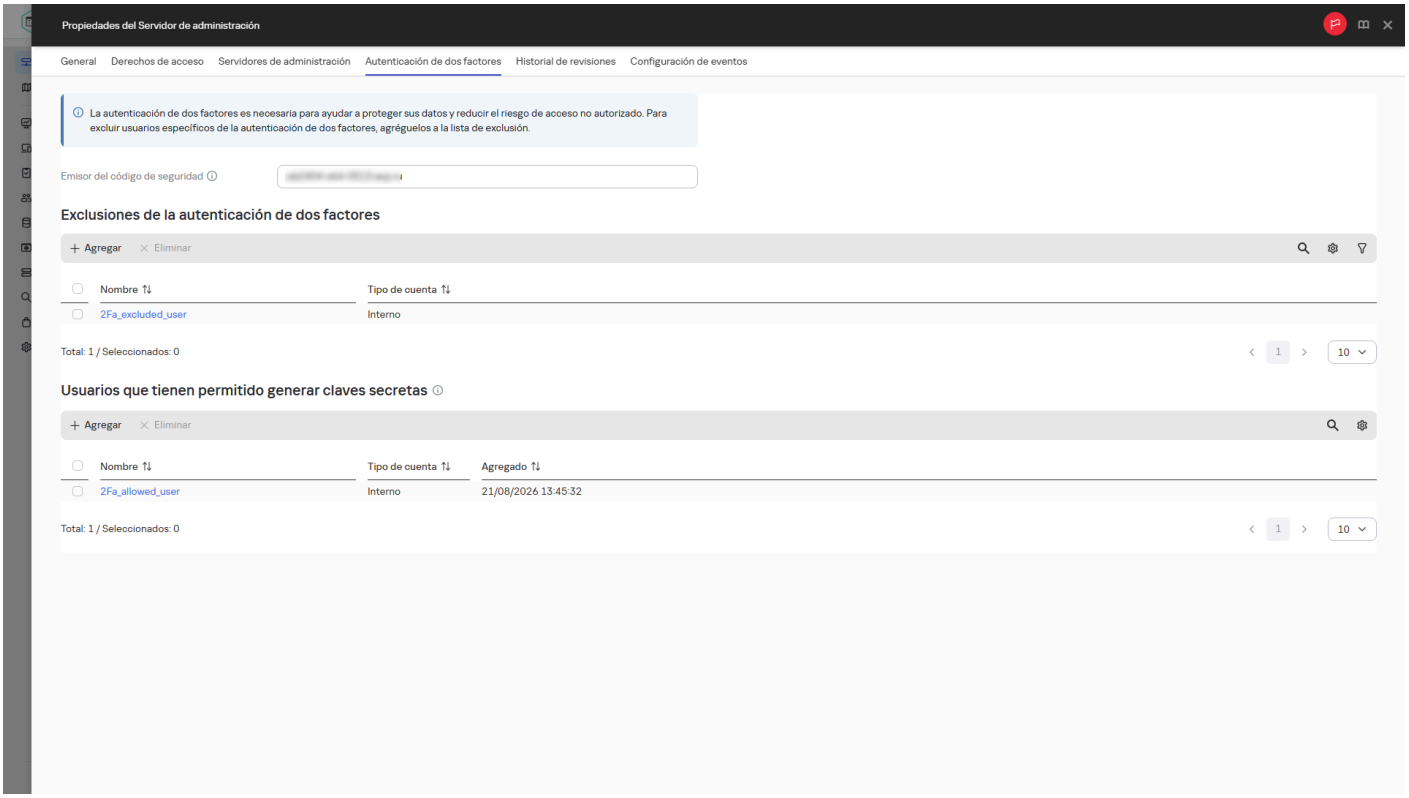
1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Autenticación de dos factores** de la ventana de propiedades, en la tabla **Exclusiones de la autenticación de dos factores**, seleccione las cuentas de usuario que desea eliminar y, a continuación, haga clic en **Eliminar**.

3. Si la cuenta está protegida contra modificaciones no autorizadas, verifique si tiene los permisos necesarios para modificarla. En la ventana **Protección de cuentas**, especifique las credenciales de su propia cuenta y el código de seguridad de un solo uso para la autenticación de dos factores.

Las cuentas de usuario seleccionadas se eliminan de la lista de exclusión.



Configurar la lista de exclusión de autenticación de dos factores

Editar el nombre del emisor de un código de seguridad

Puede tener varios identificadores (denominados emisores) para diferentes Servidores de administración. Puede cambiar el nombre del emisor de un código de seguridad en caso de que, por ejemplo, el Servidor de administración ya utilice un nombre similar de emisor del código de seguridad para otro Servidor de administración. De forma predeterminada, el nombre del emisor de un código de seguridad es el mismo que el nombre del Servidor de administración.

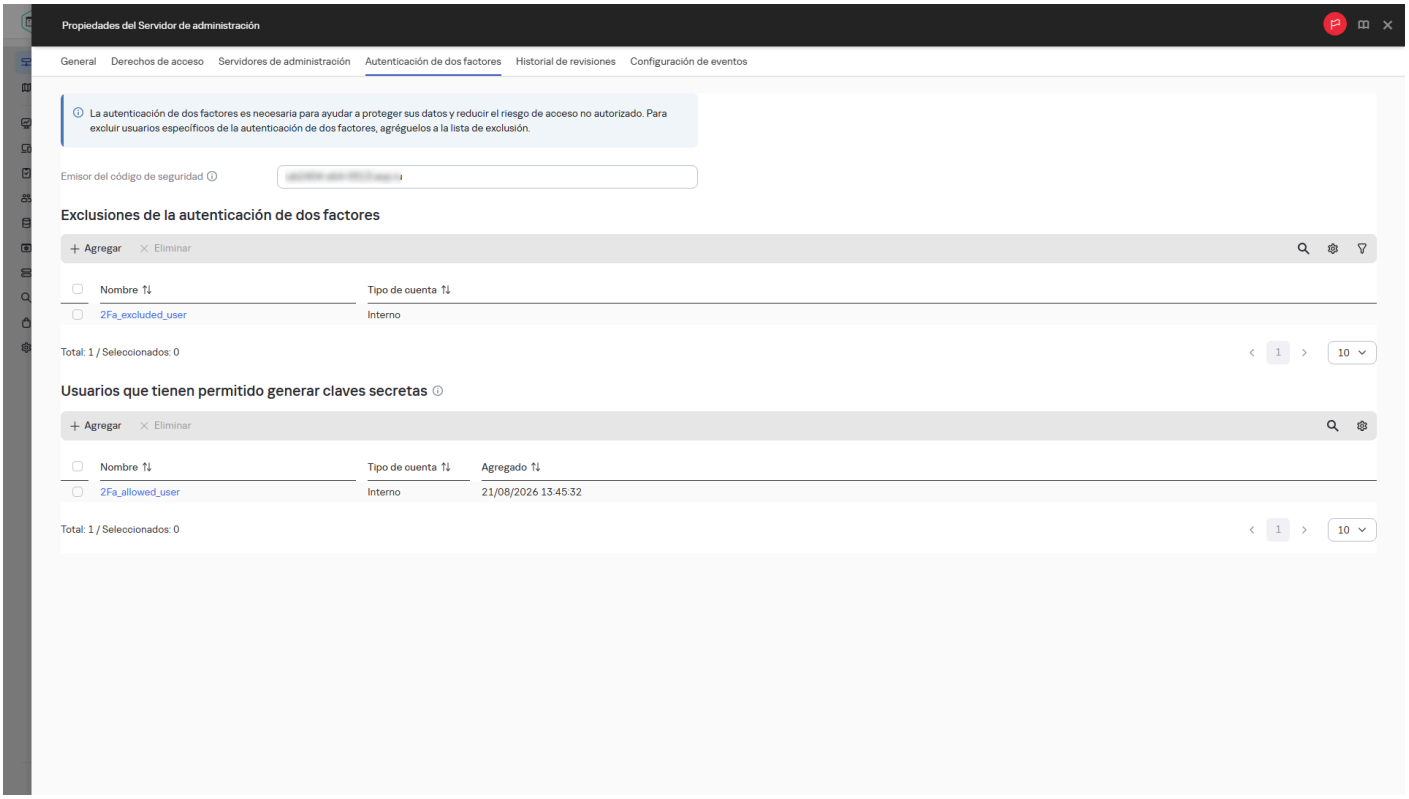
Para especificar un nuevo nombre de emisor de un código de seguridad, siga estos pasos:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Autenticación de dos factores** de la ventana de propiedades, ingrese un nuevo nombre en el campo **Emisor del código de seguridad** y luego guarde los cambios.

Se asigna un nuevo nombre de emisor del código de seguridad al Servidor de administración después del siguiente inicio de sesión.



Especificar el nombre del emisor de un código de seguridad

Cambiar el número de intentos de entrada de contraseña permitidos

El usuario de Kaspersky Security Center Linux puede introducir una contraseña no válida un número limitado de veces. Una vez que se alcanza el límite, la cuenta de usuario se bloquea durante una hora.

De manera predeterminada, el número máximo de intentos permitidos es 10. Puede cambiar el número de intentos de entrada de contraseña permitidos, como se describe en esta sección.

Para cambiar el número de intentos de entrada de contraseña permitidos

1. En el dispositivo del Servidor de administración, ejecute una línea de comando de Linux.

2. En el símbolo del sistema, ejecute el siguiente comando:

   ```
   sudo /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n SrvSplPpcLogonAttempts -t d -v N
   ```

donde N es un número de intentos para ingresar una contraseña.

3. Para aplicar los cambios, reinicie el servicio del Servidor de administración.

Se cambia el número máximo de intentos de entrada de contraseña permitidos.

Eliminar un usuario o un grupo de seguridad

Solo puede eliminar usuarios internos o grupos de seguridad internos.

Para eliminar un usuario o un grupo de seguridad:

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos**, y luego seleccione la pestaña **Usuarios** o **Grupos**.

2. Seleccione la casilla de verificación junto al usuario o el grupo de seguridad que desea eliminar.

   Siempre debe haber al menos un usuario con la autenticación de dos factores configurada para que este usuario pueda administrar la lista de permitidos para autenticación de dos factores y la lista de exclusiones.

3. Haga clic en el botón **Eliminar**.

4. En la ventana que se abre, haga clic en **Aceptar**.

Se elimina el usuario o el grupo de seguridad.

Cambiar la contraseña de una cuenta de usuario

Es posible que deba cambiar la contraseña de su propia cuenta o de la cuenta de otro usuario si la contraseña actual está a punto de caducar o si desea cambiarla por una más segura.

La contraseña debe cumplir con las siguientes reglas:

- La contraseña debe tener entre 8 y 256 caracteres.
- La contraseña debe incluir caracteres de al menos tres de los grupos enumerados a continuación:
  - Letras mayúsculas (A–Z)
  - Letras minúsculas (a-z)

- Números (0–9)
- Caracteres especiales (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

- La contraseña no debe contener espacios en blanco, caracteres Unicode ni la combinación de "." y "@" cuando "." precede a "@".

Cambiar la contraseña de su cuenta

Pasos para cambiar la contraseña de su propia cuenta:

1. En el panel superior, haga clic en el nombre de la cuenta para ir al menú de la cuenta.
2. En la lista desplegable, seleccione **Cambiar contraseña**.
3. En el panel derecho que se abre, escriba la contraseña actual y luego ingrese una nueva contraseña para la conexión con Kaspersky Security Center Linux.

   Para ver la contraseña ingresada, haga clic en .
4. Si su cuenta está protegida contra modificaciones no autorizadas, verifique si tiene los permisos necesarios para modificarla. En la ventana **Protección de cuentas**, ingrese las credenciales de su cuenta o de una cuenta que tenga el derecho Modificar ACL de objeto en el área funcional **Características generales**: **Permisos de usuario**.
5. Ingrese el código de seguridad de un solo uso generado por la app de autenticación en el dispositivo móvil.

Cambiar la contraseña de una cuenta de usuario interno

Pasos para cambiar la contraseña de una cuenta de usuario interna:

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos** y luego seleccione la pestaña **Usuarios**.
2. Haga clic en el nombre de la cuenta de usuario que desee editar.
3. En la ventana de ajustes del usuario que se abre, en la pestaña **General**, haga clic en el botón **Cambiar contraseña**.
4. Establezca la nueva contraseña con la que el usuario se conectará a Kaspersky Security Center Linux.

   Para ver la contraseña ingresada, haga clic en .
5. Si es necesario, active la opción **El usuario debe cambiar la contraseña la primera vez que inicie sesión** para forzar el cambio de contraseña la siguiente vez que el usuario se autentique.
6. Si la cuenta de usuario está protegida contra modificaciones no autorizadas, verifique si tiene los permisos necesarios para modificarla. En la ventana **Protección de cuentas**, ingrese las credenciales de una cuenta que tenga el derecho Modificar ACL de objeto en el área funcional **Características generales**: **Permisos de usuario**.
7. Ingrese el código de seguridad de un solo uso generado por la app de autenticación en el dispositivo móvil.

Configurar las opciones para cambiar la contraseña mediante indicadores del servidor

Abra la línea de comandos y pase al directorio que contenga la utilidad klscflag. La utilidad klscflag se encuentra en el directorio donde está instalado el Agente de red. El directorio de instalación predeterminado es `/opt/kaspersky/ksc64/sbin`. Ejecute el siguiente comando:

- Configuración del período de rotación de contraseñas (indicador `LP_SplPwdChangePeriodDays`)

  `./klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangePeriodDays -t d -v <rotation_period>`

  Dónde <`período_de_rotación`> es un período de tiempo en días después del cual expira la contraseña del usuario. Valores posibles: 0-730. Si el valor del parámetro es 0, la rotación de contraseñas queda deshabilitada.

- Configuración del tiempo de la advertencia preliminar sobre la necesidad de cambiar la contraseña (el indicador `LP_SplPwdChangeNotificationHours`)

  `./klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangeNotificationHours -t d -v <warning_time>`

  Dónde <`tiempo_de_advertencia`> es un período de tiempo en horas antes de que expire la contraseña del usuario. Durante este número de horas, se mostrará una notificación para indicar que se necesita un cambio de clave. Valores posibles: 0-17520. Si el valor del parámetro es 0, el tiempo de advertencia será un 25 por ciento del período de rotación de contraseñas.

- Configuración del valor predeterminado de la opción **El usuario debe cambiar la contraseña la primera vez que inicie sesión** (indicador `LP_SplPwdForceChange`)

  `./klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdForceChange -t d -v <valor>`

  Donde los posibles valores del indicador <`valor`>:

  `1`: la opción **El usuario debe cambiar la contraseña la primera vez que inicie sesión** está habilitada.

  `0`: la opción **El usuario debe cambiar la contraseña la primera vez que inicie sesión** está deshabilitada.

Para ver el valor vigente de un indicador, ejecute el siguiente comando:

`./klscflag -fget -pv .core/.independent -s KLLIM -n <indicador> -t d`

La variable <`indicador`> debe ser `LP_SplPwdChangePeriodDays`, `LP_SplPwdChangeNotificationHours` o `LP_SplPwdForceChange`.

Creación de roles de usuario

Para crear un rol de usuario:

1. En el menú principal, vaya a **Usuarios y roles** → **Roles**.
2. Haga clic en **Agregar**.
3. En la ventana **Nombre del nuevo rol** que se abre, introduzca el nombre del nuevo rol.
4. Haga clic en **Aceptar** para aplicar los cambios.

5. Cuando se abra la ventana de propiedades del rol, cambie la configuración del rol:

   - En la pestaña **General**, modifique el nombre del rol.

     No es posible modificar el nombre de los roles predefinidos.

   - En la pestaña **Configuración**, modifique el alcance del rol, así como las directivas y los perfiles asociados al rol.

   - En la pestaña **Derechos de acceso**, modifique los derechos de acceso a las aplicaciones de Kaspersky.

6. Haga clic en **Guardar** para guardar los cambios.

El nuevo rol aparece en la lista de roles de usuario.

Editar un rol de usuario

Para editar un rol de usuario:

1. En el menú principal, vaya a **Usuarios y roles** → **Roles**.

2. Haga clic en el nombre del rol que desee editar.

3. Cuando se abra la ventana de propiedades del rol, cambie la configuración del rol:

   - En la pestaña **General**, modifique el nombre del rol.

     No es posible modificar el nombre de los roles predefinidos.

   - En la pestaña **Configuración**, modifique el alcance del rol, así como las directivas y los perfiles asociados al rol.

   - En la pestaña **Derechos de acceso**, modifique los derechos de acceso a las aplicaciones de Kaspersky.

4. Haga clic en **Guardar** para guardar los cambios.

El rol actualizado aparece en la lista de roles de usuario.

Editar el alcance de un rol de usuario

El *alcance de un rol de usuario* es una combinación de usuarios y grupos de administración. Los ajustes asociados a un rol de usuario se aplican únicamente a los dispositivos que pertenecen a los usuarios que tienen ese rol, y solo cuando esos dispositivos pertenecen a grupos y subgrupos asociados al rol en cuestión.

Para agregar usuarios, grupos de seguridad y grupos de administración al alcance de un rol de usuario, puede utilizar cualquiera de los siguientes métodos:

Método 1:

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos**, y luego seleccione la pestaña **Usuarios** o **Grupos**.

2. Active las casillas de verificación ubicadas junto a los usuarios y grupos de seguridad que desee agregar al alcance del rol de usuario.

3. Haga clic en el botón **Asignar rol**.

   Se inicia el asistente de asignación de roles. Avance por el asistente utilizando el botón **Siguiente**.

4. En el paso **Seleccionar rol**, seleccione el rol de usuario que desee asignar.

5. En el paso **Definir alcance**, seleccione el grupo de administración que desee agregar al alcance del rol de usuario.

6. Haga clic en el botón **Asignar rol** para cerrar la ventana.

Los usuarios o grupos de seguridad y el grupo de administración seleccionados se agregan al alcance del rol de usuario.

Método 2:

1. En el menú principal, vaya a **Usuarios y roles** → **Roles**.

2. Haga clic en el nombre del rol cuyo alcance desee definir.

3. Cuando se abra la ventana de propiedades del rol, seleccione la pestaña **Configuración**.

4. En la sección **Alcance del rol**, haga clic en **Agregar**.

   Se inicia el asistente de asignación de roles. Avance por el asistente utilizando el botón **Siguiente**.

5. En el paso **Definir alcance**, seleccione el grupo de administración que desee agregar al alcance del rol de usuario.

6. En el paso **Seleccionar usuarios**, seleccione los usuarios y los grupos de seguridad que desee agregar al alcance del rol de usuario.

7. Haga clic en el botón **Asignar rol** para cerrar la ventana.

8. Haga clic en el botón **Cerrar** (⨯) para cerrar la ventana de propiedades del rol.

Los usuarios o grupos de seguridad y el grupo de administración seleccionados se agregan al alcance del rol de usuario.

Método 3:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Derechos de acceso**, seleccione la casilla de verificación junto al nombre del usuario o del grupo de seguridad que desee agregar al alcance de un rol de usuario y, luego, haga clic en el botón **Roles**.

   No puede seleccionar varios usuarios o grupos de seguridad al mismo tiempo. Si selecciona más de un elemento, el botón **Roles** se deshabilitará.

3. En la ventana **Roles**, seleccione el rol de usuario que desee asignar, aplíquelo y guarde los cambios.

   Los usuarios o grupos de seguridad seleccionados se agregan al alcance del rol de usuario.

Eliminar un rol de usuario

Para eliminar un rol de usuario:

1. En el menú principal, vaya a **Usuarios y roles** → **Roles**.
2. Marque la casilla ubicada junto al nombre del rol que desee eliminar.
3. Haga clic en el botón **Eliminar**.
4. En la ventana que se abre, haga clic en **Aceptar**.

Se elimina el rol de usuario.

Asociación de perfiles de directivas con roles

Los roles de usuario pueden asociarse a perfiles de directivas. Al crear una asociación entre un perfil de directiva y un rol, la regla de activación del perfil pasa a depender del rol y, en consecuencia, el perfil de directiva se activa para los usuarios que tienen el rol especificado.

A modo de ejemplo, suponga que los dispositivos de un grupo de administración, llamado Usuarios, están sujetos a una directiva que prohíbe el uso de aplicaciones de navegación GPS. Existe un solo dispositivo en el grupo que necesita contar con un navegador GPS: el dispositivo que le pertenece al mensajero. En esta situación, puede asignar un rol llamado "Mensajero" al propietario de este dispositivo y crear un perfil de directiva que permita utilizar aplicaciones de navegación GPS solo en aquellos dispositivos que pertenezcan a usuarios con el rol "Mensajero". Los demás ajustes de la directiva se mantendrán sin cambios. Solo el usuario que tenga el rol "Mensajero" podrá ejecutar el software de navegación GPS. Si posteriormente se le asigna el rol "Mensajero" a otro empleado más, esa persona también podrá ejecutar aplicaciones de navegación en el dispositivo que le provea la organización. El software de navegación GPS seguirá estando prohibido en los demás dispositivos del grupo de administración.

Para asociar un rol con un perfil de directiva:

1. En el menú principal, vaya a **Usuarios y roles** → **Roles**.
2. Haga clic en el nombre del rol que desee asociar con un perfil de directiva.

   Se abre la ventana de propiedades del rol, con la pestaña **General** seleccionada.

3. Seleccione la pestaña **Configuración** y desplácese hacia abajo hasta llegar a la sección **Directivas**.
4. Haga clic en **Editar**.

5. Asocie el rol con un perfil de directiva nuevo o existente:

   - Para asociar el rol con **un perfil de directiva existente**, haga clic en el corchete angular (>) ubicado junto al nombre de la directiva pertinente, busque el nombre del perfil con el que quiera asociar el rol y active la casilla adyacente a ese perfil.

   - Para asociar el rol con **un nuevo perfil de directiva**:

     a. Marque la casilla adyacente a la directiva para la que se vaya a crear el perfil.

     b. Haga clic en **Nuevo perfil de directiva**.

     c. Escriba el nombre del nuevo perfil y configure sus opciones.

     d. Haga clic en el botón **Guardar**.

     e. Marque la casilla adyacente al nuevo perfil.

6. Haga clic en **Asignar a rol**.

El perfil quedará asociado al rol y aparecerá en las propiedades del rol. El perfil se aplicará automáticamente al dispositivo de toda persona que tenga asignado el rol.

Propagación de roles de usuario a Servidores de administración secundarios

De forma predeterminada, las listas de funciones del usuario de los Servidores de administración principal y secundario son independientes. Puede configurar la aplicación para propagar automáticamente las funciones de usuario creadas en el Servidor de administración principal a todos los Servidores de administración secundarios. Las funciones de usuario también pueden propagarse desde un Servidor de administración secundario a sus propios Servidores de administración secundarios.

Para propagar funciones de usuario desde el Servidor de administración principal a los Servidores de administración secundarios:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abrirá la ventana de propiedades del Servidor de administración, con la pestaña **General** seleccionada.

2. Vaya a la sección **Jerarquía de Servidores de administración**.

3. Habilite la opción **Propagar la lista de roles a los Servidores de administración secundarios** y, luego, haga clic en el botón **Guardar**.

La aplicación copia las funciones de usuario del Servidor de administración principal a los Servidores de administración secundarios.

Cuando la opción **Propagar la lista de roles a los Servidores de administración secundarios** está habilitada, y las funciones de usuario se propagan, no se pueden editar ni eliminar en los Servidores de administración secundarios. Cuando crea una nueva función o edita una existente en el Servidor de administración principal, los cambios se copian automáticamente en los Servidores de administración secundarios. Cuando elimina una función de usuario en el Servidor de administración principal, esta función permanece en los Servidores de administración secundarios posteriormente, pero se puede editar o eliminar.

Las funciones que se propagan al Servidor de administración secundario desde el Servidor principal se muestran con la marca de verificación verde (✓). No puede modificar estas funciones en el Servidor de administración secundario.

Si crea una función en el Servidor de administración principal y hay una función con el mismo nombre en su Servidor de administración secundarios, el nuevo rol se copia al Servidor de administración secundario con el índice agregado a su nombre, por ejemplo, ~~ 1, ~~ 2 (el índice puede ser aleatorio).

Si deshabilita la opción **Propagar la lista de roles a los Servidores de administración secundarios**, todas las funciones de usuario permanecen en los Servidores de administración secundarios, pero se vuelven independientes de las del Servidor de administración principal. Después de volverse independientes, las funciones de usuario de los Servidores de administración secundarios se pueden editar o eliminar.

Cambiar la contraseña de una cuenta

Puede cambiar la contraseña de una cuenta local si, por ejemplo, el usuario olvida la contraseña de su cuenta local o si debe realizarse un cambio de contraseña programado.

El cambio de contraseña se aplicará incluso si el usuario no ha iniciado sesión con su cuenta. También puede cambiarse la contraseña de la cuenta root local.

Esta tarea solo se puede realizar en dispositivos Linux.

Para cambiar la contraseña de la cuenta local en dispositivos específicos:

1. En el menú principal, vaya a **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea.
3. En el campo **Tipo de tarea**, seleccione **Cambiar contraseña de la cuenta (solo Linux)**.
4. Seleccione una de las siguientes opciones:

   Asignar tarea a un grupo de administración

   La tarea se asignará a los dispositivos incluidos en un grupo de administración. Puede seleccionar un grupo existente o crear uno nuevo.

   Puede usar esta opción para, por ejemplo, ejecutar una tarea que envíe un mensaje a ciertos usuarios si el contenido atañe solamente a los dispositivos de un grupo de administración puntual.

   Si la tarea se asigna a un grupo de administración, la pestaña **Seguridad** no se mostrará en la ventana de propiedades de la tarea; esto se debe a que las tareas de grupo están sujetas a la configuración de seguridad de los grupos a los que se aplican.

   Especificar las direcciones de los dispositivos manualmente o importarlas de una lista

   Puede especificar los nombres DNS, las direcciones IP y las subredes IP de los dispositivos a los cuales desee asignar la tarea.

   Podría elegir esta opción si necesita que la tarea se ejecute en una subred específica. Esto puede ser útil si, por ejemplo, necesita instalar una aplicación solo en los dispositivos que utilizan los contadores o si quiere analizar los dispositivos de una subred puntual que probablemente esté infectada.

   Asignar tarea a una selección de dispositivos

La tarea se asignará a los dispositivos incluidos en una selección de dispositivos. Puede elegir una selección existente.

Esta opción puede ser útil para, por ejemplo, ejecutar una tarea en los dispositivos que tengan una versión específica de un sistema operativo.

La tarea *Cambiar contraseña de la cuenta (solo Linux)* se creará para los dispositivos especificados. Si seleccionó la opción **Asignar tarea a un grupo de administración**, la tarea será una tarea de grupo.

5. En el paso **Alcance de la tarea**, indique un grupo de administración, dispositivos con direcciones específicas o una selección de dispositivos.

   Los ajustes disponibles dependerán de la opción seleccionada en el paso anterior.

6. En el paso **Ingresar nombre de la cuenta y contraseña nueva**, defina los siguientes ajustes:

   - En el campo **Nombre de cuenta**, ingrese el nombre de la cuenta cuya contraseña desee cambiar.
   - En el campo **Nueva contraseña**, ingrese la contraseña que se establecerá para la cuenta indicada en el campo anterior.

     Para ver los caracteres que ha escrito, haga clic en el botón **Mostrar** y manténgalo presionado.
   - Si es necesario, marque la casilla **Establecer como contraseña de un solo uso (el usuario debe cambiar la contraseña después del primer inicio de sesión)**.

     Establecer como contraseña de un solo uso (el usuario debe cambiar la contraseña después del primer inicio de sesión)

     Si se marca esta casilla, se le pedirá al usuario que establezca una nueva contraseña después del primer inicio de sesión.

     Si no se marca esta casilla, no se le pedirá al usuario que establezca una nueva contraseña después del primer inicio de sesión.

     Esta casilla está desactivada por defecto.

7. En el paso **Finalizar la creación de la tarea**, haga clic en el botón **Finalizar** para crear la tarea y cerrar el asistente.

   Si habilitó la opción **Abrir los detalles de la tarea cuando se complete la creación**, se abrirá la ventana de configuración de la tarea. Utilice esta ventana para, de ser necesario, revisar y modificar los ajustes de la tarea o programar su ejecución.

8. En la lista de tareas, seleccione la tarea creada y haga clic en **Iniciar**.

   Como alternativa, puede esperar a que ocurra el inicio programado definido en los ajustes de la tarea.

Cuando finaliza la tarea de cambio de contraseña, se cambia la contraseña de la cuenta local indicada en los dispositivos especificados.

Para garantizar el correcto funcionamiento de las tareas de cambio de contraseña, debe deshabilitarse SELinux en el dispositivo del usuario.

Revocar los derechos de administrador local

Puede revocar los derechos de administrador local de las cuentas. Ello brinda una capa de control adicional sobre las cuentas de usuario. Los derechos de administrador local pueden revocarse, por ejemplo, una vez que finaliza un encargo puntual.

Cuando se ejecuta esta tarea, se verifica si la cuenta local indicada pertenece a grupos de administradores locales. Estos grupos se definen en la configuración de la directiva del Agente de red. Puede personalizar la lista de grupos de administradores locales en la configuración de la directiva del Agente de red. También puede ver la lista de cuentas de usuarios con privilegios especiales en el **Informe sobre usuarios privilegiados en el dispositivo (solo Linux)**.

Esta tarea solo se puede realizar en dispositivos Linux.

Para revocar los derechos de administrador local en dispositivos específicos:

1. En el menú principal, vaya a **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea.
3. En el campo **Tipo de tarea**, seleccione **Revocar derechos de administrador local (solo Linux)**.
4. Seleccione una de las siguientes opciones:

   Asignar tarea a un grupo de administración

   La tarea se asignará a los dispositivos incluidos en un grupo de administración. Puede seleccionar un grupo existente o crear uno nuevo.

   Puede usar esta opción para, por ejemplo, ejecutar una tarea que envíe un mensaje a ciertos usuarios si el contenido atañe solamente a los dispositivos de un grupo de administración puntual.

   Si la tarea se asigna a un grupo de administración, la pestaña **Seguridad** no se mostrará en la ventana de propiedades de la tarea; esto se debe a que las tareas de grupo están sujetas a la configuración de seguridad de los grupos a los que se aplican.

   Especificar las direcciones de los dispositivos manualmente o importarlas de una lista

   Puede especificar los nombres DNS, las direcciones IP y las subredes IP de los dispositivos a los cuales desee asignar la tarea.

   Podría elegir esta opción si necesita que la tarea se ejecute en una subred específica. Esto puede ser útil si, por ejemplo, necesita instalar una aplicación solo en los dispositivos que utilizan los contadores o si quiere analizar los dispositivos de una subred puntual que probablemente esté infectada.

   Asignar tarea a una selección de dispositivos

   La tarea se asignará a los dispositivos incluidos en una selección de dispositivos. Puede elegir una selección existente.

   Esta opción puede ser útil para, por ejemplo, ejecutar una tarea en los dispositivos que tengan una versión específica de un sistema operativo.

   La tarea *Revocar derechos de administrador local (solo Linux)* se creará para los dispositivos indicados. Si seleccionó la opción **Asignar tarea a un grupo de administración**, la tarea será una tarea de grupo.
5. En el paso **Alcance de la tarea**, indique un grupo de administración, dispositivos con direcciones específicas o una selección de dispositivos.

   Los ajustes disponibles dependerán de la opción seleccionada en el paso anterior.
6. En este paso del asistente, defina los siguientes ajustes:

   - En el grupo **Modo operativo**, seleccione un modo de funcionamiento:

     Revocar derechos de administrador local de las cuentas enumeradas

Si selecciona esta opción, se revocarán los derechos de administrador local de las cuentas locales indicadas.

Esta opción está seleccionada de forma predeterminada.

Excluir cuentas enumeradas de la revocación de derechos de administrador local

Si selecciona esta opción, se revocarán los derechos de administrador local de todas las cuentas locales, excepto las enumeradas.

Esta opción no está seleccionada de manera predeterminada.

- Indique las cuentas locales:
  - Haga clic en **Agregar**.
  - En la ventana que se abre, realice una de las siguientes acciones:
    - En el campo **Nombre de cuenta**, ingrese el nombre de la cuenta local.
    - En el grupo de opciones **Acción de la cuenta** (disponible solo si se ha seleccionado la opción **Revocar derechos de administrador local de las cuentas enumeradas**, seleccione la acción.
    - **Conservar cuenta**

      Si selecciona esta opción, la cuenta local no se eliminará después de que se revoquen los derechos de administrador local.

      Esta opción está seleccionada de forma predeterminada.

    - **Eliminar cuenta**

      Si selecciona esta opción, la cuenta local se eliminará independientemente de si tiene derechos de administrador local.

      Esta opción no está seleccionada de manera predeterminada.

7. En el paso **Finalizar la creación de la tarea**, haga clic en el botón **Finalizar** para crear la tarea y cerrar el asistente.

   Si habilitó la opción **Abrir los detalles de la tarea cuando se complete la creación**, se abrirá la ventana de configuración de la tarea. Utilice esta ventana para, de ser necesario, revisar y modificar los ajustes de la tarea o programar su ejecución.

8. En la lista de tareas, seleccione la tarea creada y haga clic en **Iniciar**.

   Como alternativa, puede esperar a que ocurra el inicio programado definido en los ajustes de la tarea.

Cuando se complete la tarea de revocación de derechos de administrador local, se revocarán los derechos de administrador local de las cuentas locales indicadas en los dispositivos seleccionados.

Configuración de la autenticación de dominio Kerberos

Kaspersky Security Center Linux le permite utilizar la autenticación de dominio mediante el protocolo Kerberos. La autenticación de dominio le permite habilitar la autenticación segura en Kaspersky Security Center Web Console sin tener que volver a ingresar la contraseña en la red corporativa (inicio de sesión único).

Primero debe configurar el controlador de dominio para usar Kerberos y generar un archivo keytab. Para obtener más información, consulte la documentación del controlador de dominio.

SCRIL (se requiere una tarjeta inteligente para el inicio de sesión interactivo) es compatible con Microsoft Active Directory.

Generar un archivo keytab para FreeIPA y AldPro

Para generar un archivo keytab:

1. Cree una cuenta de usuario para que IAM pueda acceder al controlador de dominio.
2. Si el Servidor de administración está fuera del dominio FreeIPA/AldPro, agregue la entrada del registro DNS y la entrada del host:

   ```
   ipa dnsrecord-add <zoneName> <recordName> --a-rec <Dirección del Servidor de administración>
   ipa host-add --password=<password> <Dirección del host del Servidor de administración>
   ```

3. Especifique el tipo de PAC al crear el servicio HTTP para el Servidor de administración:

   ```
   ipa service-add HTTP/<FQDN del host del Servidor de administración>@<DOMINIO ESCRITO EN MAYÚSCULAS> --ok-to-auth-as-delegate=true --pac-type PAD
   ```

4. Especifique la cuenta de usuario para la autenticación:

   ```
   ipa service-allow-retrieve-keytab HTTP/<Dirección del host del Servidor de administración>@<DOMINIO ESCRITO EN MAYÚSCULAS> --user=<user>
   ```

5. Exporte el archivo keytab:

   ```
   ipa-getkeytab -s <Dirección del controlador de dominio> -p HTTP/<Dirección host del Servidor de administración>@<DOMINIO ESCRITO EN MAYÚSCULAS> -k /tmp/h.keytab
   ```

Generar un archivo keytab para Microsoft Active Directory

Para generar un archivo keytab:

1. Cree una cuenta de usuario para que IAM pueda comunicarse con el controlador de dominio.
2. Habilite las siguientes opciones para la cuenta de usuario:

   - **El usuario no puede cambiar la contraseña**
   - **Cifrado Kerberos AES de 256 bits**

   Puede habilitar la opción **La contraseña nunca caduca** para evitar volver a emitir el archivo keytab cada vez que caduca la contraseña.

3. Agregue un nombre principal de servicio (SPN) a la cuenta de usuario:

   ```
   setspn -S HTTP/<FQDN del host del Servidor de administración> <DOMINIO ESCRITO EN MAYÚSCULAS>\<user>
   ```

4. Exporte el archivo keytab:

   ```
   ktpass -out C:\<folder>\< nombre del archivo keytab > -princ HTTP/< FQDN del host del Servidor de administración >@< DOMINIO ESCRITO EN MAYÚSCULAS > -mapuser < DOMINIO ESCRITO EN MAYÚSCULAS >\<user> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass <password> -mapop set
   ```

Generar un archivo keytab para Samba

Para generar un archivo keytab:

1. Cree una cuenta de usuario para que IAM pueda comunicarse con el controlador de dominio:

   ```
   samba-tool user add <user>
   ```

2. Agregue el SPN a la cuenta de usuario:

   ```
   samba-tool spn add HTTP/< FQDN del host del Servidor de administración > <user>
   ```

3. Exporte el archivo keytab:

   ```
   samba-tool domain exportkeytab /tmp/file.keytab --principal=HTTP/< FQDN del host del Servidor de administración >
   ```

Habilitar la autenticación de dominio Kerberos

Para habilitar la autenticación de dominio Kerberos:

1. Realice un sondeo del controlador de dominio.
2. En el menú principal, vaya a la sección **Configuración** → **Inicio de sesión único**.
3. Habilite la opción **Autenticación de Kerberos**.
4. Cargue el archivo keytab.
5. Asigne el rol a los usuarios del dominio que les dé acceso a Kaspersky Security Center Web Console.

   La autenticación de dominio Kerberos está habilitada para usuarios de dominio.

Actualización de las bases de datos y las aplicaciones de Kaspersky

En esta sección, se describen los pasos que debe completar para actualizar lo siguiente en forma regular:

- Las bases de datos y los módulos de software de Kaspersky
- Las aplicaciones de Kaspersky que se encuentren instaladas, incluidas las aplicaciones de seguridad y los componentes de Kaspersky Security Center Linux

Es posible que la funcionalidad de las actualizaciones (incluida la provisión de actualizaciones de firmas antivirus y actualizaciones de base de código) y la funcionalidad de KSN no estén disponibles en el software en los EE. UU.

Procedimiento: actualización regular de bases de datos y aplicaciones de Kaspersky

En esta sección, se detalla un escenario para actualizar regularmente las bases de datos, los módulos de software y las aplicaciones de Kaspersky. Una vez que complete el escenario para configurar la protección de la red, deberá mantener la fiabilidad del sistema de protección. Esto garantizará que los servidores de administración y los dispositivos administrados siempre estén protegidos contra virus, ataques de red, ataques de phishing y otras amenazas.

Para que la protección de la red mantenga su eficacia, debe actualizar periódicamente lo siguiente:

- Las bases de datos y los módulos de software de Kaspersky
- Las aplicaciones de Kaspersky que se encuentren instaladas, incluidas las aplicaciones de seguridad y los componentes de Kaspersky Security Center Linux

Al concluir este escenario, tendrá las siguientes certezas:

- Su red estará protegida por el software de Kaspersky más reciente, incluidas las últimas versiones de las aplicaciones de seguridad y de los componentes de Kaspersky Security Center Linux.
- Las bases de datos antivirus y otras bases de datos de Kaspersky críticas para la seguridad de la red estarán siempre actualizadas.

Requisitos previos

Los dispositivos administrados deben tener conexión con el Servidor de administración. Si no tienen conexión, considere actualizar las bases de datos y los módulos de software de Kaspersky de forma manual o directamente desde los servidores de actualización de Kaspersky.

El Servidor de administración debe tener conexión a Internet.

Antes de comenzar, compruebe que hizo lo siguiente:

1. Desplegó las aplicaciones de seguridad de Kaspersky en los dispositivos administrados siguiendo las instrucciones del escenario para desplegar aplicaciones de Kaspersky a través de Kaspersky Security Center Web Console.

2. Creó y configuró todas las directivas, perfiles de directivas y tareas que se requieren según el escenario para configurar la protección de red.

3. Asignó una cantidad apropiada de puntos de distribución de acuerdo con la cantidad de dispositivos administrados y la topología de la red.

El proceso para actualizar las bases de datos y las aplicaciones de Kaspersky se divide en etapas:

1. **Elegir un esquema de actualización**

   Puede usar varios esquemas para instalar actualizaciones en aplicaciones de seguridad. Elija el esquema o varios esquemas que cumplan con los requisitos de su red.

2. **Crear la tarea para descargar actualizaciones en el repositorio del Servidor de administración**

   Esta tarea se crea automáticamente con el asistente de inicio rápido de Kaspersky Security Center. Si no ejecutó el asistente, cree la tarea ahora.

   La tarea se necesita para descargar actualizaciones de los servidores de actualizaciones de Kaspersky y guardarlas en el repositorio del Servidor de administración. También se la requiere para actualizar las bases de datos y los módulos de software de Kaspersky correspondientes a Kaspersky Security Center Linux. Una vez descargadas, las actualizaciones se pueden propagar a los dispositivos administrados.

   Si su red tiene puntos de distribución asignados, las actualizaciones se descargan automáticamente desde el repositorio del Servidor de administración a los repositorios de los puntos de distribución. En este caso, los dispositivos administrados incluidos en el alcance de un punto de distribución descargan las actualizaciones desde el repositorio del punto de distribución en lugar del repositorio del Servidor de administración.

   Instrucciones: Creación de la tarea para descargar actualizaciones en el repositorio del Servidor de administración

3. **Creación de la tarea para descargar actualizaciones a los repositorios de los puntos de distribución (opcional)**

   De forma predeterminada, las actualizaciones se descargan a los puntos de distribución desde el Servidor de administración. Si lo prefiere, puede hacer que Kaspersky Security Center Linux descargue las actualizaciones en los puntos de distribución directamente de los servidores de actualizaciones de Kaspersky. Descargar las actualizaciones en los repositorios de los puntos de distribución es preferible cuando el Servidor de administración no tiene acceso a Internet o cuando transmitir datos entre el Servidor de administración y los puntos de distribución es más costoso que transmitir datos entre los puntos de distribución y los servidores de actualizaciones de Kaspersky.

   Si hay puntos de distribución asignados en su red y se creó la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución*, los puntos de distribución descargarán las actualizaciones de los servidores de actualizaciones de Kaspersky y no del repositorio del Servidor de administración.

   Instrucciones: Crear la tarea para descargar actualizaciones en los repositorios de los puntos de distribución

4. **Configurar los puntos de distribución**

   Si su red tiene puntos de distribución asignados, asegúrese de que la opción **Habilitado** esté habilitada en las propiedades de todos los puntos de distribución pertinentes. Si deja esta opción está deshabilitada en un punto de distribución, los dispositivos incluidos en el alcance del mismo obtendrán sus actualizaciones del repositorio del Servidor de administración.

5. **Habilitar el uso de archivos diff para optimizar el proceso de actualización (opcional)**

   Puede optimizar el tráfico entre el Servidor de administración y los dispositivos administrados utilizando archivos diferenciales. Cuando esta función está habilitada, el Servidor de administración o un punto de distribución descarga archivos diferenciales en lugar de archivos completos de bases de datos o módulos de software de Kaspersky. Un archivo diff describe las diferencias entre dos versiones de un archivo de una base de datos o de un módulo de software. Por lo tanto, un archivo diff ocupa menos espacio que un archivo completo. Esto reduce el tráfico entre el Servidor de administración o los puntos de distribución y los dispositivos administrados. Para usar esta función, habilite la opción **Descargar archivos diff** en las propiedades de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* o *Descargar actualizaciones en los repositorios de los puntos de distribución*.

   Instrucciones: Utilización de archivos diff para actualizar las bases de datos y los módulos de software de Kaspersky

6. **Configurar la instalación automática de actualizaciones para las aplicaciones de seguridad**

   Cree las tareas de *Actualización* para las aplicaciones administradas para que los módulos de software y las bases de datos de Kaspersky (incluidas las bases de datos antivirus) se mantengan siempre al día. Para garantizar actualizaciones a tiempo, recomendamos que, cuando defina la programación de estas tareas, elija la opción **Al descargar nuevas actualizaciones al repositorio**.

   Si una actualización exige revisar y aceptar los términos del Contrato de licencia de usuario final, es necesario aceptar esos términos para proceder con la instalación. Una vez que se aceptan los términos, la actualización se puede propagar a los dispositivos administrados.

7. **Aprobar y rechazar actualizaciones de aplicaciones de Kaspersky administradas**

   De forma predeterminada, las actualizaciones de software descargadas tienen el estado *Sin definir*. Puede cambiar este estado a *Aprobada* o *Rechazada*. Las actualizaciones aprobadas siempre se instalan. Si la actualización de una aplicación de Kaspersky administrada exige revisar y aceptar los términos del Contrato de licencia de usuario final, es necesario aceptar esos términos para proceder con la instalación. Una vez que se aceptan los términos, la actualización se puede propagar a los dispositivos administrados. Las actualizaciones a las que se les asigna el estado *Rechazada* no se instalan en los dispositivos. Si previamente se instaló una actualización rechazada para una aplicación administrada, Kaspersky Security Center Linux intentará desinstalar la actualización de todos los dispositivos.

   Aprobar y rechazar actualizaciones solo está disponible para el Agente de red y las aplicaciones Kaspersky administradas instaladas en dispositivos cliente basados en Windows y en Linux. No se admite la actualización sin interrupciones del Servidor de administración, Kaspersky Security Center Web Console y los complementos web de administración.

   Instrucciones: aprobar y rechazar actualizaciones de software

   A veces, después de la actualización del Agente de red, es posible que se le solicite que reinicie los dispositivos administrados. Si aparece la notificación de que se requiere un reinicio, haga clic en el vínculo **Ver dispositivos** en la notificación, seleccione las casillas de verificación junto a los dispositivos que se reiniciarán y luego haga clic en el botón **Reiniciar** para finalizar la actualización del Agente de red.

Resultados

Al completar este escenario, Kaspersky Security Center Linux estará configurado para actualizar las bases de datos de Kaspersky una vez que las actualizaciones se descarguen en el repositorio del Servidor de administración. La siguiente tarea será, entonces, supervisar el estado de la red.

Acerca de la actualización de las bases de datos, los módulos de software y las aplicaciones de Kaspersky

Para asegurarse de que la protección de sus servidores de administración y sus dispositivos administrados siempre esté al día, debe proporcionar actualizaciones para los siguientes elementos oportunamente:

- Las bases de datos y los módulos de software de Kaspersky

  Antes de descargar las bases de datos y los módulos de software de Kaspersky, Kaspersky Security Center Linux verifica que se pueda acceder a los servidores de Kaspersky. Si los servidores DNS configurados en el sistema no permiten acceder a los servidores de Kaspersky, la aplicación utiliza servidores DNS públicos. Esto se hace para garantizar que las bases de datos antivirus se mantengan actualizadas y para que los dispositivos administrados no vean afectado su nivel de seguridad.

- Las aplicaciones de Kaspersky que se encuentren instaladas, incluidas las aplicaciones de seguridad y los componentes de Kaspersky Security Center Linux

  Kaspersky Security Center Linux le permite actualizar el Agente de red y las aplicaciones de Kaspersky instaladas en dispositivos cliente basados en Windows y en Linux automáticamente. No se admite la actualización sin interrupciones del Servidor de administración, Kaspersky Security Center Web Console y los complementos web de administración. Para actualizar estos componentes, debe descargar las últimas versiones desde el sitio web de Kaspersky y realizar la instalación manualmente.

Existen distintos esquemas para descargar las actualizaciones necesarias y distribuirlas a los dispositivos administrados. La elección de una u otra opción depende de la configuración de la red. Estas son las posibilidades:

- Utilizar una sola tarea: *Descargar actualizaciones en el repositorio del Servidor de administración*
- Utilizar dos tareas:
  - la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*
  - La tarea *Descargar actualizaciones en los repositorios de los puntos de distribución*
- Manualmente a través de una carpeta compartida o un servidor FTP
- Realizar una descarga directa desde los servidores de actualizaciones de Kaspersky a Kaspersky Endpoint Security en los dispositivos administrados
- Utilizar una carpeta local o de red si el Servidor de administración no tiene conexión a Internet

Utilizando la tarea Descargar actualizaciones en el repositorio del Servidor de administración

En este esquema, Kaspersky Security Center Linux descarga las actualizaciones a través de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*. En redes pequeñas que contienen menos de trescientos dispositivos administrados en un solo segmento de red o menos de diez dispositivos administrados en cada segmento de red, las actualizaciones se distribuyen a los dispositivos administrados directamente desde el repositorio del Servidor de administración (vea la siguiente imagen).



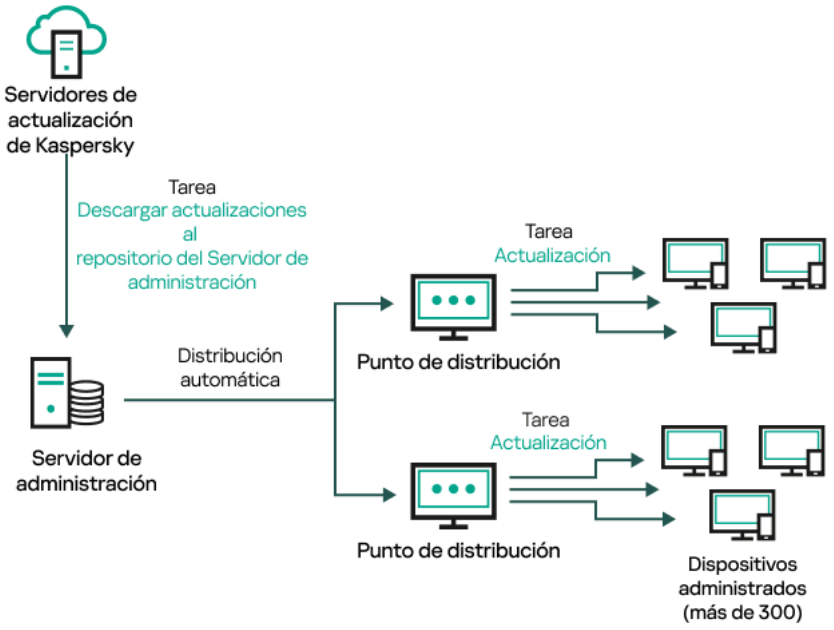
Actualización con la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* sin utilizar puntos de distribución

Como una fuente de actualizaciones, puede usar no solo los servidores de actualización de Kaspersky, sino también una carpeta local o de red.

De forma predeterminada, el Servidor de administración utiliza el protocolo HTTPS para comunicarse con los servidores de actualizaciones de Kaspersky y descargar las actualizaciones. Si lo desea, puede hacer que el Servidor de administración utilice el protocolo HTTP en lugar del protocolo HTTPS.

Si su red contiene más de 300 dispositivos administrados en un solo segmento de red o si su red consta de varios segmentos de red con más de 9 dispositivos administrados por segmento, le recomendamos que utilice puntos de distribución para propagar las actualizaciones a los dispositivos administrados (vea la siguiente imagen). Los puntos de distribución reducen la carga del Servidor de administración y optimizan el flujo de tráfico entre el Servidor de administración y los dispositivos administrados. Puede determinar cuántos puntos de distribución necesitará para su red y cuál deberá ser su configuración.

En este esquema, las actualizaciones se descargan automáticamente del repositorio del Servidor de administración a los repositorios de los puntos de distribución. Los dispositivos administrados incluidos en el alcance de un punto de distribución descargan las actualizaciones del repositorio de ese punto de distribución en lugar del repositorio del Servidor de administración.



Actualización con la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* y utilizando puntos de distribución

Cuando se ejecuta la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*, se descargan las actualizaciones para las bases de datos de Kaspersky y para los módulos de software de Kaspersky Endpoint Security en el repositorio del Servidor de administración. Estas actualizaciones se instalan a través de la tarea *Actualizar* de Kaspersky Endpoint Security.

La tarea *Descargar actualizaciones en el repositorio del Servidor de administración* no está disponible en servidores de administración virtuales. El repositorio del Servidor de administración virtual muestra las actualizaciones descargadas al Servidor de administración principal.

Si lo desea, puede verificar el buen funcionamiento de las actualizaciones en un conjunto de dispositivos de prueba. De no encontrarse errores durante la verificación, las actualizaciones se distribuirán a otros dispositivos administrados.

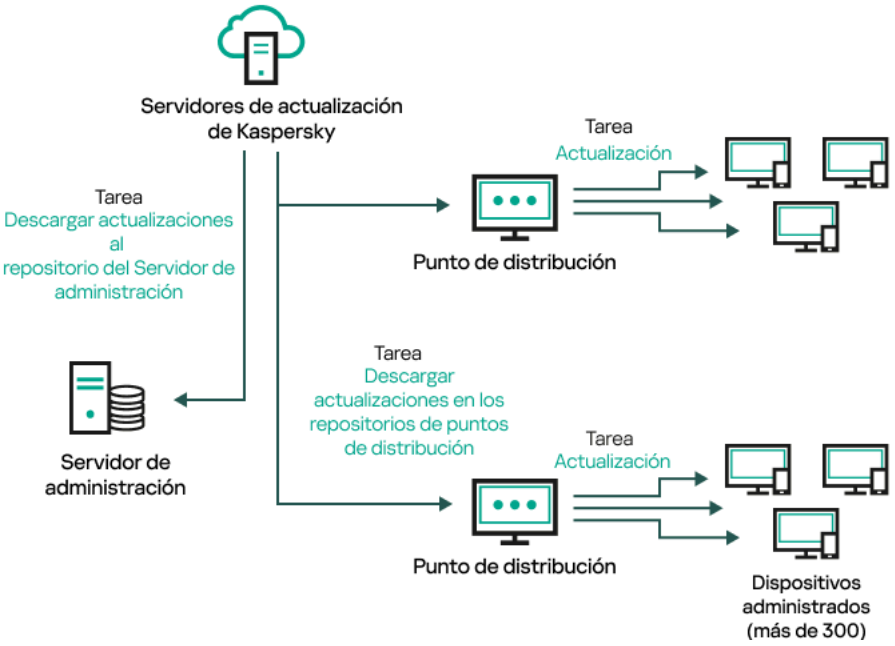
Cada aplicación de Kaspersky le solicita al Servidor de administración las actualizaciones que requiere. El Servidor de administración combina las solicitudes y descarga solo aquellas actualizaciones que han sido solicitadas por alguna aplicación. De este modo, se evita descargar la misma actualización más de una vez o descargar actualizaciones innecesarias. Para descargar las versiones correctas de las bases de datos y los módulos de software de Kaspersky, cuando se ejecuta la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*, el Servidor de administración envía la siguiente información a los servidores de actualizaciones de Kaspersky automáticamente:

- Id. y versión de la aplicación
- Id. de instalación de aplicaciones
- Id. de la clave activa
- Id. de ejecución de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*

La información transmitida no contiene datos personales ni confidenciales de ningún tipo. AO Kaspersky Lab protege la información conforme a las exigencias de la ley.

Utilizar dos tareas: la tarea Descargar actualizaciones en el repositorio del Servidor de administración y la tarea Descargar actualizaciones en los repositorios de los puntos de distribución

Las actualizaciones pueden descargarse a los repositorios de los puntos de distribución directamente desde los servidores de actualizaciones de Kaspersky (y no desde el repositorio del Servidor de administración) y, una vez descargadas, pueden distribuirse a los dispositivos administrados (vea la siguiente imagen). Descargar las actualizaciones en los repositorios de los puntos de distribución es preferible cuando el Servidor de administración no tiene acceso a Internet o cuando transmitir datos entre el Servidor de administración y los puntos de distribución es más costoso que transmitir datos entre los puntos de distribución y los servidores de actualizaciones de Kaspersky.



Actualización utilizando la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* y la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución*

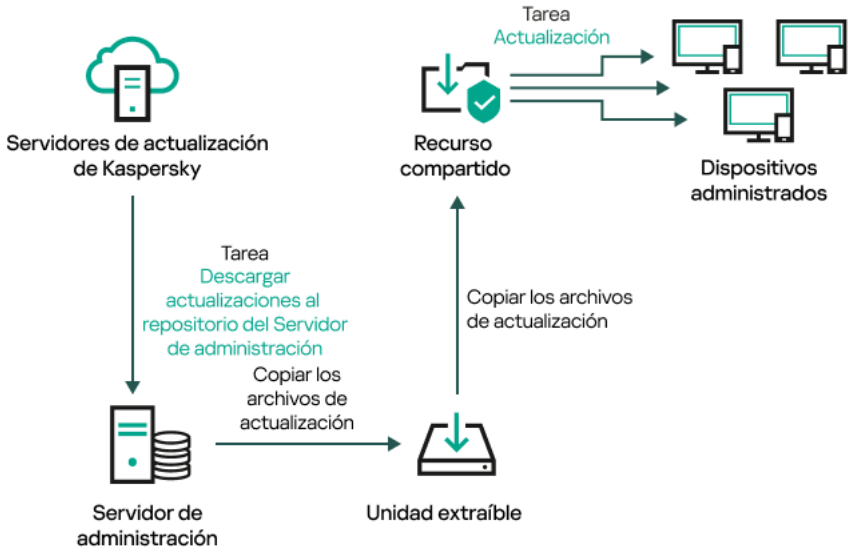
De forma predeterminada, el Servidor de administración y los puntos de distribución se comunican con los servidores de actualizaciones de Kaspersky y descargan las actualizaciones utilizando el protocolo HTTPS. Puede hacer que el Servidor de administración y/o los puntos de distribución utilicen el protocolo HTTP en lugar del protocolo HTTPS.

Para implementar este esquema, cree la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución* además de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*. Tras ello, los puntos de distribución descargarán las actualizaciones de los servidores de actualizaciones de Kaspersky y no del repositorio del Servidor de administración.

La tarea *Descargar actualizaciones en el repositorio del Servidor de administración* también es necesaria para este esquema, ya que se la utiliza para descargar las bases de datos de Kaspersky y los módulos de software de Kaspersky Security Center Linux.

Manualmente a través de una carpeta compartida o un servidor FTP

Si sus dispositivos cliente no tienen conexión con el Servidor de administración, puede usar una carpeta local o un recurso compartido como origen de actualizaciones para actualizar las bases de datos, los módulos de software y las aplicaciones de Kaspersky. De elegir esta alternativa, deberá copiar las actualizaciones requeridas del repositorio del Servidor de administración a una unidad extraíble y, luego, tendrá que copiar esas actualizaciones a la carpeta local o al recurso compartido que haya configurado como origen de actualizaciones en Kaspersky Endpoint Security (vea la siguiente imagen).



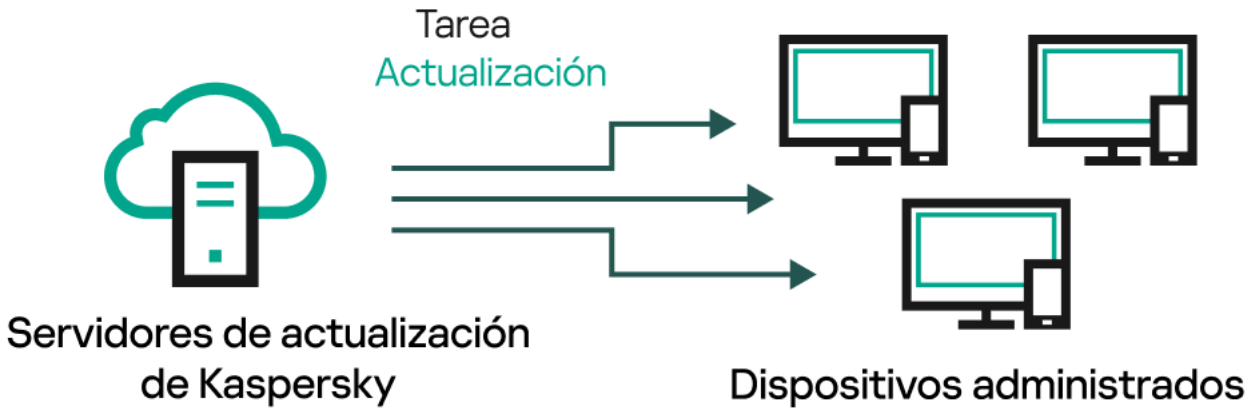
Actualización con una carpeta local, una carpeta compartida o un servidor FTP

Para obtener más información sobre los orígenes de actualizaciones en Kaspersky Endpoint Security, consulte los siguientes documentos de ayuda:

- Ayuda de Kaspersky Endpoint Security for Linux
- Ayuda de Kaspersky Endpoint Security para Windows

Realizar una descarga directa desde los servidores de actualizaciones de Kaspersky a Kaspersky Endpoint Security en los dispositivos administrados

Puede configurar Kaspersky Endpoint Security en los dispositivos administrados para que la aplicación obtenga sus actualizaciones directamente de los servidores de actualizaciones de Kaspersky (vea la siguiente imagen).



Actualización directa de las aplicaciones de seguridad utilizando los servidores de actualizaciones de Kaspersky

En este esquema, la aplicación de seguridad no utiliza los repositorios que brinda Kaspersky Security Center Linux. Para recibir actualizaciones directamente de los servidores de actualización de Kaspersky, especifique los servidores de actualización de Kaspersky como fuente de actualización en la aplicación de seguridad. Para obtener más información acerca de estos ajustes, consulte los siguientes documentos de ayuda:

- Ayuda de Kaspersky Endpoint Security para Linux
- Ayuda de Kaspersky Endpoint Security para Windows

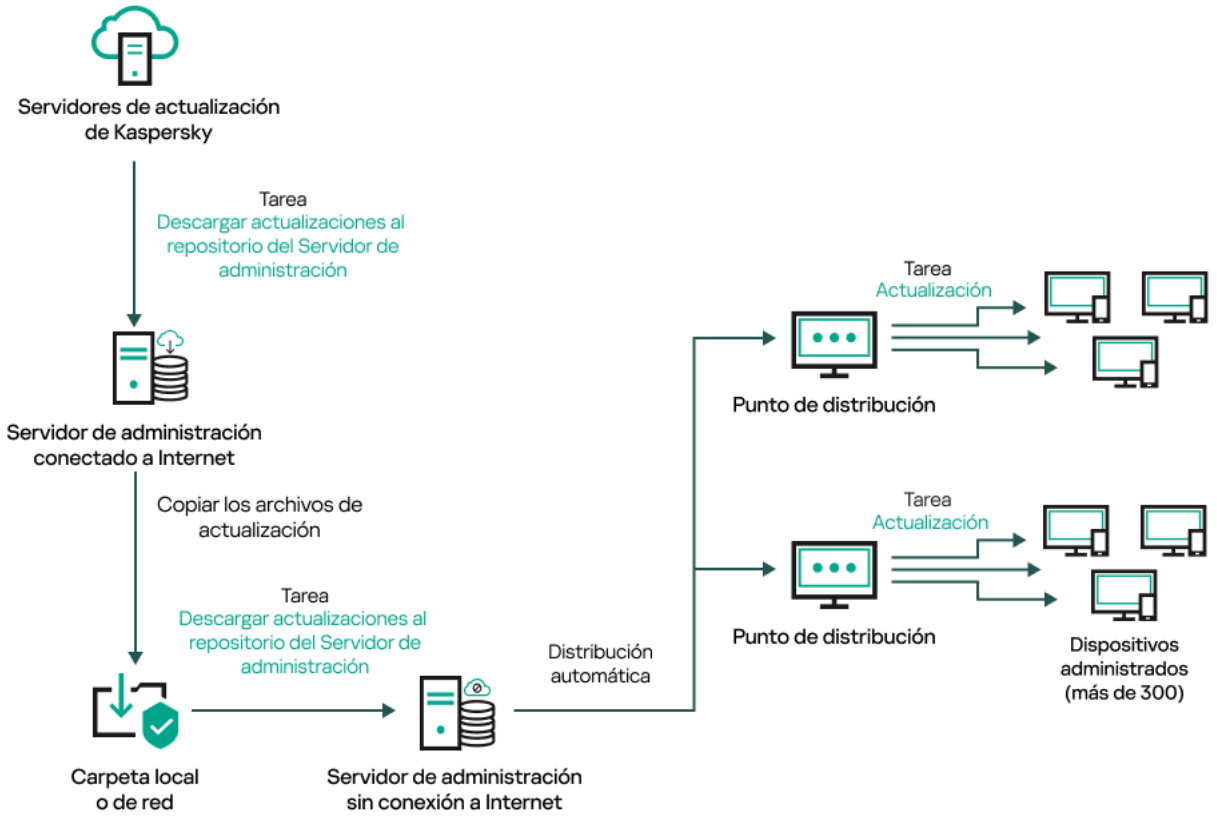
Utilizar una carpeta local o de red si el Servidor de administración no tiene conexión a Internet

Si el Servidor de administración no tiene conexión a Internet, puede configurar la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* para descargar actualizaciones desde una carpeta local o de red. En este caso, de vez en cuando debe copiar los archivos de actualización necesarios en la carpeta especificada. Por ejemplo, puede copiar los archivos de actualización necesarios desde uno de los siguientes orígenes:

- Servidor de administración que cuente con una conexión a Internet (ver la figura a continuación)

  Dado que un Servidor de administración descarga solo las actualizaciones que solicitan las aplicaciones de seguridad, los conjuntos de aplicaciones de seguridad administrados por los Servidores de administración (el que tiene conexión a Internet y el que no) deben coincidir.

  Si el Servidor de administración que usa para descargar actualizaciones tiene la versión 13.2 o anterior, abra las propiedades de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* y, a continuación, habilite la opción **Descargar las actualizaciones usando el esquema antiguo**.



Actualizar a través de una carpeta de red si el Servidor de administración no tiene conexión a Internet

- Kaspersky Update Utility

  Debido a que esta utilidad utiliza el antiguo esquema para descargar actualizaciones, abra las propiedades de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* y, a continuación, habilite la opción *Descargar las actualizaciones usando el esquema antiguo*. Si es necesario, también puede configurar la opción *Descargar automáticamente el archivo de solicitud de actualización* para que Kaspersky Update Utility descargue solo las actualizaciones necesarias.

Crear la Descarga de actualizaciones para la tarea del repositorio del Servidor de administración

La tarea *Descargar actualizaciones en el repositorio del Servidor de administración* permite descargar las actualizaciones de las bases de datos y los módulos de software para las aplicaciones de seguridad de Kaspersky desde los servidores de actualización de Kaspersky al repositorio del Servidor de Administración.

La tarea *Descargar actualizaciones en el repositorio del Servidor de administración* se crea automáticamente cuando se inicia el Servidor de administración por primera vez. En la lista de tareas, solo puede existir una tarea *Descargar actualizaciones en el repositorio del Servidor de administración*. Puede volver a crear esta tarea si se la ha eliminado de la lista de tareas del Servidor de administración.

Una vez finalizada la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* y descargadas las actualizaciones, se las puede propagar a los dispositivos administrados.

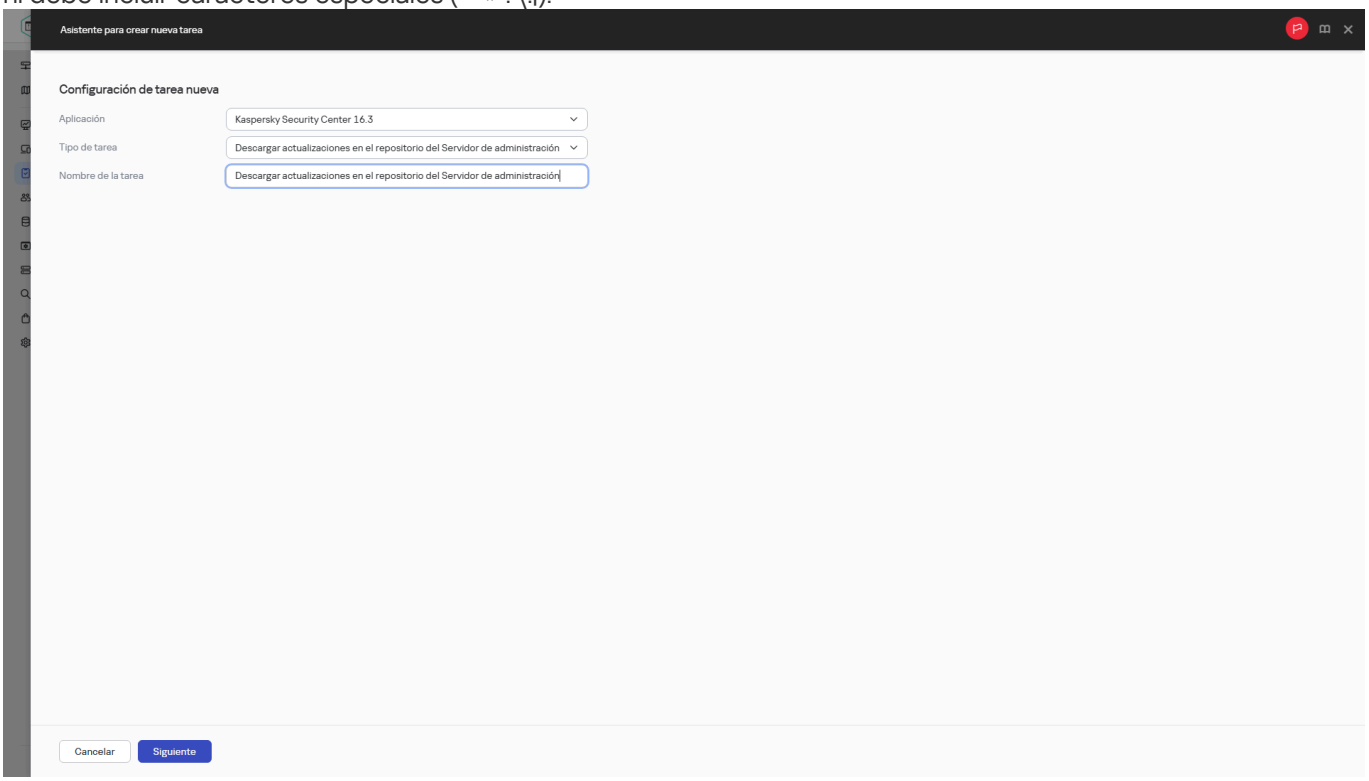
Antes de distribuir actualizaciones a los dispositivos administrados, puede ejecutar la tarea *Actualizar verificación*. Esto le permite asegurarse de que el Servidor de administración instalará las actualizaciones descargadas correctamente y que el nivel de seguridad no disminuirá debido a las actualizaciones. Para que las actualizaciones se verifiquen antes de ser distribuidas, defina la opción **Ejecutar verificación de actualizaciones** en la configuración de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*.

Para crear una tarea Descargar actualizaciones en el repositorio del Servidor de administración:

1. En el menú principal, vaya a **Tareas**.
2. Haga clic en **Agregar**.

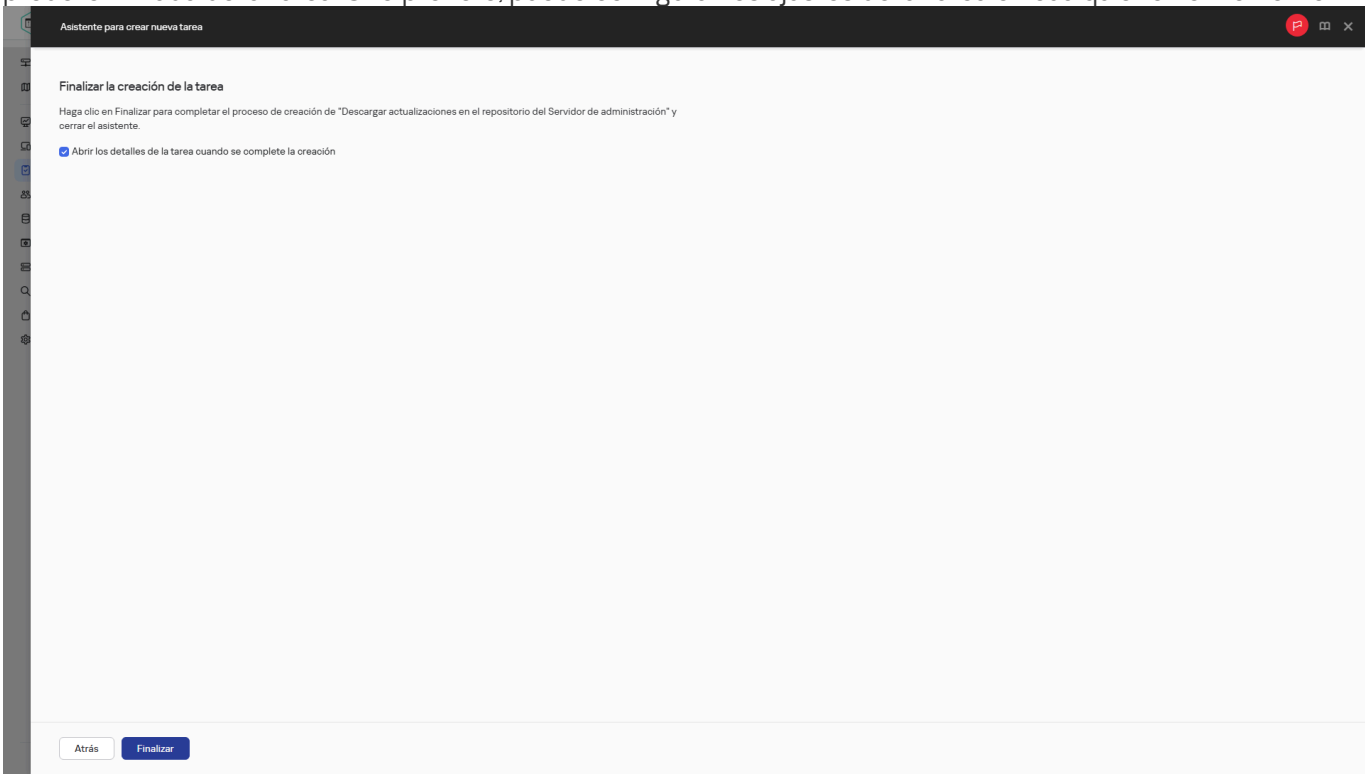
   Se inicia el Asistente para crear nueva tarea. Siga los pasos del asistente.
3. Para la aplicación Kaspersky Security Center, seleccione el tipo de tarea **Descargar actualizaciones en el repositorio del Servidor de administración**.

4. Escriba un nombre para la tarea que está creando. El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).



Crear la Descarga de actualizaciones para la tarea del repositorio del Servidor de administración

5. En la página **Finalizar la creación de la tarea**, puede habilitar la opción **Abrir los detalles de la tarea cuando se complete la creación** para abrir la ventana de propiedades de la tarea y modificar la configuración predeterminada de la tarea. Si lo prefiere, puede configurar los ajustes de la tarea en cualquier otro momento.



Finalizar la creación de la tarea

6. Haga clic en el botón **Finalizar**.

   Se crea la tarea y se la agrega a la lista de tareas.

7. Haga clic en el nombre de la tarea creada para abrir su ventana de propiedades.

8. En la ventana de propiedades de la tarea, en la pestaña **Configuración de la aplicación**, especifique la siguiente configuración:

Orígenes de actualizaciones

Como origen de actualizaciones, puede usar lo siguiente:

- Servidores de actualización de Kaspersky (seleccionados de forma predeterminada)
- Servidor de administración principal

  Este recurso se aplica a las tareas creadas para un Servidor de administración secundario o virtual.
- Carpeta local o de red

  Una carpeta local o de red con las últimas actualizaciones. La carpeta de red puede ser un servidor FTP o HTTP, o un recurso compartido SMB.

  La carpeta local debe ser una carpeta del dispositivo en el que se encuentra instalado el Servidor de administración. La ruta a la carpeta depende del sistema operativo del dispositivo. Dado que la carpeta local se encuentra en el Servidor de administración basado en Linux, debe especificar la ruta POSIX, por ejemplo: /path/to/dir.

  Al seleccionar una carpeta de red SMB como origen de actualizaciones, monte la carpeta en el dispositivo en el que está instalado el Servidor de administración antes de seleccionarla. Luego, especifique la ruta de la carpeta montada mediante su ruta en el sistema de archivos local. El acceso a la carpeta se realiza mediante el protocolo de SMB.

  Una carpeta local o de red, o un servidor FTP o HTTP que se use como origen de actualizaciones, debe contener una estructura de carpetas que coincida con la de los servidores de actualización de Kaspersky. Puede obtener esta estructura mediante Kaspersky Update Utility.

En la tarea *Descargar actualizaciones al repositorio del Servidor de administración* y *Descargar actualizaciones a los repositorios de los puntos de distribución*, la autenticación de usuario no funciona si selecciona una carpeta local o de red protegida con contraseña como fuente de actualización. Para resolver este problema, primero monte la carpeta protegida con contraseña y luego especifique las credenciales requeridas, por ejemplo, mediante el sistema operativo. Luego, puede seleccionar esta carpeta como fuente de actualización en una tarea de descarga de actualización. Kaspersky Security Center Linux no requerirá que ingrese las credenciales.

Carpeta para almacenar actualizaciones

La ruta a la carpeta especificada para almacenar las actualizaciones guardadas. Puede copiar la ruta de la carpeta especificada en el portapapeles. No puede cambiar la ruta a una carpeta específica para una tarea de grupo.

Forzar actualización de los servidores de administración secundarios

Si esta opción está habilitada, el Servidor de administración iniciará las tareas de actualización en los servidores de administración secundarios en cuanto se descarguen nuevas actualizaciones. Las tareas de actualización se inician utilizando el origen de actualización configurado en las propiedades de la tarea en los Servidores de administración secundarios.

Si esta opción no está habilitada, las tareas de actualización se iniciarán en los Servidores de administración secundarios siguiendo lo que indiquen sus programaciones.

Esta opción está deshabilitada de forma predeterminada.

Copiar actualizaciones descargadas a carpetas adicionales

Una vez que el Servidor de administración recibe actualizaciones, las copiará a las carpetas especificadas. Utilice esta opción si desea controlar manualmente la distribución de actualizaciones en la red.

Podría utilizar esta opción en, por ejemplo, la siguiente situación: la red de su organización está formada por varias subredes independientes. Los dispositivos de cada subred no tienen acceso a las demás subredes. Sin embargo, los dispositivos de todas las subredes tienen acceso a una misma carpeta compartida. En un caso así, puede hacer que el Servidor de administración de una subred descargue las actualizaciones de los servidores de actualizaciones de Kaspersky, habilitar esta opción y definir esa carpeta compartida como destino. Luego, defina esa carpeta como origen de actualizaciones en las tareas "Descargar actualizaciones en el repositorio del Servidor de administración" de los demás servidores de administración.

Si selecciona copiar las actualizaciones descargadas a una carpeta local, debe especificar una carpeta en el dispositivo que tiene el Servidor de administración instalado. La ruta a la carpeta depende del sistema operativo del dispositivo. Dado que la carpeta local se encuentra en el Servidor de administración basado en Linux, debe especificar la ruta POSIX, por ejemplo: /path/to/dir.

Cuando selecciona una carpeta de red que se encuentra en el Servidor de administración basado en Linux, debe montar la carpeta para garantizar el acceso a la carpeta de red con anticipación desde el dispositivo que tiene el Servidor de administración. El acceso a la carpeta se realiza mediante el protocolo de SMB.

Esta opción está deshabilitada de forma predeterminada.

Descargar archivos diff

Esta opción habilita la función de descarga de archivos diff.

Esta opción está deshabilitada de forma predeterminada.

Descargar actualizaciones utilizando el esquema anterior

A partir de la versión 14, Kaspersky Security Center utiliza el nuevo esquema al descargar actualizaciones para bases de datos y módulos de software. Para que la aplicación descargue las actualizaciones utilizando el nuevo esquema, el origen de actualizaciones debe contener archivos de actualización con metadatos que sean compatibles con el nuevo esquema. Si el origen de actualizaciones elegido contiene archivos de actualización con metadatos que solo son compatibles con el esquema anterior, habilite la opción **Descargar actualizaciones utilizando el esquema anterior**. De lo contrario, la tarea de descarga de actualizaciones no podrá completarse.

Habilite esta opción si, por ejemplo, seleccionó una carpeta local o de red como origen de actualizaciones y los archivos de actualización de dicha carpeta fueron descargados por alguna de las siguientes aplicaciones:

- Kaspersky Update Utility

  Esta utilidad descarga actualizaciones utilizando el esquema antiguo.

- Kaspersky Security Center 13 Linux

  Suponga, por ejemplo, que uno de sus servidores de administración no tiene conexión a Internet. En ese caso, podría utilizar un segundo Servidor de administración (que tenga conexión a Internet) para descargar las actualizaciones. Luego, podría colocar los archivos descargados en una carpeta local o de red que el primer servidor de administración pueda usar como origen de actualizaciones. Si el segundo Servidor de administración es versión 13, habilite la opción **Descargar actualizaciones utilizando el esquema anterior** en la tarea para el primer Servidor de administración.

Esta opción está deshabilitada de forma predeterminada.

Ejecutar verificación de actualizaciones

El Servidor de administración descarga las actualizaciones del origen, las guarda en un repositorio temporal y ejecuta la tarea definida en el campo **Tarea de verificación de actualizaciones**. Si la tarea se completa con éxito, las actualizaciones se copian desde el repositorio temporal a una carpeta compartida en el Servidor de administración y luego se distribuyen a todos los dispositivos para los cuales el Servidor de administración actúa como fuente de actualizaciones (tareas con el tipo de programación **Al descargar nuevas actualizaciones al repositorio** empezada). La tarea para descargar las actualizaciones en el repositorio terminará solo luego de que se complete la tarea *Verificación de actualizaciones*.

Esta opción está deshabilitada de forma predeterminada.

Descargar automáticamente el archivo de solicitud de actualización

Si desea que Kaspersky Update Utility descargue solo las actualizaciones necesarias con la configuración adecuada, active esta opción y especifique la ruta donde Kaspersky Security Center Linux creará el archivo de solicitud de actualización con información sobre las actualizaciones que se descargarán. El archivo de solicitud de actualización contiene la marca de tiempo y el hash MD5 para el control de versiones.

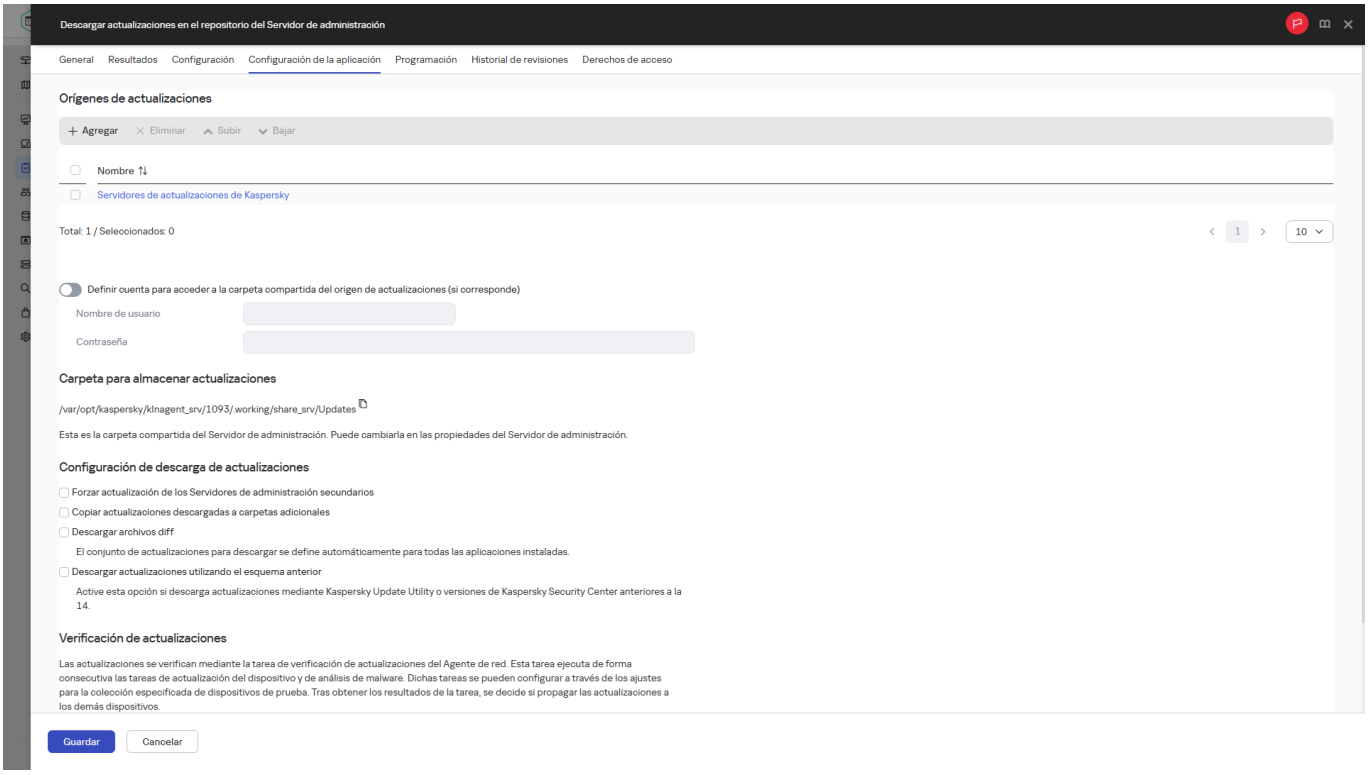
Asegúrese de que la opción **Descargar actualizaciones utilizando el esquema anterior** esté deshabilitada.

Además, se debe configurar la descarga de actualizaciones en Kaspersky Update Utility.

De forma predeterminada, está especificada la siguiente ruta: /var/opt/kaspersky/klnagent_srv/1093/.working/share_srv/retranslation_request.xml. Si es necesario, puede cambiar el nombre (retranslation_request) y la ruta predeterminadas.

> El archivo de solicitud se puede colocar en una carpeta local o compartida. Al utilizar una carpeta compartida, debe garantizar el acceso a esta carpeta desde el dispositivo que tenga el Servidor de administración instalado. Las formas de garantizar el acceso y las herramientas utilizadas dependen de su infraestructura.

Al realizar la tarea *Descargar actualizaciones en el repositorio de la tarea del Servidor de administración*, Kaspersky Security Center Linux crea el archivo de solicitud de actualización en formato .xml en la ruta que usted ha especificado. Kaspersky Update Utility obtiene automáticamente la información del archivo solicitado y luego descarga solo las actualizaciones necesarias. Si Kaspersky Update Utility no puede obtener la información automáticamente (por ejemplo, Kaspersky Update Utility no tiene acceso a la carpeta donde Kaspersky Security Center Linux creó el archivo de solicitud), deberá transmitir el archivo mediante herramientas de terceros.



Especificar las propiedades de la tarea Descargar actualizaciones en el repositorio del Servidor de administración

9. En la ventana de propiedades de la tarea, en la pestaña **Programación**, cree una programación para el inicio de la tarea. Si es necesario, configure los siguientes ajustes:

- **Iniciar tarea**:

  Manual (esta es la opción seleccionada por defecto)

  La tarea no se ejecutará automáticamente. Solo se la podrá iniciar en forma manual.

  Esta opción está seleccionada de forma predeterminada.

  Cada N minutos

  La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la hora indicada en el día en que se cree la tarea. Cada ejecución estará separada de la anterior por el número de minutos que indique.

  De forma predeterminada, la tarea se ejecutará cada treinta minutos, a partir de la hora actual del sistema.

  Cada N horas

  La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la fecha y hora indicadas. Cada ejecución estará separada de la anterior por el número de horas que indique.

  De manera predeterminada, la tarea se ejecutará cada 6 horas, a partir de la fecha y hora actuales del sistema.

  Cada N días

La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta opción permite elegir la fecha y hora de la primera ejecución. Podrá configurar estos dos ajustes si son compatibles con la aplicación para la que esté creando la tarea.

De forma predeterminada, la tarea se ejecutará todos los días, a partir de la fecha y hora actuales del sistema.

Por días de la semana

La tarea se ejecutará periódicamente en los días de la semana y a la hora que indique.

De manera predeterminada, la tarea se ejecutará todos los viernes a las 18:00:00.

Mensual

La tarea se ejecutará periódicamente, en el día del mes y a la hora que indique.

Si el día elegido no forma parte de un mes, la tarea se ejecutará el último día de ese mes.

Por defecto, la tarea se ejecutará el primer día de cada mes, a la hora actual del sistema.

Mensualmente en el día de la semana seleccionado

La tarea se ejecutará periódicamente, en los días del mes y a la hora que indique.

De manera predeterminada, la hora de inicio es a las 18:00 y no se selecciona ningún día del mes.

> Tenga en cuenta que no selecciona una fecha específica en el mes, ni el número de la semana (primera, segunda semana del mes), sino el número de secuencia del día de la semana dentro de un mes. Por ejemplo, si coloca el cursor en la celda **Ma** de la **Primero** fila, significa que la tarea se ejecutará el primer martes de cada mes nuevo.

Puede seleccionar varios días de la semana.

Al completarse otra tarea

La tarea actual se iniciará después de que se complete otra tarea. Esta opción solo funciona si ambas tareas están asignadas a los mismos dispositivos. Por ejemplo, podría ejecutar la tarea *Administrar dispositivos* con la opción **Encender el dispositivo** y hacer que, una vez completada esa tarea, se ejecute la tarea *Análisis antivirus* como una tarea desencadenante.

Debe seleccionar la tarea desencadenante de la tabla y el estado con el que esta tarea debe completarse (**Completada correctamente** o **Error**).

Si es necesario, puede buscar, ordenar y filtrar las tareas en la tabla de la siguiente manera:

- Ingrese el nombre de la tarea en el campo de búsqueda para buscar la tarea por su nombre.
- Haga clic en el ícono de ordenar para ordenar las tareas por nombre.

  De manera predeterminada, las tareas se clasifican en orden alfabético ascendente.
- Haga clic en el ícono de filtro y, en la ventana que se abre, filtre las tareas por grupo y luego haga clic en el botón **Aplicar**.

- Ajustes adicionales de la tarea:

  Ejecutar tareas no realizadas

  Esta opción determina el comportamiento de la tarea cuando la misma está por iniciarse y uno de los dispositivos cliente no está visible en la red.

Si esta opción está habilitada, el sistema intentará iniciar la tarea la siguiente vez que la aplicación de Kaspersky se ejecute en el dispositivo cliente. Si la programación de la tarea es **Manual**, **Una vez** o **Inmediatamente**, la tarea se iniciará inmediatamente después de que el dispositivo aparezca en la red o inmediatamente después de que el dispositivo sea incluido en el alcance de la tarea.

Si esta opción está deshabilitada, solo las tareas programadas se ejecutan en los dispositivos cliente. Para la programación **Manual**, **Una vez** e **Inmediatamente**, las tareas se ejecutan solo en los dispositivos cliente que están visibles en la red. Podría deshabilitar esta opción para, por ejemplo, una tarea que consuma muchos recursos y que solo deba ejecutarse fuera del horario laboral.

Esta opción está activada de forma predeterminada.

Utilizar retardo aleatorio automático para el inicio de la tarea

Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo que especifique. Se realizará, de este modo, un *inicio distribuido*. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

La hora de inicio distribuida se calcula automáticamente cuando se crea una tarea. El cálculo tiene en cuenta el número de dispositivos cliente a los que la tarea está asignada. Las ejecuciones posteriores a la inicial ocurren siempre a la hora de inicio calculada. Sin embargo, tenga en cuenta que si modifica la configuración de la tarea o inicia la tarea manualmente, la hora de inicio calculada cambiará.

Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

Esta opción está activada de forma predeterminada.

Utilizar el retardo aleatorio automático para el inicio de la tarea dentro de un intervalo de

Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo de tiempo especificado. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

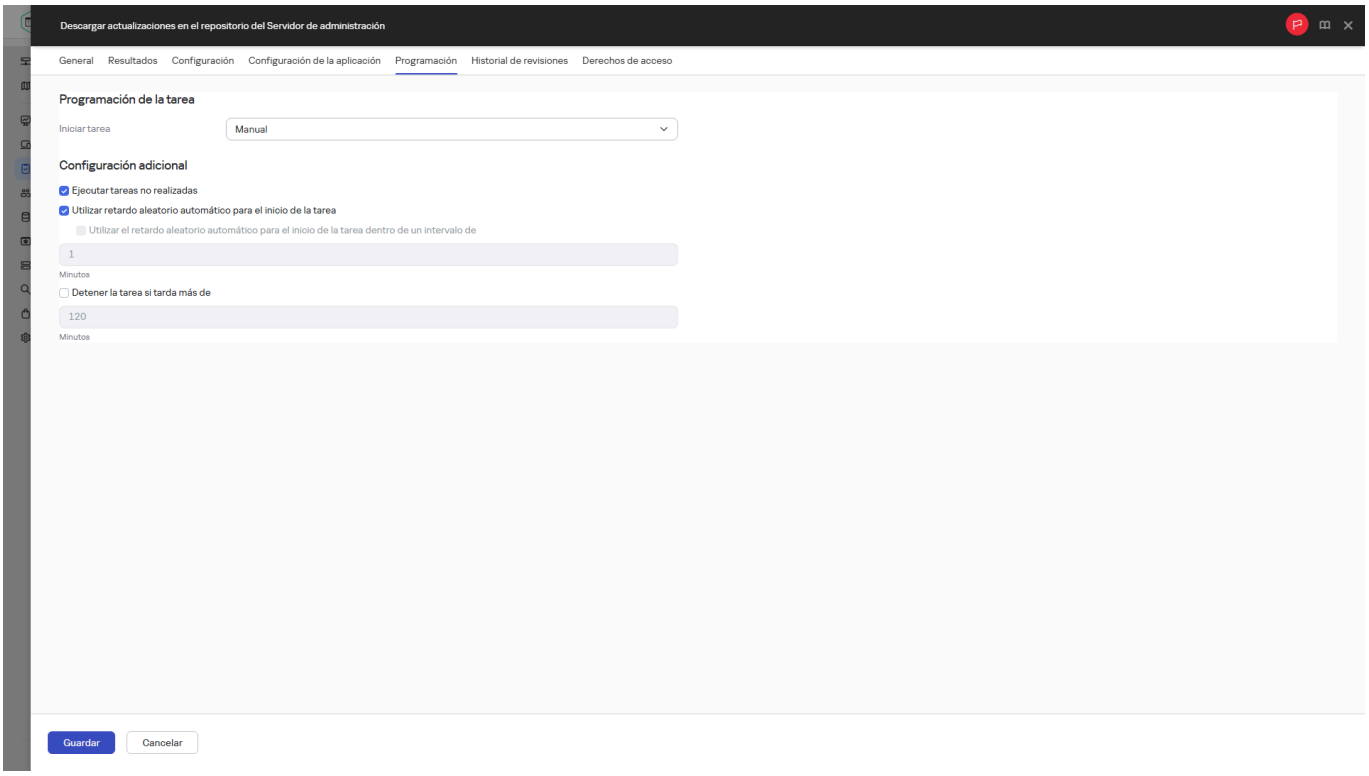
Esta opción está deshabilitada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

Detener la tarea si tarda más de

Una vez que transcurra el período especificado, la tarea se detendrá automáticamente, se haya completado o no.

Habilite esta opción si desea que las tareas que tarden mucho en completarse se interrumpan o se detengan.

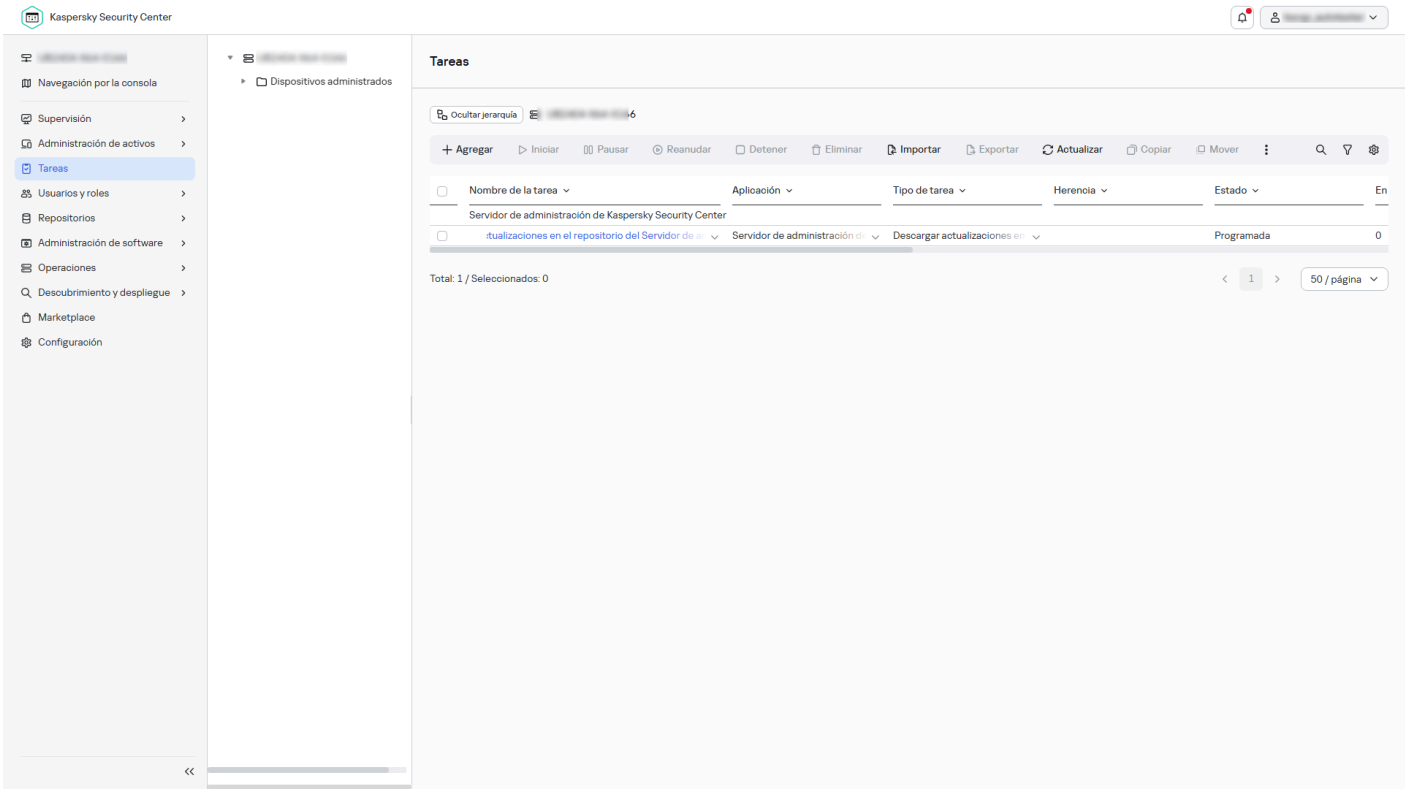
Esta opción está deshabilitada de forma predeterminada. El tiempo de ejecución por defecto para las tareas es de 120 minutos.



Especificar la programación de la tarea Descargar actualizaciones en el repositorio del Servidor de administración

10. Haga clic en el botón **Guardar**.

La tarea queda creada y configurada.



La lista de tareas

Cuando el Servidor de administración realiza la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*, las actualizaciones de las bases de datos y los módulos de software se descargan desde el origen de las actualizaciones y se almacenan en la carpeta compartida del Servidor de administración. Si crea esta tarea para un grupo de administración, la misma se aplicará solamente a los agentes de red incluidos en el grupo de administración especificado.

Las actualizaciones se distribuyen a los dispositivos cliente y a los servidores de administración secundarios desde la carpeta compartida del Servidor de administración.

Comprobar actualizaciones descargadas

Antes de instalar actualizaciones en sus dispositivos administrados, puede comprobar que las mismas no tengan errores o problemas de funcionamiento. Dispone para ello de la tarea *Verificación de actualizaciones*. La tarea *Verificación de actualizaciones* se ejecuta automáticamente cuando se realiza la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*. El Servidor de administración descarga las actualizaciones del origen, las guarda en el repositorio temporal y ejecuta la tarea *Verificación de actualizaciones*. Si esta tarea se completa sin errores, las actualizaciones se copian del repositorio temporal a la carpeta compartida del Servidor de administración. De allí, se distribuyen a los dispositivos cliente que tienen el Servidor de administración como origen de actualizaciones.

Si, como resultado de la tarea *Verificación de actualizaciones*, se determina que las actualizaciones del repositorio temporal son incorrectas, o si la tarea de verificación de actualizaciones se completa con errores, dichas actualizaciones no se copian a la carpeta compartida. El Servidor de administración guarda el conjunto de actualizaciones anterior. Además, las tareas que tienen el tipo de programación **Al descargar nuevas actualizaciones al repositorio** no se inician en ese momento. Dichas operaciones se llevarán a cabo en el siguiente inicio de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* si el análisis de las nuevas actualizaciones finaliza correctamente.

El conjunto de actualizaciones se considera inválido si una de las condiciones siguiente se cumple al menos en un dispositivo de prueba:

- Ocurrió un error de la tarea de actualización.
- El estado de protección en tiempo real de la aplicación de seguridad cambió después de haber aplicado las actualizaciones.
- Se detectó un objeto infectado mientras se ejecutaba la tarea de análisis a pedido.
- Se produjo un error en el tiempo de ejecución de la aplicación de Kaspersky.

Si estas condiciones no se cumplen en ninguno de los dispositivos de prueba, el conjunto de actualizaciones se considera válido y la tarea *Verificación de actualizaciones* se da por correctamente completada.

Antes de comenzar a crear la tarea *Verificación de actualizaciones*, complete estos pasos:

1. Cree un grupo de administración que contenga algunos dispositivos de prueba. El grupo se usará para verificar las actualizaciones.

   Recomendamos que los dispositivos del grupo tengan la protección más fiable posible y que su configuración de aplicaciones sea la más usual en la red. Con ello mejorará la fiabilidad de los análisis antivirus, aumentará la probabilidad de que se detecten virus y se reducirá la incidencia de falsos positivos. De encontrarse virus en los dispositivos de prueba, se considerará que la tarea *Verificación de actualizaciones* no se completó correctamente.

2. Cree las tareas de actualización y análisis antimalware para una aplicación compatible con Kaspersky Security Center Linux, como Kaspersky Endpoint Security for Linux. Cuando cree las tareas de actualización y análisis antimalware, seleccione el grupo de administración que contenga los dispositivos de prueba.

   La tarea *Verificación de actualizaciones* ejecutará las tareas de actualización y análisis antimalware secuencialmente en los dispositivos de prueba para verificar que todas las actualizaciones sean válidas. Cuando cree la tarea *Verificación de actualizaciones*, deberá seleccionar las tareas de actualización y análisis antimalware que se ejecutarán.

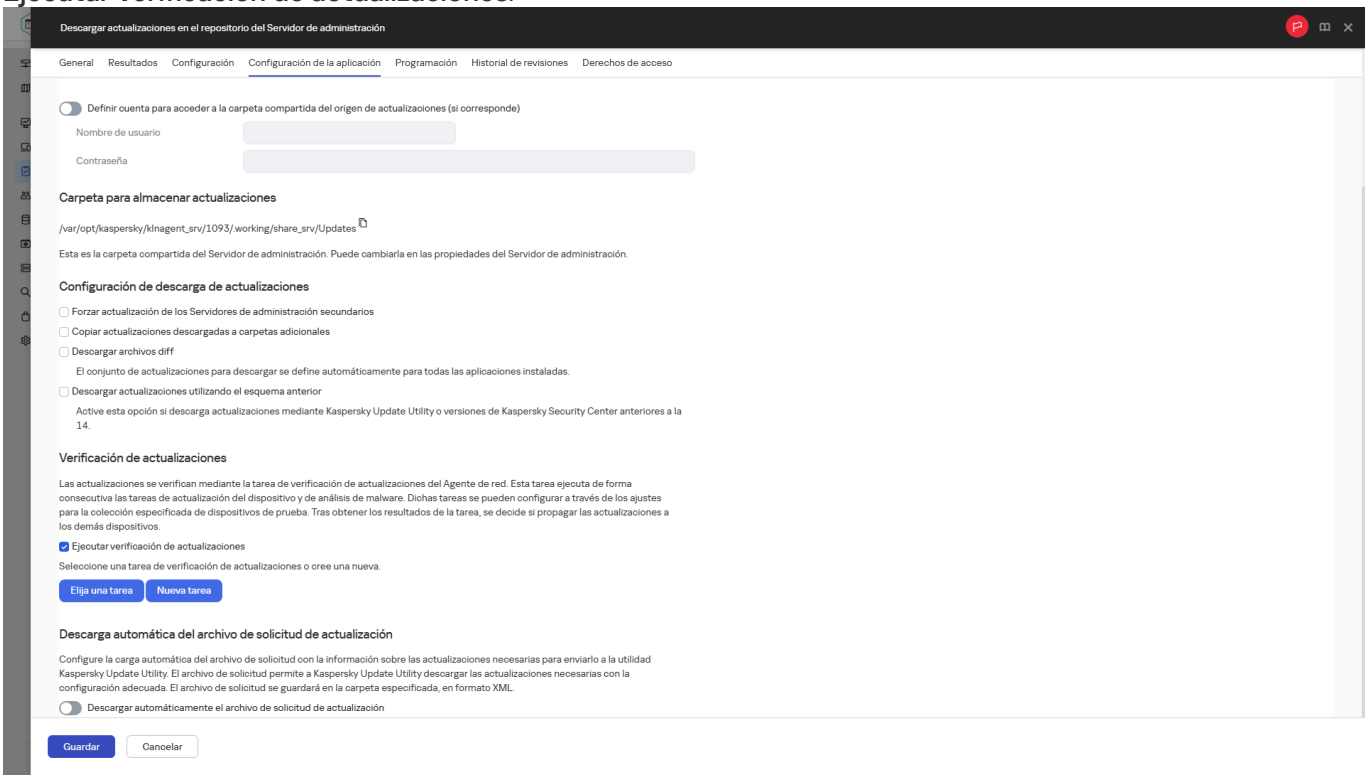
3. Cree la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*.

Para que Kaspersky Security Center Linux verifique las actualizaciones descargadas antes de distribuirlas a los dispositivos cliente:

1. En el menú principal, vaya a **Tareas**.

2. Haga clic en la tarea **Descargar actualizaciones en el repositorio del Servidor de administración**.

3. En la ventana de propiedades de la tarea, vaya a la pestaña **Configuración de la aplicación** y habilite la opción **Ejecutar verificación de actualizaciones**.



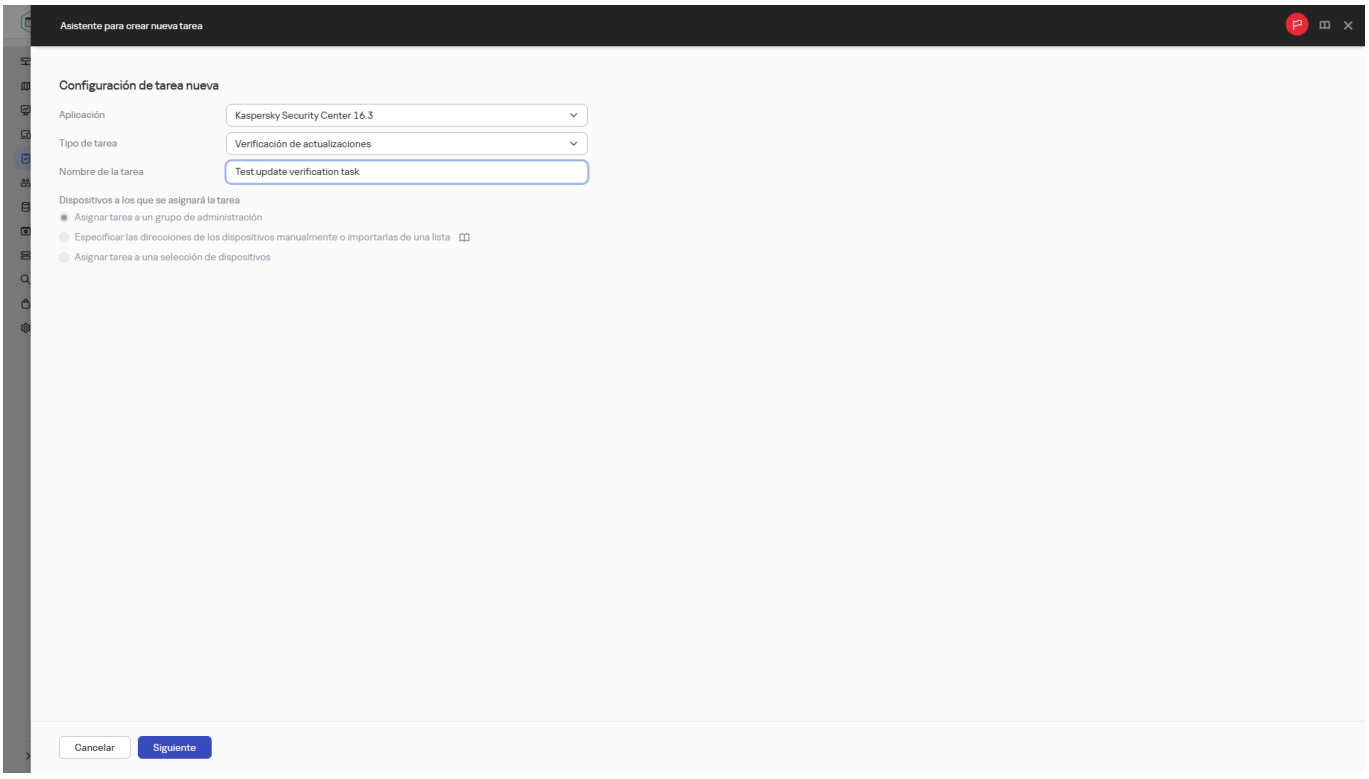
Propiedades de la tarea Descargar actualizaciones en el repositorio del Servidor de administración

4. Si la tarea *Verificación de actualizaciones* ya existe, haga clic en el botón **Elija una tarea**. En la ventana que se abre, seleccione la tarea *Verificación de actualizaciones* del grupo de administración con los dispositivos de prueba.

5. Si aún no creó la tarea *Verificación de actualizaciones*, haga lo siguiente:

a. Haga clic en el botón **Nueva tarea**.

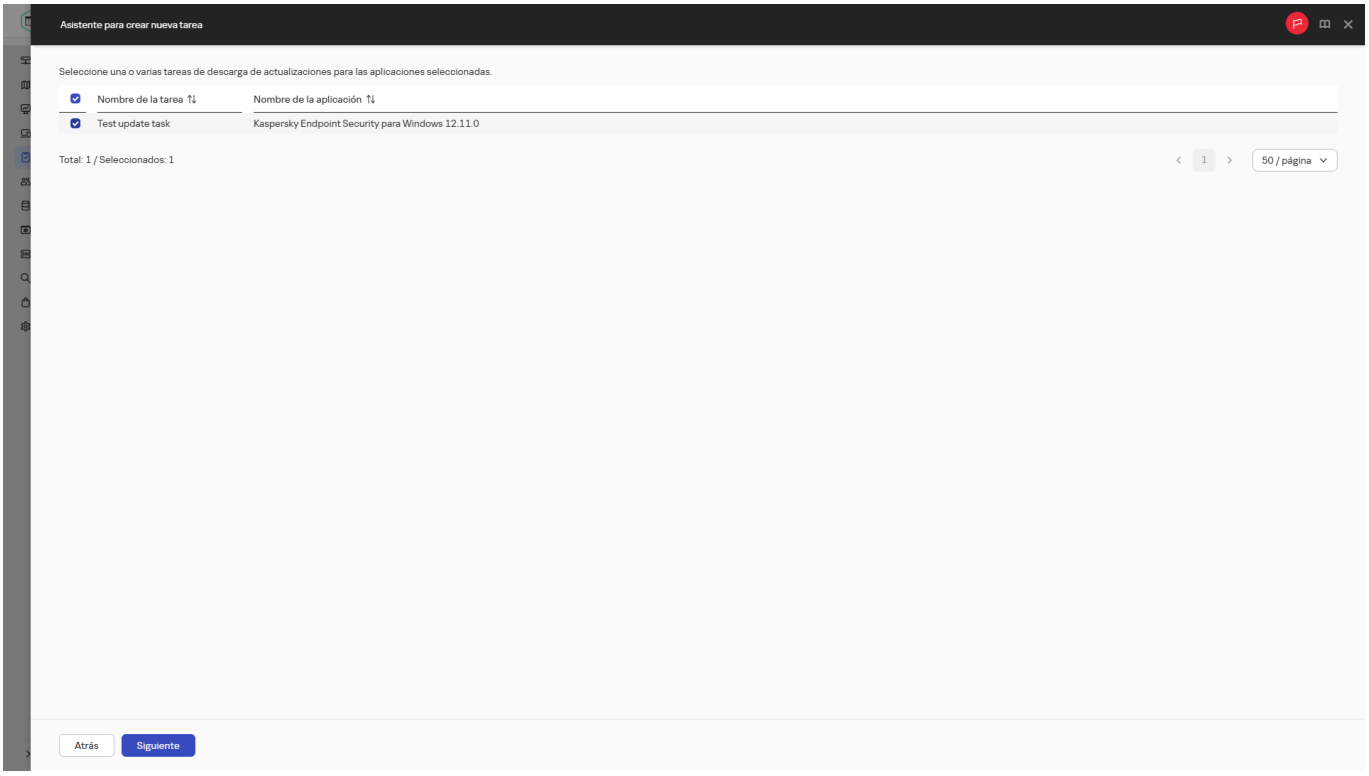
b. Se abre el Asistente para crear nueva tarea. Escriba un nombre para la tarea (si desea cambiar el nombre predeterminado).



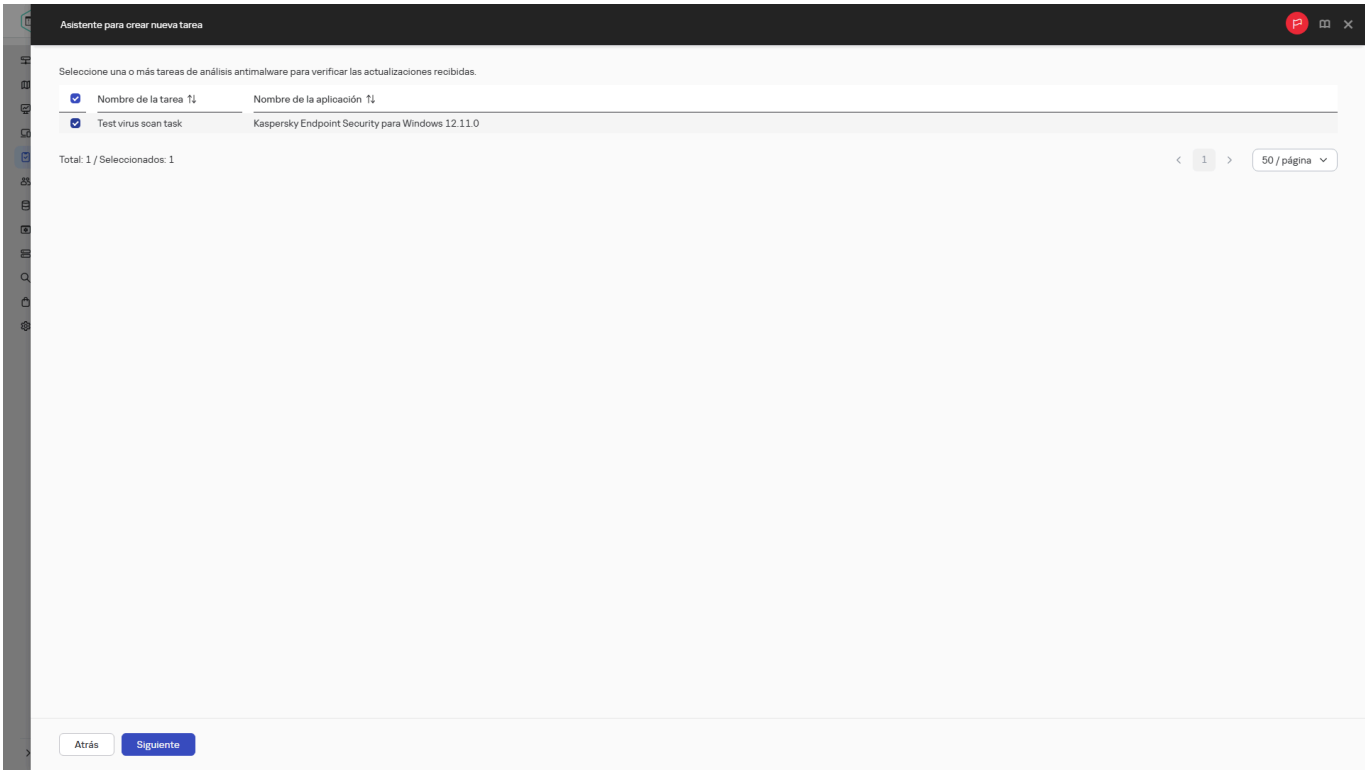
Creación de una tarea de verificación de actualizaciones

a. Seleccione el grupo de administración con dispositivos de prueba que creó en un paso anterior.

b. Seleccione la tarea de actualización de una aplicación requerida compatible con Kaspersky Security Center Linux.



a. Seleccione la tarea de análisis de malware de una aplicación requerida compatible con Kaspersky Security Center Linux.



Seleccionar la tarea de análisis de malware

Hecho esto, aparecerán las siguientes opciones. Recomendamos que las deje habilitadas.

Reiniciar el dispositivo después de la actualización de las bases de datos

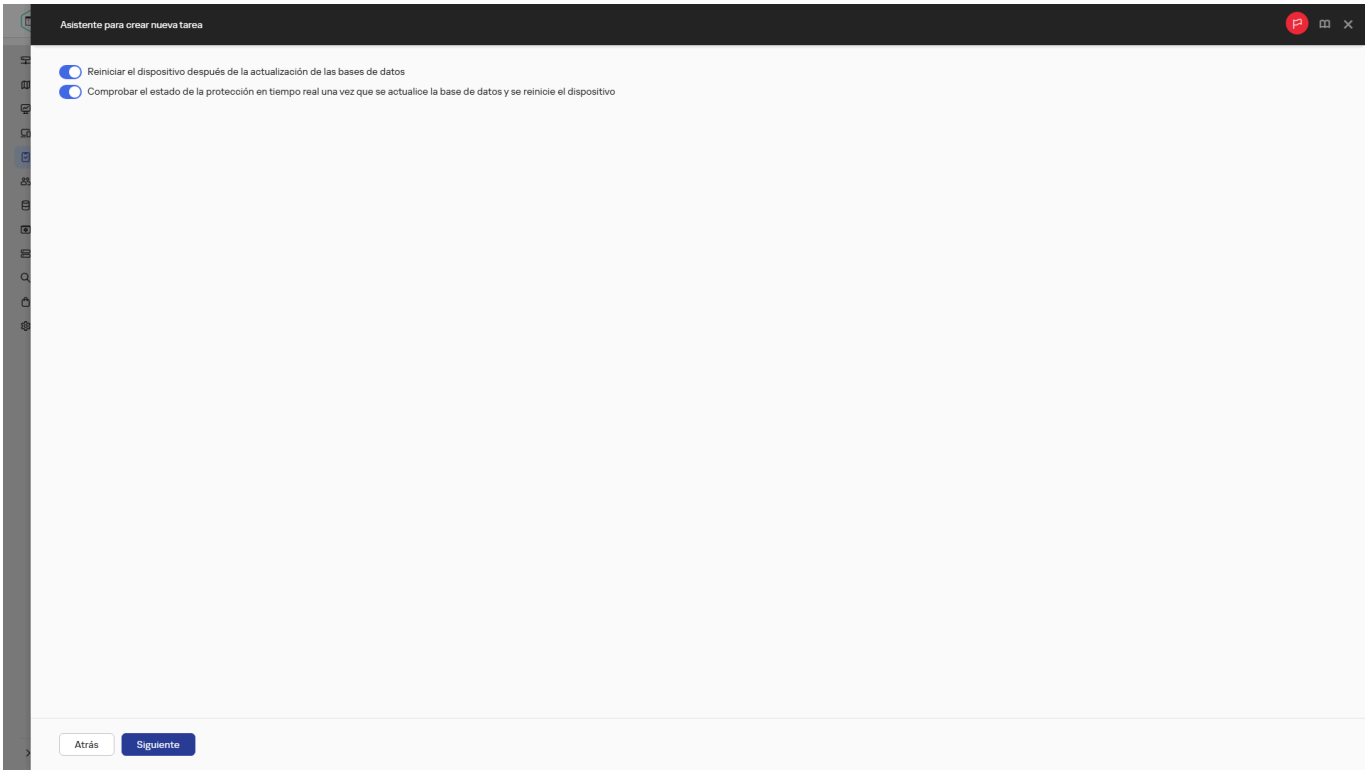
Cuando se actualizan las bases de datos antivirus de un dispositivo, es recomendable reiniciarlo.

Esta opción está activada de forma predeterminada.

Comprobar el estado de la protección en tiempo real una vez que se actualice la base de datos y se reinicie el dispositivo

Si esta opción está habilitada, la tarea *Verificación de actualizaciones* comprobará si las actualizaciones descargadas en el repositorio del Servidor de administración son válidas y si el nivel de protección disminuyó tras actualizar las bases de datos antivirus y reiniciar el dispositivo.

Esta opción está activada de forma predeterminada.



Especificar la configuración de la tarea

a. Indique qué cuenta se usará para ejecutar la tarea *Verificación de actualizaciones*. Puede usar su propia cuenta y dejar habilitada la opción **Cuenta predeterminada**. Como alternativa, puede elegir otra cuenta que tenga los derechos de acceso necesarios para ejecutar la tarea. Para ello, haga clic en **Especificar cuenta** e ingrese las credenciales de la cuenta que desee usar.

6. Haga clic en **Guardar** para cerrar la ventana de propiedades de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*.

La verificación de actualización automática está habilitada. Ahora puede ejecutar la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* y comenzará desde la verificación de actualizaciones.

Crear una tarea para descargar las actualizaciones en los repositorios de los puntos de distribución

Puede crear la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución* para un grupo de administración. Cuando la tarea se ejecute, afectará a los puntos de distribución que formen parte del grupo de administración seleccionado.

Puede usar esta tarea, por ejemplo, si el tráfico entre el Servidor de administración y los puntos de distribución es más costoso que el tráfico entre los puntos de distribución y los servidores de actualización de Kaspersky, o si el Servidor de administración no tiene acceso a Internet.

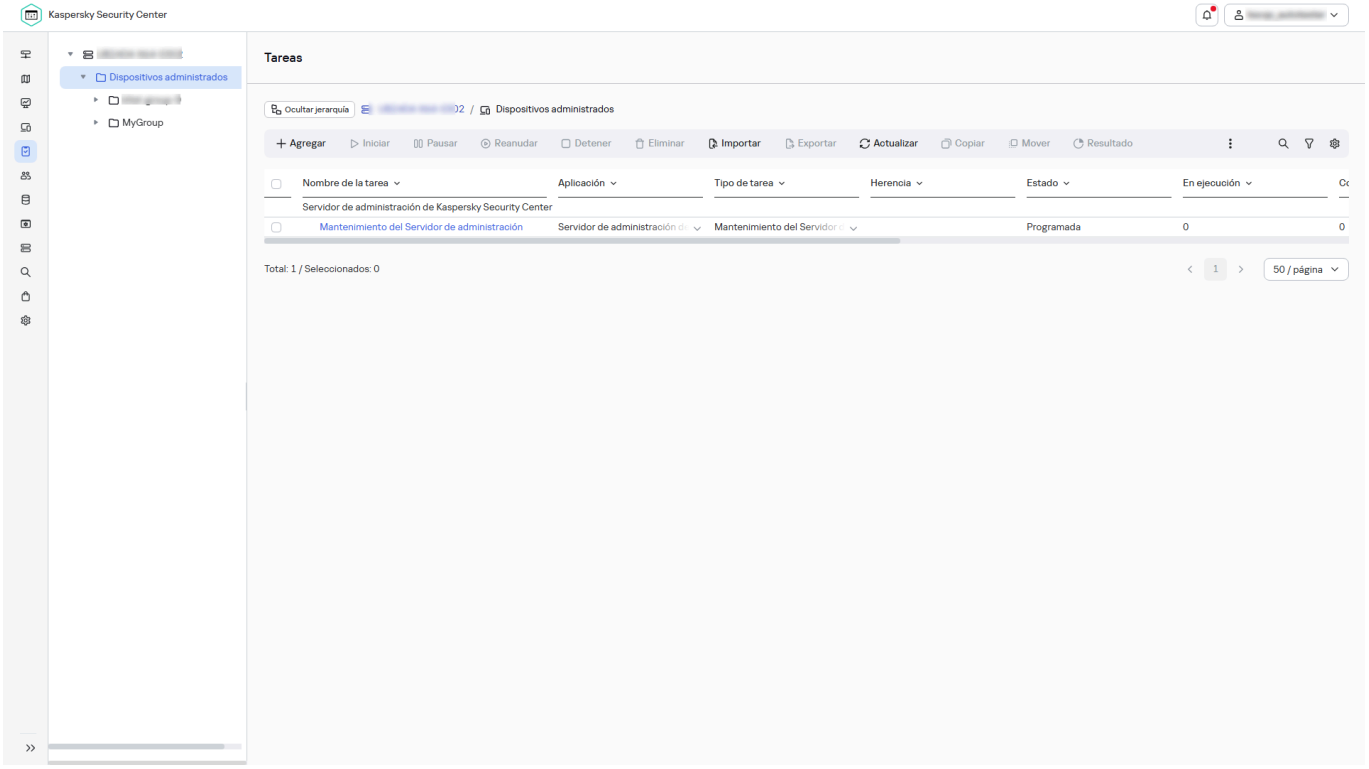
Esta tarea se necesita para descargar actualizaciones de los servidores de actualizaciones de Kaspersky en los repositorios de los puntos de distribución. La lista de actualizaciones incluye lo siguiente:

- actualizaciones para las bases de datos y los módulos de software de las aplicaciones de seguridad de Kaspersky.
- Actualizaciones a los componentes de Kaspersky Security Center.
- actualizaciones para las aplicaciones de seguridad de Kaspersky.

Una vez descargadas, las actualizaciones se pueden propagar a los dispositivos administrados.

*Para crear la tarea **Descargar actualizaciones en los repositorios de los puntos de distribución** para un grupo de administración seleccionado:*

1. En el menú principal, vaya a **Tareas**.



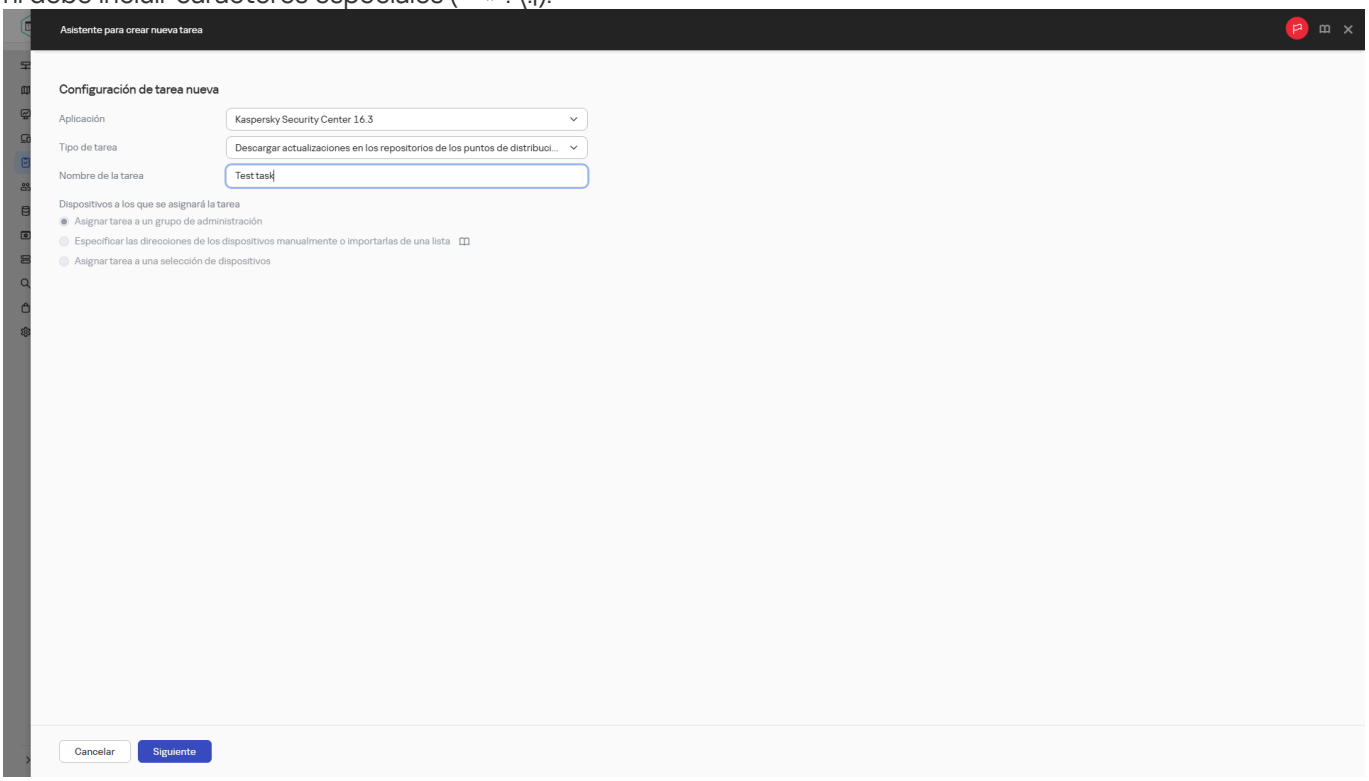
La sección Tareas

2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Siga los pasos del asistente.

3. Para la aplicación Kaspersky Security Center, en el campo **Tipo de tarea** seleccione **Descargar actualizaciones en los repositorios de los puntos de distribución**.

4. Escriba un nombre para la tarea que está creando. El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).



Creación de la tarea Descargar actualizaciones en los repositorios de los puntos de distribución

5. Seleccione un botón de opción para elegir el grupo de administración, la selección de dispositivos o los dispositivos a los que se aplicará la tarea.

6. En el paso **Finalizar la creación de la tarea**, si desea modificar la configuración predeterminada de la tarea, habilite la opción **Abrir los detalles de la tarea cuando se complete la creación**. Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Puede cambiar la configuración por defecto más tarde, en cualquier momento.

7. Haga clic en el botón **Crear**.

   Se crea la tarea y se la agrega a la lista de tareas.

8. Haga clic en el nombre de la nueva tarea para abrir la ventana de propiedades de la tarea.

9. En la pestaña **Configuración de la aplicación** de la ventana de propiedades de la tarea, configure los siguientes ajustes:

   Orígenes de actualizaciones

   Los siguientes recursos se pueden utilizar como orígenes de actualizaciones para el punto de distribución:

   - Servidores de actualizaciones de Kaspersky

     Servidores HTTP(S) de Kaspersky desde los que las aplicaciones de Kaspersky descargan actualizaciones para sus bases de datos y módulos de software.

     Esta opción está seleccionada de forma predeterminada.

   - Carpeta local o de red

     Una carpeta local o de red con las últimas actualizaciones. Solo un recurso compartido SMB montado se puede usar como carpeta de red. La carpeta local debe ser una carpeta del dispositivo en el que se encuentra instalado el Servidor de administración.

En la tarea *Descargar actualizaciones al repositorio del Servidor de administración* y *Descargar actualizaciones a los repositorios de los puntos de distribución*, la autenticación de usuario no funciona si selecciona una carpeta local o de red protegida con contraseña como fuente de actualización. Para resolver este problema, primero monte la carpeta protegida con contraseña y luego especifique las credenciales requeridas, por ejemplo, mediante el sistema operativo. Luego, puede seleccionar esta carpeta como fuente de actualización en una tarea de descarga de actualización. Kaspersky Security Center Linux no requerirá que ingrese las credenciales.

Carpeta para almacenar actualizaciones

La ruta a la carpeta especificada para almacenar las actualizaciones guardadas. Puede copiar la ruta de la carpeta especificada en el portapapeles. No puede cambiar la ruta a una carpeta específica para una tarea de grupo.

Descargar archivos diff

Esta opción habilita la función de descarga de archivos diff.

Esta opción está deshabilitada de forma predeterminada.

Descargar actualizaciones utilizando el esquema anterior

A partir de la versión 14, Kaspersky Security Center utiliza el nuevo esquema al descargar actualizaciones para bases de datos y módulos de software. Para que la aplicación descargue las actualizaciones utilizando el nuevo esquema, el origen de actualizaciones debe contener archivos de actualización con metadatos que sean compatibles con el nuevo esquema. Si el origen de actualizaciones elegido contiene archivos de actualización con metadatos que solo son compatibles con el esquema anterior, habilite la opción **Descargar actualizaciones utilizando el esquema anterior**. De lo contrario, la tarea de descarga de actualizaciones no podrá completarse.

Habilite esta opción si, por ejemplo, seleccionó una carpeta local o de red como origen de actualizaciones y los archivos de actualización de dicha carpeta fueron descargados por alguna de las siguientes aplicaciones:

- Kaspersky Update Utility

  Esta utilidad descarga actualizaciones utilizando el esquema antiguo.

- Kaspersky Security Center 13 Linux

  Suponga, por ejemplo, que un punto de distribución está configurado para tomar las actualizaciones de una carpeta local o de red. En ese caso, puede utilizar un Servidor de administración que tenga conexión a Internet para descargar las actualizaciones y colocar los archivos descargados en la carpeta local del punto de distribución. Si el Servidor de administración es versión 13, habilite la opción **Descargar actualizaciones utilizando el esquema anterior** en la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución*.

Esta opción está deshabilitada de forma predeterminada.

10. Programe la ejecución de la tarea. Si es necesario, configure las siguientes opciones:

- **Iniciar tarea**:

  Manual (esta es la opción seleccionada por defecto)

  La tarea no se ejecutará automáticamente. Solo se la podrá iniciar en forma manual.

  Esta opción está seleccionada de forma predeterminada.

  Cada N minutos

  La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la hora indicada en el día en que se cree la tarea. Cada ejecución estará separada de la anterior por el número de minutos que indique.

  De forma predeterminada, la tarea se ejecutará cada treinta minutos, a partir de la hora actual del sistema.

Cada N horas

La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la fecha y hora indicadas. Cada ejecución estará separada de la anterior por el número de horas que indique.

De manera predeterminada, la tarea se ejecutará cada 6 horas, a partir de la fecha y hora actuales del sistema.

Cada N días

La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta opción permite elegir la fecha y hora de la primera ejecución. Podrá configurar estos dos ajustes si son compatibles con la aplicación para la que esté creando la tarea.

De forma predeterminada, la tarea se ejecutará todos los días, a partir de la fecha y hora actuales del sistema.

Por días de la semana

La tarea se ejecutará periódicamente en los días de la semana y a la hora que indique.

De manera predeterminada, la tarea se ejecutará todos los viernes a las 18:00:00.

Mensual

La tarea se ejecutará periódicamente, en el día del mes y a la hora que indique.

Si el día elegido no forma parte de un mes, la tarea se ejecutará el último día de ese mes.

Por defecto, la tarea se ejecutará el primer día de cada mes, a la hora actual del sistema.

Mensualmente en el día de la semana seleccionado

La tarea se ejecutará periódicamente, en los días del mes y a la hora que indique.

De manera predeterminada, la hora de inicio es a las 18:00 y no se selecciona ningún día del mes.

> Tenga en cuenta que no selecciona una fecha específica en el mes, ni el número de la semana (primera, segunda semana del mes), sino el número de secuencia del día de la semana dentro de un mes. Por ejemplo, si coloca el cursor en la celda **Ma** de la **Primero** fila, significa que la tarea se ejecutará el primer martes de cada mes nuevo.

Puede seleccionar varios días de la semana.

Ante brotes de virus

La tarea se ejecutará cuando ocurra un evento *Brote de virus*. Seleccione los tipos de aplicaciones que se usarán para controlar si ocurre un brote de virus. Están disponibles los siguientes tipos de aplicaciones:

- Antivirus para estaciones de trabajo y servidores de archivos
- Antivirus para defensa del perímetro
- Antivirus para sistemas de correo

Por defecto, están seleccionados todos los tipos de aplicaciones.

En algunos casos, querrá ejecutar tareas diferentes según el tipo de aplicación de seguridad que dé aviso de un brote de virus. De ser así, anule la selección de los tipos de aplicaciones que no necesite.

Al completarse otra tarea

La tarea actual se iniciará después de que se complete otra tarea. Esta opción solo funciona si ambas tareas están asignadas a los mismos dispositivos. Por ejemplo, podría ejecutar la tarea *Administrar dispositivos* con la opción **Encender el dispositivo** y hacer que, una vez completada esa tarea, se ejecute la tarea *Análisis antivirus* como una tarea desencadenante.

Debe seleccionar la tarea desencadenante de la tabla y el estado con el que esta tarea debe completarse (**Completada correctamente** o **Error**).

Si es necesario, puede buscar, ordenar y filtrar las tareas en la tabla de la siguiente manera:

- Ingrese el nombre de la tarea en el campo de búsqueda para buscar la tarea por su nombre.
- Haga clic en el ícono de ordenar para ordenar las tareas por nombre.

  De manera predeterminada, las tareas se clasifican en orden alfabético ascendente.
- Haga clic en el ícono de filtro y, en la ventana que se abre, filtre las tareas por grupo y luego haga clic en el botón **Aplicar**.

- **Ejecutar tareas no realizadas**

  Esta opción determina el comportamiento de la tarea cuando la misma está por iniciarse y uno de los dispositivos cliente no está visible en la red.

  Si esta opción está habilitada, el sistema intentará iniciar la tarea la siguiente vez que la aplicación de Kaspersky se ejecute en el dispositivo cliente. Si la programación de la tarea es **Manual**, **Una vez** o **Inmediatamente**, la tarea se iniciará inmediatamente después de que el dispositivo aparezca en la red o inmediatamente después de que el dispositivo sea incluido en el alcance de la tarea.

  Si esta opción está deshabilitada, solo las tareas programadas se ejecutan en los dispositivos cliente. Para la programación **Manual**, **Una vez** e **Inmediatamente**, las tareas se ejecutan solo en los dispositivos cliente que están visibles en la red. Podría deshabilitar esta opción para, por ejemplo, una tarea que consuma muchos recursos y que solo deba ejecutarse fuera del horario laboral.

  Esta opción está activada de forma predeterminada.

- **Utilizar retardo aleatorio automático para el inicio de la tarea**

  Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo que especifique. Se realizará, de este modo, un *inicio distribuido*. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

  La hora de inicio distribuida se calcula automáticamente cuando se crea una tarea. El cálculo tiene en cuenta el número de dispositivos cliente a los que la tarea está asignada. Las ejecuciones posteriores a la inicial ocurren siempre a la hora de inicio calculada. Sin embargo, tenga en cuenta que si modifica la configuración de la tarea o inicia la tarea manualmente, la hora de inicio calculada cambiará.

  Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

  Esta opción está activada de forma predeterminada.

- **Utilizar el retardo aleatorio automático para el inicio de la tarea dentro de un intervalo de**

  Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo de tiempo especificado. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

  Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

Esta opción está deshabilitada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

11. Haga clic en el botón **Guardar**.

La tarea queda creada y configurada.

Además de los ajustes configurados durante el proceso de creación, la tarea tiene otras propiedades que se pueden modificar.

Cuando se ejecuta la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución*, las actualizaciones para las bases de datos y los módulos de software se descargan del origen de actualizaciones y se almacenan en la carpeta compartida. Las actualizaciones descargadas solo serán utilizadas por los puntos de distribución que formen parte del grupo de administración especificado y que no tengan una tarea de descarga de actualizaciones explícitamente definida para ellos.

Adición de fuentes de actualizaciones para la tarea Descargar actualizaciones al repositorio del Servidor de administración

Cuando crea o utiliza la tarea para descargar actualizaciones al repositorio del Servidor de administración, puede elegir las siguientes fuentes de actualizaciones:

- Servidores de actualizaciones de Kaspersky
- Servidor de administración principal

  Este recurso se aplica a las tareas creadas para un Servidor de administración secundario o virtual.
- Carpeta local o de red

  En la tarea *Descargar actualizaciones al repositorio del Servidor de administración* y *Descargar actualizaciones a los repositorios de los puntos de distribución*, la autenticación de usuario no funciona si selecciona una carpeta local o de red protegida con contraseña como fuente de actualización. Para resolver este problema, primero monte la carpeta protegida con contraseña y luego especifique las credenciales requeridas, por ejemplo, mediante el sistema operativo. Luego, puede seleccionar esta carpeta como fuente de actualización en una tarea de descarga de actualización. Kaspersky Security Center Linux no requerirá que ingrese las credenciales.

Los servidores de actualización de Kaspersky se utilizan de forma predeterminada, pero también puede descargar actualizaciones desde una carpeta local o de red. Es posible que desee utilizar la carpeta si su red no tiene acceso a Internet. En este caso, puede descargar manualmente las actualizaciones de los servidores de actualización de Kaspersky y colocar los archivos descargados en la carpeta necesaria. Puede especificar solo una ruta a una carpeta local o de red.

La carpeta local debe ser una carpeta del dispositivo en el que se encuentra instalado el Servidor de administración. La ruta a la carpeta depende del sistema operativo del dispositivo. Dado que la carpeta local se encuentra en el Servidor de administración basado en Linux, debe especificar la ruta POSIX, por ejemplo: /path/to/dir.

Solo un recurso compartido SMB montado se puede usar como carpeta de red. Si un recurso compartido SMB requiere autenticación, se debe montar en el sistema con las credenciales requeridas de antemano. Recomendamos no utilizar el protocolo SMB1 ya que no es seguro.

Para agregar las fuentes de actualizaciones:

1. En el menú principal, vaya a **Tareas**.
2. Haga clic en **Descargar actualizaciones en el repositorio del Servidor de administración**.
3. Vaya a la pestaña **Configuración de la aplicación**.
4. En la tabla **Orígenes de actualizaciones**, haga clic en el botón **Agregar**.
5. En la ventana que se abre, agregue los orígenes necesarios y luego haga clic en el botón **Guardar**.

   Si selecciona la casilla de verificación **Carpeta local o de red**, especifique una ruta a la carpeta.
6. Haga clic en el botón **Guardar** en la ventana de tarea.

   Ahora las actualizaciones se descargan al repositorio del Servidor de administración desde las fuentes especificadas.

Si agrega los servidores de actualización de Kaspersky y la carpeta local o de red, puede establecer prioridades para las actualizaciones. Para ello, en la tabla **Orígenes de actualizaciones**, seleccione la casilla junto a la actualización sobre la que desee cambiar la prioridad y luego haga clic en el botón **Subir** o **Bajar**.

Aprobar y rechazar actualizaciones de software

Una tarea de instalación de actualizaciones puede estar configurada para requerir la aprobación de las actualizaciones que se deban instalar. Puede aprobar las actualizaciones que deban instalarse y rechazar las que no deban instalarse.

Podría suceder, por ejemplo, que quiera instalar las actualizaciones en un entorno de prueba para verificar primero que no interfieran con el funcionamiento de los dispositivos, y solo entonces, en caso de no haber problemas, permitir que se instalen en los dispositivos cliente.

La posibilidad de aprobar y rechazar actualizaciones solo está disponible para el Agente de red y las aplicaciones administradas instaladas en los dispositivos cliente basados en Windows. No se admite la actualización sin interrupciones del Servidor de administración, Kaspersky Security Center Web Console y los complementos web de administración. Para actualizar estos componentes, debe descargar las últimas versiones desde el sitio web de Kaspersky y realizar la instalación manualmente.

Para aprobar o rechazar una o más actualizaciones:

1. En el menú principal, vaya a **Administración de software → Aplicaciones de Kaspersky → Actualizaciones sin interrupciones**.

   Se mostrará una lista con las actualizaciones disponibles.

Las actualizaciones para las aplicaciones administradas pueden requerir que la versión de Kaspersky Security Center instalada sea posterior a una versión en particular. Si está utilizando una versión anterior a la necesaria, podrá ver estas actualizaciones, pero no las podrá aprobar. Tampoco podrá crear paquetes de instalación a partir de esas actualizaciones hasta que actualice Kaspersky Security Center. Si intenta hacerlo, se le pedirá que actualice su copia de Kaspersky Security Center a la versión mínima requerida.

2. Si es necesario, acepte el EULA haciendo clic en el botón **Ver y aceptar los Contratos de licencia**.
3. Seleccione las actualizaciones que desee aprobar o rechazar.
4. Haga clic en **Aprobar** para aprobar las actualizaciones seleccionadas o en **Rechazar** para rechazarlas.

   El valor predeterminado es *Sin definir*.

Las actualizaciones a las que les asigne el estado *Aprobada* se pondrán en una cola para ser instaladas.

Las actualizaciones a las que les asigne el estado *Rechazada* se desinstalarán (si tal acción es posible) de todos los dispositivos en los que estén instaladas. Estas actualizaciones no se instalarán en otros dispositivos en el futuro.

Existen actualizaciones para las aplicaciones de Kaspersky que no se pueden desinstalar. Si les asigna el estado *Rechazada* para ellas, Kaspersky Security Center Linux no las desinstalará de los dispositivos en los que estén presentes. Sin embargo, se abstendrá de instalarlas en otros dispositivos en el futuro.

Si asigna el estado *Rechazada* a las actualizaciones de software de un tercero, estas no se instalarán en los dispositivos a los que estén asignadas, pero que aún no las hayan recibido. Las actualizaciones no se eliminarán de los dispositivos en los que ya se encuentren instaladas. Si necesita eliminarlas, deberá hacerlo manualmente, en forma local.

Instalación automática de actualizaciones para Kaspersky Endpoint Security para Windows

Puede hacer que las bases de datos y los módulos de software de Kaspersky Endpoint Security para Windows se actualicen automáticamente en los dispositivos cliente.

Para que las actualizaciones de Kaspersky Endpoint Security para Windows se descarguen y se instalen automáticamente en los dispositivos cliente, haga lo siguiente:

1. En el menú principal, vaya a **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Siga los pasos del asistente.
3. Busque la aplicación Kaspersky Endpoint Security para Windows y seleccione **Actualizar** como subtipo de tarea.
4. Escriba un nombre para la tarea que está creando. El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).

5. Elija el alcance de la tarea.

6. Elija el grupo de administración, la selección de dispositivos o los dispositivos a los que se aplicará la tarea.

7. En el paso **Finalizar la creación de la tarea**, si desea modificar la configuración predeterminada de la tarea, habilite la opción **Abrir los detalles de la tarea cuando se complete la creación**. Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Puede cambiar la configuración por defecto más tarde, en cualquier momento.

8. Haga clic en el botón **Crear**.

   Se crea la tarea y se la agrega a la lista de tareas.

9. Haga clic en el nombre de la nueva tarea para abrir la ventana de propiedades de la tarea.

10. En la pestaña **Configuración de la aplicación** de la ventana de propiedades de la tarea, defina la configuración de la tarea de actualización en modo local o modo móvil:

    - **Modo local**: existe una conexión entre el dispositivo y el Servidor de administración.

    - **Modo móvil**: no hay se establece conexión entre el dispositivo y Kaspersky Security Center Linux y el dispositivo (por ejemplo, cuando porque el dispositivo no está conectado a Internet).

11. Habilite los orígenes de actualizaciones que desee usar para actualizar las bases de datos y los módulos de Kaspersky Endpoint Security para Windows. Si es necesario, cambie las posiciones de las fuentes en la lista usando con los botones **Subir** y **Bajar**. Si habilita más de un origen de actualizaciones, Kaspersky Endpoint Security para Windows intentará conectarse a ellos en orden, uno tras otro, comenzando por el primero de la lista. La tarea de actualización descargará el paquete de actualización del primer origen disponible.

12. Habilite la opción **Instalar actualizaciones aprobadas para los módulos de la aplicación** para que, junto con las bases de datos de la aplicación, se descarguen también las actualizaciones para los módulos de software.

    Si habilita esta opción, Kaspersky Endpoint Security para Windows le informará al usuario sobre la disponibilidad de actualizaciones para los módulos de software. Cuando se ejecute la tarea de actualización, estas actualizaciones se incluirán en el paquete de actualización. Kaspersky Endpoint Security para Windows instala solo aquellas actualizaciones para las que estableció *Aprobado* como estado; se instalarán localmente a través de la interfaz de la aplicación o de Kaspersky Security Center Linux.

    También puede habilitar la opción **Instalar automáticamente actualizaciones de módulos críticas**. Cuando haya actualizaciones disponibles para los módulos de software, Kaspersky Endpoint Security para Windows instalará automáticamente las que tengan estado *Crítico*; las demás actualizaciones se instalarán cuando usted las apruebe.

    Para actualizar los módulos de software, podría resultar necesario leer y aceptar los términos del contrato de licencia y la política de privacidad. Cuando este sea el caso, la aplicación esperará a que el usuario acepte los términos de estos documentos y luego instalará las actualizaciones.

13. Marque la casilla **Copiar actualizaciones a la siguiente carpeta** para que la aplicación guarde las actualizaciones descargadas en una carpeta. A continuación, elija la carpeta de destino.

14. Defina una programación para la tarea. Recomendamos seleccionar la opción **Al descargar nuevas actualizaciones al repositorio** de manera que las actualizaciones se instalen sin demora.

15. Haga clic en el botón **Guardar**.

Cuando la tarea **Actualizar** está en ejecución, la aplicación envía solicitudes a los servidores de actualizaciones de Kaspersky.

Algunas actualizaciones requieren que estén instaladas las últimas versiones de los complementos de administración.

Acerca de la utilización de archivos diff para actualizar las bases de datos y los módulos de software de Kaspersky

Cuando Kaspersky Security Center Linux descarga actualizaciones de los servidores de actualización de Kaspersky, optimiza el tráfico mediante el uso de archivos diff. También puede habilitar el uso de archivos diff por dispositivos (Servidores de administración, puntos de distribución y dispositivos cliente) que aceptan actualizaciones de otros dispositivos en su red.

Acerca de la característica de descarga de archivos diff

Un archivo diff describe las diferencias entre dos versiones de un archivo de una base de datos o de un módulo de software. El uso de archivos diff ahorra tráfico dentro de la red de su empresa porque los archivos diff ocupan menos espacio que los archivos completos de bases de datos y módulos de software. Si la función de *descarga de archivos diff* está habilitada en el Servidor de administración o un punto de distribución, los archivos diff se guardan en este Servidor de administración o punto de distribución. Como resultado, los dispositivos que toman actualizaciones de este Servidor de administración o punto de distribución pueden usar los archivos diff guardados para actualizar sus bases de datos y módulos de software.

Para optimizar el uso de los archivos diff, le recomendamos que sincronice el programa de actualización de los dispositivos con el programa de actualización del Servidor de administración o el punto de distribución desde el cual los dispositivos reciben actualizaciones. Sin embargo, el tráfico se puede guardar incluso si los dispositivos se actualizan varias veces con menos frecuencia que el Servidor de administración o el punto de distribución desde el que reciben actualizaciones los dispositivos.

Los puntos de distribución no utilizan la multidifusión IP para la distribución automática de archivos diff.

Habilitación de la función de descarga de archivos diff

Etapas

1. **Habilitar la función en el Servidor de administración**

   Habilite la función en la configuración de una tarea *Descargar las actualizaciones en el repositorio de la tarea del Servidor de administración*.

2. **Habilite la función para un punto de distribución**

   Habilite la función para un punto de distribución que recibe actualizaciones a través de la tarea *Descargar actualizaciones en los repositorios de puntos de distribución*.

A continuación, habilite la función en la configuración de directiva del Agente de red para un punto de distribución que recibe actualizaciones del Servidor de administración.

A continuación, habilite la función para un punto de distribución que recibe actualizaciones del Servidor de administración.

La función está activada en la configuración de directivas del Agente de red y, si los puntos de distribución se asignan manualmente y si desea anular la configuración de directivas, en la sección **Puntos de distribución** de las propiedades del Servidor de administración.

Para verificar que la función de descarga de archivos diff se habilite correctamente, puede medir el tráfico interno antes y después de realizar estos pasos.

Descarga de actualizaciones por puntos de distribución

Kaspersky Security Center Linux permite a los puntos de distribución recibir actualizaciones desde el Servidor de administración, los servidores de Kaspersky o desde una carpeta local o de red.

Para configurar la descarga de actualizaciones para un punto de distribución:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, elija la sección **Puntos de distribución**.

3. Haga clic en el nombre del punto de distribución a través del cual se enviarán las actualizaciones a los dispositivos cliente del grupo.

4. En la ventana de propiedades del punto de distribución, seleccione la sección **Origen de actualizaciones**.

5. Seleccione un origen de actualizaciones para el punto de distribución:

   Origen de actualizaciones

   Seleccione un origen de actualizaciones para el punto de distribución:

   - Seleccione **Recuperar desde el Servidor de administración** para que el punto de distribución pueda recibir actualizaciones del Servidor de administración.

   - Seleccione **Usar una tarea de descarga de actualizaciones** para que el punto de distribución pueda utilizar una tarea para recibir las actualizaciones. A continuación, indique qué tarea *Descargar actualizaciones en los repositorios de los puntos de distribución* se usará:

     - Si la tarea que desea utilizar ya existe en el dispositivo, selecciónela en la lista.

     - Si la tarea aún no existe en el dispositivo, haga clic en el vínculo **Crear tarea** para crearla. Se inicia el Asistente para crear nueva tarea. Siga los pasos del asistente.

   Descargar archivos diff

   Esta opción habilita la función de descarga de archivos diff.

   Esta opción está activada de forma predeterminada.

El punto de distribución recibirá actualizaciones del origen especificado.

Actualizar las bases de datos y los módulos de software de Kaspersky en dispositivos sin conexión

Para que los dispositivos administrados siempre estén protegidos contra virus y otras amenazas, es muy importante mantener al día las bases de datos y los módulos de software de las aplicaciones de Kaspersky instaladas. Los administradores generalmente configuran actualizaciones regulares mediante el uso del repositorio del Servidor de administración.

Cuando necesite una actualización de las bases de datos y los módulos de software en un dispositivo (o un grupo de dispositivos) que no esté conectado al Servidor de administración (principal o secundario), a un punto de distribución o a Internet, tiene que usar fuentes alternativas de actualizaciones, como un servidor FTP o una carpeta local. En ese caso, tendrá que transferir los archivos de las actualizaciones mediante una unidad de memoria, un disco duro externo u otro dispositivo de almacenamiento masivo.

Puede copiar las actualizaciones requeridas desde:

- Servidor de administración.

  Para asegurarse de que el repositorio del Servidor de administración contenga las actualizaciones necesarias para la aplicación de seguridad instalada en un dispositivo sin conexión, al menos uno de los dispositivos en línea administrados debe tener la misma aplicación de seguridad instalada. Esta aplicación debe estar configurada para recibir las actualizaciones desde el repositorio del Servidor de administración a través de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*.

- Cualquier dispositivo que tenga la misma aplicación de seguridad instalada y configurada para recibir las actualizaciones desde el repositorio del Servidor de administración, un repositorio de puntos de distribución o directamente desde los servidores de actualización de Kaspersky.

A continuación se muestra un ejemplo de configuración de actualizaciones de bases de datos y módulos de software al copiarlos desde el repositorio del Servidor de administración.

Para actualizar las bases de datos y los módulos de software de Kaspersky en dispositivos sin conexión:

1. Conecte la unidad extraíble al dispositivo donde está instalado el Servidor de administración.

2. Copie los archivos de las actualizaciones a la unidad extraíble.

   De manera predeterminada, las actualizaciones se encuentran en: /var/opt/kaspersky/klnagent_srv/1093/.working/share_srv/Updates/.

   Como alternativa, puede hacer que Kaspersky Security Center Linux copie periódicamente las actualizaciones a una carpeta de su elección. A estos fines, utilice la opción **Copiar actualizaciones descargadas a carpetas adicionales** que se encuentra en las propiedades de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*. Si elige, como carpeta de destino para esta opción, una carpeta ubicada en una unidad de memoria USB o en un disco duro externo, el dispositivo de almacenamiento masivo siempre contendrá la última versión de las actualizaciones.

3. En los dispositivos sin conexión, configure Kaspersky Endpoint Security de manera tal que las actualizaciones se obtengan de una carpeta local o de un recurso compartido (por ejemplo, una carpeta compartida o un servidor FTP).

Instrucciones:

- Ayuda de Kaspersky Endpoint Security for Linux
- Ayuda de Kaspersky Endpoint Security para Windows

4. Copie los archivos de las actualizaciones de la unidad extraíble a la carpeta local o al recurso compartido que quiera usar como origen de actualizaciones.

5. En el dispositivo sin conexión en el que deban instalarse las actualizaciones, inicie la tarea *Actualizar* de Kaspersky Endpoint Security for Linux o de Kaspersky Endpoint Security para Windows, dependiendo de cuál sea el sistema operativo instalado en el dispositivo sin conexión.

Cuando se complete la tarea de actualización, el dispositivo tendrá las bases de datos y los módulos de software de Kaspersky más recientes.

Supervisión, informes y auditoría

Esta sección describe las capacidades de supervisión e informes de Kaspersky Security Center Linux. Estas prestaciones permiten obtener una visión general de la infraestructura, ver los estados de protección y acceder a información estadística.

Después del despliegue de Kaspersky Security Center Linux o durante la operación, puede configurar las funciones de supervisión e informes para que se adapten mejor a sus necesidades.

Procedimiento: Supervisión y generación de informes

En esta sección se describe un escenario para configurar la característica de supervisión y generación de informes de Kaspersky Security Center Linux.

Requisitos previos

Cuando Kaspersky Security Center Linux se haya implementado en la red de su organización, podrá supervisar su funcionamiento y generar informes al respecto.

El proceso de supervisar la red de una organización y generar informes se divide en etapas:

1. **Configurar cambios de estado para los dispositivos**

   Familiarícese con los ajustes que permiten cambiar el estado de los dispositivos en respuesta a distintas condiciones. Al cambiar estas configuraciones, puede cambiar la cantidad de eventos con niveles de importancia *Crítica* o *Advertencia*. Cuando configure los cambios de estados para los dispositivos, preste especial atención a lo siguiente:

   - La nueva configuración no debe contravenir las políticas de seguridad de datos de su organización.
   - Puede reaccionar a eventos de seguridad importantes en la red de su organización de manera oportuna.

2. **Configurar las notificaciones sobre los eventos que suceden en los dispositivos cliente**

   Instrucciones:

   Configure la notificación (por correo electrónico, SMS o ejecutando un archivo ejecutable) de eventos en dispositivos cliente

3. **Realización de acciones recomendadas para notificaciones críticas, de advertencia e informativas**

   Instrucciones:

   Realizar acciones recomendadas para la red de su organización

4. **Controlar el estado de seguridad de la red de la organización**

Instrucciones:

- Revisión del widget Estado de protección
- Generación y revisión del Informe del estado de la protección
- Genere y revise el Informe de errores

5. **Buscar dispositivos cliente que no se encuentren protegidos**

   Instrucciones:

   - Revise el widget Nuevos dispositivos
   - Genere y revise el Informe del despliegue de la protección

6. **Controlar la protección de los dispositivos cliente**

   Instrucciones:

   - Generación y revisión de informes de las categorías Estado de protección y Estadísticas de amenazas
   - Inicie y revise la selección de eventos Crítico

7. **Evaluar y limitar el impacto de los eventos en la base de datos**

   Se transfiere la información sobre eventos que ocurren durante el funcionamiento de aplicaciones administradas de un dispositivo cliente y se registra en la base de datos del Servidor de administración. Para reducir la carga del Servidor de administración, evalúe y limite la cantidad de eventos que se guardan como máximo en la base de datos.

   Instrucciones:

   - Limitar el número máximo de eventos

8. **Controlar la información de las licencias**

   Instrucciones:

   - Añadir el widget Uso de clave de licencia al panel y revisarlo
   - Genere y revise el Informe de uso de claves de licencia

Resultados

Al concluir este escenario, podrá mantenerse al corriente de la protección de su red y estará en condiciones de planificar medidas de protección adicionales.

Acerca de los tipos de funciones de supervisión y generación de informes

La información sobre eventos de seguridad en la red de una organización se almacena en la base de datos del Servidor de administración. En función de los eventos, Kaspersky Security Center Web Console proporciona los siguientes tipos de monitoreo e informes en la red de su organización:

- Panel
- Informes
- Selecciones de eventos
- Notificaciones

Panel

El panel brinda información gráfica que ayuda a controlar las tendencias de seguridad que se presentan en la red de la organización.

Informes

La función Informes permite obtener información numérica detallada sobre la seguridad de la red de la organización. La información puede guardarse en un archivo, imprimirse o enviarse por correo electrónico.

Selecciones de eventos

Las selecciones de eventos brindan una vista en pantalla de distintos conjuntos de eventos, que se toman de la base de datos del Servidor de administración y se identifican con un nombre. Estos conjuntos de eventos se agrupan y clasifican de distintas maneras:

- Por nivel de importancia: **Eventos críticos**, **Errores funcionales**, **Advertencias** y **Eventos informativos**
- Por fecha: **Eventos recientes**
- Por tipo: **Solicitudes de usuario** y **Eventos de auditoría**

Puede usar los ajustes disponibles en la interfaz de Kaspersky Security Center Web Console para ver y crear selecciones de eventos definidas por el usuario.

Notificaciones

Las notificaciones le alertan acerca de eventos y le ayudan a acelerar sus respuestas a estos eventos mediante la realización de acciones recomendadas o acciones que considere apropiadas.

Activación de reglas en modo Aprendizaje inteligente

Esta sección proporciona información sobre las detecciones realizadas en los dispositivos cliente por las reglas del Control de anomalías adaptativo de Kaspersky Endpoint Security para Windows.

Las reglas detectan y pueden bloquear comportamientos anómalos en los dispositivos cliente. Si las reglas funcionan en el modo Aprendizaje inteligente, detectan un comportamiento anómalo y envían informes sobre cada incidente al Servidor de administración. Puede ver los informes sobre el comportamiento anómalo detectado en **Repositorios → Activación de reglas en el estado Aprendizaje inteligente**. Puede confirmar si las detecciones son válidas o agregarlas como exclusiones para que el tipo de comportamiento deje de considerarse anómalo.

La información sobre las detecciones se almacena en el registro de eventos del Servidor de administración (junto con otros eventos) y en el informe del Control de anomalías adaptativo.

Para obtener más información acerca del Control de anomalías adaptativo, las reglas, sus modos y sus estados, consulte la Ayuda de Kaspersky Endpoint Security para Windows

https://support.kaspersky.com/KESWin/12.12/es-MX/176744.htm
.

Cómo ver y confirmar las detecciones realizadas con las reglas del Control de anomalías adaptativo

Para ver la lista de detecciones realizadas por las reglas del Control de anomalías adaptativo:

1. En el menú principal, vaya a **Repositorios → Activación de reglas en el estado Aprendizaje inteligente**.

   La lista muestra la siguiente información sobre las detecciones realizadas con las reglas del Control de anomalías adaptativo:

   - **Grupo de administración**

     El nombre del grupo de administración al que pertenece el dispositivo.

   - **Servidor de administración virtual**

     Servidor de administración virtual que administra el dispositivo administrado.

   - **Nombre del dispositivo**

     El nombre del dispositivo cliente en el que se aplicó la regla.

   - **Nombre**

     El nombre de la regla que se aplicó.

- **Estado**

  Excluyendo. Este estado indica que el administrador procesó el elemento y lo agregó como exclusión a las reglas. El estado se mantiene hasta la siguiente sincronización del dispositivo cliente con el Servidor de administración; después de la sincronización, el elemento desaparece de la lista.

  Confirmando. Este estado indica que el administrador procesó y confirmó el elemento. El estado se mantiene hasta la siguiente sincronización del dispositivo cliente con el Servidor de administración; después de la sincronización, el elemento desaparece de la lista.

  Si no se muestra ningún valor, el administrador no ha procesado el elemento.

- **Número de detecciones**

  El número de detecciones correspondientes a una regla heurística, un proceso y un dispositivo cliente. Kaspersky Endpoint Security cuenta este número.

- **Nombre de usuario**

  El nombre del usuario del dispositivo cliente que ejecutó el proceso que generó la detección.

- **Ruta del proceso de origen**

  Ruta al proceso de origen, es decir, al proceso que realiza la acción (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

- **Hash del proceso de origen**

  Hash SHA256 del archivo del proceso de origen (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

- **Ruta del objeto de origen**

  Ruta al objeto que inició el proceso (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

- **Hash del objeto de origen**

  Hash SHA256 del archivo de origen (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

- **Ruta del proceso de destino**

  Ruta al proceso de destino (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

- **Hash del proceso de destino**

  Hash SHA256 del archivo de destino (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

- **Ruta del objeto de destino**

  Ruta al objeto de destino (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

- **Hash del objeto de destino**

  Hash SHA256 del archivo de destino (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

- **Procesado**

  Fecha en la que se detectó la anomalía.

Para ver las propiedades de una detección:

1. En el menú principal, vaya a **Repositorios** → **Activación de reglas en el estado Aprendizaje inteligente**.
2. Realice una de las siguientes acciones:
   - En la columna **Nombre**, haga clic en el vínculo con el nombre de la detección que desea ver.
   - En la lista de detecciones, marque la casilla ubicada junto a la detección que desee ver y, luego, haga clic en el botón **Propiedades**.

   Se abre la ventana de propiedades de la detección seleccionada con información sobre ella.

Puede confirmar cualquier detección desde la lista de detecciones de las reglas de Control de anomalías adaptativo o desde la ventana de propiedades de una detección seleccionada.

Para confirmar una detección, siga estos pasos:

- Seleccione una o varias detecciones en la lista y haga clic en el botón **Confirmar**.
- Abra la ventana de propiedades de una detección seleccionada y, luego, haga clic en el botón **Confirmar**.

El estado de la detección cambia a **Confirmando**. La detección desaparece de la lista de detecciones después de la próxima sincronización del dispositivo cliente con el Servidor de administración.

Su confirmación contribuirá a las estadísticas utilizadas por las reglas. Para obtener más información, consulte la Ayuda de Kaspersky Endpoint Security para Windows.

Adición de exclusiones para las reglas del Control de anomalías adaptativo

El asistente Agregar a exclusiones de Control de anomalías adaptativo permite agregar exclusiones a las reglas de Control de anomalías adaptativo para Kaspersky Endpoint Security.

Para agregar exclusiones a las reglas del Control de anomalías adaptativo a través del Asistente, haga lo siguiente:

1. Abra el asistente de una de las siguientes formas:
   - En el menú principal, vaya a **Repositorios** → **Activación de reglas en el estado Aprendizaje inteligente**, seleccione una o varias detecciones y, luego, haga clic en el botón **Excluir**.

     Puede agregar hasta 1000 exclusiones a la vez.

     Antes de agregar una detección a las exclusiones, puede ver las propiedades de la detección si hace clic en el nombre de la detección o en el botón **Propiedades**. En la ventana de propiedades de detección que se abre, también puede hacer clic en el botón **Excluir**.
   - En el menú principal, vaya a **Supervisión** → **Selecciones de eventos**, haga clic en el vínculo con la selección de eventos que necesita, seleccione la casilla junto a la detección que desea excluir y, luego, haga clic en el botón **Excluir del Control de anomalías adaptativo**.

Se inicia el asistente Agregar a exclusiones del Control de anomalías adaptativo. Avance por el asistente utilizando el botón **Siguiente**.

2. Seleccione las directivas y los perfiles en los que desee agregar las exclusiones.

   Las directivas heredadas no se pueden actualizar. Si no tiene los derechos para modificar una directiva, esa directiva no se actualizará.

3. Haga clic en **Listo** para cerrar el asistente.

El estado de la detección cambia a **Excluyendo**. La detección desaparece de la lista de detecciones después de la próxima sincronización del dispositivo cliente con el Servidor de administración. Se configura y aplica la exclusión a las reglas del Control de anomalías adaptativo.

Panel y widgets

En esta sección, se brinda información sobre el panel y sobre los widgets que el panel ofrece. Aquí encontrará instrucciones para administrar los widgets y configurar los ajustes de los widgets.

Uso del panel

El panel brinda información gráfica que ayuda a controlar las tendencias de seguridad que se presentan en la red de la organización.

Para acceder al panel en Kaspersky Security Center Web Console, haga clic en **Panel** en la sección **Supervisión**.

El panel ofrece widgets personalizables. Existe una gran selección de widgets diferentes, presentados en forma de tablas, listas y gráficos de barras, líneas y anillos. La información que se muestra en los widgets se actualiza automáticamente; el período de actualización es de uno a dos minutos. El intervalo entre actualizaciones varía de un widget a otro. Puede actualizar los datos de un widget manualmente en cualquier momento a través del menú de configuración.

De forma predeterminada, los widgets incluyen información sobre todos los eventos almacenados en la base de datos del Servidor de administración.

Kaspersky Security Center Web Console tiene un conjunto predeterminado de widgets de las siguientes categorías:

- **Estado de protección**
- **Despliegue**
- **Actualización**
- **Estadísticas de amenazas**
- **Otros**

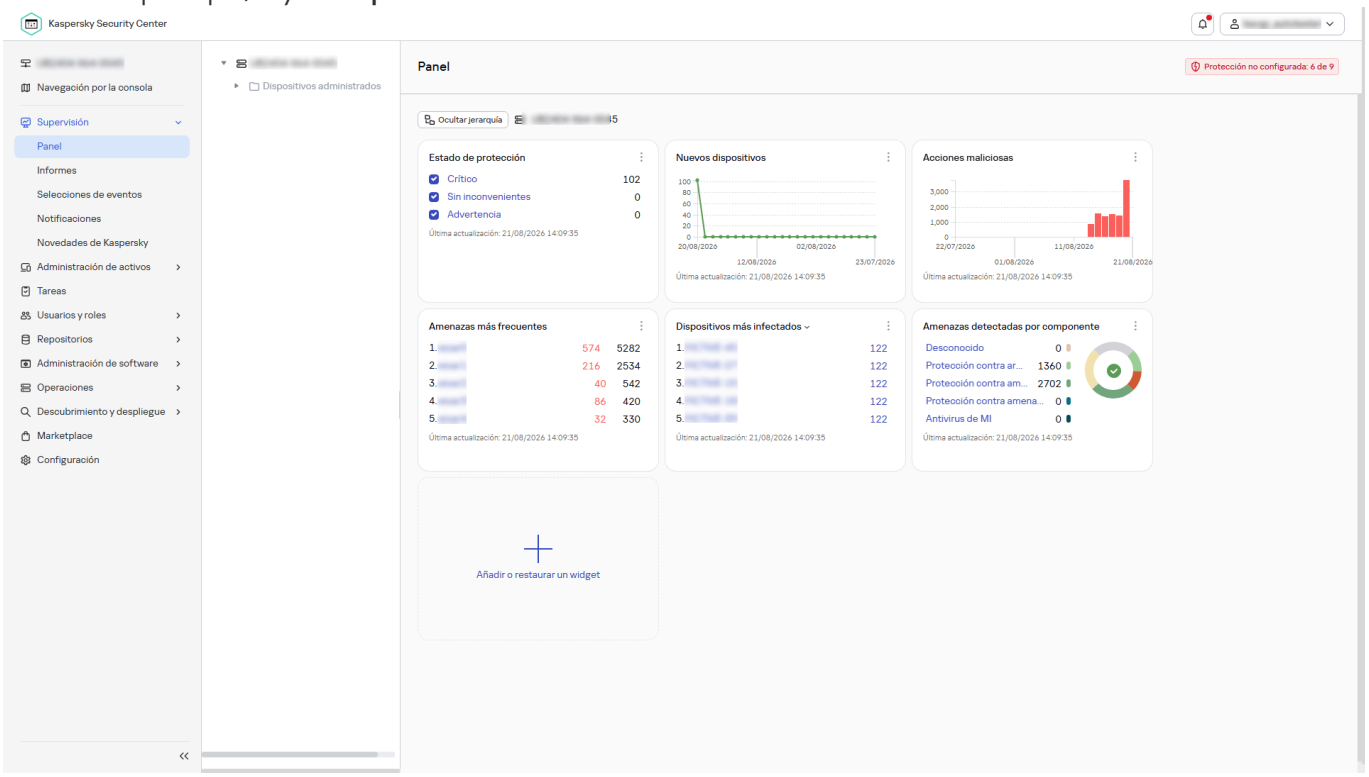
Algunos widgets tienen información de texto con vínculos. Puede ver información detallada haciendo clic en el vínculo.

Al configurar el panel, puede agregar los widgets que le resulten necesarios, ocultar los widgets que no precise, cambiar el tamaño o el aspecto de los widgets, mover los widgets y cambiar la configuración de los widgets.

Agregar widgets al panel

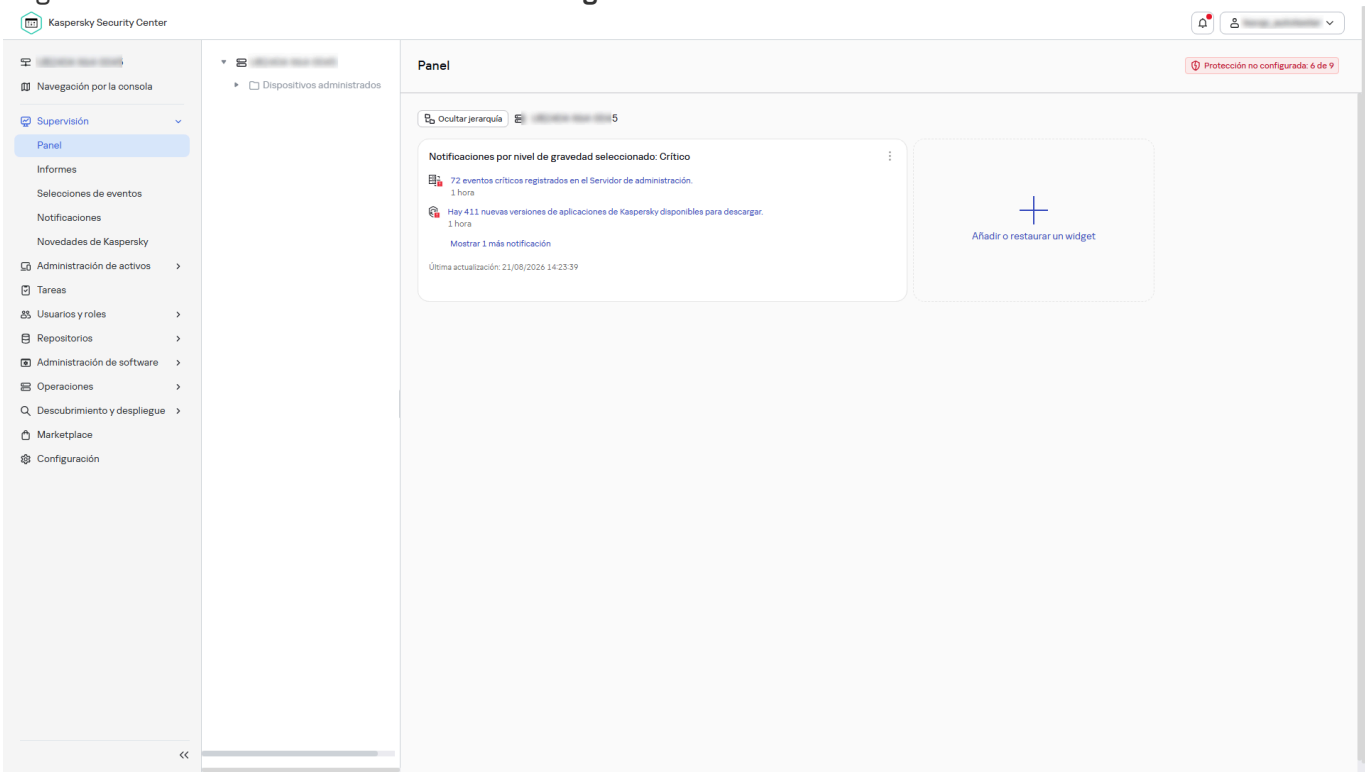
Para agregar widgets al panel:

1. En el menú principal, vaya a **Supervisión** → **Panel**.



El panel con widgets

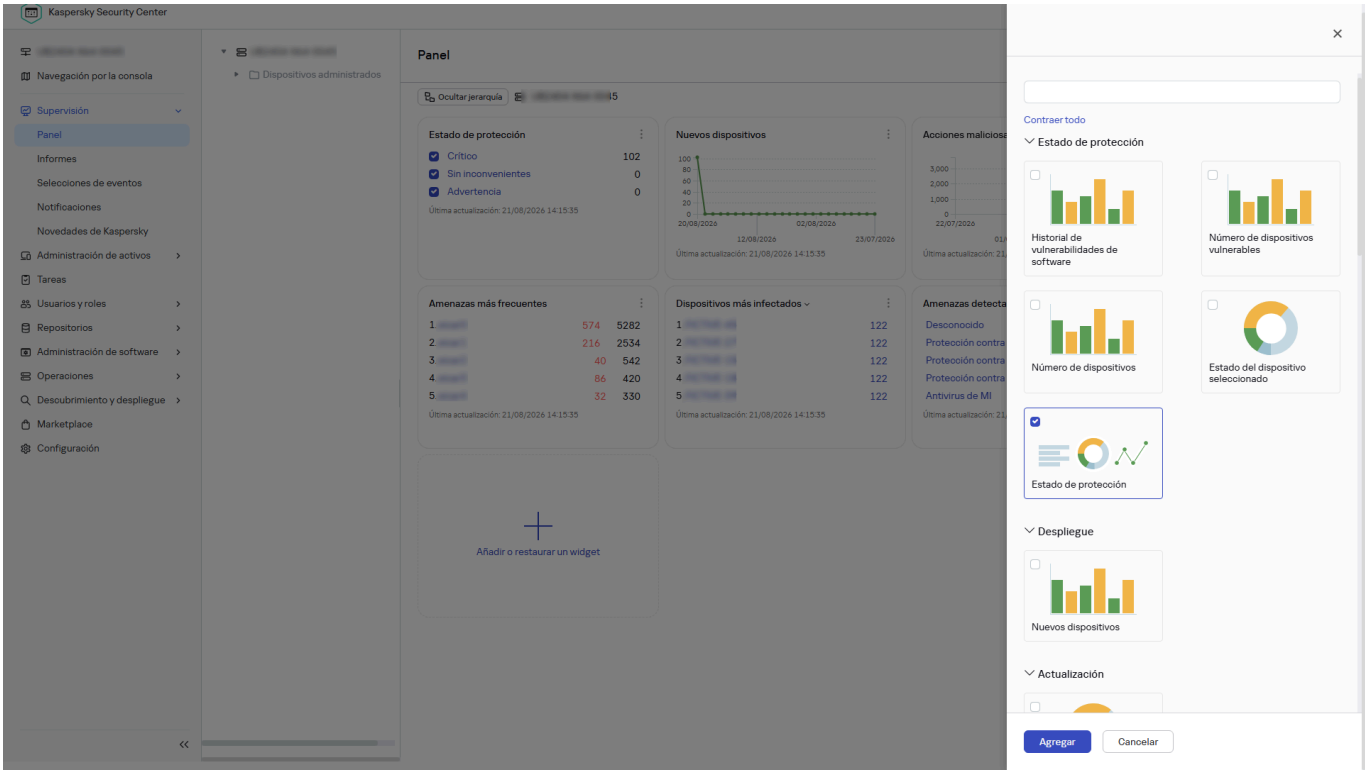
2. Haga clic en el botón **Añadir o restaurar un widget**.



Agregar un widget

3. En la lista de widgets disponibles, seleccione los widgets que desee agregar al panel.

   Los widgets se agrupan por categoría. Para ver los widgets que forman parte de una categoría, haga clic en el corchete angular (>) ubicado junto al nombre de la categoría en cuestión.



Seleccionar el tipo de widget

4. Haga clic en **Agregar**.

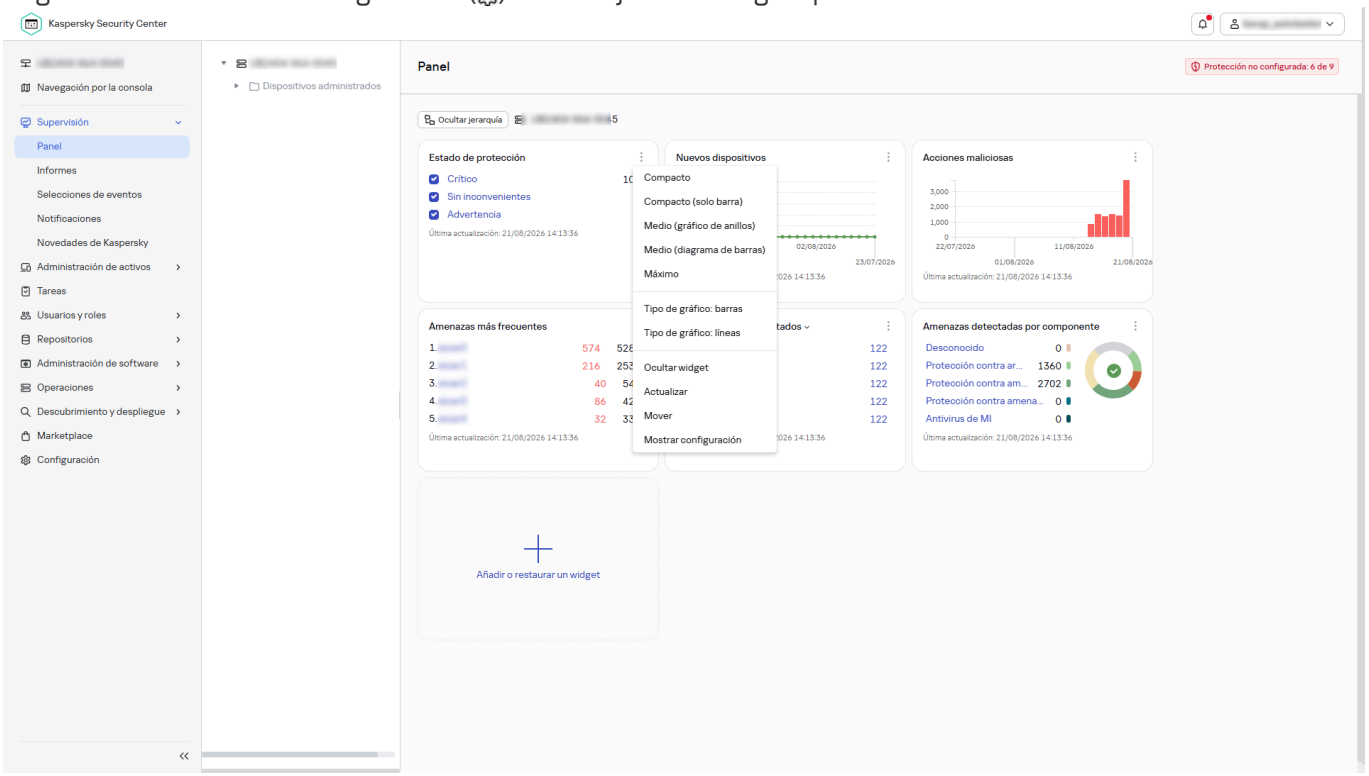
Los widgets seleccionados se agregan al final del panel.

Si lo desea, puede modificar el aspecto y la configuración de los widgets agregados.

Ocultar un widget del panel

Para ocultar uno de los widgets que se muestran en el panel:

1. En el menú principal, vaya a **Supervisión** → **Panel**.
2. Haga clic en el ícono de configuración (⚙) ubicado junto al widget que desee ocultar.



El menú del widget

3. Seleccione **Ocultar widget**.
4. En la ventana **Advertencia** que se abre, haga clic en **Aceptar**.

Se oculta el widget seleccionado. Más tarde, podrá agregar el widget al panel nuevamente.

Mover un widget en el panel

Para mover un widget en el panel:

1. En el menú principal, vaya a **Supervisión** → **Panel**.
2. Haga clic en el ícono de configuración (⚙) ubicado junto al widget que desee mover.

3. Seleccione **Mover**.

4. Haga clic en la ubicación a la que desee mover el widget. Solo puede seleccionar una ubicación que se encuentre ocupada por otro widget.

Los widgets cambiarán de ubicación recíprocamente.

Cambiar el aspecto o el tamaño de un widget

Puede modificar el aspecto de los widgets que contienen un gráfico y hacer que muestren un gráfico de barras o un gráfico de líneas. Algunos widgets también están disponibles en distintos tamaños (compacto, medio y máximo) y pueden redimensionarse.

Para cambiar el aspecto de un widget:

1. En el menú principal, vaya a **Supervisión** → **Panel**.

2. Haga clic en el ícono de configuración (⚙) ubicado junto al widget que desee modificar.

3. Realice una de las siguientes acciones:

   - Para que el widget se muestre como gráfico de barras, seleccione **Tipo de gráfico: barras**.
   - Para que el widget se muestre como gráfico de líneas, seleccione **Tipo de gráfico: líneas**.
   - Para cambiar el área ocupada por el widget, seleccione uno de los siguientes valores:
     - **Compacto**
     - **Compacto (solo barra)**
     - **Medio (gráfico de anillos)**
     - **Medio (diagrama de barras)**
     - **Máximo**

El widget seleccionado toma el nuevo aspecto.

Cambiar la configuración de un widget

Para modificar la configuración de un widget:

1. En el menú principal, vaya a **Supervisión** → **Panel**.

2. Haga clic en el ícono de configuración (⚙) ubicado junto al widget que desee modificar.

3. Seleccione **Mostrar configuración**.

4. En la ventana de configuración del widget, haga los cambios que desee en los ajustes del widget.

5. Haga clic en **Guardar** para guardar los cambios.

Se modifican los ajustes del widget seleccionado.

El conjunto de ajustes disponibles varía según el widget. Estos son algunos de los ajustes comunes:

- **Alcance del widget** (conjunto de objetos de los que muestra la información el widget): por ejemplo, un grupo de administración o selección de dispositivos.
- **Elija una tarea** define la tarea de la que el widget muestra información.
- **Intervalo de tiempo** (el intervalo de tiempo durante el cual se muestra la información en el widget): entre las dos fechas especificadas; desde la fecha especificada hasta el día actual; o desde el día actual menos el número especificado de días hasta el día actual.
- Las reglas **Establecer en Crítico si se especifica la siguiente configuración** y **Establecer en Advertencia si se especifica la siguiente configuración** determinan cómo se asignan los colores en el gráfico de estado.

Después de cambiar la configuración del widget, puede actualizar los datos en el widget manualmente.

Para actualizar datos en un widget:

1. En el menú principal, vaya a **Supervisión → Panel**.
2. Haga clic en el ícono de configuración (⚙) ubicado junto al widget que desee mover.
3. Seleccione **Actualizar**.

Se actualizan los datos del widget.

Acerca del modo solo panel

Puede configurar el modo "sólo Panel" para aquellos empleados que, sin ser responsables por la administración de la red, desean ver información estadística sobre la protección de la red en Kaspersky Security Center Linux. Esta información podría resultar de interés para un alto ejecutivo, por ejemplo. Un usuario para el que se habilitado el modo solo panel tiene acceso únicamente a un panel con un conjunto de widgets predefinido. La persona puede monitorear las estadísticas que brinda cada widget (por ejemplo, el estado de protección de los dispositivos administrados, la cantidad de amenazas detectadas en tiempo reciente o la lista de amenazas más frecuentes en la red).

Un usuario para el que se habilitado el modo solo panel está sujeto a las siguientes restricciones:

- El usuario no tiene acceso al menú principal, lo cual le impide modificar los ajustes de protección de la red.
- El usuario no puede realizar ninguna acción con los widgets: no puede, por ejemplo, agregar widgets nuevos ni quitar los widgets agregados. Debido a estas restricciones, usted deberá agregar al panel todos los widgets que el usuario precise y deberá encargarse, asimismo, de configurarlos (tendrá que fijar la regla de conteo de objetos, definir el intervalo de tiempo, etc.).

Un usuario no puede asignarse a sí mismo el modo solo panel. Si desea trabajar en este modo, comuníquese con su administrador de sistemas, con su proveedor de servicios administrados (MSP) o con un usuario que tenga el derecho **Modificar ACL de objetos** en el área funcional **Características generales: Permisos de usuario**.

Configuración del modo solo panel

Si desea configurar el modo solo panel, asegúrese primero de que se cumplan los siguientes requisitos:

- Usted cuenta con el derecho **Modificar ACL de objetos** en el área funcional **Características generales: Permisos de usuario**. Si no tiene este derecho, no encontrará la pestaña para configurar el modo.
- El usuario tiene asignado el derecho Leer en el área funcional **Características generales**: **Funcionalidad básica**.

> Si creó una jerarquía de Servidores de administración en su red, para configurar el modo solo panel, vaya al Servidor que tenga disponible la cuenta de usuario en la pestaña **Usuarios** de la sección **Usuarios y roles** → **Usuarios y grupos**. Puede ser un Servidor principal o un Servidor secundario físico. Este modo no puede ajustarse en servidores virtuales.

Para configurar el modo solo panel:

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos** y luego seleccione la pestaña **Usuarios**.
2. Haga clic en el nombre de la cuenta de usuario para la que desee ajustar el panel con widgets.
3. En la ventana que se abre, que contendrá los ajustes de la cuenta, seleccione la pestaña **Panel**.

   En la pestaña que se abre, verá un panel. El panel será el mismo panel para usted que para el usuario.
4. Si la opción **Mostrar la consola en modo solo panel** está habilitada, cambie la posición del interruptor para deshabilitarla.

   El sistema no le permitirá hacer cambios en el panel mientras esta opción se encuentre habilitada. Una vez que deshabilite esta opción, podrá operar con los widgets.
5. Configure la apariencia del panel. El conjunto de widgets preparados en la pestaña **Panel** estará disponible para el usuario con la cuenta personalizable. El usuario no podrá agregar widgets nuevos al panel ni podrá quitar los widgets agregados; tampoco podrá modificar los ajustes o el tamaño de estos elementos. Debido a estas limitaciones, debe ocuparse usted de ajustar los widgets de manera tal que el usuario tenga acceso a las estadísticas sobre la protección de la red. Para ello, en la pestaña **Panel**, puede realizar con los widgets las mismas acciones que en la sección **Supervisión** → **Panel**:
   - Agregar nuevos widgets al panel.
   - Ocultar widgets que el usuario no necesite.
   - Mover los widgets y colocarlos en otro orden.
   - Cambiar el tamaño o el aspecto de los widgets.
   - Modificar los ajustes de los widgets.
6. Active el interruptor para habilitar la opción **Mostrar la consola en modo solo panel**.

   Una vez que habilite esta opción, el usuario solamente tendrá acceso al panel. Podrá ver las estadísticas, pero no podrá hacer cambios en los ajustes de protección de la red ni podrá modificar el aspecto del panel. Como el panel es el mismo para usted que para el usuario, usted tampoco podrá hacer ajustes en el panel.

Si deja esta opción deshabilitada, el usuario tendrá acceso al menú principal y, desde allí, podrá realizar distintas acciones en Kaspersky Security Center Linux, como modificar los widgets y cambiar los ajustes de seguridad.

7. Haga clic en el botón **Guardar** cuando haya terminado de configurar el modo solo panel. El usuario no verá el panel preparado sino hasta que usted guarde los cambios.

8. Si el usuario desea ver las estadísticas de las aplicaciones de Kaspersky compatibles y necesita, para ello, contar con determinados derechos de acceso, configure los derechos del usuario. Tras ello, el usuario verá los datos de las aplicaciones de Kaspersky en los widgets correspondientes a esas aplicaciones.

Al concluir este procedimiento, el usuario podrá iniciar sesión en Kaspersky Security Center Linux con su cuenta personalizada y utilizar el modo "sólo Panel" para monitorear las estadísticas de protección de la red.

Informes de administración y protección

En esta sección, se brindan instrucciones para trabajar con los informes, administrar plantillas de informes personalizadas, usar plantillas de informes para generar nuevos informes y crear tareas de entrega de informes.

Utilización de informes

La función Informes permite obtener información numérica detallada sobre la seguridad de la red de la organización. La información puede guardarse en un archivo, imprimirse o enviarse por correo electrónico.

Para acceder a los informes en Kaspersky Security Center Web Console, ingrese a la sección **Supervisión** y haga clic en **Informes**.

Por defecto, los informes contienen información de los últimos treinta días.

Kaspersky Security Center Linux tiene un conjunto predeterminado de informes de las siguientes categorías:

- **Estado de protección**
- **Despliegue**
- **Actualización**
- **Estadísticas de amenazas**
- **Otros**

Puede crear plantillas de informe personalizadas y modificar o eliminar las plantillas de informe existentes.

Puede crear informes basados en las plantillas existentes, exportar informes a archivos y crear tareas de entrega de informes.

Creando una plantilla de informe

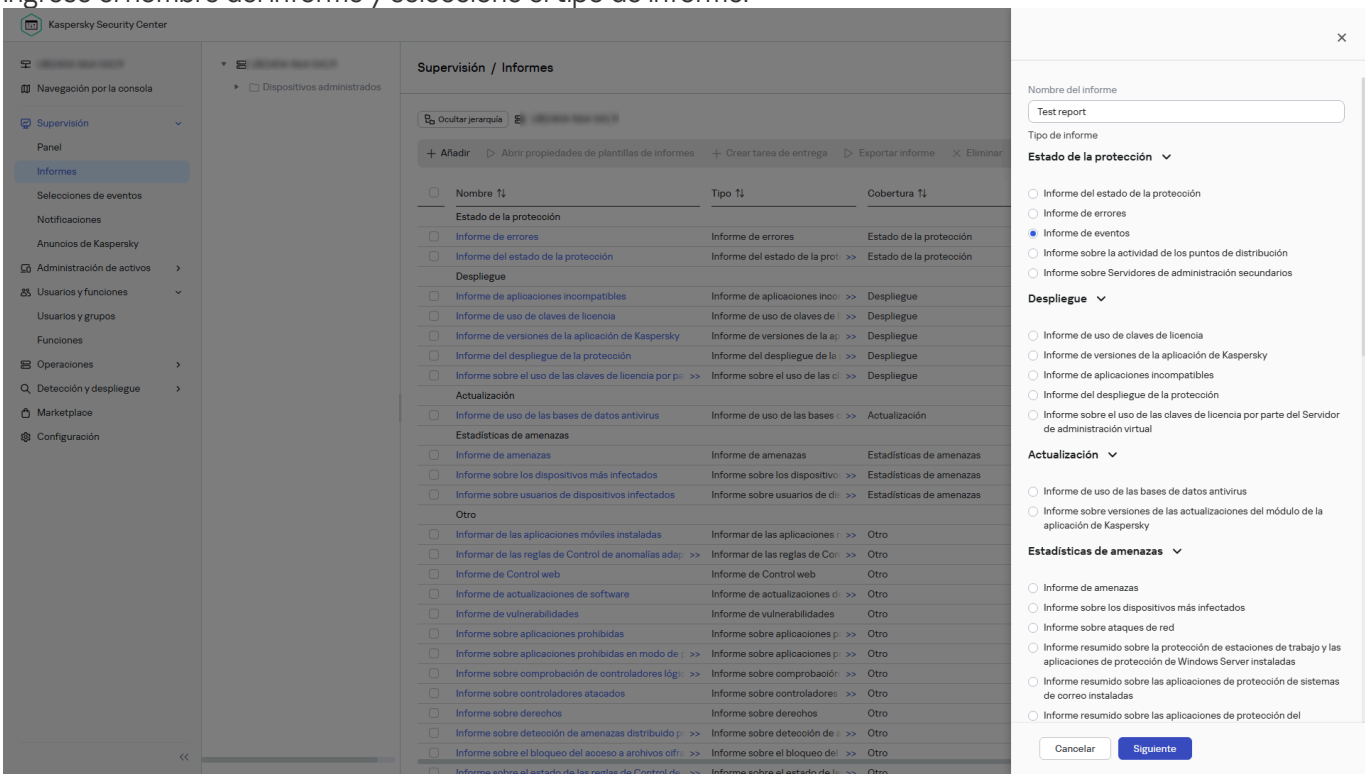
Para crear una plantilla de informe:

1. En el menú principal, vaya a **Supervisión** → **Informes**.

2. Haga clic en **Agregar**.

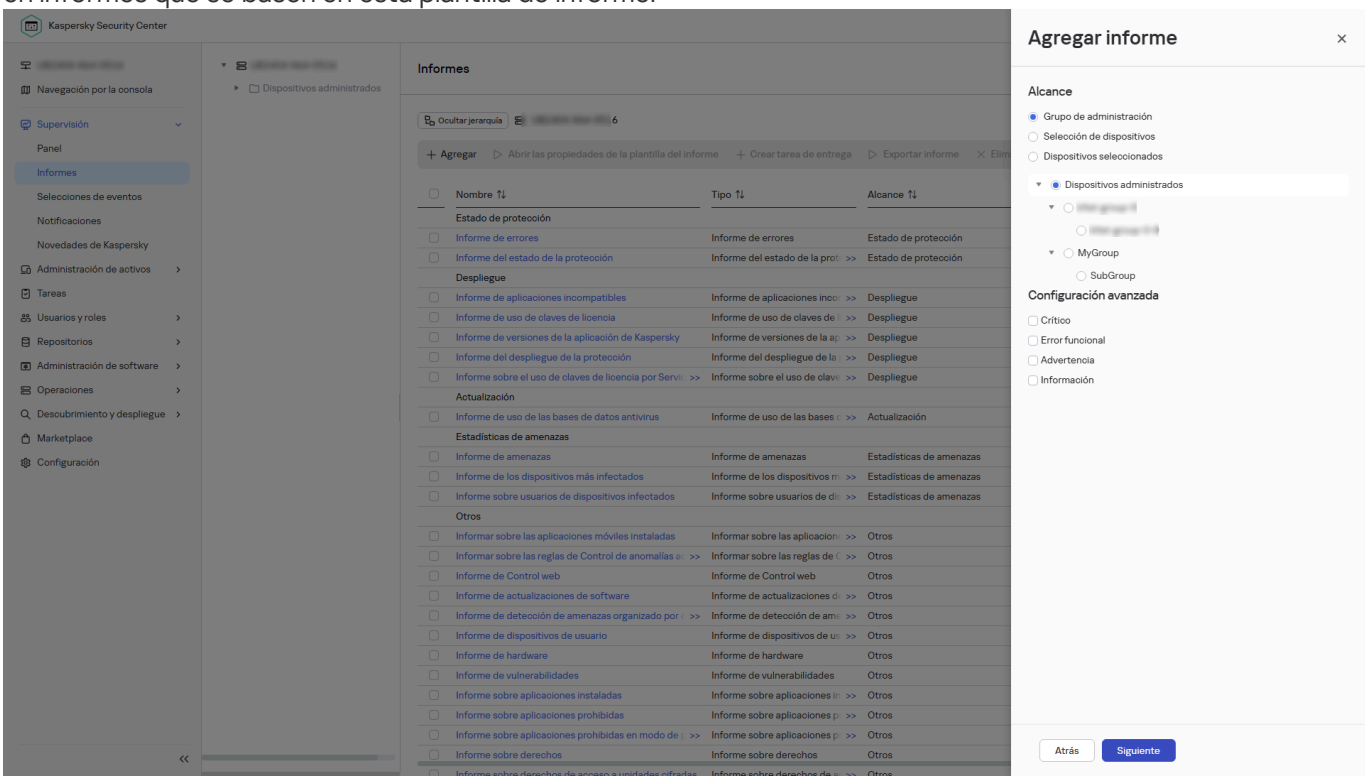
   Se abre el Asistente de nueva plantilla de informe. Avance por el asistente utilizando el botón **Siguiente**.

3. Ingrese el nombre del informe y seleccione el tipo de informe.



Especificar el nombre del informe y seleccionar el tipo de informe

4. En el paso **Alcance** del asistente, seleccione el conjunto de dispositivos cliente (grupo de administración, selección de dispositivos, dispositivos seleccionados o todos los dispositivos de red) cuyos datos se mostrarán en informes que se basen en esta plantilla de informe.

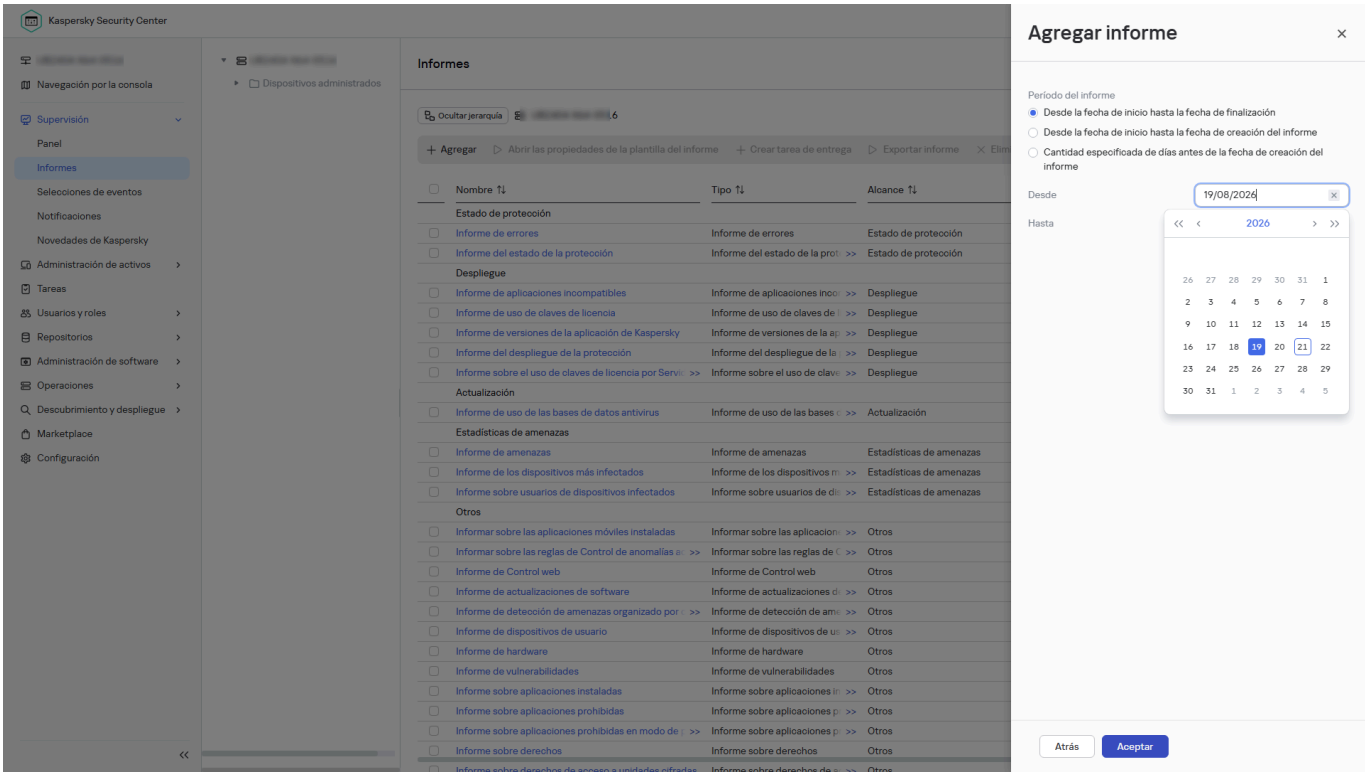


Especificar el alcance del informe

5. En el paso **Período del informe**, especifique el período del informe. Valores disponibles:

   - Entre dos fechas específicas
   - Desde una fecha específica hasta la fecha de creación del informe
   - Desde cierta cantidad de días antes de la creación del informe hasta la fecha de creación del informe

Esta página puede no aparecer para algunos informes.



Especificación del período del informe

6. Haga clic en **Aceptar** para cerrar el asistente.

7. Realice una de las siguientes acciones:

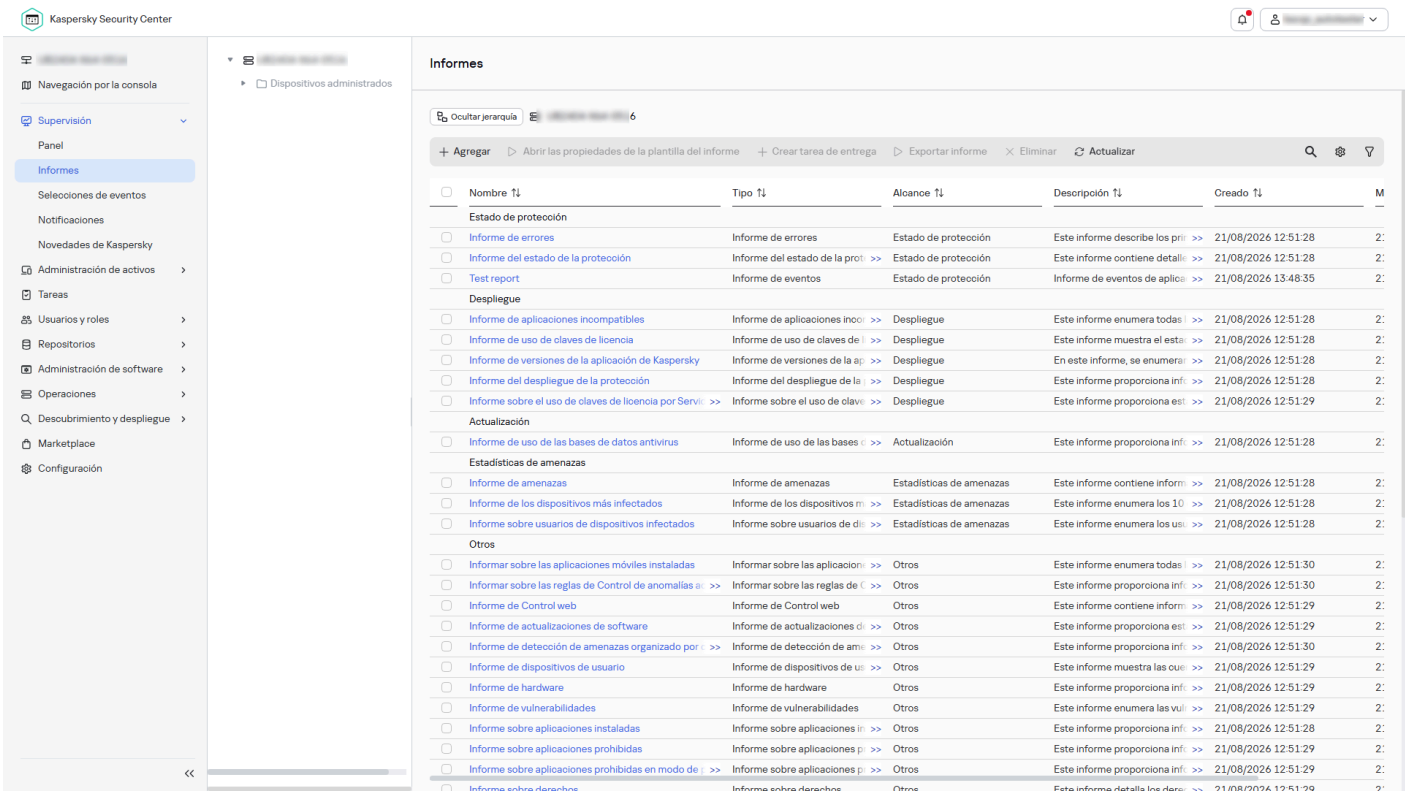
   - Haga clic en el botón **Guardar y ejecutar** para guardar la nueva plantilla de informe y crear un informe basado en ella.

     Se guardará la plantilla de informe. Se generará el informe.

   - Haga clic en el botón **Guardar** para guardar la nueva plantilla de informe.

     Se guardará la plantilla de informe.

Puede utilizar la nueva plantilla para generar y ver informes.



La lista de informes

Ver y editar las propiedades de una plantilla de informe

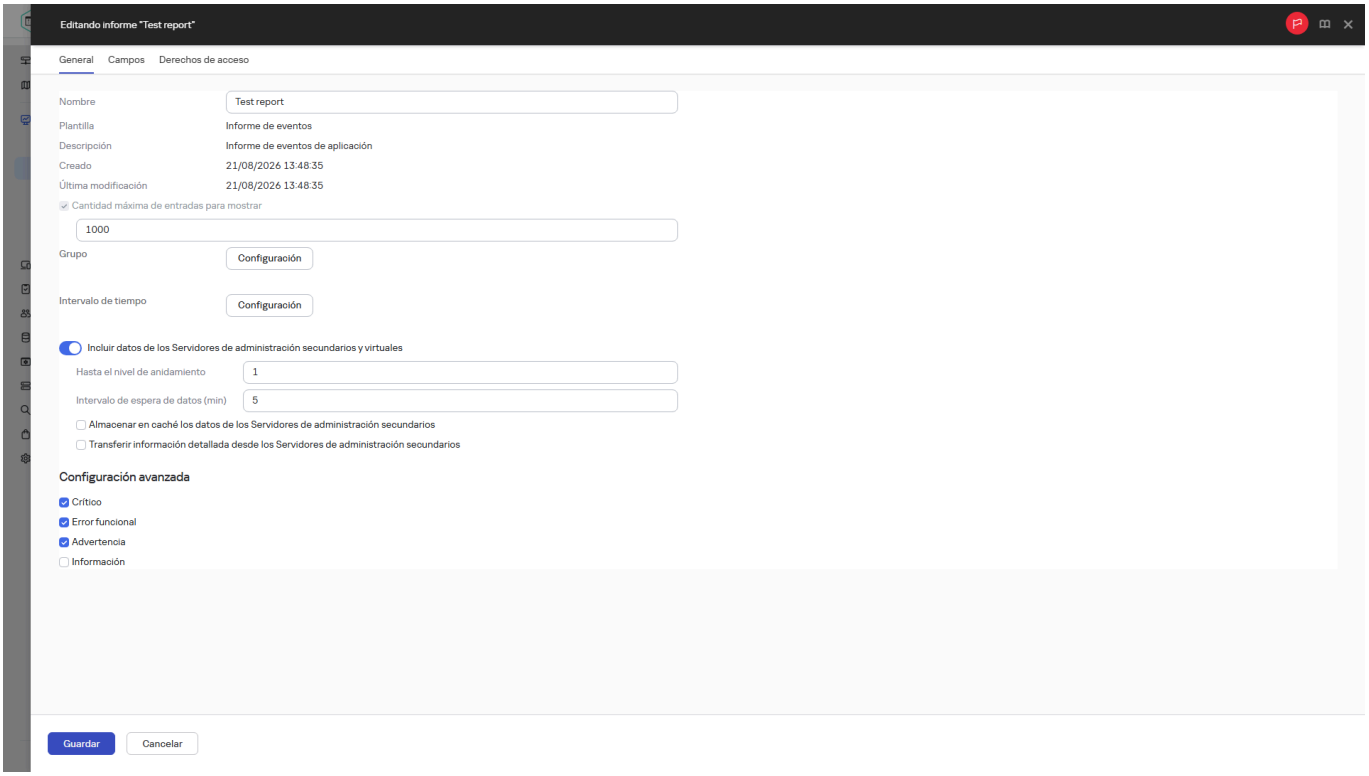
Puede ver y editar las propiedades básicas de las plantillas de informe (por ejemplo, el nombre de las plantillas o los campos que se muestran en los informes).

Para ver y editar las propiedades de una plantilla de informe:

1. En el menú principal, vaya a **Supervisión** → **Informes**.
2. Marque la casilla ubicada junto a la plantilla de informe cuyas propiedades desee ver o editar.

   Como alternativa, genere un informe y luego haga clic en el botón **Editar**.
3. Haga clic en el botón **Abrir las propiedades de la plantilla del informe**.

Se abre la ventana **Editando informe "<nombre del informe>"**. La pestaña **General** estará seleccionada.



Las propiedades de la plantilla de informe

4. Modifique las propiedades de la plantilla de informe:

   - Pestaña **General**:

     - Nombre de la plantilla de informe

     - **Cantidad máxima de entradas para mostrar**

       Si esta opción está habilitada, la tabla con los datos detallados del informe mostrará, como máximo, el número de entradas indicado aquí. Tenga en cuenta que esta opción no afecta el número máximo de eventos que se pueden incluir en el informe si se lo exporta un archivo.

       Las entradas del informe se ordenan primero siguiendo las reglas especificadas en la sección **Campos → Campos Detalles** de las propiedades de la plantilla de informe, y luego se conservan solo las primeras de las entradas resultantes. El encabezado de la tabla con los datos detallados del informe indica el número de entradas mostradas y el total de entradas disponibles que coinciden con otros parámetros de la plantilla del informe.

       Si deshabilita esta opción, se mostrarán todas las entradas disponibles en la tabla con los datos detallados del informe. No recomendamos deshabilitar esta opción. Al limitar el número de entradas que se muestran en un informe, se aminora la carga en el sistema de administración de bases de datos y se reduce el tiempo requerido para generar y exportar el informe. Algunos de los informes contienen demasiadas entradas. En tales casos, no es sencillo leer y analizar todas las entradas. Además, el dispositivo puede quedarse sin memoria al generar dicho informe. Esto puede impedirle ver el informe.

       Esta opción está activada de forma predeterminada. El valor predeterminado es 1000.

     - **Grupo**

       Haga clic en el botón **Configuración** para cambiar el conjunto de dispositivos cliente para los que se crea el informe. Este botón puede no estar disponible para algunos tipos de informes. La configuración aplicada depende de la configuración especificada durante la creación de la plantilla de informe.

     - **Intervalo de tiempo**

Haga clic en el botón **Configuración** para modificar el período comprendido por el informe. Este botón puede no estar disponible para algunos tipos de informes. Valores disponibles:

- Entre dos fechas específicas
- Desde una fecha específica hasta la fecha de creación del informe
- Desde cierta cantidad de días antes de la creación del informe hasta la fecha de creación del informe

- **Incluir datos de los Servidores de administración secundarios y virtuales**

  Cuando esta opción se encuentra habilitada, el informe incluye información de los servidores de administración secundarios y virtuales que están subordinados al Servidor de administración para el cual se ha creado la plantilla de informe.

  Deshabilite esta opción si solo desea ver datos del Servidor de administración con el que está trabajando.

  Esta opción está activada de forma predeterminada.

- **Hasta el nivel de anidamiento**

  El informe incluirá datos de los servidores de administración secundarios y virtuales que se encuentren <n> o más niveles de anidamiento por debajo del Servidor de administración con el que se esté trabajando, siendo <n> el valor especificado.

  El valor predeterminado es 1. Puede cambiar este valor si necesita recuperar información de servidores de administración secundarios que se encuentren aún más abajo en el árbol.

- **Intervalo de espera de datos (min)**

  Antes de generar el informe, el Servidor de administración para el que se haya creado la plantilla de informe esperará, durante el tiempo especificado, a que los servidores de administración secundarios le envíen datos. Transcurrido este período de espera, el Servidor generará el informe aunque no haya recibido información de los servidores de administración secundarios. En ese caso, en lugar de los datos reales, el informe mostrará el valor **N/D** (no disponible) o, si la opción **Almacenar en caché los datos de los Servidores de administración secundarios** está habilitada, mostrará información tomada de la caché.

  El valor predeterminado es 5 minutos.

- **Almacenar en caché los datos de los Servidores de administración secundarios**

  Los servidores de administración secundarios transfieren datos periódicamente al Servidor de administración para el que se ha creado la plantilla de informe. Una vez allí, los datos transferidos se guardan en una caché.

  Si, al momento de generar un informe, el Servidor de administración no puede recibir datos de algún Servidor de administración secundario, el informe contendrá los datos de esta caché. La fecha en que los datos se transfirieron a la caché estará indicada en el informe.

  Si habilita esta opción, podrá ver datos de los servidores de administración secundarios incluso cuando no se pueda obtener información actualizada. Sin embargo, los datos mostrados podrían ser obsoletos.

  Esta opción está deshabilitada de forma predeterminada.

- **Frecuencia de actualización de la caché (h)**

  Los servidores de administración secundarios transfieren datos periódicamente al Servidor de administración para el que se ha creado la plantilla de informe. Puede especificar el largo de este intervalo en horas. Si fija el valor en 0 horas, solamente se transferirá información cuando se genere el informe.

El valor predeterminado es 0.

- **Transferir información detallada desde los Servidores de administración secundarios**

  En el informe generado, la tabla con los datos detallados del informe contendrá datos de los servidores de administración secundarios que estén subordinados al Servidor de administración para el cual se haya creado la plantilla de informe.

  Si habilita esta opción, los informes tardarán más tiempo en generarse y habrá más tráfico entre los servidores de administración. Sin embargo, podrá ver toda la información en un solo informe.

  En lugar de habilitar esta opción, podría analizar los datos detallados de un informe para detectar un Servidor de administración secundario con problemas y, hecho esto, generar ese mismo informe únicamente para ese Servidor de administración.

  Esta opción está deshabilitada de forma predeterminada.

- Pestaña **Campos**

  Seleccione los campos que desea que se muestren en el informe. Use los botones **Subir** y **Bajar** para cambiar el orden en que se muestran los campos. Use los botones **Agregar** o **Editar** para especificar si los campos se usarán para filtrar y ordenar los datos del informe.

  La sección **Filtros de los campos Detalles** contiene un botón llamado **Convertir filtros**. Haga clic en este botón para comenzar a usar el formato de filtrado ampliado. Este formato permite combinar, mediante la operación lógica OR, las condiciones de filtrado especificadas en distintos campos. Si hace clic en el botón, se abrirá el panel **Convertir filtros** en el lado derecho. Haga clic en el botón **Convertir filtros** para confirmar la conversión. Tras ello, podrá definir un filtro convertido con condiciones de la sección **Campos Detalles** que se apliquen utilizando la operación lógica OR.

  > Cuando un informe se convierte al formato que permite definir condiciones de filtrado complejas, el mismo deja de ser compatible con las versiones anteriores de Kaspersky Security Center (11 y anteriores). Los informes convertidos no incluyen datos de servidores de administración secundarios basados en versiones incompatibles.

5. Haga clic en **Guardar** para guardar los cambios.
6. Cierra la ventana **Editando informe "<nombre del informe>"**.

La plantilla de informe actualizada aparece en la lista de plantillas de informe.

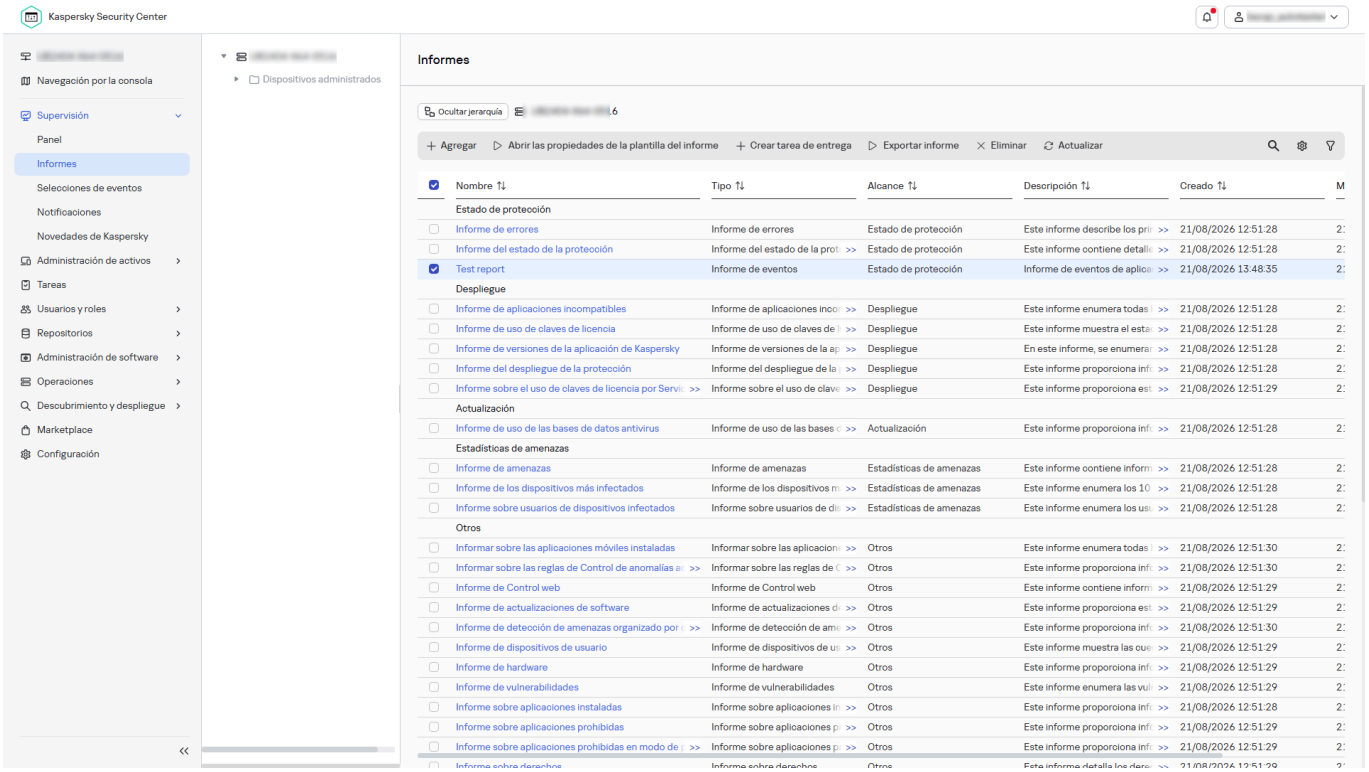
Exportación de un informe a un archivo

Puede guardar uno o varios informes en los formatos XML, HTML y PDF. Kaspersky Security Center Linux permite exportar hasta diez informes por vez a archivos de estos formatos.

Para exportar un informe a un archivo:

1. En el menú principal, vaya a **Supervisión → Informes**.
2. Elija los informes que desee exportar.

Si selecciona más de 10 informes, el botón **Exportar informe** se deshabilitará.



La lista de informes

3. Haga clic en el botón **Exportar informe**.

4. En la ventana que se abrirá, defina los siguientes parámetros de exportación:

   - **Nombre de archivo**.

     Si seleccionó un único informe para exportar, ingrese el nombre que desee dar al archivo del informe.

     Si seleccionó más de un informe, el nombre de cada archivo será el de la plantilla con la que se haya generado el informe seleccionado.

   - **Número máximo de entradas**.

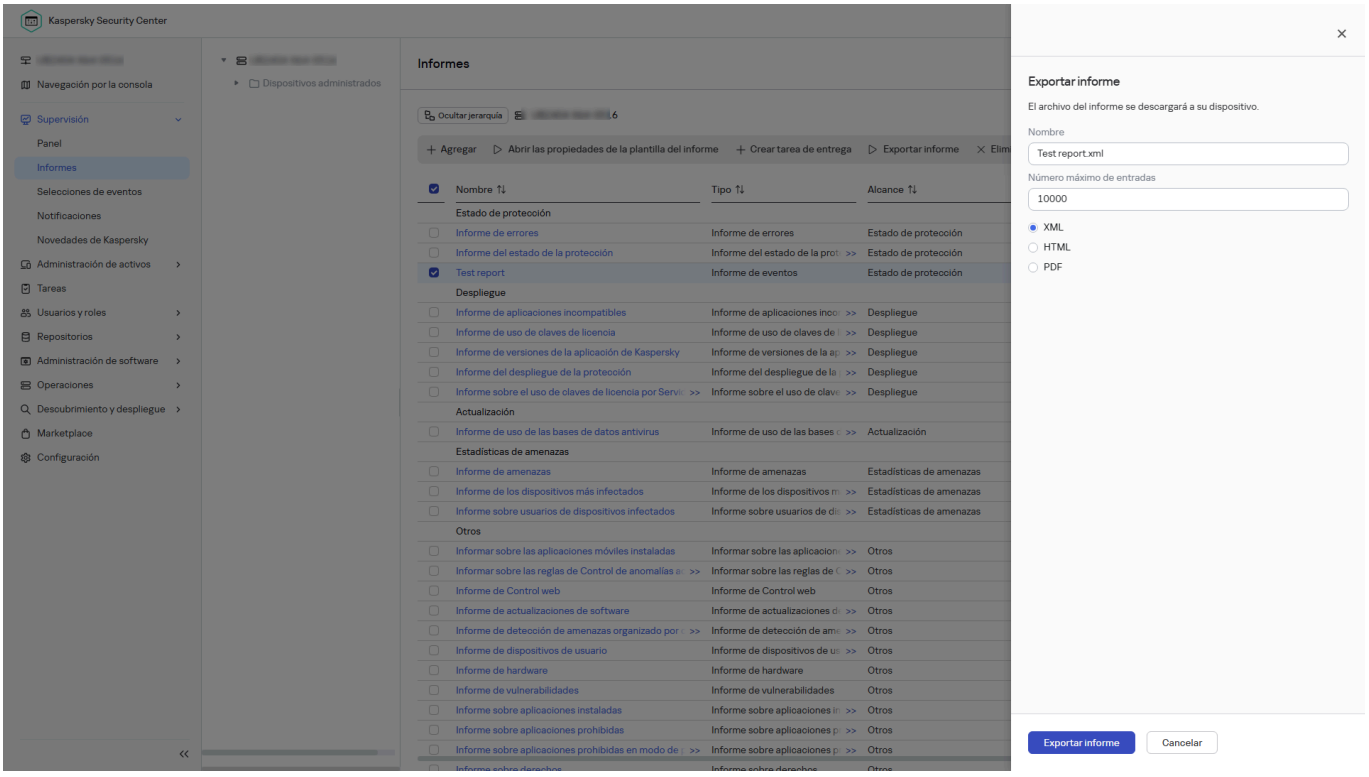
     Especifique el número máximo de entradas incluidas en el archivo del informe. El valor predeterminado es 10000.

     Puede exportar un informe con un número ilimitado de entradas. Tenga en cuenta que si el informe contiene una gran cantidad de entradas, se necesitará más tiempo para generar y exportar el informe.

   - **Formato de archivo**.

     Seleccione el formato de archivo al que se exportará el informe: XML, HTML o PDF. Si exporta más de un informe, cada informe seleccionado se guardará en un archivo individual del formato seleccionado.

Se requiere la herramienta wkhtmltopdf para convertir un informe a PDF. Cuando selecciona la opción PDF, el Servidor de administración verifica si la herramienta wkhtmltopdf está instalada en el dispositivo. Si la herramienta no está instalada, la aplicación muestra un mensaje sobre la necesidad de instalar la herramienta en el dispositivo del Servidor de administración. Instale la herramienta manualmente y luego continúe con el siguiente paso.



Especificar la configuración de exportación del informe

5. Haga clic en el botón **Exportar informe**.

El informe se guarda en un archivo del formato seleccionado.

Generar y ver un informe

Para crear y ver un informe:

1. En el menú principal, vaya a **Supervisión** → **Informes**.
2. Haga clic en el nombre de la plantilla de informe con la que desee crear el informe.

   Se creará y mostrará un informe basado en la plantilla seleccionada.

Los datos del informe se muestran respetando los ajustes de localización definidos para el Servidor de administración.

La fuente de los diagramas puede no mostrarse correctamente en los informes generados. Para resolver este problema, instale la biblioteca fontconfig. Además, verifique que las fuentes correspondientes a la configuración regional de su sistema operativo estén, efectivamente, instaladas en el sistema operativo.

El informe contendrá los siguientes datos:

- En la pestaña **Resumen**:
  - El nombre del informe, el tipo de informe, una descripción breve, el período comprendido por el informe e información sobre el grupo de dispositivos para los que se generó el informe.
  - Un gráfico con los datos más representativos del informe.
  - Una tabla unificada con los indicadores calculados del informe.
- En la pestaña **Detalles**, una tabla con datos detallados del informe.

Crear una tarea de entrega de informes

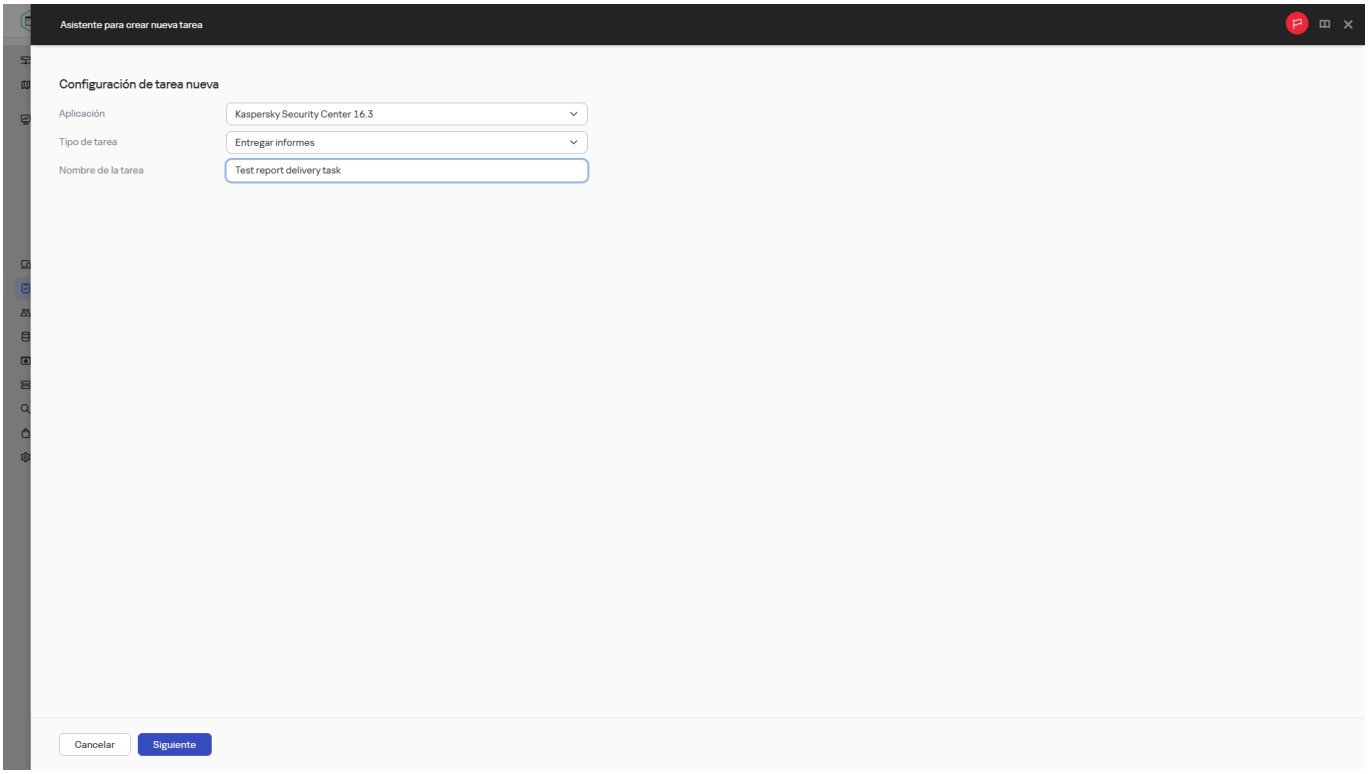
Puede crear una tarea para entregar informes específicos.

Para crear una tarea de entrega de informes:

1. En el menú principal, vaya a **Supervisión** → **Informes**.
2. Active las casillas ubicadas junto a las plantillas de informe para las que desee crear una tarea de entrega de informes.
3. Haga clic en el botón **Crear tarea de entrega**.

   Se inicia el Asistente para crear nueva tarea. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.
4. En el paso **Configuración de tarea nueva** del asistente, ingrese el nombre de la tarea.

   El nombre predeterminado es **Entregar informes.** Si ya existe una tarea con este nombre, se agrega un número de secuencia (<N>) al nombre de la tarea.



Crear una tarea de entrega de informes

5. En el paso **Configuración del informe** del asistente, especifique la siguiente configuración:

   a. Seleccione las plantillas de informe que entregará la tarea.

   b. Defina el formato de los informes: HTML, XLS o PDF.

      Se requiere la herramienta wkhtmltopdf para convertir un informe a PDF. Cuando selecciona la opción PDF, el Servidor de administración verifica si la herramienta wkhtmltopdf está instalada en el dispositivo. Si la herramienta no está instalada, la aplicación muestra un mensaje sobre la necesidad de instalar la herramienta en el dispositivo del Servidor de administración. Instale la herramienta manualmente y luego continúe con el siguiente paso.

   c. Indique si los informes se enviarán por correo electrónico y, de ser así, defina los ajustes de notificación por correo electrónico.

      Puede especificar hasta 20 direcciones de correo electrónico. Para separar direcciones de correo electrónico, presione **Intro**. También puede pegar una lista de direcciones de correo electrónico separadas por comas y luego presionar **Intro**.

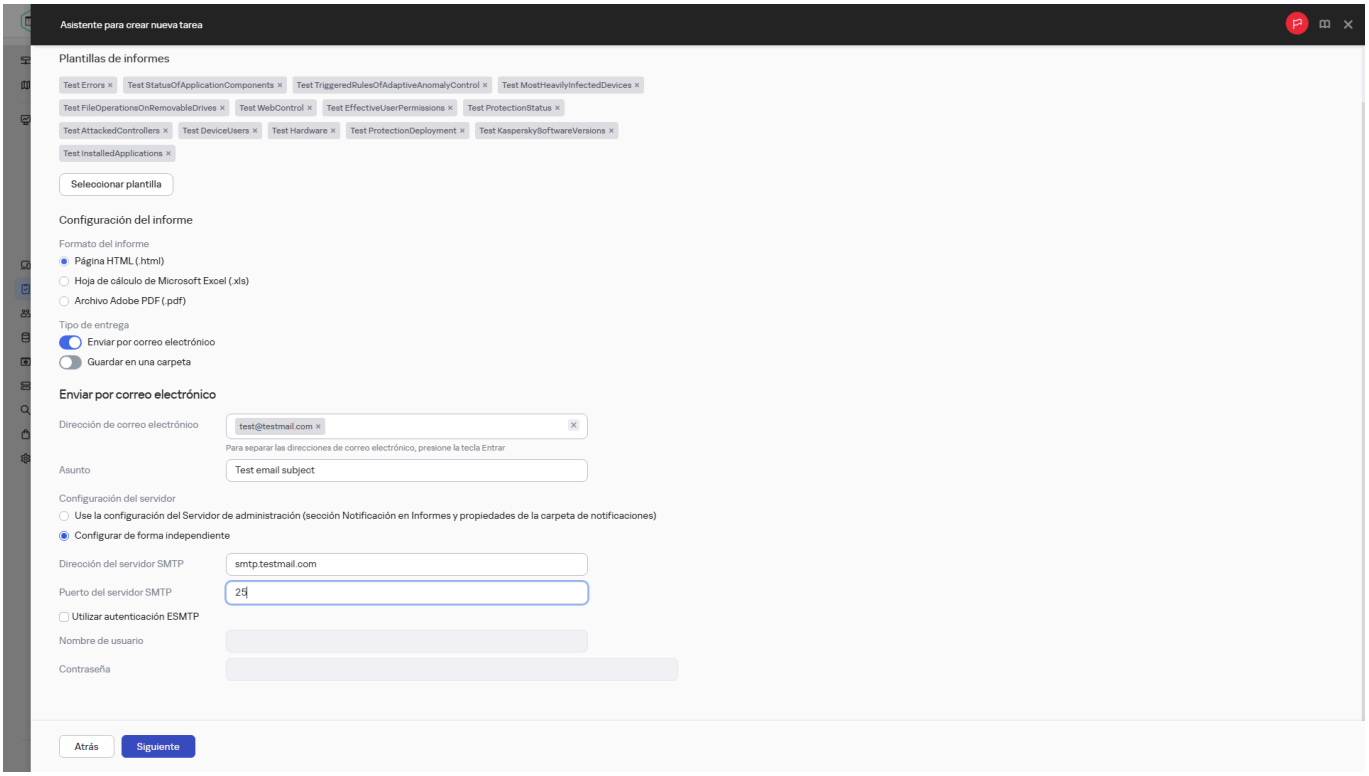
   d. Si los informes deben guardarse en una carpeta, junto con los ajustes correspondientes.

      Después de habilitar la opción **Guardar en una carpeta** debe especificar una ruta POSIX a la carpeta. Si desea guardar los informes en una carpeta compartida, también deberá seleccionar la casilla de verificación **Especificar cuenta para acceder a carpeta compartida** y luego especificar la cuenta de usuario y la contraseña para acceder a esta carpeta.

      > Si selecciona guardar los informes en una carpeta compartida, debe garantizar el acceso a esta carpeta desde el dispositivo que tenga instalado el Servidor de administración. Las formas de garantizar el acceso y las herramientas utilizadas dependen de su infraestructura.

      Al guardar los informes en una carpeta local, generalmente no se necesitan credenciales ya que la cuenta con la que se ejecuta el Servidor de administración tiene acceso a esta carpeta. De ser necesario, puede especificar las credenciales del usuario en el paso **Seleccione una cuenta con la que ejecutar la tarea** del asistente.

Independientemente de la carpeta que elija, también puede marcar la casilla **Sobrescribir informes antiguos del mismo tipo** si desea que el nuevo archivo de informe sobrescriba el archivo que se guardó en la carpeta de informes durante el inicio de la tarea anterior.



Especificar la configuración de la tarea

6. En el paso **Configurar programación de tarea** del asistente, seleccione la programación de inicio de la tarea.

   Están disponibles las siguientes opciones de programación de tareas:

   - **Manual**

     La tarea no se ejecutará automáticamente. Solo se la podrá iniciar en forma manual.

     Esta opción está seleccionada de forma predeterminada.

   - **Cada N minutos**

     La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la hora indicada en el día en que se cree la tarea. Cada ejecución estará separada de la anterior por el número de minutos que indique.

     De forma predeterminada, la tarea se ejecutará cada treinta minutos, a partir de la hora actual del sistema.

   - **Cada N horas**

     La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la fecha y hora indicadas. Cada ejecución estará separada de la anterior por el número de horas que indique.

     De manera predeterminada, la tarea se ejecutará cada 6 horas, a partir de la fecha y hora actuales del sistema.

   - **Cada N días**

     La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta opción permite elegir la fecha y hora de la primera ejecución. Podrá configurar estos dos ajustes si son compatibles con la aplicación para la que esté creando la tarea.

     De forma predeterminada, la tarea se ejecutará todos los días, a partir de la fecha y hora actuales del sistema.

- **Cada N semanas**

  La tarea se ejecutará periódicamente, a intervalos regulares, en el día de la semana y a la hora que especifique. Cada ejecución estará separada de la anterior por el número de semanas que indique.

  De manera predeterminada, la tarea se ejecutará cada viernes a la hora actual del sistema.

- **Mensual**

  La tarea se ejecutará periódicamente, en el día del mes y a la hora que indique.

  Si el día elegido no forma parte de un mes, la tarea se ejecutará el último día de ese mes.

  Por defecto, la tarea se ejecutará el primer día de cada mes, a la hora actual del sistema.

- **En los días especificados**

  La tarea se ejecutará periódicamente, en los días del mes y a la hora que indique.

  De manera predeterminada, la hora de inicio es a las 18:00 y no se selecciona ningún día del mes.

  > Tenga en cuenta que no selecciona una fecha específica en el mes, ni el número de la semana (primera, segunda semana del mes), sino el número de secuencia del día de la semana dentro de un mes. Por ejemplo, si coloca el cursor en la celda **Ma** de la **Primero** fila, significa que la tarea se ejecutará el primer martes de cada mes nuevo.

  Puede seleccionar varios días de la semana.

- **Ante brotes de virus**

  La tarea se ejecutará cuando ocurra un evento *Brote de virus*. Seleccione los tipos de aplicaciones que se usarán para controlar si ocurre un brote de virus. Están disponibles los siguientes tipos de aplicaciones:

  - Antivirus para estaciones de trabajo y servidores de archivos
  - Antivirus para defensa del perímetro
  - Antivirus para sistemas de correo

  Por defecto, están seleccionados todos los tipos de aplicaciones.

  En algunos casos, querrá ejecutar tareas diferentes según el tipo de aplicación de seguridad que dé aviso de un brote de virus. De ser así, anule la selección de los tipos de aplicaciones que no necesite.

- **Al completarse otra tarea**

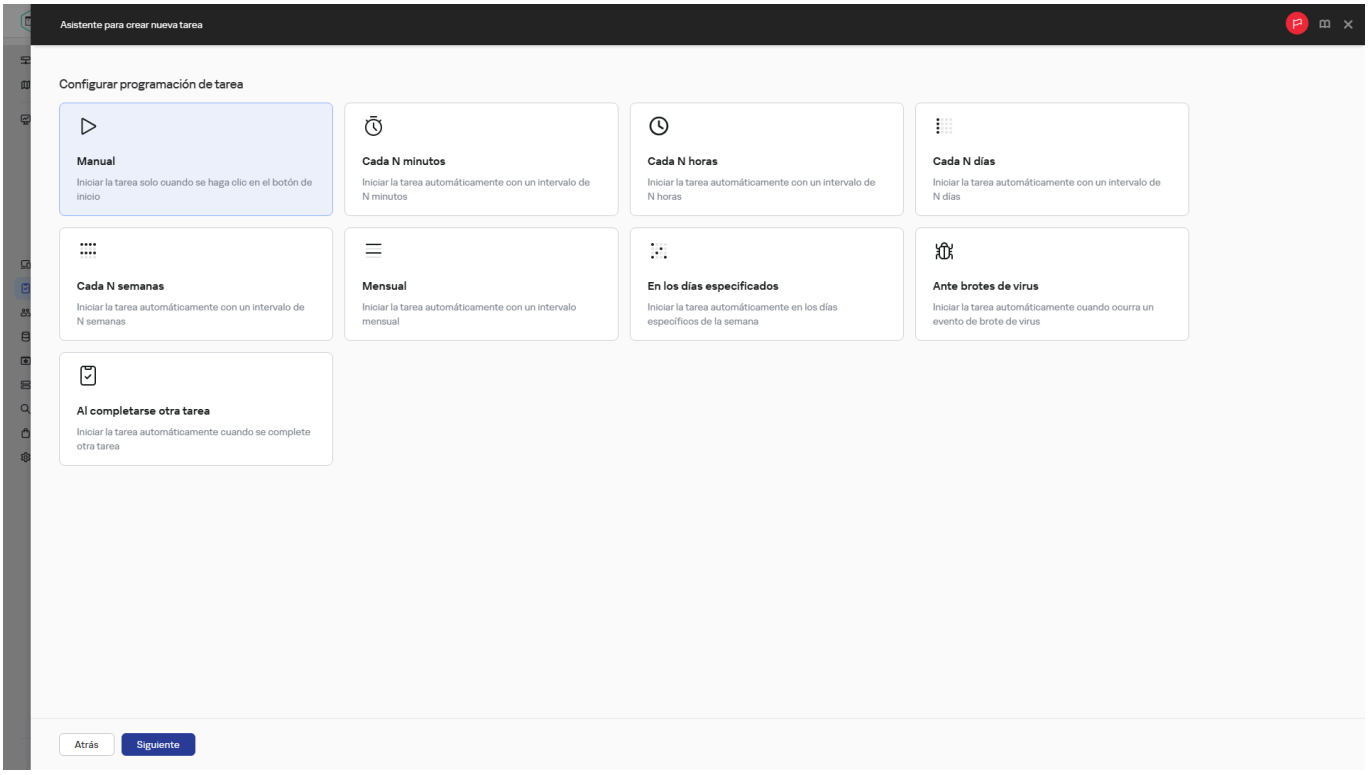
  La tarea actual se iniciará después de que se complete otra tarea. Esta opción solo funciona si ambas tareas están asignadas a los mismos dispositivos. Por ejemplo, podría ejecutar la tarea *Administrar dispositivos* con la opción **Encender el dispositivo** y hacer que, una vez completada esa tarea, se ejecute la tarea *Análisis antivirus* como una tarea desencadenante.

  Debe seleccionar la tarea desencadenante de la tabla y el estado con el que esta tarea debe completarse (**Completada correctamente** o **Error**).

Si es necesario, puede buscar, ordenar y filtrar las tareas en la tabla de la siguiente manera:

- Ingrese el nombre de la tarea en el campo de búsqueda para buscar la tarea por su nombre.
- Haga clic en el ícono de ordenar para ordenar las tareas por nombre.

  De manera predeterminada, las tareas se clasifican en orden alfabético ascendente.
- Haga clic en el ícono de filtro y, en la ventana que se abre, filtre las tareas por grupo y luego haga clic en el botón **Aplicar**.



Seleccionar la programación de inicio de la tarea

7. En este paso del asistente, configure otras opciones de programación de tareas:

- En la sección **Programación de la tarea**, verifique o reconfigure la programación previamente seleccionada, y establezca el intervalo de tiempo, los días del mes o la semana, establezca la condición de brote de virus o la finalización de otra tarea como disparador para iniciar la tarea. También se puede especificar una hora de inicio en esta sección si se selecciona una programación aplicable.
- En la sección **Configuración adicional**, especifique las siguientes configuraciones:
  - **Ejecutar tareas no realizadas**

    Esta opción determina el comportamiento de la tarea cuando la misma está por iniciarse y uno de los dispositivos cliente no está visible en la red.

    Si esta opción está habilitada, el sistema intentará iniciar la tarea la siguiente vez que la aplicación de Kaspersky se ejecute en el dispositivo cliente. Si la programación de la tarea es **Manual**, **Una vez** o **Inmediatamente**, la tarea se iniciará inmediatamente después de que el dispositivo aparezca en la red o inmediatamente después de que el dispositivo sea incluido en el alcance de la tarea.

    Si esta opción está deshabilitada, solo las tareas programadas se ejecutan en los dispositivos cliente. Para la programación **Manual**, **Una vez** e **Inmediatamente**, las tareas se ejecutan solo en los dispositivos cliente que están visibles en la red. Podría deshabilitar esta opción para, por ejemplo, una tarea que consuma muchos recursos y que solo deba ejecutarse fuera del horario laboral.

    Esta opción está activada de forma predeterminada.

- **Utilizar retardo aleatorio automático para el inicio de la tarea**

  Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo que especifique. Se realizará, de este modo, un *inicio distribuido*. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

  La hora de inicio distribuida se calcula automáticamente cuando se crea una tarea. El cálculo tiene en cuenta el número de dispositivos cliente a los que la tarea está asignada. Las ejecuciones posteriores a la inicial ocurren siempre a la hora de inicio calculada. Sin embargo, tenga en cuenta que si modifica la configuración de la tarea o inicia la tarea manualmente, la hora de inicio calculada cambiará.

  Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

  Esta opción está activada de forma predeterminada.

- **Utilizar el retardo aleatorio automático para el inicio de la tarea dentro de un intervalo de**

  Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo de tiempo especificado. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

  Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

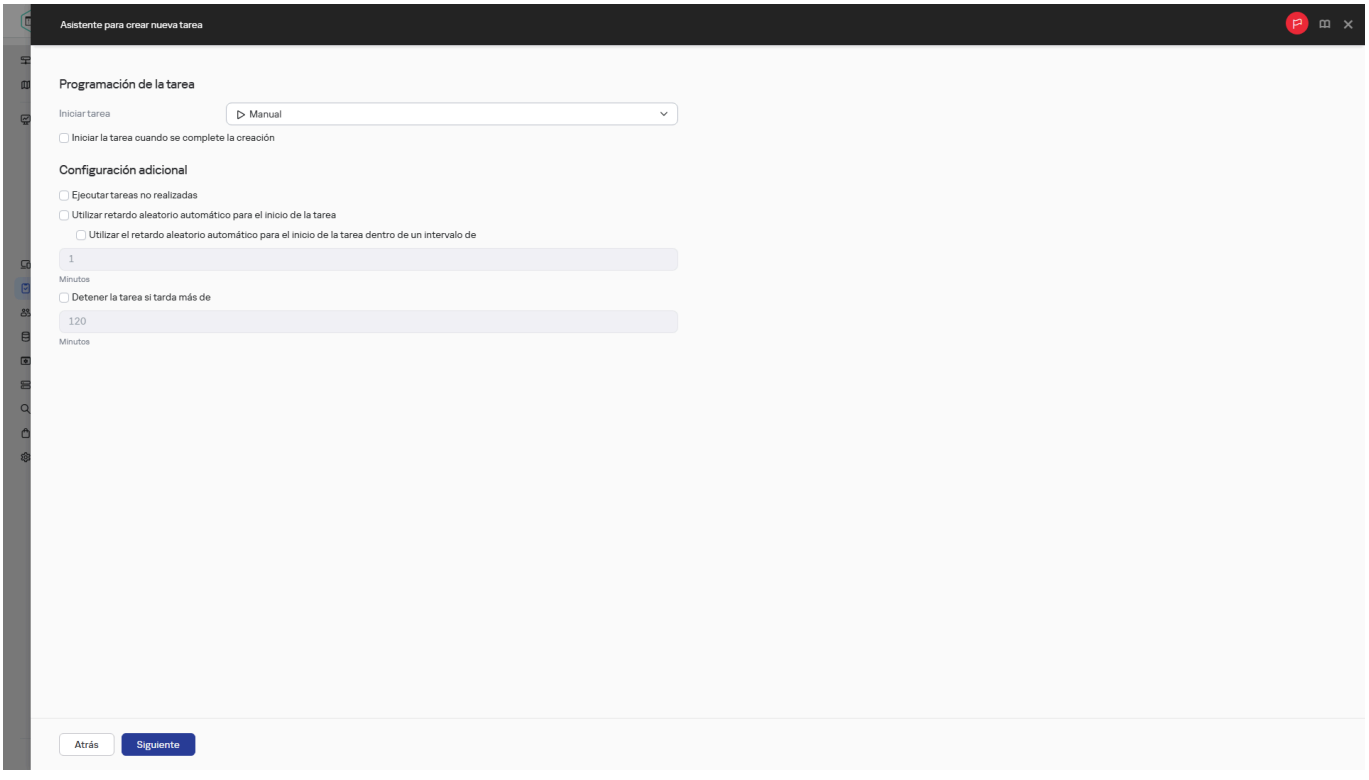
  Esta opción está deshabilitada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

- **Detener la tarea si tarda más de**

  Una vez que transcurra el período especificado, la tarea se detendrá automáticamente, se haya completado o no.

  Habilite esta opción si desea que las tareas que tarden mucho en completarse se interrumpan o se detengan.

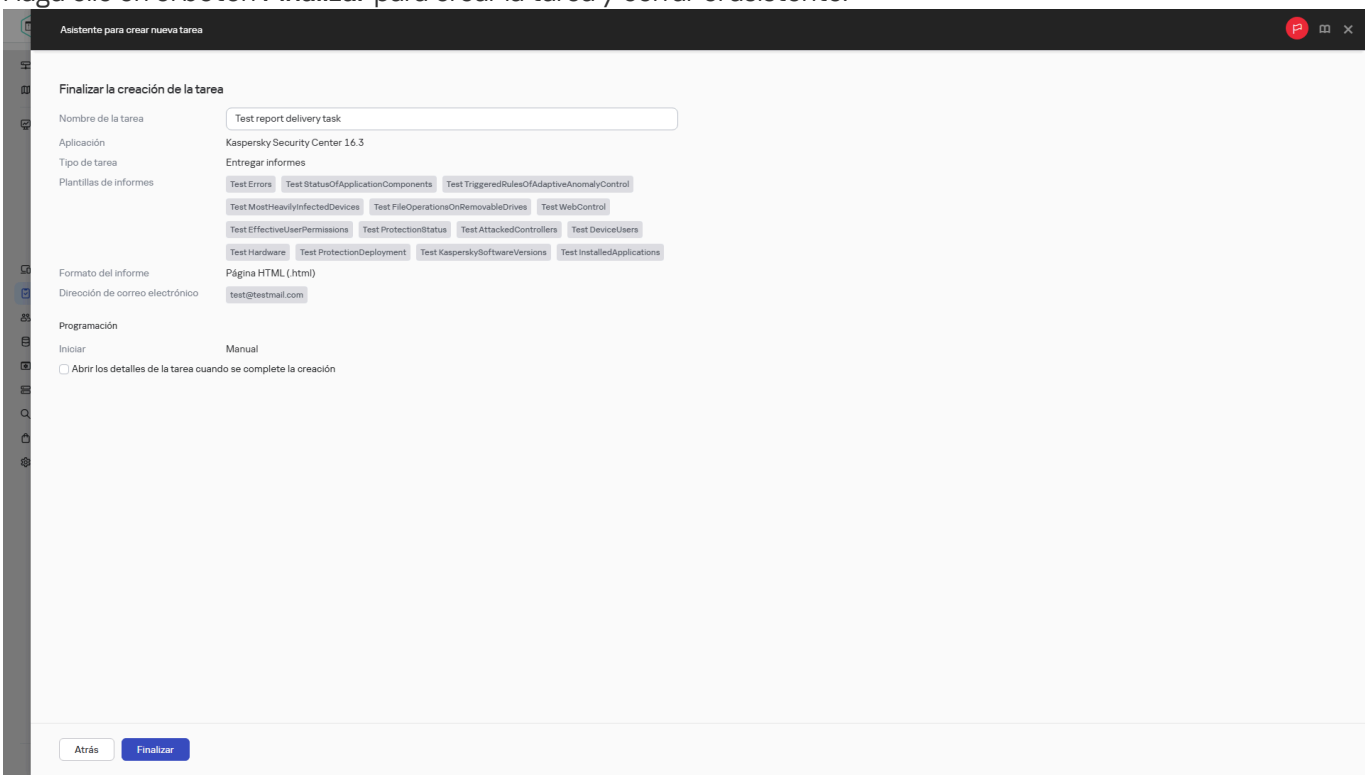
  Esta opción está deshabilitada de forma predeterminada. El tiempo de ejecución por defecto para las tareas es de 120 minutos.



8. En el paso **Seleccione una cuenta con la que ejecutar la tarea** del asistente, especifique las credenciales de la cuenta de usuario que se utiliza para ejecutar la tarea.

9. Si desea modificar otros ajustes de la tarea después de crearla, en el paso **Finalizar la creación de la tarea** del asistente, habilite la opción **Abrir los detalles de la tarea cuando se complete la creación**. Esta opción está activada de forma predeterminada.

10. Haga clic en el botón **Finalizar** para crear la tarea y cerrar el asistente.



Finalizar la creación de la tarea

Se creará la tarea de entrega de informes. Si la opción **Abrir los detalles de la tarea cuando se complete la creación** está habilitada, se abrirá la ventana de configuración de la tarea.

Eliminación de plantillas de informes

Para eliminar una o varias plantillas de informes:

1. En el menú principal, vaya a **Supervisión** → **Informes**.

2. Marque las casillas ubicadas junto a las plantillas de informes que desee eliminar.

3. A continuación, haga clic en el botón **Eliminar**.

4. En la ventana que se abre, haga clic en **Aceptar** para confirmar su selección.

Se eliminan las plantillas de informes seleccionadas. Si las plantillas formaban parte de una o más tareas de entrega de informes, se las eliminará también de esas tareas.

Centro de refuerzo de seguridad

El Centro de refuerzo de seguridad muestra información actualizada sobre la protección del Servidor de administración y los puntos de distribución. Esta información se presenta mediante indicadores del nivel de protección. Estos indicadores permiten supervisar la implementación de la Guía para reforzar la seguridad y abordar oportunamente los problemas de seguridad de su infraestructura a medida que surjan.

El indicador puede tener uno de los siguientes estados:

- Protección configurada.
- Protección parcialmente configurada.
- Protección no configurada.

Cómo ver información detallada sobre el nivel de protección

El estado general del indicador está determinado por los estados de los parámetros de protección.

*Para abrir el **Centro de refuerzo de seguridad**:*

1. En el menú principal, vaya a la sección **Supervisión** → **Panel**.
2. Haga clic en el estado de la protección en la esquina superior derecha.

   En la ventana **Centro de refuerzo de seguridad** que se abre, los parámetros se agrupan por objetos protegidos: Servidor de administración y puntos de distribución.

Cada parámetro de protección se muestra en uno de los estados según sus derechos de acceso:

- ✅ si no hay problemas por resolver o si no tiene los derechos de acceso necesarios.
- ⚠️ o ❌ si hay problemas por resolver.

Los siguientes parámetros se muestran solo para el Servidor de administración:

- Copia de seguridad configurada
- Mantenimiento del Servidor de administración configurado
- Cifrado TLS habilitado

Los siguientes parámetros se muestran tanto para el Servidor de administración como para los puntos de distribución:

- Aplicación de seguridad instalada
- Se aplicó la directiva de aplicación de seguridad

- Actualizaciones de la base de datos antivirus configuradas
- Todos los dispositivos están administrados

  Esta configuración también se muestra para los dispositivos que no son puntos de distribución ni dispositivos del Servidor de administración.

Consideraciones especiales para el Servidor de administración:

- Todos los parámetros de protección se calculan solo para el servidor de administración físico y no se aplican a los servidores virtuales.

  Si tiene una estructura jerárquica de varios Servidores de administración, el indicador de nivel de protección se calcula para cada servidor físico por separado.

- Los parámetros **Aplicación de seguridad instalada**, **Se aplicó la directiva de aplicación de seguridad** y **Actualizaciones de la base de datos antivirus configuradas** se calculan para un dispositivo que tiene instalado el Servidor de administración.

- Al implementar un clúster de conmutación por error de Kaspersky Security Center Linux, los parámetros **Aplicación de seguridad instalada**, **Se aplicó la directiva de aplicación de seguridad, Actualizaciones de la base de datos antivirus configuradas** y **Todos los dispositivos están administrados** se evalúan para cada nodo. El nodo se tiene en cuenta en el cálculo del estado del indicador solo después de activarse.

Cómo se calcula el estado del indicador

La siguiente tabla describe cómo se evalúa el estado del indicador.

Estado del indicador	Condición
Protección configurada.	Todos los parámetros de protección están en el estado ✓.
Protección parcialmente configurada.	El parámetro **Actualizaciones de la base de datos antivirus configuradas** está en el estado ⚠, mientras que todos los demás parámetros están en el estado ✓.
Protección no configurada.	Si al menos uno de los siguientes parámetros de protección está en el estado ✗.

Aplicación de seguridad instalada

Las aplicaciones de seguridad le permiten proteger sus dispositivos contra varios tipos de amenazas, incluidos ataques de red, suplantación de identidad (phishing) y estafas.

El parámetro se muestra en el estado si se cumple una de las condiciones:

- No tiene derechos de acceso a los dispositivos.
- Tiene el derecho **Leer** en el área funcional **Características generales → Funcionalidad básica**, mientras que el Agente de red y una aplicación de seguridad están instalados en los dispositivos.

  La condición debe cumplirse en todos los dispositivos a los que tiene acceso según sus derechos de acceso, excepto los dispositivos con una aplicación instalada que no requiere protección antivirus (por ejemplo, un sistema operativo protegido), los dispositivos que no tienen instalado el Agente de red y cuya información apareció en el Servidor de administración hace menos de 24 horas, y los dispositivos sin conexión que se conectaron por última vez al Servidor de administración hace 7 días o más.

El parámetro se muestra en el estado si se cumple al menos una de las siguientes condiciones.

Debe hacer clic en el botón **Ver dispositivos** y realizar las acciones descritas en la tabla para los dispositivos mostrados.

Condición	Solución
El Agente de red no está instalado en el dispositivo	Instale el Agente de red: Para el dispositivo del Servidor de administración, la forma más sencilla de instalar el Agente de red es usar un paquete de instalación independiente.
El dispositivo está incluido en el grupo **Dispositivos no asignados**	Mueva el dispositivo al grupo Dispositivos administrados o a su subgrupo
No se encontraron aplicaciones de seguridad, o la protección en tiempo real no se está ejecutando para la aplicación de seguridad instalada	Instale una aplicación de seguridad. La aplicación transmitirá datos sobre el estado de la protección al Servidor de administración. Puede ver el estado de protección de un dispositivo en la sección Configuración del dispositivo: **General → Estado del dispositivo**. En el dispositivo del Servidor de administración, debe instalar Kaspersky Endpoint Security for Linux.

Directiva aplicada

Una directiva es un conjunto de valores de configuración que se aplican a una aplicación de seguridad en un grupo de administración y sus subgrupos.

El parámetro se muestra en el estado ✅ si se cumple una de las condiciones:

- No tiene derechos de acceso a los dispositivos.
- Tiene el permiso **Leer** en el área funcional **Características generales → Funcionalidad básica**, mientras que una aplicación de seguridad está instalada en sus dispositivos y se aplica una directiva activa de esta aplicación de seguridad a los dispositivos.

> La condición debe cumplirse en todos los dispositivos a los que tiene acceso según sus derechos de acceso, excepto los dispositivos con una aplicación instalada que no requiere protección antivirus (por ejemplo, un sistema operativo protegido), los dispositivos que no tienen instalado el Agente de red y cuya información apareció en el Servidor de administración hace menos de 24 horas, y los dispositivos sin conexión que se conectaron por última vez al Servidor de administración hace 7 días o más.

El parámetro se muestra en el estado ❌ si se cumple al menos una de las siguientes condiciones.

Debe hacer clic en el botón **Ver dispositivos** y realizar las acciones descritas en la tabla para los dispositivos mostrados.

Condición	Solución
La aplicación de seguridad no está instalada en el dispositivo.	Asegúrese de que el dispositivo no esté en la selección del parámetro de protección Aplicación de seguridad instalada.
No se aplica ninguna directiva al dispositivo.	Asegúrese de que la directiva se haya creado para el grupo de administración al que pertenece el dispositivo. Si no es así, cree y active la directiva. Si es así, asegúrese de que: • La directiva creada esté activa. Si no es así, active la directiva. • El estado de distribución de la directiva sea **Aplicada correctamente**. Si el estado es **Aplicada con error**, el problema debe corregirse en la aplicación de seguridad.

Actualización de las bases de datos antivirus configurada

Dado que las bases de datos antivirus protegen sus dispositivos contra las amenazas, debe actualizar las bases de datos en los dispositivos de forma regular y oportuna.

El parámetro se muestra en el estado ✅ si se cumple una de las condiciones:

- No tiene derechos de acceso a los dispositivos.
- Tiene el derecho Leer en el área funcional Características generales → Funcionalidad básica, y las bases de datos de antivirus están actualizadas en los dispositivos.

> La condición debe cumplirse en todos los dispositivos a los que tiene acceso según sus derechos de acceso, excepto los dispositivos con una aplicación instalada que no requiere protección antivirus (por ejemplo, un sistema operativo protegido), los dispositivos que no tienen instalado el Agente de red y cuya información apareció en el Servidor de administración hace menos de 24 horas, y los dispositivos sin conexión que se conectaron por última vez al Servidor de administración hace 7 días o más.

El parámetro se muestra con el estado ⚠ si las bases de datos antivirus se actualizaron por última vez en un dispositivo hace más de tres días.

El parámetro se muestra con el estado ✖ si las bases de datos antivirus se actualizaron por última vez en un dispositivo hace más de siete días.

Para resolver el problema:

1. Haga clic en el botón Ver dispositivos junto al parámetro.
2. Para los dispositivos que se muestran, realice las siguientes acciones:
   a. Asegúrese de que se haya establecido la conexión entre el Agente de red y el Servidor de administración.
      Si no es así, consulte los siguientes artículos:
      Solución de problemas relacionados con la actualización de las bases de datos antivirus de Kaspersky Endpoint Security for Linux
      Problemas al actualizar las bases de datos antivirus desde el repositorio de Kaspersky Security Center
   b. Asegúrese de que la aplicación de Kaspersky cuyas bases de datos antivirus está revisando no esté detenida.
      Si la aplicación está detenida, iníciela.
   c. En el dispositivo, vea los errores que ocurrieron después de la actualización.

Copia de seguridad configurada

Para obtener recomendaciones sobre la copia de seguridad de los datos del Servidor de administración, consulte Copia de seguridad y restauración de los datos del Servidor de administración.

El parámetro se muestra en el estado ✔ si se cumple una de las condiciones:

- No tiene permisos de acceso para trabajar con la tarea de copia de seguridad de los datos del Servidor de administración.
- Tiene los permisos **Leer, Modificar** y **Ejecutar** en el área funcional **Características generales → Operaciones en el Servidor de administración**, y la copia de seguridad está configurada y se realiza periódicamente.

El parámetro se muestra en el estado ✖ si se cumple al menos una de las siguientes condiciones.

Condición	Solución
No se ha creado la tarea de copia de seguridad de los datos del Servidor de administración.	Cree la tarea.
Los ajustes de programación necesarios no están configurados para la tarea de copia de seguridad de los datos del Servidor de administración.	En la tarea de mantenimiento del Servidor de administración, especifique la configuración de **Iniciar tarea** con una opción diferente a **Ante brotes de virus** y **Manual**.

Mantenimiento del Servidor de administración configurado

El mantenimiento del Servidor de administración le permite liberar espacio en la carpeta del Servidor de administración, así como minimizar el tamaño de la base de datos. Esto ayuda a acelerar el procesamiento de solicitudes y aumenta la estabilidad general del sistema.

El parámetro se muestra en el estado ✅ si se cumple una de las condiciones:

- No tiene derechos de acceso para trabajar con la tarea de mantenimiento del Servidor de administración.
- Tiene los derechos **Leer y Modificar** y **Ejecutar** en el área funcional **Características generales → Operaciones en el Servidor de administración**, mientras que el mantenimiento del Servidor de administración está configurado y se realiza con regularidad.

  > Los derechos deben establecerse en el nivel del Servidor de administración.

El parámetro se muestra en el estado ❌ si se cumple al menos una de las siguientes condiciones.

Condición	Solución
No se creó la tarea de mantenimiento del Servidor de administración.	Cree la tarea.
Los ajustes de programación necesarios no están configurados para la tarea de mantenimiento del Servidor de administración.	En la tarea de mantenimiento del Servidor de administración, especifique la configuración de **Iniciar tarea** con una opción diferente a **Ante brotes de virus** y **Manual**.

Cifrado TLS habilitado

Debe asegurarse de que solo se permitan las versiones 1.2 y 1.3 del protocolo TLS. Permitir versiones anteriores genera graves riesgos para la seguridad de los datos y hace que los sistemas sean vulnerables a ataques.

El parámetro se muestra en el estado ✅ si solo se permiten las versiones 1.2 y 1.3 del protocolo TLS.

El parámetro se muestra en el estado ❌ si se permiten versiones de TLS obsoletas anteriores a la 1.2.

Para resolver el problema, debe establecer el indicador `SrvUseStrictSslSettings` en el valor `4` o `5`.

Todos los dispositivos están administrados

Puede usar este parámetro para identificar los dispositivos que podrían estar fuera de control.

Este parámetro se muestra con el estado cuando se cumple una de las siguientes condiciones:

- No tiene derechos de acceso a los dispositivos.
- Tiene el permiso **Leer** en el área funcional **Características generales → Funcionalidad básica**, los dispositivos están en el grupo **Dispositivos administrados** y se ha establecido una conexión entre el Servidor de administración y el Agente de red en los dispositivos.

  Esta condición debe cumplirse en todos los dispositivos disponibles para usted según sus derechos de acceso, excepto en los dispositivos cuya información apareció en el Servidor de administración hace menos de 24 horas y los dispositivos que se conectaron por última vez al Servidor de administración hace siete días o más.

Este parámetro se muestra con el estado si hay al menos un dispositivo que cumple alguna de las siguientes condiciones.

Debe hacer clic en el botón **Ver dispositivos** y realizar las acciones descritas en la tabla para los dispositivos mostrados.

Condición	Solución
El Agente de red no está instalado en un dispositivo incluido en el grupo **Dispositivos administrados**.	Instale el Agente de red:
El Servidor de administración detecta un dispositivo administrado durante un análisis de la red, pero este dispositivo no se ha conectado al Servidor de administración durante tres intervalos de sincronización consecutivos.	Haga lo siguiente: 1. Ejecute la utilidad klnagchk en el dispositivo con problemas para comprobar si el servicio está en ejecución y si el Agente de red puede conectarse al Servidor de administración. 2. Compruebe la accesibilidad de red del Servidor de administración y de las pasarelas de conexión. 3. Restaure la conexión del dispositivo con el Servidor de administración mediante la utilidad klmover. 4. Elimine los dispositivos obsoletos de los grupos de administración. Si tiene una infraestructura no estándar, puede seguir estos pasos para los dispositivos con problemas: a. Compruebe que el dispositivo esté administrado por el Servidor de administración. b. Mueva este dispositivo a otro grupo de administración. c. En este grupo de administración, asigne al evento **El dispositivo ha cambiado a no administrado** cualquier estado que no sea *Crítico*.

Eventos y selecciones de eventos

En esta sección, se brinda información sobre los eventos y las selecciones de eventos, sobre los tipos de eventos que ocurren en los componentes de Kaspersky Security Center Linux y sobre cómo puede administrar el bloqueo de eventos frecuentes.

Acerca de los eventos en Kaspersky Security Center Linux

Kaspersky Security Center Linux le permite recibir información sobre los eventos que ocurren durante el funcionamiento del Servidor de administración y aplicaciones de Kaspersky instaladas en dispositivos administrados. La información sobre estos eventos se guarda en la base de datos del Servidor de administración.

Eventos por tipo

En Kaspersky Security Center Linux existen los siguientes tipos de eventos:

- Eventos generales. Esta clase de evento ocurre en todas las aplicaciones de Kaspersky administradas. Un ejemplo de evento general es Brote de virus. Los eventos generales tienen una sintaxis y una semántica estrictamente definidas. Los eventos generales se utilizan en, por ejemplo, los paneles e informes.
- Eventos específicos de las aplicaciones de Kaspersky administradas. Cada aplicación de Kaspersky administrada tiene su propio conjunto de eventos.

Eventos por origen

Puede ver la lista completa de los eventos que puede generar una aplicación en la pestaña **Configuración de eventos** de la directiva de la aplicación. Para el Servidor de administración, también puede ver la lista de eventos en las propiedades del Servidor de administración.

Los eventos pueden ser generados por las siguientes aplicaciones:

- Componentes de Kaspersky Security Center Linux:
  - Servidor de administración
  - Agente de red
- Aplicaciones administradas por Kaspersky

  Para obtener detalles sobre los eventos generados por las aplicaciones administradas por Kaspersky, consulte la documentación de la aplicación correspondiente.

Eventos por nivel de importancia

Cada evento tiene su propio nivel de importancia. El nivel de importancia que se le asigna a un evento puede variar según las circunstancias en las que ocurre. Existen cuatro niveles de importancia:

- Un *evento crítico* es un evento que se registra cuando ocurre un problema de extrema gravedad, que puede derivar en pérdidas de información, en un error crítico o en un fallo de funcionamiento.
- Un *error funcional* es un evento que indica la aparición de un problema, error o mal funcionamiento grave que se produjo durante el funcionamiento de la aplicación o mientras se realizaba un procedimiento.
- Una *advertencia* es un evento que no necesariamente es grave, pero que anticipa un posible problema en el futuro. La mayoría de los eventos se catalogan como advertencias si, a pesar de que el evento haya ocurrido, la aplicación puede recuperarse sin sufrir una pérdida de información o de funcionalidad.
- Un evento *informativo* es un evento que se registra para informar que una operación o procedimiento se completaron sin errores o que la aplicación funciona correctamente.

Cada evento tiene un plazo de almacenamiento definido, durante el cual lo puede ver o modificar en Kaspersky Security Center Linux. Algunos eventos no se guardan en la base de datos del Servidor de administración de forma predeterminada porque su plazo de almacenamiento está definido en cero. Para que un evento pueda exportarse, debe permanecer almacenado al menos un día en la base de datos del Servidor de administración.

Eventos de los componentes de Kaspersky Security Center Linux

Cada componente de Kaspersky Security Center Linux tiene su propio conjunto de tipos de evento. Esta sección enumera los tipos de eventos que ocurren en el Servidor de administración y en el Agente de red. Los tipos de eventos que pueden ocurrir en las aplicaciones de Kaspersky no se detallan en esta sección.

Para cada evento que una aplicación puede generar, puede especificar la configuración de notificación y la configuración de almacenamiento en la pestaña **Configuración de eventos** en la directiva de la aplicación. Para el Servidor de administración, también puede ver y configurar la lista de eventos en las propiedades del Servidor de administración. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

Estructura de datos utilizada para describir los tipos de eventos

Cada tipo de evento tiene especificado su nombre, identificador (id.), código alfabético, descripción y plazo de almacenamiento predeterminado.

- **Nombre que se muestra para el tipo de evento**. Este texto se muestra en Kaspersky Security Center Linux cuando configura los eventos y cuando ocurren.
- **Id. del tipo de evento**. Un código numérico que se utiliza para procesar los eventos con una herramienta de análisis de eventos desarrollada por un tercero.
- **Tipo de evento** (código alfabético). Este código se usa cuando navega y procesa eventos utilizando vistas públicas que se proporcionan en la base de datos de Kaspersky Security Center Linux y cuando los eventos se exportan a un sistema SIEM.

- **Descripción**. Un texto en el que se describen las situaciones en las que ocurren un evento y las acciones que se pueden tomar en cada caso.

- **Plazo de almacenamiento predeterminado**. El número de días por los que cada evento queda almacenado en la base de datos del Servidor de administración. Este es, también, el tiempo por el que el evento aparece en la lista de eventos del Servidor de administración. Transcurrido este período, el evento se elimina. Cuando el plazo de almacenamiento es 0, el evento se detecta, pero no se lo muestra en la lista de eventos del Servidor de administración. Si se configuró para guardar dichos eventos en el registro de eventos del sistema operativo, puede encontrarlos allí.

  Puede cambiar el plazo de almacenamiento de los eventos: Establecer el plazo de almacenamiento para un evento.

Eventos del Servidor de administración

En esta sección, se brinda información sobre los eventos relacionados con el Servidor de administración.

Eventos del Servidor de administración: nivel Crítico

La siguiente tabla muestra los eventos del Servidor de administración que tienen el nivel de gravedad **Crítico**.

Para cada evento que una aplicación puede generar, puede especificar la configuración de notificación y la configuración de almacenamiento en la pestaña **Configuración de eventos** en la directiva de la aplicación. Para el Servidor de administración, también puede ver y configurar la lista de eventos en las propiedades del Servidor de administración. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

Eventos del Servidor de administración: nivel Crítico

Nombre que se muestra para el tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo de almacenamiento predeterminado
El certificado del Servidor de administración para dispositivos móviles caducó	6129	KLSRV_EV_SRV_CERT_EXPIRED_DN	Este tipo de evento ocurre cuando caducan los certificados del Servidor de administración para los dispositivos móviles y dispositivos UEFI. Debe actualizar el certificado caducado.	180 días
Auditoría: La exportación a SIEM produjo un error	5130	KLAUD_EV_SIEM_EXPORT_ERROR	Los eventos de este tipo ocurren cuando la exportación de eventos al sistema SIEM falla debido a un error de conexión con el sistema SIEM.	180 días
El dispositivo ha cambiado a no administrado	4111	KLSRV_HOST_OUT_CONTROL	Este tipo de eventos ocurren si un dispositivo administrado es visible en la red pero no se ha conectado al Servidor de administración durante un período específico. Averigüe qué impide el correcto funcionamiento del Agente de red en el dispositivo. El problema podría deberse a un inconveniente en la red, por ejemplo, o al hecho de que el Agente de red se haya eliminado del dispositivo.	180 días
El estado del dispositivo es Crítico	4113	KLSRV_HOST_STATUS_CRITICAL	Este tipo de evento ocurre cuando se le asigna el estado *Crítico* a un dispositivo administrado. Puede configurar las condiciones bajo las cuales el estado del dispositivo se cambia a *Crítico*.	180 días

Nombre que se muestra para el tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo de almacenamiento predeterminado
La licencia está por caducar	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Este tipo de evento ocurre cuando se acerca la fecha de caducidad de una licencia comercial. Una vez al día, Kaspersky Security Center Linux comprueba si se acerca la fecha de caducidad de la licencia. Los eventos de este tipo se publican 30 días, 15 días, 5 días y 1 día antes de la fecha de caducidad de la licencia. El número de días no se puede modificar. Si el Servidor de administración se encuentra apagado el día especificado antes de la fecha de caducidad de la licencia, el evento no se publicará sino hasta el día siguiente. Cuando caduca la licencia comercial, Kaspersky Security Center Linux solo brinda acceso a las funciones básicas. Puede responder al evento de los siguientes modos: • Asegúrese de tener una clave de licencia de reserva agregada en el Servidor de administración. • Si usa una suscripción, no olvide renovarla. Una suscripción ilimitada se renueva automáticamente si el proveedor de servicios recibe a término y por adelantado el pago correspondiente.	180 días
Se ha superado el límite de la licencia	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Una vez al día, Kaspersky Security Center Linux comprueba si se superó algún límite de licencia. Este tipo de evento ocurre cuando el Servidor de administración detecta que las aplicaciones de Kaspersky instaladas en los dispositivos cliente han superado algún límite de sus licencias y si se ha utilizado más de un 110 % del total de unidades con licencia cubiertas por una sola licencia. Los dispositivos cliente se mantienen protegidos aun cuando ocurre este evento. Puede responder al evento de los siguientes modos: • Revise la lista de dispositivos administrados. Elimine los dispositivos que no estén en uso. • Agregue una licencia para más dispositivos (agregue un código de activación válido o un archivo de clave en el Servidor de administración). Kaspersky Security Center Linux determina las reglas para generar eventos cuando se supera un límite de licencia.	180 días

Nombre que se muestra para el tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo de almacenamiento predeterminado
Modo de funcionalidad limitada	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	Los eventos de este tipo ocurren cuando Kaspersky Security Center Linux empieza a funcionar con funcionalidad básica, sin las funciones Administración de vulnerabilidades y parches ni Administración de dispositivos móviles. Las causas de este evento y las maneras de responder son las siguientes: • El periodo de vigencia de la licencia ha caducado. Proporcione una licencia para utilizar el modo de funcionalidad completa de Kaspersky Security Center Linux (añada un código de activación válido o un archivo clave al Servidor de administración). • El Servidor de administración gestiona más dispositivos de los que permite el límite de la licencia. Mueva los dispositivos de los grupos de administración de un Servidor de administración a los grupos de administración de otro Servidor de administración (si el límite de licencia del otro Servidor de administración lo admite).	180 días
El certificado de MDM caducó	4132	KLSRV_CERTIFICATE_EXPIRED	Los eventos de este tipo ocurren cuando caduca el certificado cliente en los dispositivos móviles.	180 días
El archivo de clave está en la lista de claves rechazadas	4124	KLSRV_LICENSE_BLACKLISTED	Este tipo de evento ocurre cuando Kaspersky ha agregado el código de activación o el archivo de clave utilizados a la lista de rechazados. Comuníquese con nuestro servicio de soporte técnico para más información.	180 días

Nombre que se muestra para el tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo de almacenamiento predeterminado
Se revocaron las actualizaciones de los módulos de la aplicación de Kaspersky	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	Los eventos de este tipo ocurren si los expertos de Kaspersky han revocado las actualizaciones, por ejemplo, para reemplazarlas por versiones más recientes. El estado de dichas actualizaciones es *Revocado*. El evento afecta a los parches de Kaspersky Security Center Linux pero no a los módulos de las aplicaciones de Kaspersky administradas. La razón por la que no se instaló la actualización sin interrupciones se indica en el evento.	180 días
Brote de virus	• 26 (para Protección contra archivos peligrosos) • 27 (para Protección contra amenazas de correo) • 28 (para el firewall)	GNRL_EV_VIRUS_OUTBREAK	Los eventos de este tipo ocurren cuando el número de objetos maliciosos detectados en varios dispositivos administrados supera el umbral en un corto período de tiempo. Puede responder al evento de los siguientes modos: • Configure el umbral en las propiedades del Servidor de administración. • Cree una directiva más estricta que se active cuando ocurra este evento (o, como alternativa, cree una tarea que se ejecute cuando ocurra el evento).	

Eventos del Servidor de administración: nivel Error funcional

En la siguiente tabla, se enumeran los eventos del Servidor de administración que tienen el nivel de importancia **Error funcional**.

Para cada evento que una aplicación puede generar, puede especificar la configuración de notificación y la configuración de almacenamiento en la pestaña **Configuración de eventos** en la directiva de la aplicación. Para el Servidor de administración, también puede ver y configurar la lista de eventos en las propiedades del Servidor de administración. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

Eventos del Servidor de administración: nivel Error funcional

Nombre que se muestra para el tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo de almacenamiento predeterminado
Error al copiar las actualizaciones a la carpeta especificada	4123	KLSRV_UPD_REPL_FAIL	Los eventos de este tipo se producen cuando las actualizaciones de software se copian en una carpeta compartida adicional. Puede responder al evento de los siguientes modos: • Verifique si la cuenta de usuario que se emplea para obtener acceso a la(s) carpeta(s) tiene permiso de escritura. • Compruebe si se cambiaron nombre de usuario o contraseña de las carpetas. • Compruebe la conexión a Internet, ya que podría ser la causa del evento. Siga las instrucciones para actualizar las bases de datos y los módulos de software.	180 días

Nombre que se muestra para el tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo de almacenamiento predeterminado
Error al sondear el segmento de la nube	4143	KLSRV_KLCLOUD_SCAN_ERROR	Los eventos de este tipo ocurren cuando el Servidor de administración no puede sondear un segmento de red en un entorno de nube. Lea los detalles en la descripción del evento y responda en consecuencia.	No se almacena
Límite de instalaciones excedido en uno de los grupos de aplicaciones con licencia	4126	KLSRV_INVLICPROD_EXCEDED	El Servidor de administración genera eventos de este tipo periódicamente (cada una hora). Los eventos de este tipo ocurren si administra claves de licencia de aplicaciones de terceros en Kaspersky Security Center Linux y si el número de instalaciones ha superado el límite establecido por la clave de licencia de la aplicación de terceros. Puede responder al evento de los siguientes modos: • Revise la lista de dispositivos administrados. Si la aplicación del tercero no se está utilizando en algún dispositivo, desinstálela de ese equipo. • Solicite al tercero una licencia para más dispositivos. Para administrar las claves de licencia de sus aplicaciones de terceros, utilice la característica de grupos de aplicaciones con licencia. Un grupo de aplicaciones con licencia está formado por aplicaciones de terceros que cumplen con los criterios que usted define.	180 días
No queda espacio libre en disco	4107	KLSRV_DISK_FULL	Los eventos de este tipo ocurren cuando el disco duro del dispositivo donde está instalado el Servidor de administración se queda sin espacio libre. Libere espacio en el disco del dispositivo.	180 días
No hay espacio libre en la base de datos del Servidor de administración	4110	KLSRV_DATABASE_FULL	Los eventos de este tipo ocurren cuando no hay espacio libre en la base de datos del Servidor de administración. El Servidor de administración no funciona cuando su base de datos ha alcanzado su capacidad y cuando no es posible realizar un nuevo registro en la base de datos. Las siguientes son las causas de este evento (agrupadas por DBMS) y distintas maneras en las que puede responder al mismo: • Limite el número de eventos que se almacenan en la base de datos del Servidor de administración. • La base de datos del Servidor de administración contiene demasiados eventos enviados por el componente Control de aplicaciones. Puede abrir la directiva de Kaspersky Endpoint Security y modificar los ajustes vinculados al almacenamiento de eventos de Control de aplicaciones en la base de datos del Servidor de administración. Revise la información sobre la selección del DBMS.	180 días
Error en tiempo de ejecución	4125	KLSRV_RUNTIME_ERROR	Los eventos de este tipo ocurren debido a problemas desconocidos. En la mayoría de los casos, estos son problemas de DBMS, problemas de red y otros problemas de software y hardware. Los detalles del evento se pueden encontrar en la descripción del evento.	180 días

Nombre que se muestra para el tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo de almacenamiento predeterminado
La carpeta compartida no está disponible	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	Los eventos de este tipo se producen si la carpeta compartida del Servidor de administración no está disponible. Puede responder al evento de los siguientes modos: • Compruebe si el Servidor de administración (donde se encuentra la carpeta compartida) está encendido y disponible. • Compruebe si se cambió/cambiaron un nombre de usuario y / o una contraseña de la carpeta. • Compruebe la conexión de red.	180 días
La base de datos del Servidor de administración no está disponible	4109	KLSRV_DATABASE_UNAVAILABLE	Los eventos de este tipo ocurren si la base de datos del Servidor de administración deja de estar disponible. Puede responder al evento de los siguientes modos: • Compruebe si el servidor remoto que tiene instalado DBMS está disponible. • Vea los registros de DBMS para descubrir el motivo de la falta de disponibilidad de la base de datos del Servidor de administración.	180 días

Eventos del Servidor de administración: nivel Advertencia

En la siguiente tabla se muestran los eventos del Agente de red que tienen el nivel de gravedad **Advertencia**.

Para cada evento que una aplicación puede generar, puede especificar la configuración de notificación y la configuración de almacenamiento en la pestaña **Configuración de eventos** en la directiva de la aplicación. Para el Servidor de administración, también puede ver y configurar la lista de eventos en las propiedades del Servidor de administración. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

Eventos del Servidor de administración: nivel Advertencia

Nombre que se muestra para el tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo de almacenamiento predeterminado
El certificado del Servidor de administración para dispositivos móviles está a punto de caducar	6128	KLSRV_EV_SRV_CERT_EXPIRES_SOON	Este tipo de evento ocurre cuando caducan los certificados del Servidor de administración para los dispositivos móviles y dispositivos UEFI. Debe actualizar el certificado caducado.	90 días
El certificado de APNs caducará pronto	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	Este tipo de evento ocurre cuando quedan menos de catorce días para que caduque el certificado de APNs. Cuando el certificado de APNs caduca, debe renovarlo manualmente e instalarlo en un servidor de MDM para iOS. Le recomendamos que programe la renovación del certificado de APNs para antes de la fecha de caducidad.	No se almacena

Nombre que se muestra para el tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo de almacenamiento predeterminado
El certificado de APNs caducó	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Este tipo de evento ocurre cuando caduca un certificado de APNs. Debe renovar manualmente el certificado de APNs e instalarlo en un servidor de MDM para iOS.	No se almacena
Auditoría: La prueba de conexión al servidor de SIEM produjo un error	5120	KLAUD_EV_SIEM_TEST_FAILED	Los eventos de este tipo ocurren cuando se produce un error en una prueba de conexión automática al servidor SIEM.	90 días
Se eliminó el certificado	4134	KLSRV_CERTIFICATE_REMOVED	Este tipo de evento ocurre cuando un administrador elimina un certificado de cualquier tipo (general, de correo o de VPN) para Administración de dispositivos móviles. Después de que se elimina un certificado, los dispositivos móviles que lo habían utilizado para conectarse pierden la capacidad de establecer conexión con el Servidor de administración. Este evento puede resultar útil a la hora de investigar fallas asociadas con la administración de dispositivos móviles.	90 días
Se solicitó el certificado	4133	KLSRV_CERTIFICATE_REQUESTED	Este tipo de evento ocurre cuando un certificado de la característica Administración de dispositivos móviles no se vuelve a emitir automáticamente. Estas pueden ser las causas del evento y las respuestas adecuadas: • Se intentó reemitir automáticamente un certificado para el que estaba deshabilitada la opción **Volver a emitir certificados automáticamente si es posible**. Esto puede deberse a un error ocurrido durante la creación del certificado. Es posible que se requiera la reemisión manual del certificado. • Si utiliza una integración con una infraestructura de clave pública, la causa podría ser la falta de un atributo SAM-Account-Name de la cuenta utilizada para la integración con PKI y para la emisión del certificado. Revise las propiedades de la cuenta.	90 días
Conflicto de nombres de dispositivo	4102	KLSRV_EVENT_HOSTS_CONFLICT	Este tipo de evento ocurre cuando el Servidor de administración considera que dos o más dispositivos administrados son un mismo dispositivo. A menudo, esto sucede cuando se utiliza un disco duro clonado para desplegar aplicaciones en los dispositivos administrados, pero el Agente de red del dispositivo de referencia no estaba puesto en el modo de clonación de disco dedicado. Para evitar este problema, ponga el Agente de red en modo de clonación de disco en el dispositivo de referencia antes de clonar el disco duro de ese dispositivo.	90 días
Se interrumpió la conexión con el Servidor de administración principal	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	Este tipo de evento ocurre cuando se interrumpe una conexión con el Servidor de administración principal. Consulte el registro del sistema operativo en el dispositivo en el que esté instalado el Servidor de administración principal y responda en consecuencia.	90 días

Nombre que se muestra para el tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo de almacenamiento predeterminado
Se interrumpió la conexión con el Servidor de administración secundario	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	Este tipo de evento ocurre cuando se interrumpe una conexión con el Servidor de administración secundario. Consulte el registro del sistema operativo en el dispositivo en el que esté instalado el Servidor de administración secundario y responda en consecuencia.	90 días
El dispositivo estuvo inactivo en la red por mucho tiempo	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	Este tipo de evento ocurre cuando un dispositivo administrado se encuentra inactivo durante cierto tiempo. La mayoría de las veces, esto sucede porque el dispositivo se ha dado de baja. Puede responder al evento de los siguientes modos: • Elimine el dispositivo manualmente de la lista de dispositivos administrados. Defina el intervalo de tiempo después del cual se creará el evento **El dispositivo ha estado inactivo en la red por mucho tiempo** a través de Kaspersky Security Center Web Console. • Defina el intervalo de tiempo después del cual el dispositivo se eliminará automáticamente del grupo a través de Kaspersky Security Center Web Console.	90 días
El estado del dispositivo es Advertencia	4114	KLSRV_HOST_STATUS_WARNING	Este tipo de evento ocurre cuando se le asigna el estado *Advertencia* a un dispositivo administrado. Puede configurar las condiciones en las cuales el estado del dispositivo se cambia a *Advertencia*.	90 días
No se pudo descargar el archivo en el dispositivo	4165	KLSRV_FILE_DOWNLOAD_FAILED	Los eventos de este tipo ocurren en los siguientes casos: • Intenta descargar un archivo al contenedor corporativo, pero no se creó un contenedor corporativo. • No hay suficiente espacio en el dispositivo. • La información acerca del archivo no se pudo descargar del servidor. • El contenido del archivo no se pudo descargar del servidor. • No se pudo crear la carpeta en el dispositivo. • Falta el permiso de acceso al archivo en el dispositivo personal. • Falta el permiso de acceso al archivo en el contenedor corporativo.	90 días

Nombre que se muestra para el tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo de almacenamiento predeterminado
No se pudo enviar el mensaje de FCM al servidor de FCM	4140	KLSRV_GCM_GENERAL_ERROR	Este tipo de evento ocurre cuando suceden errores inesperados del lado del Servidor de administración al utilizar el protocolo HTTP de Google Firebase Cloud Messaging. Lea los detalles en la descripción del evento y responda en consecuencia. Si no puede encontrar la solución a un problema por su cuenta, le recomendamos que se comunique con el servicio de soporte técnico de Kaspersky.	90 días
No se pudo enviar el mensaje de FCM al dispositivo móvil	4138	KLSRV_GCM_DEVICE_ERROR	Los eventos de este tipo ocurren cuando la Administración de dispositivos móviles está configurada para usar Google Firebase Cloud Messaging (FCM) para conectarse a dispositivos móviles administrados con un sistema operativo Android y el servidor de FCM no puede manejar algunas de las solicitudes recibidas del Servidor de administración. Lo que esto significa es que algunos de los dispositivos móviles administrados no recibirán una notificación push. Lea el código HTTP en los detalles de la descripción del evento y responda en consecuencia. Para obtener más información sobre los códigos HTTP recibidos del servidor de FCM y los errores relacionados, consulte la documentación del servicio Google Firebase (en especial, el capítulo "Códigos de respuesta de errores de mensajes descendentes").	90 días
Se detectaron eventos frecuentes		KLSRV_EVENT_SPAM_EVENTS_DETECTED	Este tipo de evento ocurre cuando el Servidor de administración detecta un evento frecuente en un dispositivo administrado. Consulte la siguiente sección para obtener más información: Bloquear eventos frecuentes.	90 días
El disco duro está casi lleno	4105	KLSRV_NO_SPACE_ON_VOLUMES	Este tipo de evento ocurre cuando se agota el espacio en el disco duro del dispositivo en el que está instalado el Servidor de administración. Libere espacio en el disco del dispositivo.	90 días

Nombre que se muestra para el tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo de almacenamiento predeterminado
Error de HTTP al enviar un mensaje del FCM al servidor de FCM	4139	KLSRV_GCM_HTTP_ERROR	Los eventos de este tipo ocurren cuando la Administración de dispositivos móviles está configurada para usar Google Firebase Cloud Messaging (FCM) para conectar dispositivos móviles administrados con el sistema operativo Android y el servidor de FCM devuelve al Servidor de administración una solicitud con un código HTTP distinto de 200 (OK). Estas pueden ser las causas del evento y las respuestas adecuadas: • Problemas en el servidor de FCM. Lea el código HTTP en los detalles de la descripción del evento y responda en consecuencia. Para obtener más información sobre los códigos HTTP recibidos del servidor de FCM y los errores relacionados, consulte la documentación del servicio Google Firebase (en especial, el capítulo "Códigos de respuesta de errores de mensajes descendentes"). • Problemas en el servidor proxy (si usa un servidor proxy). Lea el código HTTP en los detalles de la descripción del evento y responda en consecuencia.	90 días
Se superó el límite de la licencia	4098	KLSRV_EV_LICENSE_CHECK_100_110	Una vez al día, Kaspersky Security Center Linux comprueba si se superó algún límite de licencia. Este tipo de evento ocurre cuando el Servidor de administración detecta que las aplicaciones de Kaspersky instaladas en los dispositivos cliente han superado algún límite de sus licencias y si se ha utilizado entre un 100 % y un 110 % del total de unidades con licencia cubiertas por una sola licencia. Los dispositivos cliente se mantienen protegidos aun cuando ocurre este evento. Puede responder al evento de los siguientes modos: • Revise la lista de dispositivos administrados. Elimine los dispositivos que no estén en uso. • Agregue una licencia para más dispositivos (agregue un código de activación válido o un archivo de clave en el Servidor de administración). Kaspersky Security Center Linux determina las reglas para generar eventos cuando se supera un límite de licencia.	90 días

Nombre que se muestra para el tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo de almacenamiento predeterminado
Pronto se alcanzará el límite de instalaciones para uno de los grupos de aplicaciones con licencia	4128	KLSRV_INVLICPROD_EXPIRED_SOON	Los eventos de este tipo ocurren cuando una de las claves de licencia para aplicaciones de terceros incluidas en un grupo de aplicaciones con licencia está a punto de caducar. Como resultado, se reducirá el límite de instalación para uno de los grupos. Puede responder al evento de los siguientes modos: • Si la aplicación de terceros no se utiliza en algunos de los dispositivos administrados, elimínela de esos dispositivos. • Si estima que la cantidad de instalaciones para la aplicación de terceros superará el máximo permitido en un futuro próximo, considere contactarse con el tercero antes de que eso suceda para obtener una licencia para una cantidad de dispositivos mayor. Para administrar las claves de licencia de sus aplicaciones de terceros, utilice la característica de grupos de aplicaciones con licencia.	90 días
Se registraron nuevas actualizaciones para los módulos de la aplicación de Kaspersky	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	Este tipo de evento ocurre cuando el Servidor de administración registra nuevas actualizaciones para el software de Kaspersky instalado en los dispositivos administrados y se necesita que usted apruebe la instalación de esas actualizaciones. Apruebe o rechace las actualizaciones mediante Kaspersky Security Center Web Console.	90 días
No hay espacio libre en la base de datos del Servidor de administración	4106	KLSRV_NO_SPACE_IN_DATABASE	Este tipo de evento ocurre cuando el espacio disponible en la base de datos del Servidor de administración es demasiado limitado. De no resolverse esta situación, la base de datos del Servidor de administración alcanzará rápidamente su límite de capacidad y el Servidor de la administración dejará de funcionar. Las siguientes son las causas de este evento (agrupadas por DBMS) y las distintas maneras en las que puede responder. • No limite el número de eventos que se almacenan en la base de datos del Servidor de administración. • Reduzca la lista de eventos que se almacenan en la base de datos del Servidor de administración. Revise la información sobre la selección del DBMS.	90 días

Nombre que se muestra para el tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo de almacenamiento predeterminado
Se superó el límite del número de eventos en la base de datos, se inició la eliminación de eventos	4145	KLSRV_EVP_DB_TRUNCATING	Este tipo de evento ocurre cuando el sistema comienza a eliminar eventos antiguos de la base de datos del Servidor de administración por haberse alcanzado el límite de capacidad de la misma. Puede responder al evento de los siguientes modos: • Cambie el número de eventos que se conservará, como máximo, en la base de datos del Servidor de administración. • Reduzca la lista de eventos que se almacenan en la base de datos del Servidor de administración.	No se almacena
Se superó el límite del número de eventos en la base de datos, se eliminaron los eventos	4146	KLSRV_EVP_DB_TRUNCATED	Este tipo de evento ocurre cuando el sistema eliminó eventos antiguos de la base de datos del Servidor de administración por haberse alcanzado el límite de capacidad de la misma. Puede responder al evento de los siguientes modos: • Cambie el número de eventos que se conservará, como máximo, en la base de datos del Servidor de administración. • Reduzca la lista de eventos que se almacenan en la base de datos del Servidor de administración.	No se almacena

Eventos del Servidor de administración: nivel Información

En la siguiente tabla, se enumeran los eventos del Servidor de administración que tienen el nivel de importancia **Información**.

Para cada evento que una aplicación puede generar, puede especificar la configuración de notificación y la configuración de almacenamiento en la pestaña **Configuración de eventos** en la directiva de la aplicación. Para el Servidor de administración, también puede ver y configurar la lista de eventos en las propiedades del Servidor de administración. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

Eventos del Servidor de administración: nivel Información

Nombre que se muestra para el tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo de almacenamiento predeterminado
Se está renovando el certificado del Servidor de administración para dispositivos móviles	6127	KLSRV_EV_SRV_CERT_RENEWED	Este evento ocurre tras renovarse el certificado del Servidor de administración.	30 días
Auditoría: Se envió el comando al dispositivo	4170	KLAUD_EV_COMMAND_SENT	Los eventos de este tipo ocurren cuando el usuario envía un comando al dispositivo móvil.	30 días
Auditoría: Se cerró la conexión con el Servidor de administración	4151	KLAUD_EV_SERVERDISCONNECT		30 días

Nombre que se muestra para el tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo de almacenamiento predeterminado
Auditoría: Se estableció la conexión con el Servidor de administración	4147	KLAUD_EV_SERVERCONNECT	Los eventos de este tipo ocurren cuando un usuario se conecta al Servidor de administración mediante Kaspersky Security Center Web Console. Estos eventos incluyen la dirección IP del dispositivo donde está instalado el Servidor de Kaspersky Security Center Web Console.	30 días
Auditoría: Claves de cifrado importadas/exportadas	5100	KLAUD_EV_DPEKEYSEXPORT	Por ejemplo, este evento tiene lugar durante la migración.	30 días
Auditoría: La configuración del grupo se modificó	4149	KLAUD_EV_ADMGROUP_CHANGED	Los eventos de este tipo ocurren cuando se edita un grupo de seguridad.	30 días
Auditoría: El objeto se modificó	4148	KLAUD_EV_OBJECTMODIFY	Este evento responde a cambios ocurridos en los siguientes objetos: • Grupo de administración • Grupo de seguridad • Usuario • Dispositivo administrado • Paquete • Tarea • Directiva • Servidores • Servidor virtual	30 días
Auditoría: Las propiedades del objeto se modificaron	4152	KLAUD_EV_OBJECTPROPMODIFIED	Este evento responde a cambios ocurridos en las siguientes propiedades: • Usuario • Licencia • Servidores • Servidor virtual	30 días
Auditoría: El estado del objeto se modificó	4150	KLAUD_EV_TASK_STATE_CHANGED	Este evento ocurre, por ejemplo, cuando una tarea no se completa debido a un error.	30 días
Auditoría: La prueba de conexión al servidor de SIEM se realizó correctamente	5110	KLAUD_EV_SIEM_TEST_SUCCESS	Los eventos de este tipo ocurren cuando una prueba de conexión al servidor SIEM se realiza correctamente.	30 días
Auditoría: Las propiedades del usuario se modificaron	4153	KLAUD_EV_OBJECTACLMODIFIED	Este evento ocurre cuando se modifican los permisos del usuario.	30 días
Se estableció la conexión con el Servidor de administración principal	4117	KLSRV_EV_MASTER_SRV_CONNECTED		30 días

Nombre que se muestra para el tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo de almacenamiento predeterminado
Se estableció la conexión con el Servidor de administración secundario	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	Consulte el siguiente artículo para obtener más detalles: Creación de una jerarquía de servidores de administración: agregar un Servidor de administración secundario.	30 días
Las bases de datos se actualizaron	4144	KLSRV_UPD_BASES_UPDATED	Los eventos de este tipo ocurren cuando la tarea **Descargar actualizaciones en el repositorio del Servidor de administración** termina de actualizar las bases de datos.	30 días
El dispositivo se movió automáticamente de acuerdo con una regla	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	Este tipo de evento ocurre cuando los dispositivos se trasladaron a un grupo mediante las reglas de movimiento de dispositivos. Se publica un evento independiente por cada dispositivo trasladado.	30 días
Dispositivo eliminado del grupo: estuvo inactivo en la red por mucho tiempo	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	Los eventos de este tipo ocurren cuando los dispositivos se eliminan automáticamente de un grupo por inactividad.	30 días
El id. de instancia de FCM cambió en este dispositivo móvil	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	Los eventos de este tipo ocurren cuando el token de Firebase Cloud Messaging (FCM) cambia en el dispositivo. Para obtener información sobre la rotación de tokens de FCM, consulte la documentación del servicio Firebase.	30 días
Archivo cargado al Servidor de administración	4162	KLSRV_FILE_UPLOADED	Los eventos de este tipo ocurren si el administrador ha cargado un archivo en la lista de **Administración de activos → Mobile → Apps & files → Files**.	30 días
Archivo eliminado del Servidor de administración	4163	KLSRV_FILE_REMOVED	Los eventos de este tipo ocurren si el administrador ha eliminado un archivo de la lista de **Administración de activos → Mobile → Apps & files → Files**.	30 días
Archivo descargado en el dispositivo	4164	KLSRV_FILE_DOWNLOADED	Los eventos de este tipo ocurren en los siguientes casos: • El administrador ha descargado un archivo de la lista **Administración de activos → Mobile → Apps & files → Files** de Web Console a la estación de trabajo del administrador. • Se ha descargado un archivo de la lista **Administración de activos → Mobile → Apps & files → Files** a un dispositivo en el que está instalado Kaspersky Endpoint Security para Android.	30 días

Nombre que se muestra para el tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo de almacenamiento predeterminado
No se ha podido descargar el archivo al dispositivo	4165	KLSRV_FILE_DOWNLOAD_FAILED	Los eventos de este tipo ocurren en los siguientes casos: • Se produjo un error cuando el administrador intentó descargar un archivo de la lista **Administración de activos → Mobile → Apps & files → Files** de Web Console a la estación de trabajo del administrador. • Se produjo un error al descargar un archivo de la lista **Administración de activos → Mobile → Apps & files → Files** a un dispositivo en el que está instalado Kaspersky Endpoint Security para Android.	30 días
Se encontraron archivos para enviar a Kaspersky para su análisis	4131	KLSRV_APS_FILE_APPEARED		30 días
El límite de instalaciones está por alcanzarse (se consumió más del 90 %) en uno de los grupos de aplicaciones con licencia	4127	KLSRV_INVLICPROD_FILLED	Los eventos de este tipo ocurren cuando el número de instalaciones de aplicaciones de terceros incluidas en un grupo de aplicaciones con licencia alcanza el 90 % del valor máximo permitido especificado en las propiedades de la clave de licencia. Puede responder al evento de los siguientes modos: • Si la aplicación de terceros no se utiliza en algunos de los dispositivos administrados, elimínela de esos dispositivos. • Si estima que la cantidad de instalaciones para la aplicación de terceros superará el máximo permitido en un futuro próximo, considere contactarse con el tercero antes de que eso suceda para obtener una licencia para una cantidad de dispositivos mayor. Para administrar las claves de licencia de sus aplicaciones de terceros, utilice la característica de grupos de aplicaciones con licencia.	30 días
Se detectó un nuevo dispositivo	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	Este tipo de evento ocurre cuando se descubren nuevos dispositivos en red.	30 días

Nombre que se muestra para el tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo de almacenamiento predeterminado
Se consumió más del 90 % de la clave de licencia	4097	KLSRV_EV_LICENSE_CHECK_90	Este tipo de evento ocurre cuando el Servidor de administración detecta que las aplicaciones de Kaspersky instaladas en los dispositivos cliente han superado algún límite de sus licencias y si se ha utilizado más de un 90 % del total de unidades con licencia cubiertas por una sola licencia. Los dispositivos cliente están protegidos incluso cuando se supera un límite de licencia. Puede responder al evento de los siguientes modos: • Revise la lista de dispositivos administrados. Elimine los dispositivos que no estén en uso. • Agregue una licencia para más dispositivos (agregue un código de activación válido o un archivo de clave en el Servidor de administración). Kaspersky Security Center Linux determina las reglas para generar eventos cuando se supera un límite de licencia.	30 días
Se creó el certificado de reserva del Servidor de administración para dispositivos móviles	6126	KLSRV_EV_SRV_CERT_RESERVE_CREATED	Este evento ocurre tras crearse un certificado del Servidor de Administración.	30 días
Las actualizaciones se copiaron correctamente en la carpeta especificada	4122	KLSRV_UPD_REPL_OK	Los eventos de este tipo ocurren cuando la tarea **Descargar actualizaciones en el repositorio del Servidor de administración** termina de copiar archivos en una carpeta específica.	30 días

Los eventos de **Certificado de reserva creado** y de **Renovación del certificado** se publican automáticamente mediante el Servidor de administración y se muestran en la Consola de administración solo cuando las operaciones relativas a estos eventos se realizan respecto de certificados del Servidor de administración para dispositivos móviles y dispositivos UEFI.

Eventos del Agente de red

En esta sección, se brinda información sobre los eventos relacionados con el Agente de red.

Eventos del Agente de red: nivel Error funcional

En la siguiente tabla, se muestran los eventos del Agente de red de Kaspersky Security Center Linux que tienen el nivel de gravedad **Error funcional**.

Puede definir los ajustes de notificación y los ajustes de almacenamiento para cada uno de los eventos que pueda generar una aplicación; para ello debe dirigirse a la pestaña **Configuración de eventos** en la directiva de la aplicación. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

Eventos del Agente de red: nivel Error funcional

Nombre que se muestra para el tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo de almacenamiento predeterminado
No se pudieron instalar los certificados raíz	7728	KLNAG_EV_ROOT_CERT_INSTALL_ERR	El evento contiene la descripción correspondiente al error de instalación de los certificados.	30 días
Error al instalar la actualización de software de terceros	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	Este tipo de evento ocurre cuando se utiliza la función Administración de vulnerabilidades y parches y la instalación de actualizaciones de software de terceros no se realiza correctamente. Compruebe si el enlace al software desarrollado por el tercero es válido. Lea la descripción del evento.	30 días
Error al instalar las actualizaciones de Windows Update	7717	KLNAG_EV_WUA_INSTALL_ERROR	Este tipo de evento ocurre cuando no se pueden instalar las actualizaciones de Windows. Lea la descripción del evento. Busque el error en Microsoft Knowledge Base. Póngase en contacto con el servicio de soporte técnico de Microsoft si no puede resolver el problema por su cuenta.	30 días
No se pudieron eliminar los certificados raíz	7730	KLNAG_EV_ROOT_CERT_REMOVE_ERR	El evento contiene la descripción correspondiente al error de eliminación de certificados.	30 días
No se pudo restaurar el archivo sudoers al valor de referencia	7726	KLNAG_EV_SUDOER_RESTORED_ERR	El evento contiene la descripción correspondiente al error de reemplazo del archivo sudoers.	30 días
Error de instalación de la actualización	7702	KLNAG_EV_PATCH_INSTALL_ERROR	Los eventos de este tipo se producen si la actualización automática y la aplicación de parches para los componentes de Kaspersky Security Center Linux no se realizaron correctamente. El evento no está vinculado a la actualización de las aplicaciones de Kaspersky administradas. Lea la descripción del evento. El evento puede tener su origen en un problema de Windows ocurrido en el Servidor de administración. Si la descripción menciona algún problema con la configuración de Windows, resuelva ese problema.	30 días
Administración de usuarios: errores	7723	KLNAG_EV_USR_MNG_ERR	Evento de advertencia general.	30 días

Eventos del Agente de red: nivel Advertencia

En la siguiente tabla se muestran los eventos del Agente de red que tienen el nivel de gravedad **Advertencia**.

Puede definir los ajustes de notificación y los ajustes de almacenamiento para cada uno de los eventos que pueda generar una aplicación; para ello debe dirigirse a la pestaña **Configuración de eventos** en la directiva de la aplicación. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

Eventos del Agente de red: nivel Advertencia

Nombre que se muestra para el tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo de almacenamiento predeterminado
Se inició el Proxy de KSN. No se pudo comprobar la disponibilidad de KSN	7718	KSNPROXY_STARTED_CON_CHK_FAILED	Los eventos de este tipo ocurren cuando falla la conexión de prueba de la conexión configurada del proxy de KSN.	30 días
Ocurrió un problema de seguridad	549	GNRL_EV_APP_INCIDENT_OCCURED	Los eventos de este tipo ocurren al descubrir un incidente en un dispositivo. Por ejemplo, este evento tiene lugar cuando el dispositivo tiene poco espacio en disco.	30 días
El archivo sudoers encontrado no coincide con el valor de referencia	7724	KLNAG_EV_SUDOER_DIFFERENT	Los eventos de este tipo ocurren cuando hay una discrepancia entre el archivo sudoers y el archivo de referencia.	30 días
La instalación de la actualización de software de terceros se ha pospuesto	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	Por ejemplo, los eventos de este tipo tienen lugar cuando se rechaza el EULA al instalar una actualización de terceros.	30 días
La instalación de la actualización de software de terceros se ha completado con una advertencia	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	Descargue los archivos de seguimiento y verifique el valor del campo KLRI_PATCH_RES_DESC para obtener más información.	30 días
Administración de usuarios: advertencias	7722	KLNAG_EV_USR_MNG_WRN	Evento de advertencia general.	30 días
Se ha devuelto una advertencia durante la instalación de la actualización del módulo de software	7701	KLNAG_EV_PATCH_INSTALL_WARNING	Descargue los archivos de seguimiento y verifique el valor del campo KLRI_PATCH_RES_DESC para obtener más información.	30 días

Eventos del Agente de red: nivel Información

En la siguiente tabla se muestran los eventos del Agente de red que tienen el nivel de gravedad **Información**.

Puede definir los ajustes de notificación y los ajustes de almacenamiento para cada uno de los eventos que pueda generar una aplicación; para ello debe dirigirse a la pestaña **Configuración de eventos** en la directiva de la aplicación. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

Eventos del Agente de red: nivel Información

Nombre que se muestra para el tipo de evento	Id. del tipo de evento	Tipo de evento	Plazo de almacenamiento predeterminado
Se instaló una aplicación	7703	KLNAG_EV_INV_APP_INSTALLED	30 días
Se desinstaló una aplicación	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 días
Se recibió el certificado para el puerto HTTPS del Servidor web	—	WEB_SERVER_CERTIFICATE_RENEWED	30 días
Dispositivo autorizado	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 días
Se detectó un nuevo dispositivo	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 días
Dispositivo eliminado	7709	KLNAG_EV_DEVICE_REMOVE	30 días
Se ha iniciado la instalación de la actualización para los módulos de software	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 días

Nombre que se muestra para el tipo de evento	Id. del tipo de evento	Tipo de evento	Plazo de almacenamiento predeterminado
El proxy de KSN se ha iniciado. La disponibilidad de KSN se verificó correctamente	7719	KSNPROXY_STARTED_CON_CHK_OK	30 días
El Proxy de KSN se detuvo	7720	KSNPROXY_STOPPED	30 días
Se instaló una aplicación supervisada	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 días
Se desinstaló una aplicación supervisada	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 días
Nuevo dispositivo agregado	7708	KLNAG_EV_DEVICE_ARRIVAL	30 días
Certificados raíz instalados	7727	KLNAG_EV_ROOT_CERT_INSTALLED	30 días
Certificados raíz eliminados	7729	KLNAG_EV_ROOT_CERT_REMOVED	30 días
El archivo sudoers se restauró correctamente al valor de referencia	7725	KLNAG_EV_SUDOER_RESTORED	30 días
Se instaló una aplicación de terceros	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 días
La actualización de software de terceros se ha instalado correctamente	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 días
Se ha iniciado la instalación de la actualización de software de terceros	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 días
La actualización para los módulos de software se instaló correctamente	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 días
Administración de usuarios: información	7721	KLNAG_EV_USR_MNG_INF	30 días
Servidor web iniciado en el host	—	WEB_SERVER_STARTED	30 días
Servidor web detenido en el host	—	WEB_SERVER_STOPPED	30 días
Windows Desktop Sharing: la aplicación ha sido iniciada	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 días
Windows Desktop Sharing: el archivo ha sido modificado	7713	KLUSRLOG_EV_FILE_MODIFIED	30 días
Windows Desktop Sharing: el archivo ha sido leído	7712	KLUSRLOG_EV_FILE_READ	30 días
Windows Desktop Sharing: iniciado	7715	KLUSRLOG_EV_WDS_BEGIN	30 días
Windows Desktop Sharing: detenido	7716	KLUSRLOG_EV_WDS_END	30 días

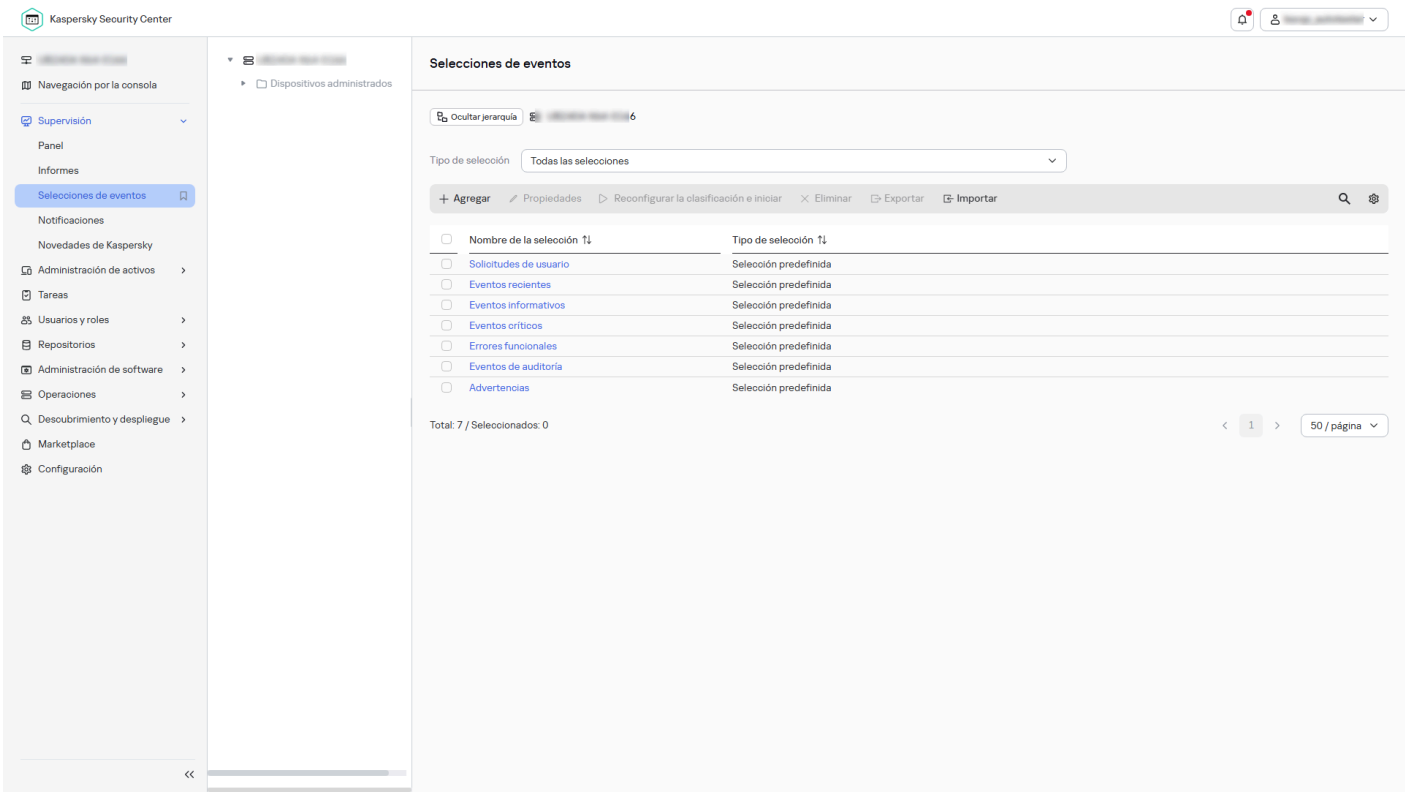
Utilización de selecciones de eventos

Las selecciones de eventos brindan una vista en pantalla de distintos conjuntos de eventos, que se toman de la base de datos del Servidor de administración y se identifican con un nombre. Estos conjuntos de eventos se agrupan y clasifican de distintas maneras:

- Por nivel de importancia: **Eventos críticos**, **Errores funcionales**, **Advertencias** y **Eventos informativos**
- Por fecha: **Eventos recientes**
- Por tipo: **Solicitudes de usuario** y **Eventos de auditoría**

Puede usar los ajustes disponibles en la interfaz de Kaspersky Security Center Web Console para ver y crear selecciones de eventos definidas por el usuario.

Para acceder a las selecciones de eventos disponibles en Kaspersky Security Center Web Console, vaya a la sección **Supervisión** y haga clic en **Selecciones de eventos**.



La lista de selecciones de eventos

De manera predeterminada, las selecciones de eventos incluyen información de los últimos siete días.

Kaspersky Security Center Linux tiene un conjunto predeterminado de las selecciones (predefinidas) de evento:

- Eventos con distintos niveles de importancia:
  - **Eventos críticos**
  - **Error funcional**
  - **Advertencias**
  - **Eventos informativos**
- **Solicitudes de usuario** (eventos de aplicaciones administradas)
- **Eventos recientes** (de la semana anterior)
- Eventos de auditoría.

De ser necesario, puede crear y configurar selecciones adicionales, llamadas selecciones definidas por el usuario. Los eventos de estas selecciones pueden filtrarse de distintas maneras: utilizando las propiedades de los dispositivos que dieron origen a los eventos (el nombre, el intervalo IP y el grupo de administración de esos dispositivos), por tipo de evento, por nivel de gravedad del evento, por intervalo de tiempo y por nombre de aplicación y componente. El ámbito de búsqueda también puede incluir resultados de tareas. Existe además un campo de búsqueda simple, que permite escribir una o varias palabras. Utilice este campo para que se muestren todos los eventos que contengan, en cualquiera de sus atributos (nombre del evento, descripción, nombre del componente, etc.), alguna de las palabras indicadas.

Puede limitar el número de eventos que se muestran y el número de registros que se buscan tanto en las selecciones predefinidas como en las selecciones definidas por el usuario. Ambas opciones afectan al tiempo que tarda Kaspersky Security Center Linux en mostrar los eventos. Cuanto más grande es la base de datos, más lento puede ser el proceso.

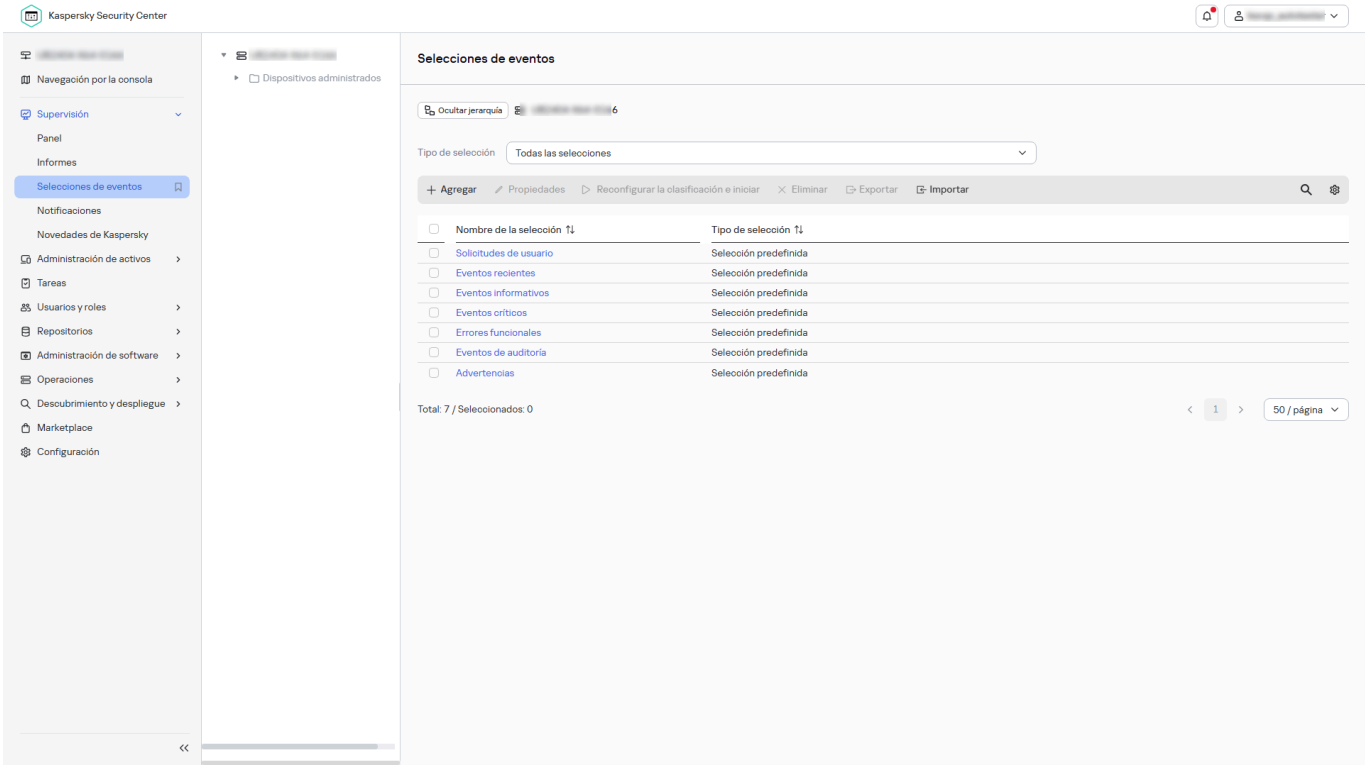
Puede hacer lo siguiente:

- Editar propiedades de selecciones de eventos
- Generar selecciones de eventos
- Ver detalles de las selecciones de eventos
- Eliminar selecciones de eventos
- Eliminar eventos de la base de datos del Servidor de administración

Crear una selección de eventos

Para crear una selección de eventos:

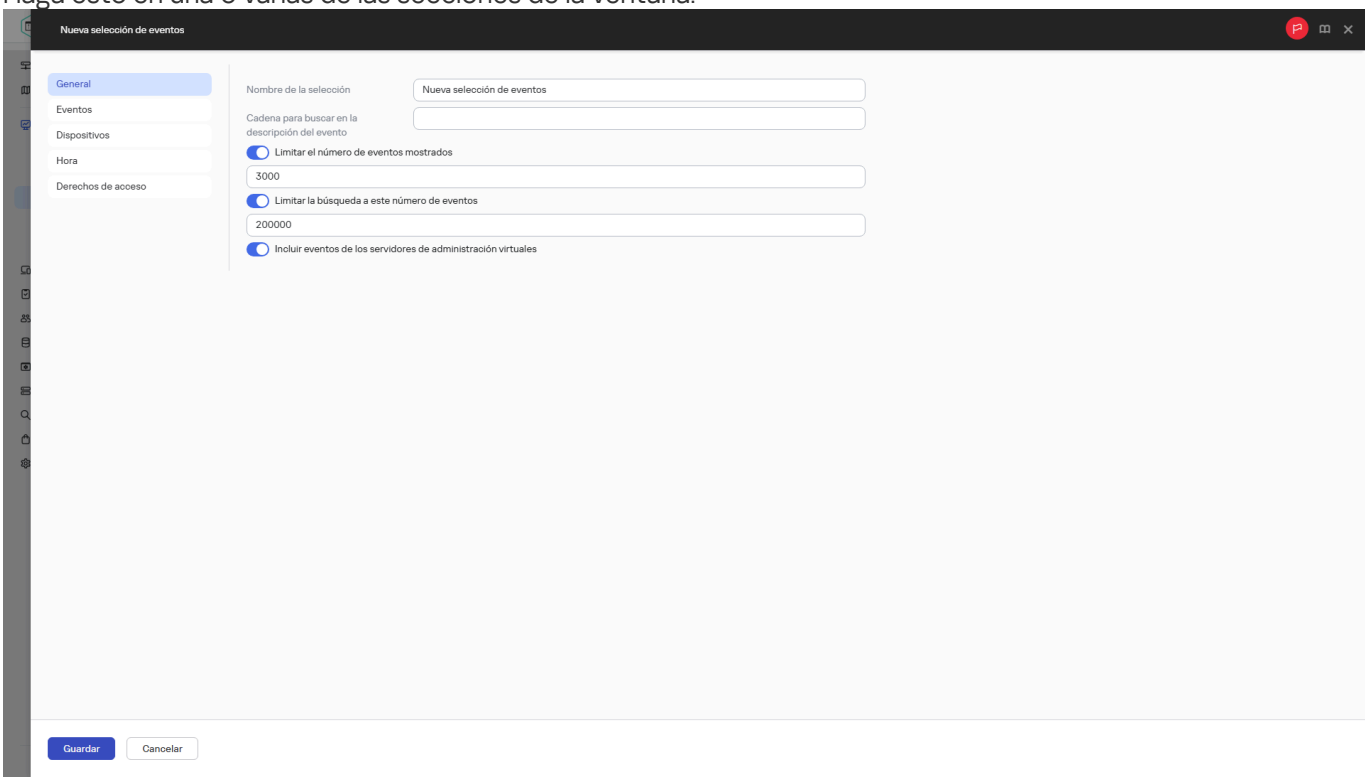
1. En el menú principal, vaya a **Supervisión** → **Selecciones de eventos**.



La lista de selecciones de eventos

2. Haga clic en **Agregar**.

3. En la ventana **Nueva selección de eventos** que se abre, defina los ajustes de la nueva selección de eventos. Haga esto en una o varias de las secciones de la ventana.



Crear una nueva selección de eventos

4. Haga clic en **Guardar** para guardar los cambios.

   Se abre una ventana de confirmación.

5. Para ver el resultado de la selección de eventos, deje marcada la casilla **Ir al resultado de la selección**.

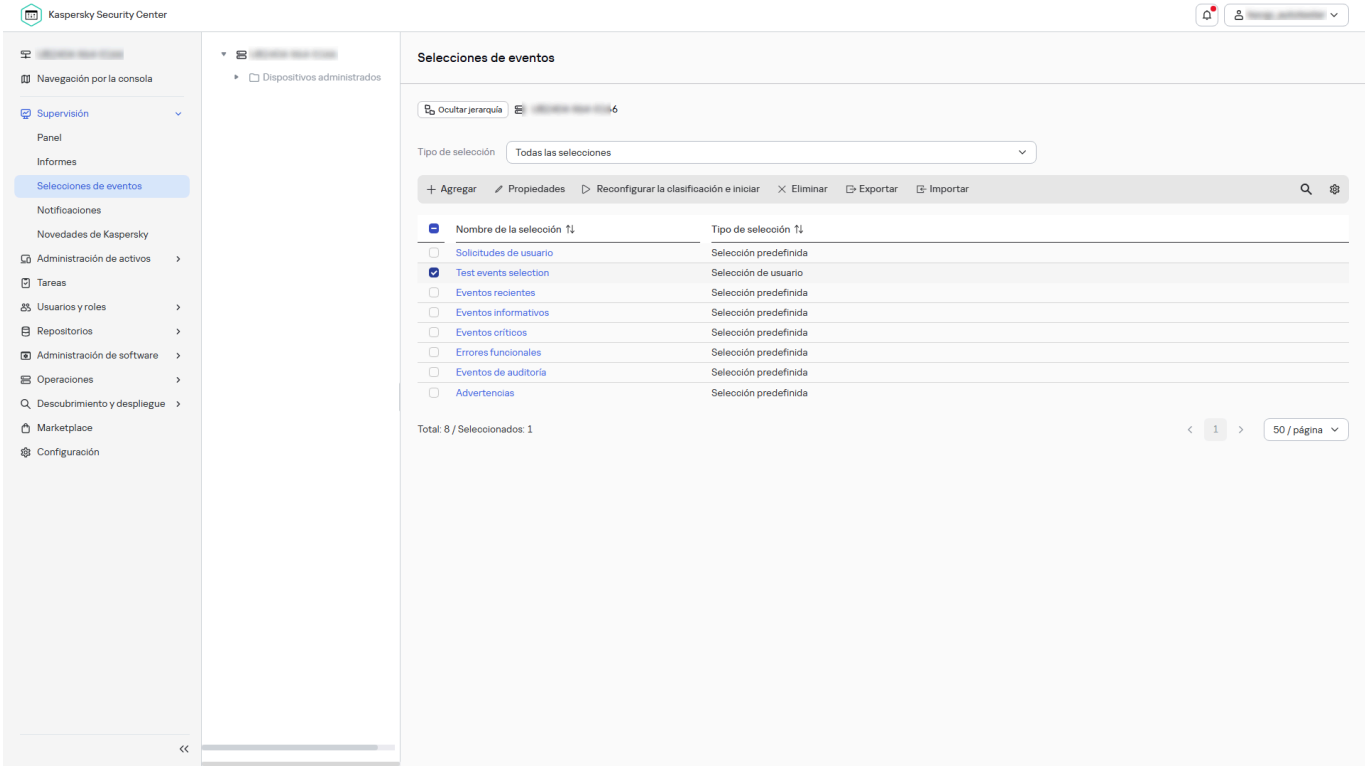
6. Haga clic en **Guardar** para confirmar que desea crear la selección de eventos.

Si dejó marcada la casilla **Ir al resultado de la selección**, verá el resultado de la selección de eventos. De lo contrario, encontrará la nueva selección de eventos en la lista de selecciones de eventos.

Editar una selección de eventos

Para editar una selección de eventos:

1. En el menú principal, vaya a **Supervisión** → **Selecciones de eventos**.
2. Marque la casilla ubicada junto a la selección de eventos que desee editar.



La lista de selecciones de eventos

3. Haga clic en el botón **Propiedades**.

   Se abrirá una ventana para configurar la selección de eventos.

4. Modifique las propiedades de la selección de eventos.

   > Si eligió una selección de eventos predefinida, solo podrá editar las propiedades disponibles en las pestañas **General** (excepto el nombre de la selección), **Hora** y **Derechos de acceso**.

   Si eligió una selección de eventos definida por el usuario, podrá editar cualquiera de las propiedades.

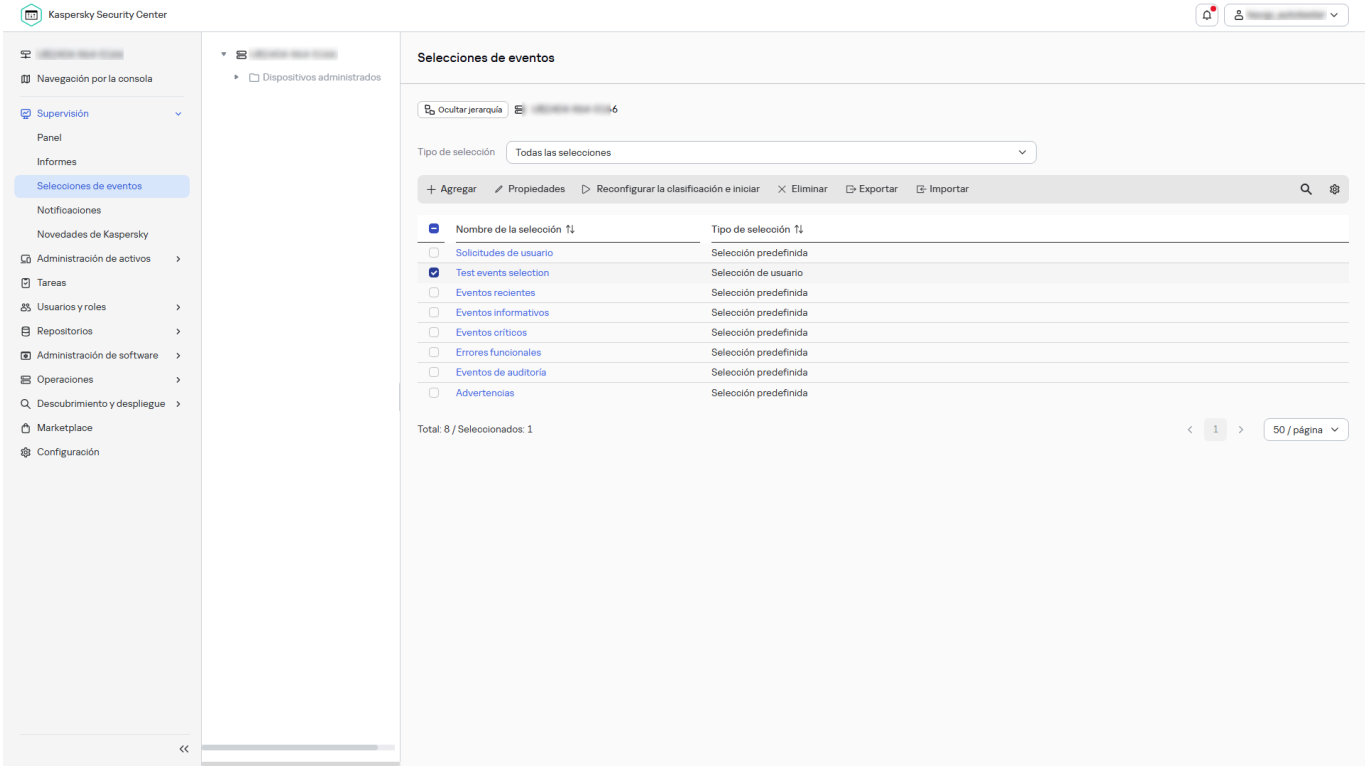
5. Haga clic en **Guardar** para guardar los cambios.

La selección de eventos editada se muestra en la lista.

Ver una lista de una selección de eventos

Para ver una selección de eventos:

1. En el menú principal, vaya a **Supervisión** → **Selecciones de eventos**.
2. Marque la casilla ubicada junto a la selección de eventos que desee iniciar.



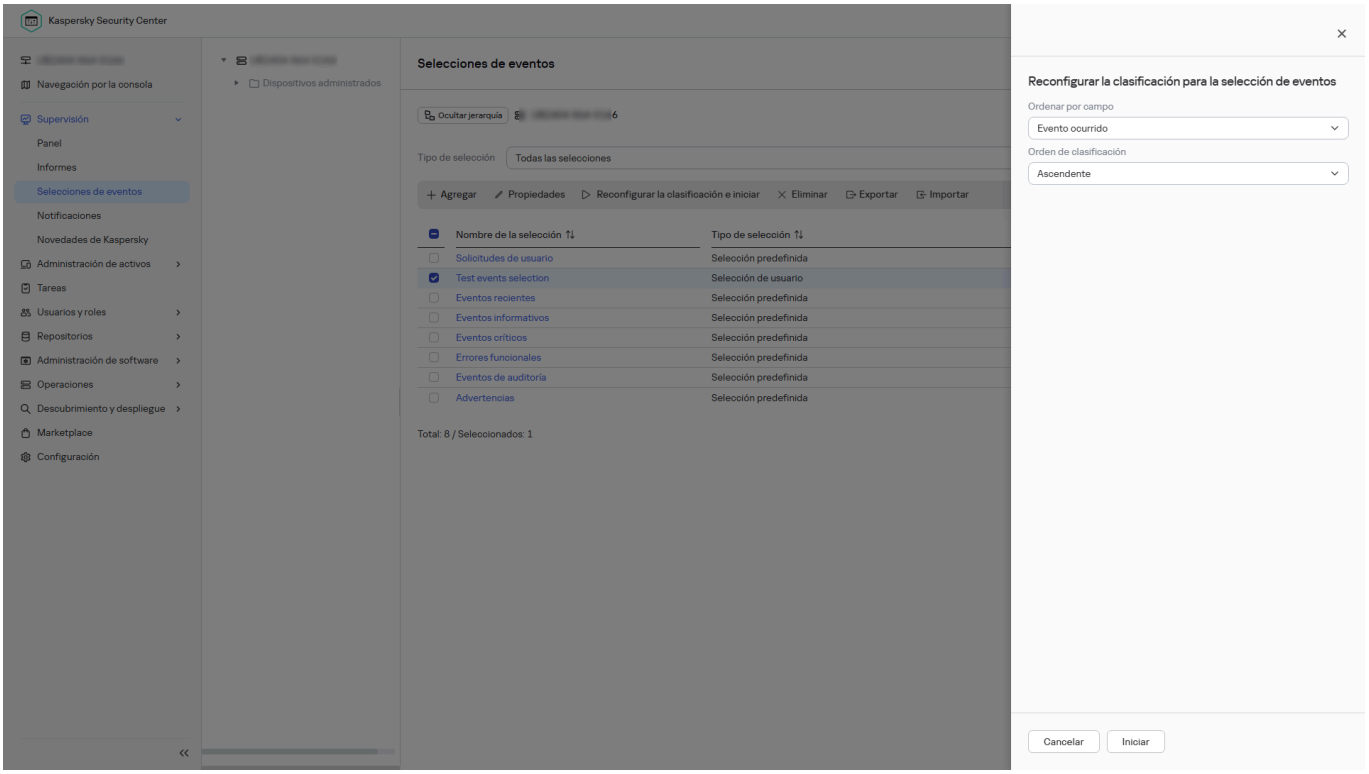
La lista de selecciones de eventos

3. Realice una de las siguientes acciones:

- Si desea configurar la clasificación en el resultado de la selección de eventos, haga lo siguiente:

  a. Haga clic en el botón **Reconfigurar la clasificación e iniciar**.

  b. Cuando se abra la ventana **Reconfigurar la clasificación para la selección de eventos**, ajuste las opciones de clasificación.

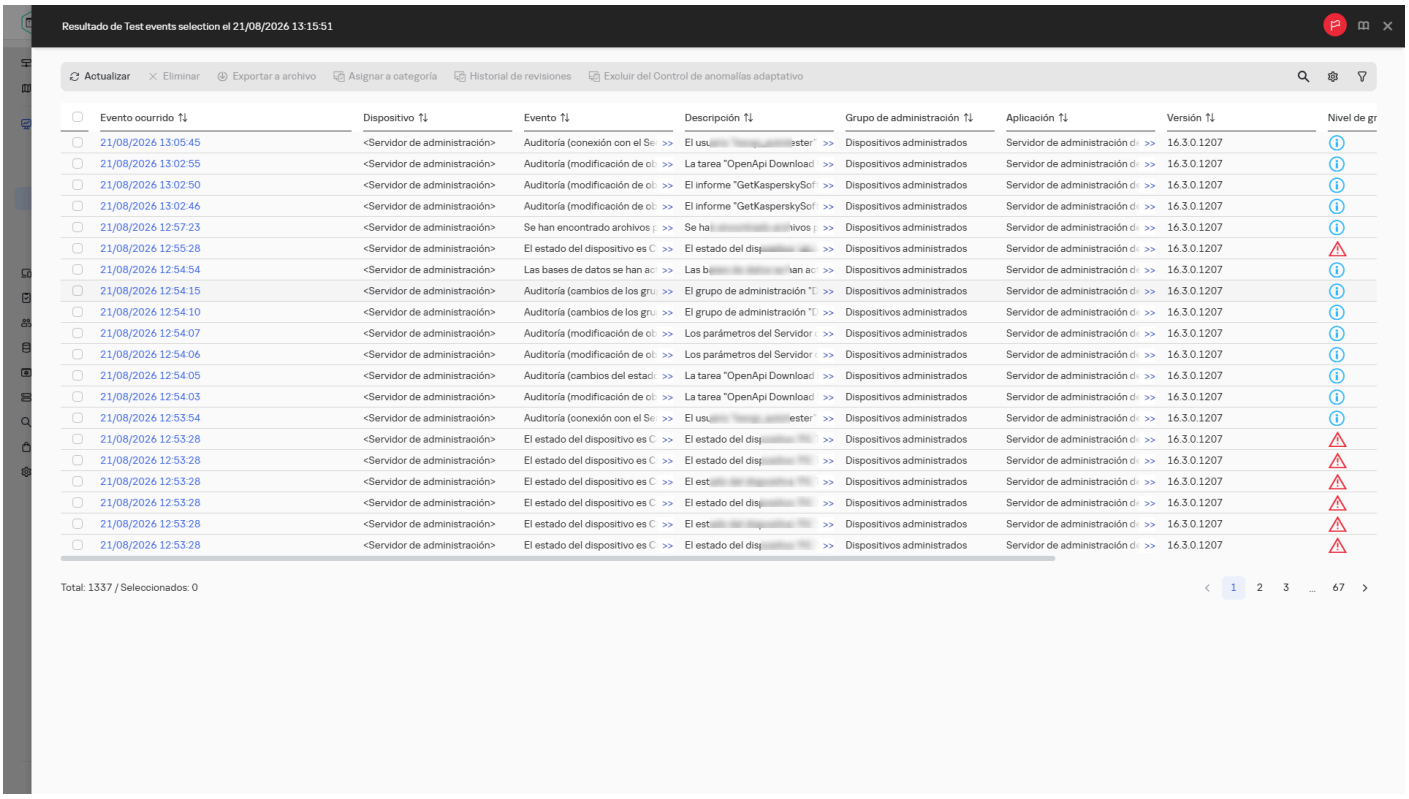


Especificar la configuración de clasificación de la selección de eventos

  a. Haga clic en el nombre de la selección.

- Si, por el contrario, desea ver la lista de eventos tal como están ordenados en el Servidor de administración, haga clic en el nombre de la selección.

Se muestra el resultado de la selección de eventos.



El resultado de la selección de eventos

Exportar una selección de eventos

Kaspersky Security Center Linux permite guardar una selección de eventos y su configuración en un archivo KLO. El archivo KLO puede usarse para importar la selección de eventos guardada en Kaspersky Security Center Windows o Kaspersky Security Center Linux.

Tenga en cuenta que solo puede exportar selecciones de eventos definidas por el usuario. Las selecciones de eventos del conjunto predeterminado de Kaspersky Security Center Linux (selecciones predefinidas) no se pueden guardar en un archivo.

Para exportar una selección de eventos:

1. En el menú principal, vaya a **Supervisión → Selecciones de eventos**.
2. Marque la casilla ubicada junto a la selección de eventos que desee exportar.

   No es posible exportar más de una selección de eventos a la vez. Si selecciona más de una selección, el botón **Exportar** se desactivará.
3. Haga clic en el botón **Exportar**.
4. En la ventana abierta **Guardar como**, especifique el nombre y la ruta del archivo de selección de eventos y luego haga clic en el botón **Guardar**.

   La ventana **Guardar como** aparecerá solo si utiliza los navegadores Google Chrome, Microsoft Edge u Opera. Si utiliza otro navegador, el archivo de la selección de eventos se guardará automáticamente en la carpeta **Descargas**.

Importar una selección de eventos

Kaspersky Security Center Cloud Linux permite importar una selección de eventos de un archivo KLO. El archivo KLO contiene la selección de eventos exportada y su configuración.

Para importar una selección de eventos:

1. En el menú principal, vaya a **Supervisión** → **Selecciones de eventos**.
2. Haga clic en el botón **Importar** y luego elija un archivo de selección de eventos que desee importar.
3. En la ventana que se abre, especifique la ruta al archivo KLO y haga clic en el botón **Abrir**. Tenga en cuenta que no podrá seleccionar más de un archivo de selección de eventos.

   Comienza el procesamiento de selección de eventos.

Aparecerá una notificación con los resultados de la importación. Si la selección de eventos se importa correctamente, puede hacer clic en el vínculo **Ver detalles de importación** para ver las propiedades de la selección de eventos.

Una vez que se complete la importación, la selección de eventos aparece en la lista de selección. Los ajustes de la selección de eventos también se importan.

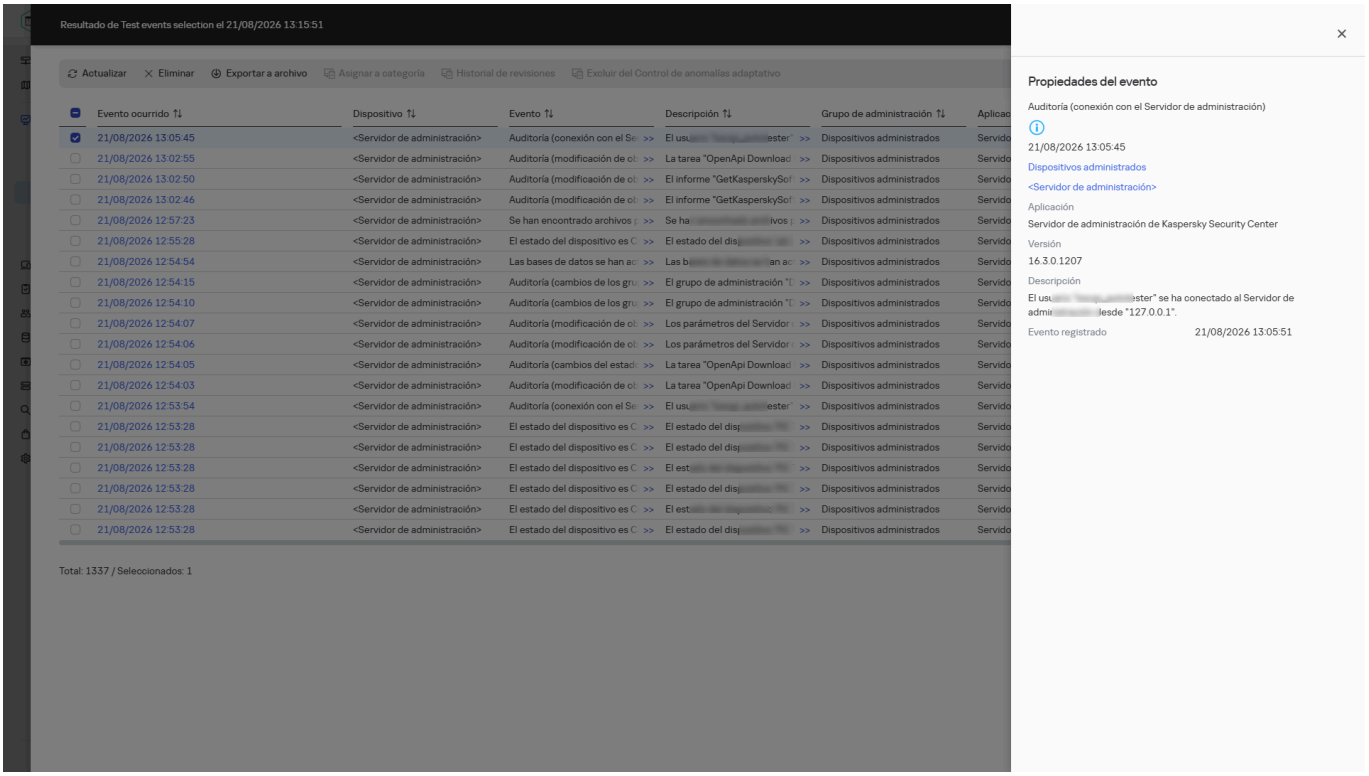
Si la selección de eventos importada tiene el mismo nombre que una selección de eventos existente, el nombre de la selección importada se complementa con un índice secuencial en formato **(<siguiente número secuencial>)**, por ejemplo **(1)**, **(2)**.

Visualización de las áreas de detalles del evento

Para ver los detalles de un evento:

1. Genere una selección de eventos.
2. Haga clic en la hora del evento por el que desee consultar.

Se abre la ventana **Propiedades del evento**.



La ventana de propiedades del evento

3. En la ventana que se abre, puede hacer lo siguiente:

   - Ver la información del evento seleccionado
   - Ir al dispositivo en el que ocurrió el evento
   - Ir al grupo de administración del dispositivo en el que ocurrió el evento
   - Si el evento está relacionado con una tarea, ir a las propiedades de esa tarea

Exportar eventos a un archivo

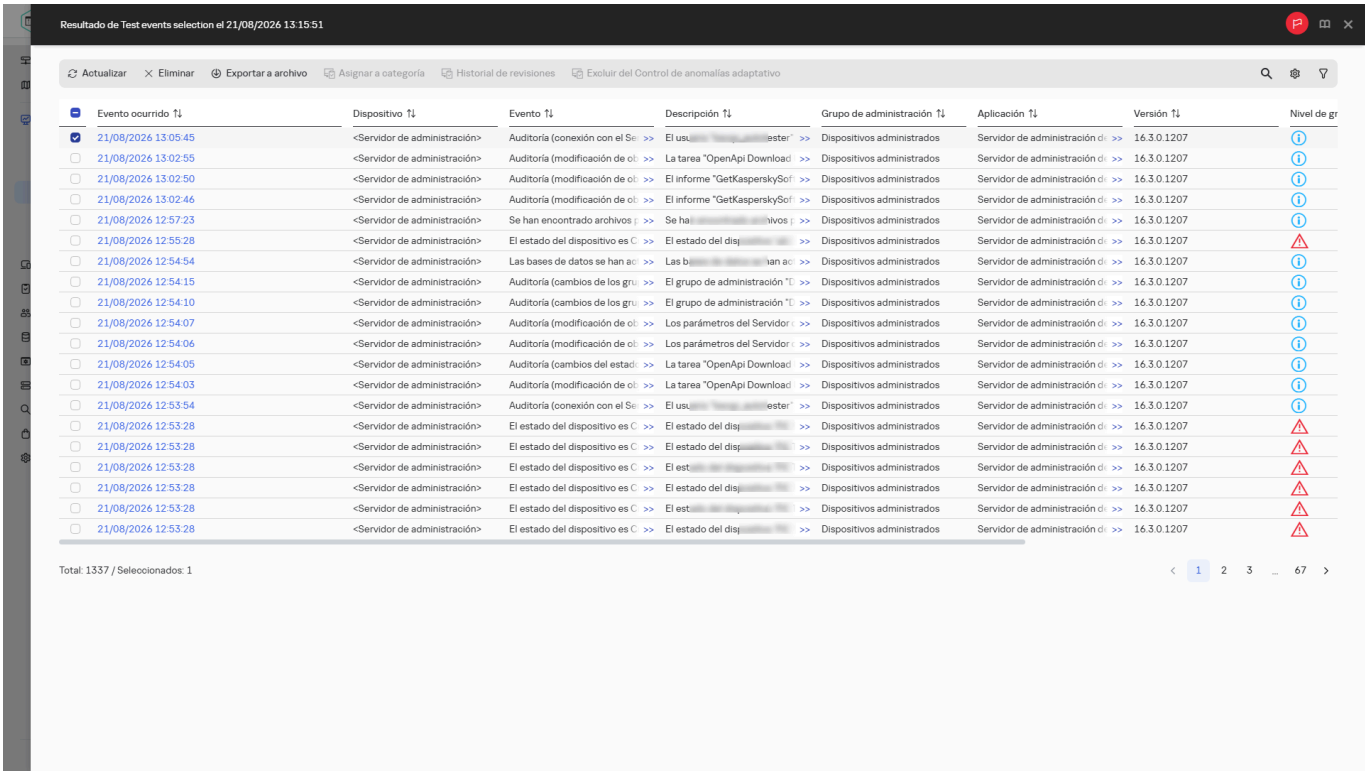
Kaspersky Security Center Linux puede guardar eventos en un archivo CSV o TXT.

Para exportar eventos de la selección de eventos:

1. En el menú principal, vaya a **Supervisión** → **Selecciones de eventos**.
2. Haga clic en el nombre de la selección que necesita.

3. Seleccione los eventos:

   - Si desea exportar uno o varios eventos, seleccione las casillas junto a los eventos.
   - Si desea exportar todos los eventos de la página actual, seleccione la casilla sobre la lista de eventos y haga clic en **Seleccionar todo en la página actual**.
   - Si desea exportar todos los eventos de una selección, seleccione la casilla sobre la lista de eventos y haga clic en **Seleccionar todo**.



El resultado de la selección de eventos

4. Haga clic en el botón **Exportar** y seleccione **Exportar a CSV** o **Exportar a TXT**.

Para exportar eventos de la lista de eventos de un dispositivo:

1. Abra la lista de dispositivos.

   - Para dispositivos administrados: **Administración de activos** → **Dispositivos administrados**.
   - Para dispositivos no asignados: **Administración de activos** → **Dispositivos no asignados**.

2. En la lista de dispositivos, haga clic en el vínculo con el nombre del dispositivo requerido y luego vaya a la pestaña **Eventos**.

3. Seleccione los eventos:

   - Si desea eliminar uno o varios eventos, seleccione las casillas junto a ellos.
   - Si desea eliminar todos los eventos en la página actual, seleccione la casilla sobre la lista de eventos y haga clic en la opción **Seleccionar todo en la página actual**.
   - Si desea eliminar todos los eventos de una selección, seleccione la casilla sobre la lista de eventos y haga clic en la opción **Seleccionar todo**.

4. Haga clic en el botón **Exportar** y seleccione **Exportar a CSV** o **Exportar a TXT**.

Se exportará toda la información sobre los eventos seleccionados incluidos en la tabla.

Acceder al historial de un objeto desde un evento

Puede acceder al historial de revisiones de un objeto compatible con la administración de revisiones desde un evento relacionado con la creación o modificación de ese objeto.

Para acceder al historial de un objeto desde un evento:

1. Genere una selección de eventos.
2. Marque la casilla ubicada junto al evento pertinente.
3. Haga clic en el botón **Historial de revisiones**.

Se abre el historial de revisiones del objeto.

Eliminar eventos

Para eliminar eventos de la selección de eventos:

1. Genere una selección de eventos.
2. Seleccione los eventos:

   - Si desea eliminar uno o varios eventos, seleccione las casillas junto a ellos.
   - Si desea eliminar todos los eventos en la página actual, seleccione la casilla sobre la lista de eventos y haga clic en la opción **Seleccionar todo en la página actual**.
   - Si desea eliminar todos los eventos de una selección, seleccione la casilla sobre la lista de eventos y haga clic en la opción **Seleccionar todo**.

3. Haga clic en el botón **Eliminar**.
4. En la ventana que se abre, haga clic en **Eliminar**.

Para eliminar eventos de una lista de eventos de dispositivos:

1. Abra la lista de dispositivos.
   - Para dispositivos administrados: **Administración de activos** → **Dispositivos administrados**.
   - Para dispositivos no asignados: **Administración de activos** → **Dispositivos no asignados**.
2. En la lista de dispositivos, haga clic en el vínculo con el nombre del dispositivo requerido y luego vaya a la pestaña **Eventos**.
3. Seleccione los eventos:
   - Si desea eliminar uno o varios eventos, seleccione las casillas junto a ellos.
   - Si desea eliminar todos los eventos en la página actual, seleccione la casilla sobre la lista de eventos y haga clic en la opción **Seleccionar todo en la página actual**.
   - Si desea eliminar todos los eventos de una selección, seleccione la casilla sobre la lista de eventos y haga clic en la opción **Seleccionar todo**.
4. Haga clic en **Eliminar** y luego confirme la acción.
5. En la ventana que se abre, haga clic en **Eliminar**.

Los eventos seleccionados se eliminan. No los podrá recuperar.

Eliminación de selecciones de eventos

Solo es posible eliminar selecciones de eventos definidas por el usuario. Las selecciones de eventos predefinidas no se pueden eliminar.

Para eliminar una o varias selecciones de eventos:

1. En el menú principal, vaya a **Supervisión** → **Selecciones de eventos**.
2. Marque las casillas ubicadas junto a las selecciones de eventos que desee eliminar.
3. Haga clic en el botón **Eliminar**.
4. En la ventana que se abre, haga clic en **Aceptar**.

Se elimina la selección de eventos.

Configuración del plazo de almacenamiento para un evento

Kaspersky Security Center Linux le permite recibir información sobre los eventos que ocurren durante el funcionamiento del Servidor de administración y aplicaciones de Kaspersky instaladas en dispositivos administrados. La información sobre estos eventos se guarda en la base de datos del Servidor de administración. Puede que deba almacenar algunos eventos durante un periodo más largo o más corto que el que se especifica en los valores predeterminados. Puede cambiar la configuración predeterminada del término de almacenamiento para un evento.

Si no le interesa almacenar algunos eventos en la base de datos del Servidor de administración, puede deshabilitar la configuración adecuada en la directiva del Servidor de administración y la directiva de la aplicación de Kaspersky, o en las propiedades del Servidor de administración (solo para eventos del Servidor de administración). Esto reducirá el número de tipos de evento en la base de datos.

Cuanto más largo sea el término de almacenamiento para un evento, más rápidamente alcanzará su capacidad máxima la base de datos. Al mismo tiempo, cuanto mayor sea el plazo de almacenamiento, más extenso será el período que podrán abarcar las tareas de supervisión y generación de informes.

Para establecer el término de almacenamiento para un evento en la base de datos del Servidor de administración:

1. En el menú principal, vaya a **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva pertinente.

   Puede seleccionar una directiva de una aplicación de Kaspersky administrada, un Agente de red o un Servidor de administración. En el caso del Servidor de administración, también puede configurar el plazo de almacenamiento de los eventos si hace clic en el nombre del Servidor de administración.
3. Seleccione la pestaña **Configuración de eventos**.

   Se muestra una lista de los tipos de evento relacionados con la sección **Crítico**. Si es necesario, puede pasar a la sección **Error funcional**, **Advertencia** o **Información**.
4. En la lista de tipos de evento en el panel derecho, haga clic en el vínculo del evento cuyo término de almacenamiento desea cambiar.

   En la sección **Registro de los eventos** de la ventana que se abre, la opción **Guardar en la base de datos del Servidor de administración por (días)** está habilitada.
5. En el cuadro de edición debajo de este botón de alternancia, introduzca la cantidad de días para almacenar el evento.
6. Si no desea almacenar un evento en la base de datos del Servidor de administración, deshabilite la opción **Guardar en la base de datos del Servidor de administración por (días)**.

> Si configura los eventos del Servidor de administración en la ventana de propiedades del Servidor de administración y la configuración de eventos está bloqueada en la directiva del Servidor de administración, no podrá redefinir el plazo de almacenamiento de un evento.

7. Haga clic en **Aceptar** y, una vez que se cierre el panel derecho, haga clic en el botón **Guardar**.

   La ventana de propiedades de la directiva está cerrada.

En lo sucesivo, cuando el Servidor de administración reciba y almacene los eventos del tipo seleccionado, se aplicará el plazo de almacenamiento modificado. El Servidor de administración no cambiará el plazo de almacenamiento de los eventos ya recibidos.

Bloquear eventos frecuentes

Esta sección proporciona información sobre la administración del bloqueo de eventos frecuentes y la eliminación del bloqueo de eventos frecuentes.

Acerca del bloqueo de eventos frecuentes

Una aplicación administrada, por ejemplo, Kaspersky Endpoint Security for Linux, instalada en uno o varios dispositivos administrados puede enviar muchos eventos del mismo tipo al Servidor de administración. La recepción de eventos frecuentes puede sobrecargar la base de datos del Servidor de administración y sobrescribir otros eventos. El Servidor de administración comienza a bloquear los eventos más frecuentes cuando el número de todos los eventos recibidos supera el límite especificado para la base de datos.

El Servidor de administración bloquea la recepción de los eventos frecuentes automáticamente. No puede bloquear los eventos frecuentes usted mismo, ni elegir qué eventos bloquear.

Si quiere saber si un evento está bloqueado, puede ver la lista de notificaciones o puede verificar si este evento está presente en la sección **Bloqueo de eventos frecuentes** de las propiedades del Servidor de administración. Si el evento está bloqueado, puede hacer lo siguiente:

- Si quiere evitar que se sobrescriba la base de datos, puede seguir bloqueando la recepción de dicho tipo de eventos.
- Por ejemplo, si quiere encontrar el motivo del envío de los eventos frecuentes al Servidor de administración puede desbloquear los eventos frecuentes y seguir recibiendo los eventos de este tipo de todas formas.
- Si quiere seguir recibiendo los eventos frecuentes hasta que se vuelvan a bloquear, puede eliminar el bloqueo de los eventos frecuentes.

Administrar el bloqueo de eventos frecuentes

El Servidor de administración bloquea la recepción automática de los eventos frecuentes, pero se puede desbloquear y seguir recibiendo los eventos frecuentes. También puede bloquear la recepción de los eventos frecuentes que haya desbloqueado antes.

Para administrar el bloqueo de eventos frecuentes:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, vaya a la sección **Bloquear eventos frecuentes**.

3. En la sección **Bloquear eventos frecuentes**:

   - Si desea desbloquear la recepción de eventos frecuentes:

     a. Seleccione los eventos frecuentes que desea desbloquear y, a continuación, haga clic en el botón **Excluir**.

     b. Haga clic en el botón **Guardar**.

   - Si desea bloquear la recepción de eventos frecuentes:

     a. Seleccione los eventos frecuentes que desea bloquear y haga clic en el botón **Bloquear**.

     b. Haga clic en el botón **Guardar**.

El Servidor de administración recibe los eventos frecuentes desbloqueados y no recibe los eventos frecuentes bloqueados.

Eliminar el bloqueo de eventos frecuentes

Puede eliminar el bloqueo de los eventos frecuentes y empezar a recibirlos hasta que el Servidor de administración vuelva a bloquear estos eventos frecuentes.

Para eliminar el bloqueo de eventos frecuentes:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, vaya a la sección **Bloquear eventos frecuentes**.

3. En la sección **Bloquear eventos frecuentes**, seleccione los tipos de eventos frecuentes para los que desea eliminar el bloqueo.

4. Haga clic en el botón **Eliminar del bloqueo**.

El evento frecuente se elimina de la lista de eventos frecuentes. El Servidor de administración recibirá los eventos de este tipo.

Almacenamiento y procesamiento de eventos en el Servidor de administración

La información sobre eventos que ocurren durante la operación de la aplicación y los dispositivos administrados se guarda en la base de datos del Servidor de administración. A cada evento se le atribuye un tipo y un nivel de gravedad (*Evento crítico*, *Error funcional*, *Advertencia* o *Información*). Según las condiciones en las que se produce un evento, la aplicación puede asignar diferentes niveles de gravedad a eventos del mismo tipo.

Se pueden ver los tipos y niveles de gravedad asignados a los eventos en la sección **Configuración de eventos** de la ventana de propiedades del Servidor de administración. En la sección **Configuración de eventos**, también puede configurar el procesamiento de todos los eventos por parte del Servidor de administración:

- El registro de eventos en el Servidor de administración y en los registros de eventos del sistema operativo en un dispositivo y en el Servidor de administración.
- El método utilizado para notificar al administrador acerca de un evento (por ejemplo, un mensaje de texto o un mensaje de correo electrónico).

En la sección Repositorio de eventos de la ventana de propiedades del Servidor de administración, puede editar la configuración del almacenamiento de eventos en la base de datos del Servidor de administración limitando el número de registros de eventos o el tiempo de almacenamiento de los registros. Cuando se especifica el número máximo de eventos, la aplicación calcula una cantidad aproximada de espacio de almacenamiento requerido para el número especificado. Puede utilizar este cálculo aproximado para evaluar si tiene suficiente espacio libre en el disco para evitar el desbordamiento de la base de datos. La capacidad predeterminada de la base de datos del Servidor de administración es de 400 000 eventos. La capacidad máxima recomendada de la base de datos es de 45 millones de eventos.

La aplicación comprueba la base de datos cada 10 minutos. Si la cantidad de eventos alcanza el valor máximo especificado más 10 000, la aplicación elimina los eventos más antiguos para que solo quede la cantidad máxima de eventos especificada.

Cuando el Servidor de administración elimina los eventos antiguos, no puede guardar los nuevos eventos en la base de datos. Durante este período, la información sobre los eventos que se rechazaron se escribe en el registro del sistema operativo. Los nuevos eventos se ponen en cola y se guardan en la base de datos una vez finalizada la operación de borrado. De manera predeterminada, la cola se limita a 20 000 eventos. Puede personalizar el límite de la cola editando el valor del indicador KLEVP_MAX_POSTPONED_CNT.

Notificaciones y estados de los dispositivos

En esta sección, encontrará información para ver las notificaciones, configurar el envío de notificaciones, usar los estados de los dispositivos y habilitar los cambios de estado para los dispositivos.

Acerca de las notificaciones

Las notificaciones le informan sobre eventos importantes y le ayudan a responder rápidamente realizando las acciones recomendadas o cualquier otra acción adecuada.

Según el método de la notificación elegido, están disponibles los siguientes tipos de notificaciones:

- Notificaciones en pantalla.
- Notificaciones por SMS.
- Notificaciones por correo electrónico.
- Notificaciones por archivo ejecutable o script.

Notificaciones en pantalla.

Las notificaciones en pantalla están disponibles en el panel desplegable que se abre al hacer clic en el icono de notificaciones ( ) y en el Centro de notificaciones. Se les asigna una de las siguientes categorías de importancia: **Crítico**, **Advertencia** o **Información**.

Si el icono de notificaciones tiene un punto rojo, hay notificaciones no leídas.

Las notificaciones en pantalla se agrupan en los siguientes tipos:

- **Se requiere atención**

  Notificaciones que requieren su atención. Las notificaciones de la categoría **Crítico** se muestran en el panel principal, además de en el Centro de notificaciones.

- **Sistema**

  Notificaciones del sistema. Se dividen en las siguientes categorías:

  - **Despliegue**
  - **Dispositivos**
  - **Protección**
  - **Actualizaciones** (incluye notificaciones sobre aplicaciones de Kaspersky disponibles para descargar, notificaciones sobre actualizaciones de bases de datos antivirus descargadas y notificaciones sobre dispositivos, si los hay, que requieren reiniciarse después de una actualización del Agente de red)
  - **Prevención de exploits**
  - **Servidor de administración** (incluye solo eventos relacionados con el Servidor de administración)

- **Anuncios**

  Notificaciones que proporcionan información relacionada con su versión de Kaspersky Security Center Linux y las aplicaciones administradas instaladas en los dispositivos administrados.

Puede supervisar la red de su organización viendo las notificaciones en pantalla y respondiendo a ellas en tiempo real.

Notificaciones por correo electrónico, por SMS y por archivo ejecutable o script

Kaspersky Security Center Linux ofrece la capacidad de supervisar la red de su organización enviando notificaciones sobre cualquier evento que considere importante. Para cualquier evento, puede configurar notificaciones por correo electrónico, SMS o ejecutando un archivo ejecutable o un script.

Al recibir notificaciones por correo electrónico o SMS, puede decidir su respuesta a un evento. Esta respuesta debe ser la más adecuada para la red de su organización. Al ejecutar un archivo ejecutable o una secuencia de comandos, predefinirá una respuesta a un evento. También puede considerar ejecutar un archivo ejecutable o una secuencia de comandos como respuesta principal a un evento. Después de que se ejecute el archivo ejecutable, puede seguir otros pasos para responder al evento.

Visualización de notificaciones que requieren atención

Las notificaciones que requieren atención le informan sobre eventos que pueden requerir su atención. Se les asigna una de las siguientes categorías de importancia: **Crítico**, **Advertencia** o **Información**.

Las notificaciones de la categoría **Crítico** se muestran en Web Console, además de en el Centro de notificaciones. Si hay varias notificaciones críticas disponibles, Web Console muestra una sola notificación que indica el número total de notificaciones críticas.

Puede ver las notificaciones que requieren atención de una de las siguientes maneras:

- En el panel desplegable

  En el panel desplegable solo se muestran las notificaciones no leídas que requieren atención. Si no hay notificaciones no leídas que requieran atención, no se muestra la pestaña **Se requiere atención**.

- En el Centro de notificaciones

  El Centro de notificaciones muestra todas las notificaciones que requieren atención, incluidas las notificaciones leídas y no leídas. Si no hay notificaciones que requieran atención, no se muestra la pestaña **Se requiere atención**.

Para ver las notificaciones que requieren atención en el panel desplegable:

1. En la parte superior de Web Console, haga clic en el icono de notificación ( ).

   Se abre el panel desplegable **Notificaciones**.

2. En la pestaña **Se requiere atención**, vea las notificaciones no leídas.

3. Si es necesario, marque las notificaciones que requieren atención como leídas de una de las siguientes maneras:

   - Para marcar una notificación como leída, haga clic en el icono de cierre (×) junto a la notificación.

   - Para marcar todas las notificaciones como leídas, haga clic en **Marcar todo como leído**.

   Después de revisar y marcar como leídas las notificaciones que requieren atención, la pestaña **Se requiere atención** ya no se muestra en el panel desplegable **Notificaciones**. Puede ver todas las notificaciones leídas que requieren atención en el Centro de notificaciones.

Para ver las notificaciones que requieren atención en el Centro de notificaciones:

1. En la parte superior de Web Console, haga clic en el icono de notificación ( ).

2. En el panel desplegable **Notificaciones** que se abre, haga clic en el botón **Ir al Centro de notificaciones**.

   Se abre la ventana **Centro de notificaciones**.

3. En la pestaña **Se requiere atención**, seleccione una de las siguientes secciones:

   - **Todas las notificaciones que requieren atención**–Muestra todas las notificaciones que requieren atención, independientemente de su categoría.
   - **Crítico**–Muestra las notificaciones de la categoría **Crítico**.
   - **Advertencia**–Muestra las notificaciones de la categoría **Advertencia**.
   - **Información**–Muestra las notificaciones de la categoría **Información**.

4. Para mostrar solo las notificaciones no leídas, active el botón de alternancia **Mostrar solo lo no leído**.
5. En la lista de notificaciones, haga clic en una notificación para ver su mensaje. La notificación completa se muestra en el panel de detalles de la derecha.

   Cuando ve una notificación, esta se marca automáticamente como leída.

6. Para marcar las notificaciones como leídas manualmente, realice una de las siguientes acciones:

   - Para marcar una notificación como leída, selecciónela en la lista de notificaciones y, a continuación, haga clic en el botón **Marcar como leído**.
   - Para marcar todas las notificaciones como leídas, haga clic en el botón **Marcar todo como leído**.

7. Si es necesario, puede marcar una notificación como no leída seleccionándola en la lista de notificaciones y haciendo clic en el botón **Marcar como no leído**.

Se revisan las notificaciones que requieren atención.

Visualización de notificaciones del sistema

Las notificaciones del sistema le informan sobre eventos relacionados con Web Console y dispositivos administrados. Las notificaciones del sistema se agrupan por tipos y se les asigna una de las siguientes categorías de importancia: **Crítico**, **Advertencia** o **Información**.

Puede ver las notificaciones del sistema de una de las siguientes maneras:

- En el panel desplegable
- En el Centro de notificaciones

Para ver las notificaciones del sistema en el panel desplegable:

1. En la parte superior de Web Console, haga clic en el icono de notificación ( ).

   Se abre el panel desplegable **Notificaciones**.

2. En la pestaña **Sistema**, vea las notificaciones no leídas.

3. Si es necesario, marque las notificaciones del sistema como leídas de una de las siguientes maneras:

   - Para marcar una notificación como leída, haga clic en el icono de cierre (×) junto a la notificación.
   - Para marcar todas las notificaciones como leídas, haga clic en **Marcar todo como leído**.

Después de revisar todas las notificaciones del sistema y marcarlas como leídas, el panel desplegable **Notificaciones** muestra un mensaje que indica que no hay notificaciones nuevas. Puede ver todas las notificaciones del sistema, incluidas las notificaciones leídas y no leídas, en el Centro de notificaciones.

Para ver las notificaciones del sistema en el Centro de notificaciones:

1. En la parte superior de Web Console, haga clic en el icono de notificación ().
2. En el panel desplegable **Notificaciones** que se abre, haga clic en el botón **Ir al Centro de notificaciones**.

   Se abre la ventana **Centro de notificaciones**.
3. En la pestaña **Sistema**, seleccione una de las siguientes secciones:

   - **Todas las notificaciones del sistema**
   - **Despliegue**
   - **Dispositivos**
   - **Protección**
   - **Actualizaciones**
   - **Prevención de exploits**
   - **Servidor de administración**
4. Para mostrar solo las notificaciones no leídas, active el botón de alternancia **Mostrar solo lo no leído**.
5. En la lista de notificaciones, haga clic en una notificación para ver su mensaje. La notificación completa se muestra en el panel de detalles de la derecha.

   Cuando ve una notificación, esta se marca automáticamente como leída.
6. Para marcar las notificaciones como leídas manualmente, realice una de las siguientes acciones:

   - Para marcar una notificación como leída, selecciónela en la lista de notificaciones y, a continuación, haga clic en el botón **Marcar como leído**.
   - Para marcar todas las notificaciones como leídas, haga clic en el botón **Marcar todo como leído**.
7. Si es necesario, puede marcar una notificación como no leída seleccionándola en la lista de notificaciones y haciendo clic en el botón **Marcar como no leído**.

Se revisan las notificaciones del sistema.

Visualización de novedades

Las novedades son un tipo de notificación que proporciona información sobre su versión de Kaspersky Security Center Linux y las aplicaciones de Kaspersky instaladas en sus dispositivos administrados. Solo se muestran las novedades relevantes para el Servidor de administración conectado actualmente y para las aplicaciones de Kaspersky instaladas en los dispositivos administrados de este Servidor de administración. Las novedades se muestran por separado para cada Servidor de administración, ya sea principal, secundario o virtual.

Si varios administradores utilizan Kaspersky Security Center Linux y configuran diferentes idiomas para la interfaz, Kaspersky Security Center Linux muestra las novedades de Kaspersky en todos los idiomas utilizados por los administradores. Si cambia el idioma de la interfaz, las novedades de Kaspersky en el idioma seleccionado se agregan a la sección automáticamente después de que cierre sesión en Web Console y vuelva a iniciar sesión.

Las novedades incluyen los siguientes tipos de información:

- Información relacionada con la seguridad

  Las novedades relacionadas con la seguridad incluyen actualizaciones críticas, reparaciones de vulnerabilidades y recomendaciones para resolver problemas en las aplicaciones de Kaspersky. Las novedades sobre seguridad están habilitadas de forma predeterminada. Si no desea recibir estas novedades relacionadas con la seguridad, puede deshabilitar esta función.

  Las novedades sobre temas de seguridad no se pueden deshabilitar cuando Kaspersky Security Center Linux opera en modo de prueba.

  Para proporcionar información relevante para la configuración de protección de su red, Kaspersky Security Center Linux transmite datos a los servidores de Kaspersky en la nube y recibe solo novedades relacionadas con las aplicaciones de Kaspersky instaladas en su red. Los datos que se pueden enviar a los servidores se describen en el Contrato de licencia de usuario final que acepta al instalar Kaspersky Security Center Linux.

- Información de marketing

  Las novedades de marketing incluyen ofertas especiales, noticias sobre productos y publicidad relacionada con las aplicaciones de Kaspersky. Las novedades de marketing están disponibles solo si Kaspersky Security Network (KSN) está habilitada. Para deshabilitar las novedades de marketing, deshabilite KSN.

  Para proporcionar información que pueda ayudarle a proteger los dispositivos de su red y realizar tareas cotidianas, Kaspersky Security Center Linux transmite datos a los servidores de Kaspersky en la nube y recibe novedades relevantes. Los datos que se pueden enviar a los servidores se describen en la sección Datos procesados de la Declaración de KSN.

A las novedades se les asigna una de las siguientes categorías de importancia: **Crítico**, **Advertencia** o **Información**.

Puede ver las novedades de una de las siguientes maneras:

- En el panel desplegable
- En el Centro de notificaciones

Para ver las novedades en el panel desplegable:

1. En la parte superior de Web Console, haga clic en el icono de notificación ( ).

   Se abre el panel desplegable **Notificaciones**.

2. En la pestaña **Anuncios**, vea las notificaciones no leídas.

3. Si es necesario, marque las notificaciones como leídas de una de las siguientes maneras:

   - Para marcar una notificación como leída, haga clic en el icono de cierre (×) junto a la notificación.
   - Para marcar todas las notificaciones como leídas, haga clic en **Marcar todo como leído**.

Después de revisar todas las notificaciones y marcarlas como leídas, el panel desplegable **Notificaciones** muestra un mensaje que indica que no hay notificaciones nuevas. Puede ver todas las notificaciones, tanto leídas como no leídas, en el Centro de notificaciones.

Para ver las novedades en el Centro de notificaciones:

1. En la parte superior de Web Console, haga clic en el icono de notificación ( ).

2. En el panel desplegable **Notificaciones** que se abre, haga clic en el botón **Ir al Centro de notificaciones**.

   Se abre la ventana **Centro de notificaciones**.

3. En la pestaña **Anuncios**, seleccione una de las siguientes secciones:

   - **Todos los anuncios**: muestra todas las notificaciones, independientemente de su categoría.
   - **Crítico**–Muestra las notificaciones de la categoría **Crítico**.
   - **Advertencia**–Muestra las notificaciones de la categoría **Advertencia**.
   - **Información**–Muestra las notificaciones de la categoría **Información**.

4. Para mostrar solo las notificaciones no leídas, active el botón de alternancia **Mostrar solo lo no leído**.

5. En la lista de notificaciones, haga clic en una notificación para ver su mensaje. La notificación completa se muestra en el panel de detalles de la derecha.

   Cuando ve una notificación, esta se marca automáticamente como leída.

6. Para marcar las notificaciones como leídas manualmente, realice una de las siguientes acciones:

   - Para marcar una notificación como leída, selecciónela en la lista de notificaciones y, a continuación, haga clic en el botón **Marcar como leído**.
   - Para marcar todas las notificaciones como leídas, haga clic en el botón **Marcar todo como leído**.

7. Si es necesario, puede marcar una notificación como no leída seleccionándola en la lista de notificaciones y haciendo clic en el botón **Marcar como no leído**.

Los anuncios se revisan.

Dejar de recibir las novedades de Kaspersky

La sección Novedades de Kaspersky (**Supervisión → Novedades de Kaspersky**) le permite mantenerse informado al proporcionarle información relacionada con su versión de Kaspersky Security Center Linux y con las aplicaciones administradas instaladas en los dispositivos administrados. Si ya no desea recibir novedades de Kaspersky, puede deshabilitar esta función.

Kaspersky publica dos clases de novedades: novedades sobre temas de seguridad y novedades con fines publicitarios.

Para dejar de recibir novedades sobre temas de seguridad:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, vaya a la sección **Anuncios de Kaspersky**.

3. Cambie el botón de alternar a la posición **Los anuncios relacionados con la seguridad están deshabilitados**.

4. Haga clic en el botón **Guardar**.

   Ya no recibirá novedades de Kaspersky.

Las novedades con fines publicitarios están deshabilitadas de forma predeterminada. Solo recibirá este tipo de novedades si ha habilitado Kaspersky Security Network (KSN). Puede deshabilitar este tipo de anuncio deshabilitando KSN.

La deshabilitación de KSN puede afectar a las aplicaciones de Kaspersky administradas que usan los servicios de KSN. Es posible que dichas aplicaciones ya no puedan comunicarse con Kaspersky para enviar o recibir datos de reputación, telemetría o estadísticas.

Configurar cambios de estado para los dispositivos

Puede cambiar las condiciones bajo las cuales se le asignan los estados *Crítico* o *Advertencia* a un dispositivo.

Para habilitar el cambio de estado a Crítico para los dispositivos:

1. En el menú principal, vaya a **Administración de activos → Jerarquía de grupos**.

2. Realice una de las siguientes acciones a fin de visualizar las propiedades del grupo de administración para el que desee cambiar el estado del dispositivo:

   - Haga clic en el nombre del grupo de administración.

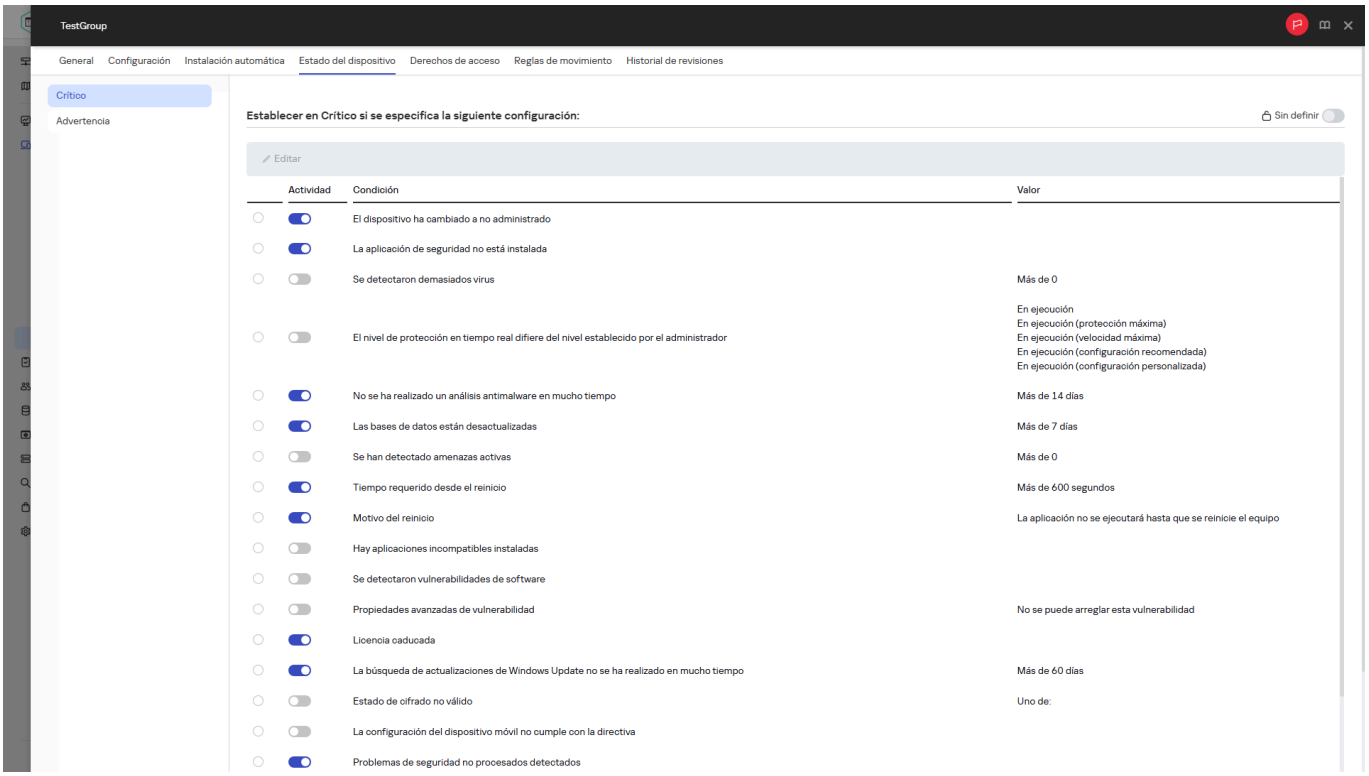
   - Haga clic en el botón **Mostrar jerarquía** en la parte superior de la página. En el panel de navegación que se abre, coloque el cursor sobre el nombre del grupo que necesite y luego haga clic en el ícono de configuración (⚙).

   Se abrirá la ventana de propiedades del grupo de administración.

3. En la ventana de las propiedades, seleccione la pestaña **Estado del dispositivo**.

4. En el panel izquierdo, seleccione **Crítico**.

5. En el panel derecho, en la sección **Establecer en Crítico si se especifica la siguiente configuración**, habilite la condición bajo la cual el estado de un dispositivo cambiará a *Crítico*.



> Solo podrá modificar los ajustes que no estén bloqueados en la directiva primaria.

6. En la lista, seleccione el botón de opción ubicado junto a la condición.

7. En la esquina superior izquierda de la lista, haga clic en el botón **Editar**.

8. Configure el valor necesario para la condición seleccionada.

   No es posible configurar valores para todas las condiciones.

9. Haga clic en **Aceptar**.

10. Haga clic en **Guardar** para guardar los cambios.

Cuando se cumplan las condiciones especificadas, se asignará el estado *Crítico* al dispositivo administrado.

Para habilitar el cambio de estado a Advertencia para los dispositivos:

1. En el menú principal, vaya a **Administración de activos** → **Jerarquía de grupos**.

2. En la lista de grupos que se abre, haga clic en el vínculo con el nombre del grupo que contenga los dispositivos para los que desee modificar el cambio de estado.

3. En la ventana de las propiedades que se abre, seleccione la pestaña **Estado del dispositivo**.

4. En el panel izquierdo, seleccione **Advertencia**.

5. En el panel derecho, en la sección **Establecer en Advertencia si se especifica la siguiente configuración**, habilite la condición que hará que el estado de un dispositivo cambie a *Advertencia*.

   Solo podrá modificar los ajustes que no estén bloqueados en la directiva primaria.

6. En la lista, seleccione el botón de opción ubicado junto a la condición.
7. En la esquina superior izquierda de la lista, haga clic en el botón **Editar**.
8. Configure el valor necesario para la condición seleccionada.

   No es posible configurar valores para todas las condiciones.

9. Haga clic en **Aceptar**.
10. Haga clic en **Guardar** para guardar los cambios.

Cuando se cumplan las condiciones especificadas, se asignará el estado *Advertencia* al dispositivo administrado.

Configurar el envío de notificaciones

Puede configurar notificaciones sobre eventos que ocurren en Kaspersky Security Center Linux. Según el método de la notificación elegido, están disponibles los siguientes tipos de notificaciones:

- Correo electrónico: cuando se produce un evento, Kaspersky Security Center Linux envía una notificación a las direcciones de correo electrónico especificadas.
- SMS: cuando se produce un evento, Kaspersky Security Center Linux envía una notificación a los números de teléfono móvil especificados.
- Archivo ejecutable: cuando ocurre un evento, el archivo ejecutable se ejecuta en el Servidor de administración.

Para configurar la entrega de notificaciones de eventos que ocurren en Kaspersky Security Center Linux:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abrirá la ventana de propiedades del Servidor de administración, con la pestaña **General** seleccionada.

2. Haga clic en la sección **Notificación**, y en el panel derecho seleccione la pestaña para el método de notificación que desee:

   - **Correo electrónico**

     La pestaña **Correo electrónico** permite configurar la notificación de eventos por correo electrónico.

     En el campo **Servidores SMTP**, especifique las direcciones del servidor de correo, separándolas con punto y coma. Puede utilizar los siguientes parámetros:

     - Dirección IPv4 o IPv6
     - Nombre DNS del servidor SMTP

     En el campo **Puerto de los servidores SMTP**, especifique el número de un puerto de comunicación del servidor SMTP. El número de puerto predeterminado es 25.

Si habilita la opción **Usar búsqueda de MX por DNS**, puede utilizar varios registros MX de las direcciones IP para el mismo nombre DNS del servidor SMTP. El mismo nombre DNS puede tener varios registros MX con diferentes valores de prioridad de recepción de mensajes de correo electrónico. El Servidor de administración intenta enviar notificaciones del correo electrónico al servidor SMTP en orden ascendente de prioridad de registros MX.

Si habilita la opción **Usar búsqueda de MX por DNS** y no habilita el uso de la configuración de TLS, le recomendamos que use la configuración de DNSSEC en el dispositivo de su servidor como medida adicional de protección en el envío de notificaciones del correo electrónico.

Si habilita la opción **Utilizar autenticación ESMTP**, puede especificar la configuración de autenticación ESMTP en los campos **Nombre de usuario** y **Contraseña**. De forma predeterminada, la opción está deshabilitada y la configuración de autenticación ESMTP no está disponible.

Puede especificar la configuración de TLS para la conexión con un servidor SMTP:

- **No usar TLS**

Puede seleccionar esta opción si desea deshabilitar el cifrado de mensajes de correo electrónico.

- **Usar TLS si es compatible con el servidor SMTP**

Puede seleccionar esta opción si desea usar una conexión TLS con un servidor SMTP. Si el servidor SMTP no es compatible con TLS, el Servidor de administración se conecta con el servidor SMTP sin usar TLS.

- **Usar siempre TLS, comprobar la validez del certificado del servidor**

Puede seleccionar esta opción si desea usar la configuración de autenticación de TLS. Si el servidor SMTP no es compatible con TLS, el Servidor de administración no puede conectarse al servidor SMTP.

Le recomendamos que use esta opción para una mejor protección de la conexión con un servidor SMTP. Si selecciona esta opción, puede establecer la configuración de autenticación para una conexión TLS.

Si selecciona el valor **Usar siempre TLS, comprobar la validez del certificado del servidor**, puede especificar un certificado para la autenticación del servidor SMTP y elegir si desea habilitar la comunicación a través de cualquier versión de TLS o solo a través de TLS 1.2 o versiones posteriores. También puede especificar un certificado para la autenticación de un cliente en el servidor SMTP.

Puede especificar certificados para una conexión TLS al hacer clic en el enlace **Especificar certificados**:

- Busque un archivo de certificados del servidor SMTP:

Puede recibir un archivo con la lista de certificados de una autoridad de certificación confiable y cargar el archivo al Servidor de administración. Kaspersky Security Center Linux verifica si el certificado de un servidor SMTP también está firmado por una autoridad de certificación confiable. Si el certificado de un servidor SMTP no se recibe de una autoridad de certificación confiable, Kaspersky Security Center Linux no podrá conectarse al servidor SMTP.

- Busque un archivo de certificados cliente:

Puede utilizar un certificado obtenido de cualquier fuente (por ejemplo, de una entidad de certificación de confianza). Deberá especificar el certificado y su clave privada. Puede usar, para ello, alguno de los siguientes tipos de certificado:

- Certificado X-509:

Debe especificar un archivo con el certificado y un archivo con la clave privada. Los dos archivos son independientes entre sí. El orden en que se carguen los archivos no importa. Cuando se cargan ambos archivos, debe especificar la contraseña para decodificar la clave privada. Si la clave privada no está codificada, puede dejar la contraseña en blanco.

- Contenedor pkcs12:

Debe cargar un solo archivo que contenga el certificado y la clave privada. Cuando se carga el archivo, debe especificar la contraseña para decodificar la clave privada. Si la clave privada no está codificada, puede dejar la contraseña en blanco.

Al hacer clic en el botón **Enviar mensaje de prueba**, podrá verificar si configuró las notificaciones correctamente: la aplicación envía una notificación de prueba a las direcciones de correo electrónico que especificó.

En el campo **Direcciones de los destinatarios**, especifique las direcciones de correo electrónico a las que la aplicación enviará notificaciones. Puede especificar varias direcciones en este campo, separándolas con punto y coma.

En el campo **Asunto**, escriba el asunto del correo electrónico con parámetros de sustitución, por ejemplo: `[KSC-SAMARA-1] [%SEVERITY%] %EVENT%`. Ejemplo de cómo se muestra el asunto cuando se detecta una amenaza: `[KSC-SAMARA-1] [Critical] Threat detected`. Puede dejar este campo vacío.

En la lista desplegable **Plantilla de asunto**, seleccione la plantilla para su asunto. Una variable determinada por la plantilla seleccionada se coloca automáticamente en el campo **Asunto**. Puede crear un asunto de correo electrónico seleccionando varias plantillas de asunto.

En el campo **Dirección de correo electrónico del remitente: Si deja este campo en blanco, se usará la dirección del destinatario. Advertencia: No se recomienda usar una dirección ficticia**, escriba la dirección de correo electrónico del remitente. Si deja este campo vacío, de forma predeterminada, se utiliza la dirección del destinatario. Se recomienda no utilizar direcciones de correo electrónico falsas.

El campo **Mensaje de notificación** contiene texto estándar con información sobre el evento que la aplicación envía cuando ocurre un evento. Este texto incluye parámetros sustitutos, como el nombre del evento, el nombre del dispositivo y el nombre del dominio. Puede editar el texto del mensaje agregando otros parámetros sustitutos con detalles más relevantes del evento.

Ejemplo de valor de campo

```
Sender - KSC-SAMARA-1

Host: %COMPUTER%

Product: %KL_PRODUCT%

Version: %KL_VERSION%

Occurred at: %RISE_TIME%

Event: %EVENT%

Details:

%DESCR%
```

La cadena `Sender` es opcional. Por ejemplo, si tiene varios Servidores de administración, puede especificar el nombre del Servidor de administración del que se recibió la notificación: `Sender - KSC-SAMARA-1`.

Ejemplo del aspecto del texto de la notificación:

```
Sender - KSC-SAMARA-1
```

```
Host: nb-123456.example.net

Product: Kaspersky Endpoint Security 12.5 for Linux

Version: 12.5.0.1569

Occurred at: 2026-08-17T13:15:36

Event: Threat detected

Details:

Initiator: Product; Task type: ODS; ID of running task: 107; User receiving access:
root; Object type: File; File owner: user; Detection certainty: Sure; File:
/home/user/eicar_com.zip//eicar.com; Detected object name: EICAR-Test-File; Detected
object type: Virware; MD5 hash: <hash>; Unique ID: <ID>
```

Si el texto de la notificación contiene un signo de porcentaje (%), debe escribirlo dos veces seguidas para permitir el envío de mensajes. Por ejemplo: "La carga de la CPU es 100 %%".

Al hacer clic en el vínculo **Configurar el límite numérico de notificaciones** podrá especificar el número máximo de notificaciones que la aplicación puede enviar durante el intervalo de tiempo especificado.

- **SMS**

  La ficha **SMS** permite configurar la transmisión de notificaciones por SMS de diversos eventos a un teléfono celular. Los mensajes SMS se envían a través de una pasarela de correo.

  En el campo **Servidores SMTP**, especifique las direcciones del servidor de correo, separándolas con punto y coma. Puede utilizar los siguientes parámetros:

  - Dirección IPv4 o IPv6
  - Nombre de la red de Windows (nombre NetBIOS) del dispositivo
  - Nombre DNS del servidor SMTP

  En el campo **Puerto de los servidores SMTP**, especifique el número de un puerto de comunicación del servidor SMTP. El número de puerto predeterminado es 25.

  Si habilita la opción **Utilizar autenticación ESMTP**, puede especificar la configuración de autenticación ESMTP en los campos **Nombre de usuario** y **Contraseña**. De forma predeterminada, la opción está deshabilitada y la configuración de autenticación ESMTP no está disponible.

  Puede especificar la configuración de TLS para la conexión con un servidor SMTP:

  - **No usar TLS**

  Puede seleccionar esta opción si desea deshabilitar el cifrado de mensajes de correo electrónico.

  - **Usar TLS si es compatible con el servidor SMTP**

  Puede seleccionar esta opción si desea usar una conexión TLS con un servidor SMTP. Si el servidor SMTP no es compatible con TLS, el Servidor de administración se conecta con el servidor SMTP sin usar TLS.

  - **Usar siempre TLS, comprobar la validez del certificado del servidor**

  Puede seleccionar esta opción si desea usar la configuración de autenticación de TLS. Si el servidor SMTP no es compatible con TLS, el Servidor de administración no puede conectarse al servidor SMTP.

Le recomendamos que use esta opción para una mejor protección de la conexión con un servidor SMTP. Si selecciona esta opción, puede establecer la configuración de autenticación para una conexión TLS.

Si selecciona el valor **Usar siempre TLS, comprobar la validez del certificado del servidor**, puede especificar un certificado para la autenticación del servidor SMTP y elegir si desea habilitar la comunicación a través de cualquier versión de TLS o solo a través de TLS 1.2 o versiones posteriores. También puede especificar un certificado para la autenticación de un cliente en el servidor SMTP.

Puede especificar un archivo de certificado de servidor de SMTP al hacer clic en el enlace **Especificar certificados**:

Puede recibir un archivo con la lista de certificados de una autoridad de certificación confiable y cargar el archivo al Servidor de administración. Kaspersky Security Center Linux verifica si el certificado de un servidor SMTP también está firmado por una autoridad de certificación confiable. Si el certificado de un servidor SMTP no se recibe de una autoridad de certificación confiable, Kaspersky Security Center Linux no podrá conectarse al servidor SMTP.

En el campo **Direcciones de los destinatarios**, especifique las direcciones de correo electrónico a las que la aplicación enviará notificaciones. Puede especificar varias direcciones en este campo, separándolas con punto y coma. Las notificaciones se enviarán a los números de teléfono asociados con las direcciones de correo electrónico especificadas.

En el campo **Asunto**, especifique el asunto del correo electrónico.

En la lista desplegable **Plantilla de asunto**, seleccione la plantilla para su asunto. Una variable de acuerdo con la plantilla seleccionada se coloca en el campo **Asunto**. Puede crear un asunto de correo electrónico seleccionando varias plantillas de asunto.

En el campo **Dirección de correo electrónico del remitente: Si deja este campo en blanco, se usará la dirección del destinatario. Advertencia: No se recomienda usar una dirección ficticia**, escriba la dirección de correo electrónico del remitente. Si deja este campo vacío, de forma predeterminada, se utiliza la dirección del destinatario. Se recomienda no utilizar direcciones de correo electrónico falsas.

En el campo **Teléfonos de destinatarios de SMS**, especifique los números de teléfono celular de los destinatarios de notificaciones por SMS.

En el campo **Mensaje de notificación** se especifica un con información sobre el evento que la aplicación envía cuando un evento ocurre. Este texto puede incluir parámetros sustitutos, como el nombre del evento, el nombre del dispositivo y el nombre del dominio.

Si el texto de la notificación contiene un signo de porcentaje (%), debe escribirlo dos veces seguidas para permitir el envío de mensajes. Por ejemplo: "La carga de la CPU es 100 %%".

Haga clic en el vínculo **Configurar el límite numérico de notificaciones** para especificar el número máximo de notificaciones que la aplicación puede enviar durante el intervalo de tiempo especificado.

Haga clic en **Enviar mensaje de prueba** para verificar si configuró las notificaciones correctamente: la aplicación envía una notificación de prueba al destinatario que especificó.

- **Archivo ejecutable para ejecutar**

  El archivo ejecutable debe contener las variables de entorno del evento que desea que reciba el Administrador.

  En el campo **Archivo ejecutable que se ejecutará en el Servidor de administración cuando ocurra un evento**, escriba el nombre y la carpeta del archivo que se ejecutará.

  Ejemplo de valor del campo:

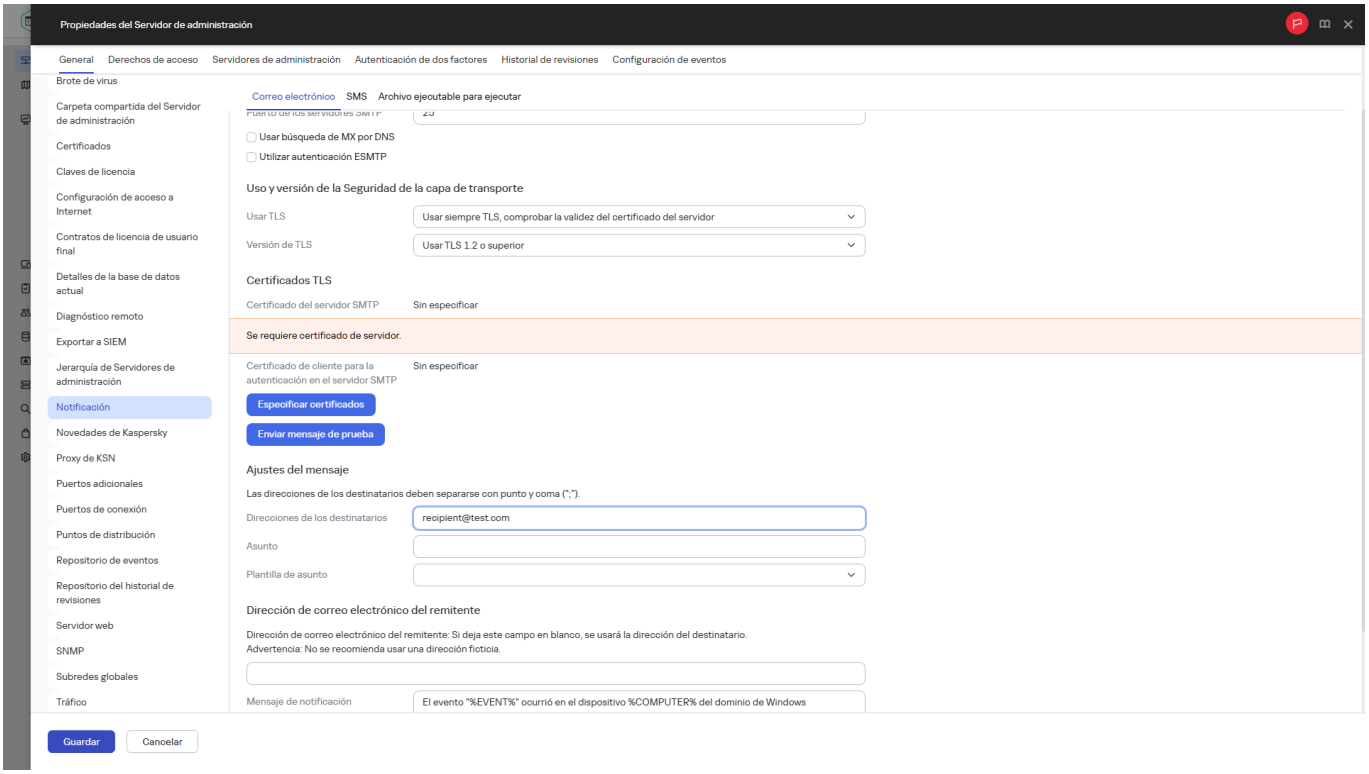
  ```
  /opt/scripts/notifications.sh
  ```

El archivo debe prepararse con anticipación especificando parámetros de sustitución que representen la información del evento que se enviará en el mensaje. La carpeta y el archivo deben estar ubicados en el Servidor de administración.

Ejemplo de script para pruebas o depuración:

```
#!/usr/bin/env bash
touch /tmp/ksc_notification.txt
echo "$RISE_TIME $COMPUTER $EVENT" >> /tmp/ksc_notification.txt
```

Al hacer clic en el vínculo **Configurar el límite numérico de notificaciones** podrá especificar el número máximo de notificaciones que la aplicación puede enviar durante el intervalo de tiempo especificado.



Selección del método de notificación

3. En la pestaña, defina la configuración de la notificación.

4. Haga clic en **Guardar** para guardar los cambios y cerrar la ventana de propiedades del Servidor de administración.

La configuración de entrega de notificaciones guardada se aplica a todos los eventos que ocurren en Kaspersky Security Center Linux.

Puede anular la configuración de entrega de notificación para ciertos eventos en la sección **Configuración de eventos** de la Configuración del Servidor de administración, de una configuración de directiva o de una configuración de aplicación.

Notificaciones de prueba

Para verificar si se envían las notificaciones de eventos, la aplicación usa la notificación de detección de virus de prueba EICAR en los dispositivos cliente.

Para comprobar el envío de las notificaciones de eventos, haga lo siguiente:

1. Detenga la tarea de protección del sistema de archivos en tiempo real en un dispositivo cliente y copie el virus de prueba EICAR en ese equipo cliente. Ahora vuelva a habilitar la protección en tiempo real del sistema de archivos.

2. Ejecute una tarea de análisis para los dispositivos cliente de un grupo de administración o para una serie de dispositivos específicos, incluido uno que tenga el virus de prueba de EICAR.

   Si la tarea de análisis se configuró correctamente, se detectará el virus de prueba. Si las notificaciones se configuraron correctamente, recibirá una notificación informándole que se detectó un virus.

Para abrir un registro de la prueba de detección de virus:

1. En el menú principal, vaya a **Supervisión → Selecciones de eventos**.

2. Haga clic en el nombre de selección **Eventos recientes**.

   En la ventana que se abre, se muestra la notificación sobre el virus de prueba.

El virus de prueba EICAR no contiene código que pueda dañar su dispositivo. Sin embargo, las aplicaciones de seguridad de la mayoría de los fabricantes identifican este archivo como virus. Puede descargar el virus de prueba del sitio web oficial de EICAR.

Acerca de los estados de los dispositivos

Kaspersky Security Center Linux le asigna un estado a cada dispositivo administrado. El estado asignado depende de que se cumplan las condiciones definidas por el usuario. En algunos casos, al asignar un estado a un dispositivo, Kaspersky Security Center Linux tiene en cuenta el indicador de visibilidad del dispositivo en la red (consulte la tabla a continuación). Por ejemplo, si a un dispositivo administrado se le asigna el estado *Crítico* por cumplirse la condición *Las bases de datos están desactualizadas*, y luego se activa el indicador de visibilidad para ese dispositivo, el estado del dispositivo cambia a *Sin inconvenientes*. Si Kaspersky Security Center Linux no encuentra un dispositivo en la red en un plazo de dos horas, el indicador de visibilidad del dispositivo se establece en *No visible*.

Los estados son los siguientes:

- *Crítico* o *Crítico/Visible*
- *Advertencia* o *Advertencia/Visible*
- *Sin inconvenientes* o *Sin inconvenientes/Visible*

En la siguiente tabla, se enumeran las condiciones predeterminadas que se deben cumplir para que se asignen los estados *Crítico* o *Advertencia* a un dispositivo, con todos los valores posibles.

Condiciones para que se asigne un estado a un dispositivo

Condición	Descripción de la condición	Valores disponibles
La aplicación de seguridad no está instalada	El Agente de red está instalado en el dispositivo, pero no hay una aplicación de seguridad instalada.	• Interruptor activado. • Interruptor desactivado.

Condición	Descripción de la condición	Valores disponibles
Se detectaron demasiados virus	Una tarea de detección de virus (por ejemplo, la tarea Análisis antimalware) detectó en el dispositivo una cantidad de virus superior al valor especificado.	Más de 0.
El nivel de protección en tiempo real difiere del nivel establecido por el administrador	El dispositivo es visible en la red, pero el nivel de la protección en tiempo real no se corresponde con el que el administrador configuró (en la condición) para el estado del dispositivo.	• Detenida. • Suspendida. • En ejecución.
No se ha realizado un análisis antimalware en mucho tiempo	El dispositivo está visible en la red y tiene instalada una aplicación de seguridad, pero la tarea *Análisis antimalware* no se ha ejecutado en el intervalo de tiempo especificado. Esta condición se aplica solo a los dispositivos que se agregaron al menos siete días antes a la base de datos del Servidor de administración.	Más de 1 día.
Las bases de datos están desactualizadas	El dispositivo es visible en la red y tiene instalada una aplicación de seguridad, pero sus bases de datos antivirus no se han actualizado en el período de tiempo especificado. Esta condición se aplica solo a los dispositivos que se agregaron al menos un día antes a la base de datos del Servidor de administración.	Más de 1 día.
Sin conexión desde hace mucho tiempo	El Agente de red está instalado en el dispositivo, pero el dispositivo está apagado y no se ha conectado a un Servidor de administración durante el período de tiempo especificado.	Más de 1 día.
Se han detectado amenazas activas	El número de objetos no procesados en la carpeta **Amenazas activas** supera el valor especificado.	Más de 0 elementos.
Tiempo requerido desde el reinicio	El dispositivo está visible en la red, pero una aplicación requirió un reinicio durante más tiempo que el intervalo de tiempo especificado.	Más de 0 minutos.
Motivo del reinicio	El dispositivo está visible en la red, pero una aplicación requiere un reinicio del dispositivo por uno de los motivos seleccionados.	• Motivo desconocido • La aplicación no se ejecutará hasta que se reinicie el equipo • Se debe reiniciar el dispositivo para completar la actualización que está ejecutando la aplicación • Se requiere reiniciar para iniciar la actualización • Se debe reiniciar el dispositivo para completar el análisis o la desinfección • Se requiere reiniciar para completar la instalación o la desinstalación remotas • Completando cifrado de datos en disco
Hay aplicaciones incompatibles instaladas	El dispositivo es visible en la red, pero, al hacer un inventario de software a través del Agente de red, se detectaron aplicaciones incompatibles instaladas en el dispositivo.	• Interruptor desactivado. • Interruptor activado.
Se detectaron vulnerabilidades de software	El dispositivo es visible en la red y tiene instalado el Agente de red, pero la tarea *Buscar vulnerabilidades y actualizaciones requeridas* ha encontrado aplicaciones instaladas en el dispositivo que tienen vulnerabilidades con el nivel de gravedad especificado.	• Crítico • Alto. • Medio. • Ignorar si la vulnerabilidad no se puede reparar. • Ignorar si hay una actualización asignada para instalarse.
Licencia caducada	El dispositivo es visible en la red, pero la licencia ha caducado.	• Interruptor desactivado. • Interruptor activado.
La licencia está por caducar	El dispositivo es visible en la red, pero la licencia instalada en el mismo caduca en menos días que el número de días especificado.	Más de 0 días.

Condición	Descripción de la condición	Valores disponibles
La búsqueda de actualizaciones de Windows Update no se ha realizado en mucho tiempo	El dispositivo es visible en la red, pero la tarea *Buscar vulnerabilidades y actualizaciones requeridas* no se ejecutó durante el intervalo de tiempo especificado.	Más de 1 día.
Estado de cifrado no válido	El Agente de red está instalado en el dispositivo, pero el resultado del cifrado del dispositivo es igual al valor especificado.	• No cumple con la directiva porque el usuario no dio su consentimiento (solo para dispositivos externos). • No cumple con la directiva debido a un error. • Se debe reiniciar el dispositivo al aplicar la directiva. • No se ha especificado una directiva de cifrado. • No compatible. • Al aplicar la directiva.
La configuración del dispositivo móvil no cumple con la directiva	Los ajustes del dispositivo móvil no son los que se encontraron en la directiva de Kaspersky Endpoint Security para Android durante el chequeo de reglas de cumplimiento normativo.	• Interruptor desactivado. • Interruptor activado.
Problemas de seguridad no procesados detectados	Se han encontrado problemas de seguridad sin procesar en el dispositivo. Los problemas de seguridad se pueden crear manualmente por el administrador o automáticamente por las aplicaciones de Kaspersky administradas que se han instalado en el dispositivo cliente.	• Interruptor desactivado. • Interruptor activado.
Estado del dispositivo definido por la aplicación	El estado del dispositivo es definido por la aplicación administrada. Los dispositivos administrados pueden tener un estado definido por las aplicaciones administradas independientemente de la configuración de Kaspersky Security Center Linux. Después de que este estado devuelve uno de los estados definidos por Kaspersky Security Center Linux, el Servidor de administración asigna a un dispositivo administrado el estado más crítico de los devueltos por la aplicación administrada y asignados por el Servidor de administración. Los estados definidos por la administración de aplicaciones tienen descripciones transferidas por las aplicaciones administradas. Puede ver las descripciones en la lista de dispositivos administrados, en la columna **Descripción del estado**.	• Interruptor desactivado. • Interruptor activado.
El dispositivo no tiene espacio en el disco	El espacio libre en el disco del dispositivo es inferior al valor especificado o el dispositivo no se pudo sincronizar con el Servidor de administración. Los estados *Crítico* o *Advertencia* cambiarán por el estado *Sin inconvenientes* cuando el dispositivo se sincronice correctamente con el Servidor de administración y el espacio libre en el dispositivo supere o iguale el valor especificado.	Más de 0 MB.
El dispositivo ha cambiado a no administrado	Durante el descubrimiento de dispositivos, el dispositivo se reconoció como visible en la red, pero hubo más de tres intentos de sincronizar el dispositivo con el Servidor de administración que terminaron con un error.	• Interruptor desactivado. • Interruptor activado.
Protección deshabilitada	El dispositivo es visible en la red, pero la aplicación de seguridad del dispositivo ha estado deshabilitada por un tiempo superior al especificado. En este caso, el estado de la aplicación de seguridad es *detenida* o *error*, y difiere del siguiente: *iniciada*, *en ejecución* o *suspendida*.	Más de 0 minutos.
La aplicación de seguridad no está en ejecución	El dispositivo es visible en la red y tiene instalada una aplicación de seguridad, pero esa aplicación no se está ejecutando.	• Interruptor desactivado. • Interruptor activado.

Kaspersky Security Center Linux permite que usted configure la conmutación automática del estado de un dispositivo en un grupo de administración cuando las condiciones especificadas se cumplen. El estado del dispositivo cliente puede hacerse pasar a *Crítico* o *Advertencia* si se cumplen las condiciones especificadas. Si no se cumplen estas condiciones, el dispositivo cliente toma el estado *Sin inconvenientes*.

Cada estado puede corresponderse con distintos valores de una misma condición. De forma predeterminada, por ejemplo, cuando la condición **Las bases de datos están desactualizadas** tiene el valor **Más de 3 días**, se asigna el estado *Advertencia* al dispositivo cliente; si el valor es **Más de 7 días**, se asigna el estado *Crítico*.

Si actualiza Kaspersky Security Center Linux desde la versión anterior, los valores de la condición **Las bases de datos están desactualizadas** para asignar el estado a *Crítico* o *Advertencia* no cambian.

Parámetros y variables de entorno para describir un evento

Al configurar las notificaciones sobre eventos de Kaspersky Security Center Linux, puede usar parámetros y variables de entorno para describir los eventos (consulte la siguiente tabla).

Si eligió ejecutar un archivo ejecutable como método de notificación, use variables al escribir el archivo.

Si desea enviar notificaciones sobre eventos por correo electrónico o SMS, también puede especificar variables en los campos **Asunto** y **Mensaje de notificación** al configurar las notificaciones en la pestaña correspondiente.

Parámetros y variables de entorno para describir un evento

Parámetro de sustitución (para usar en notificaciones)	Variable de entorno (para usar en scripts)	Descripción de la variable de entorno
%SEVERITY%	$SEVERITY	Gravedad del evento. Valores posibles: • **Información** • **Advertencia** • **Error** • **Crítico**
%COMPUTER%	$COMPUTER	Nombre del dispositivo en el cual sucedió el evento. La longitud máxima del nombre del dispositivo es de 256 caracteres.
%DOMAIN%	$DOMAIN	Nombre de dominio del dispositivo en el cual sucedió el evento.
%EVENT%	$EVENT	Nombre del tipo de evento. La longitud máxima del nombre del tipo de evento es de 50 caracteres.
%DESCR%	$DESCR	Descripción del evento. La longitud máxima de la descripción es de 1000 caracteres.
%RISE_TIME%	$RISE_TIME	Hora de creación del evento.
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	$KLCSAK_EVENT_TASK_DISPLAY_NAME	Nombre de la tarea. La longitud máxima del nombre de la tarea es de 100 caracteres.
%KL_PRODUCT%	$KL_PRODUCT	Nombre de la aplicación.
%KL_VERSION%	$KL_VERSION	Número de versión de la aplicación.
%$KLCSAK_EVENT_SEVERITY_NUM%	$KLCSAK_EVENT_SEVERITY_NUM	Número de gravedad del evento. Valores posibles: • 1—**Información** • 2—**Advertencia** • 3—**Error** • 4—**Crítico**
%HOST_IP%	$HOST_IP	Dirección IP del dispositivo en el cual sucedió el evento.
%HOST_CONN_IP%	$HOST_CONN_IP	Dirección IP de conexión del dispositivo en el cual sucedió el evento.

Ver información sobre la detección de amenazas

Puede indicar si desea que la aplicación muestre u oculte información sobre las alertas.

Después de activar el Servidor de administración con una licencia de Kaspersky Extended Detection and Response Optimum o de Kaspersky Next XDR Optimum, Kaspersky Security Center Web Console muestra automáticamente la subsección **Alertas** en la sección **Supervisión** del menú principal.

*Para indicar si se deberá mostrar la sección **Alertas** en el menú principal:*

1. En el menú principal, vaya a **Configuración** → **Opciones de interfaz**.
2. Habilite o deshabilite la opción **Mostrar alertas EDR**.
3. Haga clic en el botón **Guardar**.

Cuando se habilita la opción **Mostrar alertas EDR**, la consola muestra la subsección **Alertas** en la sección **Supervisión** del menú principal. En la subsección **Alertas**, podrá ver información sobre la detección de amenazas en los endpoints.

Si lo prefiere, también puede agregar un widget que muestre información sobre las alertas.

Para que la tarjeta de alerta muestre correctamente la información detallada sobre las amenazas detectadas, se debe instalar el complemento de Kaspersky Endpoint Agent y la versión compatible del complemento de Kaspersky Endpoint Security (Kaspersky Endpoint Security for Linux 12.1 o posterior, Kaspersky Endpoint Security for Mac 12.1 o posterior, o Kaspersky Endpoint Security para Windows 12.6 o posterior).

Utilice el menú **Filtro** para filtrar las alertas por fecha y valores de campo.

El campo **Tipo de objeto** contiene los siguientes valores:

- desconocido
- Vínculo de phishing
- virus
- Troyano
- herramienta maliciosa
- puerta trasera
- gusano
- otra aplicación
- Adware
- Software pornográfico

- Programa empaquetado peligroso
- Comportamiento peligroso

El campo **Respuesta automática** contiene los siguientes valores:

- Se detectó un objeto malicioso
- Objeto eliminado
- Objeto desinfectado
- El objeto no pudo ser desinfectado
- Objeto puesto en cuarentena
- Archivo protegido por contraseña detectado
- Virus detectados

Integraciones para responder a alertas

Si tiene la licencia de Kaspersky Next XDR Optimum, puede configurar integraciones con las siguientes soluciones para responder a las amenazas:

- Kaspersky Automated Security Awareness Platform
- Kaspersky Threat Intelligence Portal Sandbox
- Active Directory

Estas integraciones están disponibles si activó el Servidor de administración con una licencia de Kaspersky Next XDR Optimum.
Para realizar acciones de respuesta, debe implementar la clave de licencia de Kaspersky Next XDR Optimum en sus aplicaciones administradas.
Al utilizar la funcionalidad de Kaspersky Next XDR Optimum con una licencia de prueba, primero debe agregar un Servidor de administración secundario físico, activarlo con la licencia de prueba y luego implementar la clave de licencia en los dispositivos administrados mediante este Servidor de administración.

Si está utilizando la licencia de Kaspersky Next EDR Optimum, no es necesario que active las aplicaciones instaladas en sus dispositivos administrados con la licencia de Kaspersky Next XDR Optimum. Debe hacerlo solo para dispositivos nuevos, en caso de que los hubiera.

Como la licencia de Kaspersky Next XDR Optimum es compatible con el multiinquilinato, puede distribuir la clave de licencia de manera centralizada a las aplicaciones administradas. No se admite la distribución automática de la licencia a servidores de administración secundarios y virtuales.

Para configurar las integraciones, debe tener los derechos **Leer** y **Escribir** para el área funcional **Características generales: Integración de aplicaciones**.

Configurar la integración con Active Directory para realizar acciones de respuesta

La integración con Active Directory le permite realizar acciones de respuesta para los usuarios de Active Directory afectados o involucrados en la alerta.

Para configurar la integración con Active Directory para responder a las alertas, debe usar el Servidor de administración de Kaspersky Security Center Linux versión 15.4 o una versión posterior.

La integración con Active Directory para responder a las alertas y la configuración para analizar el controlador de dominio de Active Directory (la dirección y las credenciales de usuario del controlador de dominio) que especifica al configurar un sondeo de controlador de dominio son dos configuraciones diferentes. Dado que debe asegurarse de que el usuario para el que se va a realizar una acción de respuesta tenga una cuenta de Active Directory, debe configurar ambas integraciones: para el análisis y para la respuesta. El orden no es importante.

La configuración de integración no se hereda y se aplica solo al Servidor de administración (físico o virtual) en el que se configuran estas opciones.

Para configurar la integración con Active Directory para responder a las alertas:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abrirá la ventana de propiedades del Servidor de administración, con la pestaña **General** seleccionada.

2. Realice una de las siguientes acciones:

   - Seleccione la sección **Puntos de distribución**, haga clic en el nombre del punto de distribución requerido y, a continuación, en la ventana de propiedades que se abre, seleccione la sección **Active Directory**.

   - Seleccione la sección **Respuesta de Active Directory**.

3. En el panel derecho, habilite el botón de alternancia de la **Integración con Active Directory**.

   Más tarde, si desea desactivar la integración, solo puede hacerlo para todas las conexiones deshabilitando el botón de alternancia de la **Integración con Active Directory**. No se puede desactivar la integración para una conexión diferente. En su lugar, puede eliminar la conexión.

   > Cuando habilita o deshabilita el botón de alternancia de la **Integración con Active Directory**, la configuración se aplica tanto a la sección **Respuesta de Active Directory** como a la sección **Puntos de distribución**.

4. Cree una conexión al controlador de dominio de Active Directory haciendo clic en el botón **Agregar**.

5. En la ventana que se abrirá, defina los siguientes parámetros para la conexión:

   - **Dirección del controlador de dominio**

     Nombre del equipo, por ejemplo: `server.mycompany.com`.

     Puede especificar varias direcciones. Todos los controladores de dominio cuyas direcciones especifique deben pertenecer al mismo dominio.

   - **Nombre de dominio de Active Directory**

Nombre de dominio completo DNS, por ejemplo: `mycompany.com`

También puede especificar el nombre SAM o NetBIOS, por ejemplo: `mycompany`

Utilice letras minúsculas. Si crea varias conexiones para el Servidor de administración o un punto de distribución, especifique nombres diferentes para cada conexión.

> Para realizar acciones de respuesta, el nombre de dominio de Active Directory que especifique en este campo debe coincidir con el nombre de dominio de Active Directory especificado en la alerta.

- **Nombre de usuario**

  Nombre de usuario de la cuenta de Active Directory con derechos de administrador con la cual se realizarán las acciones de respuesta.

- **Contraseña**

  Contraseña de la cuenta de Active Directory con derechos de administrador con la cual se realizarán las acciones de respuesta.

6. Si desea verificar el estado de la conexión, haga clic en el botón **Comprobar conexión**.

   Si la conexión se establece correctamente, se muestra el estado **Conectado**. De lo contrario, el estado es **Error** y se muestra un mensaje de error con los controladores de dominio a los que no pudo conectarse.

> Debe tener en cuenta cómo se realiza la conexión a Active Directory: **desde un dispositivo Linux o desde un dispositivo Windows**.

Conexión desde un dispositivo Linux

Por defecto, al conectarse y realizar la autenticación a un controlador de dominio desde un dispositivo Linux, la lógica es la siguiente:

1. El Servidor de administración o el punto de distribución intentan conectarse al controlador de dominio mediante el protocolo LDAPS.

   Se requiere una verificación estricta del certificado del servidor LDAP.

2. La parte pública del certificado del controlador de dominio se coloca en el repositorio de certificados del sistema para validar el certificado.

   Se usa la ruta de acceso a la autoridad de certificación (CA) del sistema, que depende del sistema operativo, para acceder a la cadena de certificados.

   Por ejemplo:

   - /etc/ssl/certs/ca-certificates.crt: ruta para sistemas operativos basados en Debian (Debian, Ubuntu, Astra).
   - /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem: ruta para CentOS o Red Hat.

3. Si la conexión LDAPS falla, se produce un error y no se utiliza ningún otro protocolo de conexión.

> En caso de problemas con LDAPS, puede comunicarse con el Soporte técnico de Kaspersky.

Si no desea instalar el certificado en el repositorio de certificados del sistema, puede usar el indicador KLNAG_LDAP_SSL_CACERT para establecer la ruta al certificado del controlador de dominio. Para hacerlo, ejecute el comando:

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "</path/to/domain-controller/cert>"
```

dónde `</path/to/domain-controller/cert>` es la ruta a la parte pública del certificado del controlador de dominio.

Por ejemplo, si la ruta es `"/var/opt/kaspersky/ldap_cert.crt"`, el comando es `klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "/var/opt/kaspersky/ldap_cert.crt"`

Conexión desde un dispositivo Windows

Al conectarse y realizar la autenticación a un controlador de dominio desde un dispositivo Windows, la configuración de la conexión la define el dominio.

Solo debe asegurarse de que:

- El LDAPS esté habilitado y el puerto 636 esté disponible en el dispositivo.
- Se permitan las conexiones al controlador de dominio a través de un firewall o un servidor proxy.

7. Haga clic en el botón **Guardar**.

La ventana se cierra y la conexión se muestra en la tabla de conexiones.

En la tabla de conexiones, puede hacer lo siguiente:

- Editar los parámetros de conexión.

  Para hacer esto, haga clic en el vínculo con el parámetro **Dirección del controlador de dominio** para la conexión requerida. En la ventana que se abre, cambie la configuración necesaria y, luego, haga clic en el botón **Guardar**.

  Solo puede editar los parámetros **Nombre de usuario** y **Contraseña**.

- Eliminar conexiones.

  Para hacer esto, seleccione la casilla que se encuentra junto a la conexión que desee eliminar, haga clic en el botón **Eliminar** en la barra de herramientas y luego confirme la eliminación de la conexión.

Configuración de la integración con Kaspersky Automated Security Awareness Platform

La integración con Kaspersky Automated Security Awareness Platform (en adelante, también denominada KASAP) le permite asignar cursos de aprendizaje KASAP a los usuarios asociados a las alertas.

La configuración de integración no se hereda y se aplica solo al Servidor de administración (físico o virtual) en el que se configuran estas opciones.

Antes de configurar una integración en Kaspersky Security Center Web Console, debe crear un token de autorización y obtener una URL para las solicitudes de API en KASAP.

Para configurar la integración con Kaspersky Automated Security Awareness Platform, siga estos pasos:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abrirá la ventana de propiedades del Servidor de administración, con la pestaña **General** seleccionada.

2. Elija la sección **KASAP**.

3. En el panel derecho, habilite el botón de alternancia de la **Integración con KASAP**.

4. Especifique la configuración que se utilizará para la conexión a KASAP:

   - **Token de API**: el token que creó para acceder a KASAP Open API.
   - **Dirección URL**: URL para las solicitudes de API que obtuvo al crear el token de API.
   - **Usar un servidor proxy**: botón de alternancia que habilita el uso de un servidor proxy cuando se conecta a KASAP.

     El botón de alternancia está desactivado de forma predeterminada.

5. Si es necesario, verifique la configuración que especificó haciendo clic en el botón **Comprobar conexión**.

   Se muestra el estado de la conexión.

6. Haga clic en el botón **Guardar**.

La integración con Kaspersky Automated Security Awareness Platform está configurada.

Después de guardar la configuración de la integración con KASAP, puede ver la lista de grupos de aprendizaje de KASAP haciendo clic en el botón **Ver grupos**.

Si es necesario, cuando se muestra la lista de grupos, puede actualizarla haciendo clic en el botón **Actualizar grupos**.

No puede ocultar la lista después de abrirla. Si deshabilita el botón de alternancia de la **Integración con KASAP**, no se muestra la lista de grupos KASAP.

Configurar la integración con Kaspersky Threat Intelligence Portal Sandbox

La integración con Kaspersky Threat Intelligence Portal (en adelante también denominado Kaspersky TIP) le permite ejecutar los archivos movidos a la sección **Cuarentena** usando Kaspersky Sandbox: un entorno seguro aislado de su red corporativa.

La configuración de integración no se hereda y se aplica solo al Servidor de administración (físico o virtual) en el que se configuran estas opciones.

Antes de configurar la integración, debe obtener un token de autorización para las solicitudes de API en Kaspersky TIP.

Para configurar la integración con Kaspersky TIP Sandbox:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abrirá la ventana de propiedades del Servidor de administración, con la pestaña **General** seleccionada.

2. Seleccione **Kaspersky TIP**.

3. En el panel derecho, habilite el botón de alternancia **Integración**.

   Se muestra la configuración para la conexión a Kaspersky TIP.

   Si después de configurar y guardar la configuración de integración deshabilita el botón de alternancia **Integración**, la configuración no se elimina, pero no se puede realizar la acción de respuesta.

4. Haga clic en el botón **Agregar token**, especifique en la ventana que aparece el token que obtuvo anteriormente de Kaspersky TIP y, a continuación, haga clic en el botón **Agregar**.

   La ventana se cierra y se agrega el token de API.

5. Si desea utilizar un servidor proxy al conectarse a Kaspersky TIP, habilite el botón de alternancia **Usar un servidor proxy**.

   El botón de alternancia está desactivado de forma predeterminada.

6. Haga clic en el botón **Guardar**.

La integración con Kaspersky TIP Sandbox está configurada.

Ahora puede enviar archivos desde la sección **Cuarentena** a Kaspersky TIP Sandbox para el análisis de amenazas. El tamaño máximo de un archivo es de 100 megabytes (MB).

Debido a que la licencia de Kaspersky Next XDR Optimum es compatible con el multiinquilinato, los archivos colocados en **Cuarentena** están divididos por inquilinos. Esta separación a nivel de inquilino también se aplica al enviar archivos a Kaspersky TIP Sandbox y ver los resultados si el administrador usa una cuenta de TIP dedicada y un token de API relacionado con cada inquilino. Sin embargo, la administración centralizada de la sección **Cuarentena** para todos los inquilinos no es posible, ya que la lista de cuarentena no muestra objetos de acuerdo con la jerarquía del servidor.

Agrupación de alertas por atributos

La combinación de alertas ayuda a identificar las alertas que pueden estar relacionadas con el mismo incidente, lo que simplifica el proceso de investigación.

Para habilitar la funcionalidad de combinación de alertas, debe hacer lo siguiente:

- Habilite la subsección **Alertas** en el menú principal.
- Active el Servidor de Administración con una licencia de Kaspersky Next XDR Optimum y, luego, implemente la clave de licencia de Kaspersky Next XDR Optimum en sus aplicaciones administradas.

  Al usar una funcionalidad de Kaspersky Next XDR Optimum con una licencia de prueba en el modo de prueba, primero debe agregar un Servidor de administración físico secundario y luego activar dicho servidor con esta licencia.

Si está utilizando la licencia de Kaspersky Next EDR Optimum, no es necesario que active las aplicaciones instaladas en sus dispositivos administrados con la licencia de Kaspersky Next XDR Optimum. Debe hacerlo solo para dispositivos nuevos, en caso de que los hubiera.
Como la licencia de Kaspersky Next XDR Optimum es compatible con el multiinquilinato, puede distribuir la clave de licencia de manera centralizada a las aplicaciones administradas. No se admite la distribución automática de la licencia a servidores de administración secundarios y virtuales.

Puede combinar alertas por nombre de dispositivo, cuenta o nombre de hash (SHA256).

> Las alertas se combinan por un atributo solo si ese atributo no está vacío.

Las alertas se combinan si comparten al menos un atributo y ocurren dentro de las 24 horas posteriores a cualquier otra alerta en el grupo.

Para combinar alertas por atributos:

1. En el menú principal, vaya a **Supervisión** → **Alertas**.
2. Realice una de las siguientes acciones:
   - Habilite el botón de alternancia de **Agregación de alertas** y, luego, seleccione uno o más atributos para combinar alertas de la siguiente manera:
     - **Nombre del dispositivo**
     - **Cuenta**
     - **Hash de archivo**Nombre de hash (SHA256)

     Los atributos **Nombre del dispositivo** y **Cuenta** están seleccionados de manera predeterminada.
   - Haga clic en el ícono de configuración (⚙). En el panel **Configuración de tabla** que se abre, vaya a la pestaña **Agrupación**. Seleccione **Id. del grupo de agregación** y haga clic en **Aplicar**.

Cuando la combinación está habilitada, las alertas se ordenan según la **Fecha y hora del evento**, del más reciente al más antiguo. No se admiten opciones de clasificación adicionales. Si selecciona una opción de agrupación diferente, se deshabilitará la combinación.

La tabla muestra las alertas combinadas por atributos. Las alertas no combinadas se muestran en la parte inferior de la tabla.

Cada alerta se asigna a un solo grupo después de la combinación.

Cloud Discovery

Kaspersky Security Center Linux permite supervisar el uso de servicios en la nube en dispositivos con Windows administrados y bloquear el acceso a los servicios en la nube que usted no considere deseables. Cloud Discovery monitorea los intentos de los usuarios de acceder a estos servicios desde navegadores y aplicaciones de escritorio. También supervisa los intentos de los usuarios de acceder a servicios en la nube mediante conexiones no cifradas (por ejemplo, a través del protocolo HTTP). La función permite detectar y detener el uso de servicios en la nube por parte de la llamada "TI invisible".

La capacidad de bloqueo solo está disponible si ha activado Kaspersky Security Center Linux con una licencia Kaspersky Next EDR Optimum o Kaspersky Next XDR Expert.

La capacidad de bloqueo solo estará disponible si utiliza Kaspersky Endpoint Security para Windows 11.2 o una versión posterior. Las versiones anteriores de la aplicación de seguridad solo permiten supervisar el uso de servicios en la nube.

Puede habilitar la función Cloud Discovery y seleccionar las directivas o los perfiles de seguridad para los que desee habilitar la función. También puede habilitar o deshabilitar la función para cada directiva o perfil de seguridad de forma independiente. Puede bloquear el acceso a los servicios en la nube a los que no desee que accedan los usuarios.

Para poder bloquear el acceso a servicios en la nube no deseados, asegúrese de que se cumplan los siguientes requisitos previos:

- Utiliza Kaspersky Endpoint Security 11.2 para Windows o una versión posterior. Las versiones anteriores de la aplicación de seguridad solo permiten supervisar el uso de servicios en la nube.
- Compró una licencia del nivel de Kaspersky Next que incluye la posibilidad de bloquear el acceso a servicios en la nube no deseados. Para obtener más información, consulte la Ayuda de Kaspersky Next.

El widget de Cloud Discovery y los informes de Cloud Discovery muestran información sobre los intentos concretados y bloqueados de acceder a servicios en la nube. El widget también muestra el nivel de riesgo de cada servicio en la nube. Kaspersky Security Center Linux obtiene información sobre el uso de servicios en la nube únicamente de aquellos dispositivos administrados que se han protegido con perfiles de seguridad que tienen la función habilitada.

Habilitar Cloud Discovery mediante el widget

La función Cloud Discovery permite obtener información sobre el uso de servicios en la nube de todos los dispositivos administrados que se han protegido con directivas de seguridad que tengan la función habilitada. Puede habilitar o deshabilitar Cloud Discovery exclusivamente para la directiva de Kaspersky Endpoint Security para Windows.

Existen dos formas de habilitar la función Cloud Discovery:

- utilizar el widget de Cloud Discovery;
- modificar las propiedades de la directiva de Kaspersky Endpoint Security para Windows.

  Para obtener información detallada sobre cómo habilitar la función Cloud Discovery en las propiedades de la directiva de Kaspersky Endpoint Security para Windows, consulte la sección Cloud Discovery en la Ayuda de Kaspersky Endpoint Security para Windows.

Tenga en cuenta que la función Cloud Discovery solo se puede deshabilitar en los ajustes de la directiva de Kaspersky Endpoint Security para Windows.

Para habilitar Cloud Discovery, debe tener el derecho **Modificar** en el área funcional **Características generales: funcionalidad básica**.

Para habilitar la función Cloud Discovery mediante el widget:

1. Vaya a Kaspersky Security Center Linux.
2. En el menú principal, vaya a **Supervisión** → **Panel**.
3. En el widget de **Cloud Discovery**, haga clic en el botón **Habilitar**.

   Si tiene instalada la versión 12.4 de Kaspersky Endpoint Security para Windows, habilite la función Cloud Discovery en las propiedades de la directiva de Kaspersky Endpoint Security para Windows. Para obtener más información, consulte la sección Cloud Discovery de la Ayuda de Kaspersky Endpoint Security para Windows.

   Si su versión de Kaspersky Endpoint Security para Windows es anterior a la 12.4, actualice el complemento de Kaspersky Endpoint Security para Windows a la versión 12.5.

4. En la ventana **Habilitar Cloud Discovery** que se abre, seleccione las directivas de seguridad para las que desea habilitar la función y, luego, haga clic en el botón **Habilitar**.

   Los siguientes ajustes de la directiva se habilitarán automáticamente: **Inyectar script en el tráfico web para interactuar con las páginas web**, **Monitor de sesión web** y **Análisis de conexiones cifradas**.

La función Cloud Discovery queda habilitada y el widget se agrega al panel.

Agregar el widget de Cloud Discovery al panel

Puede agregar el widget de **Cloud Discovery** al panel para supervisar el uso de servicios en la nube en los dispositivos administrados.

Para agregar el widget de Cloud Discovery al panel, debe tener el derecho **Modificar** en el área funcional **Características generales: Funcionalidad básica**.

Para agregar el widget de Cloud Discovery al panel:

1. Vaya a Kaspersky Security Center Linux.
2. En el menú principal, vaya a **Supervisión** → **Panel**.
3. Haga clic en el botón **Añadir o restaurar un widget**.
4. En la lista de widgets disponibles, haga clic en el ícono del corchete angular (>) ubicado junto a la categoría **Otro**.
5. Seleccione el widget **Cloud Discovery** y, luego, haga clic en el botón **Agregar**.

   Si la función Cloud Discovery está deshabilitada, siga las instrucciones en la sección "Habilitar Cloud Discovery mediante el widget".

El widget seleccionado se agrega al final del panel.

Ver información sobre el uso de servicios en la nube

Puede ver el widget de **Cloud Discovery**, que muestra información sobre los intentos de acceso a servicios en la nube. El widget también muestra el nivel de riesgo de cada servicio en la nube. Kaspersky Security Center Linux obtiene información sobre el uso de servicios en la nube de todos los dispositivos administrados que están protegidos únicamente por perfiles de seguridad que tienen habilitada esta función.

Antes de acceder a la información, asegúrese de que se cumplan los siguientes requisitos:

- Que el widget de Cloud Discovery se haya agregado al panel.
- Que la función Cloud Discovery esté habilitada.
- Que tenga el derecho de **Leer** en el área funcional **Características generales: funcionalidad básica**.

Para ver el widget de Cloud Discovery:

1. Vaya a Kaspersky Security Center Linux.
2. En el menú principal, vaya a **Supervisión** → **Panel**.

   El widget de **Cloud Discovery** se muestra en el panel.

3. En el lado izquierdo del widget de **Cloud Discovery**, seleccione una categoría de servicios en la nube.

   En la tabla ubicada en el lado derecho del widget, se mostrarán hasta cinco servicios de la categoría seleccionada a los que los usuarios intenten acceder con mayor frecuencia. Se cuentan tanto los intentos exitosos como los bloqueados.

4. En el lado derecho del widget, seleccione un servicio específico.

   En la tabla que verá a continuación, se mostrarán los diez dispositivos que hayan intentado acceder a un servicio con mayor frecuencia. Puede usar esta tabla para generar dos tipos de informes: un informe sobre los intentos de acceso exitosos y un informe sobre los intentos de acceso bloqueados.

   Además, en esta tabla puede bloquear el acceso a un servicio en la nube para un dispositivo específico.

El widget mostrará la información solicitada.

En el widget que se abre, puede hacer lo siguiente:

- Diríjase a la sección **Supervisión** → **Informes** para ver los informes de Cloud Discovery.
- bloquear o permitir el acceso a un servicio de nube seleccionado.

La capacidad de bloqueo solo está disponible si ha activado Kaspersky Security Center Linux con una licencia Kaspersky Next EDR Optimum o Kaspersky Next XDR Expert.
La función de bloqueo solo está disponible si utiliza Kaspersky Endpoint Security 11.2 for Windows o una versión posterior. Las versiones anteriores de la aplicación de seguridad solo permiten supervisar el uso de servicios en la nube.

Nivel de riesgo de un servicio en la nube

Cloud Discovery indica un nivel de riesgo para cada servicio en la nube. El nivel de riesgo ayuda a determinar qué servicios no se ajustan a los requisitos de seguridad de la organización. Posiblemente quiera tener en cuenta el nivel de riesgo a la hora de decidir si bloqueará el acceso a un determinado servicio.

El nivel de riesgo es un índice estimado; no indica la calidad de un servicio en la nube o del proveedor del servicio. El nivel de riesgo es simplemente una recomendación de los expertos de Kaspersky.

Los niveles de riesgo de los servicios en la nube se muestran en el widget de Cloud Discovery y en la lista de todos los servicios en la nube supervisados.

Bloquear el acceso a servicios en la nube no deseados

Puede bloquear el acceso a los servicios en la nube a los que no desea que accedan los usuarios. También puede permitir el acceso a servicios en la nube que se encuentren bloqueados.

Al decidir si bloqueará el acceso a un servicio determinado, entre otras consideraciones, es posible que desee tener en cuenta el nivel de riesgo.

El acceso a los servicios en la nube puede bloquearse o permitirse en una directiva o en un perfil de seguridad.

Existen dos formas de bloquear el acceso a servicios en la nube no deseados:

- Utilizar el widget de Cloud Discovery.

  Si elige esta opción, puede bloquear el acceso a servicios individuales.

- Modificar las propiedades de la directiva de Kaspersky Endpoint Security para Windows.

  Si elige esta opción, puede bloquear el acceso a servicios individuales o incluso a categorías completas.

  Para obtener información detallada sobre cómo habilitar la función Cloud Discovery en las propiedades de la directiva de Kaspersky Endpoint Security para Windows, consulte la sección Cloud Discovery en la Ayuda de Kaspersky Endpoint Security para Windows.

Para bloquear o permitir el acceso a un servicio en la nube mediante el widget:

1. Abra el widget de Cloud Discovery y seleccione el servicio en la nube en cuestión.
2. En el panel **Los 10 principales dispositivos que utilizan el servicio**, busque la directiva o el perfil de seguridad en que desee bloquear o permitir el servicio.
3. En la línea correspondiente, en la columna **Estado del acceso en la directiva o el perfil**, realice una de las siguientes acciones:
   - Para bloquear el servicio, seleccione **Bloqueado** en la lista desplegable.
   - Para permitir el servicio, seleccione **Permitido** en la lista desplegable.
4. Haga clic en el botón **Guardar**.

El acceso al servicio seleccionado queda bloqueado o permitido en la directiva o el perfil de seguridad.

Exportación de eventos a sistemas SIEM

En esta sección, se brindan instrucciones para configurar la exportación de eventos a un sistema SIEM.

Configurar la exportación de eventos a sistemas SIEM

Kaspersky Security Center Linux permite configurar la exportación de eventos a sistemas SIEM mediante uno de los siguientes métodos: exportar a cualquier sistema SIEM que utilice el formato Syslog, exportar a los sistemas SIEM Kaspersky SIEM, QRadar, Splunk y ArcSight que utilizan los formatos LEEF y CEF, o exportar eventos a sistemas SIEM directamente desde la base de datos de Kaspersky Security Center. Cuando complete este escenario, el Servidor de administración enviará los eventos al sistema SIEM automáticamente.

Requisitos previos

Antes de configurar la exportación de eventos en Kaspersky Security Center Linux:

- Lea sobre los métodos disponibles para exportar eventos.
- Asegúrese de contar con los valores de la configuración del sistema.

Los pasos aquí descritos pueden realizarse en cualquier orden.

El proceso para exportar eventos a un sistema SIEM consiste de los siguientes pasos:

- **Configuración el sistema SIEM para recibir eventos de Kaspersky Security Center Linux**

  Instrucciones: Configurar la exportación de eventos en un sistema SIEM

- **Seleccionar los eventos que desea exportar al sistema SIEM**

  Seleccione qué eventos desea exportar al sistema SIEM. Primero, marque los eventos generales que ocurren en todas las aplicaciones administradas de Kaspersky. Luego, puede marcar los eventos para aplicaciones de Kaspersky administradas específicas.

- **Configuración de la exportación de eventos al sistema SIEM**

  Puede exportar los eventos mediante uno de los siguientes métodos:

  - Uso de los protocolos TCP, UDP o TLS sobre TCP.
  - Exportación de eventos directamente desde la base de datos de Kaspersky Security Center. La base de datos de Kaspersky Security Center contiene un conjunto de vistas públicas; puede encontrar una descripción de estas vistas públicas en el documento klakdb.chm.

Resultados

Tras configurar la exportación de eventos a un sistema SIEM, si marcó eventos como exportables, podrá ver los resultados de la exportación.

Requisitos previos

Al configurar la exportación automática de eventos en Kaspersky Security Center Linux, debe especificar algunas de las configuraciones del sistema SIEM. Se recomienda que verifique estas configuraciones de antemano a fin de prepararse para configurar Kaspersky Security Center Linux.

Para configurar correctamente el envío automático de eventos a un sistema SIEM, debe conocer los valores de los siguientes parámetros:

- **Dirección del servidor del sistema SIEM**

  La dirección IP del servidor en el que está instalado el sistema SIEM. Encontrará este valor en la configuración del sistema SIEM.

- **Puerto del servidor del sistema SIEM**

  El número de puerto usado para establecer una conexión entre Kaspersky Security Center Linux y su servidor del sistema SIEM. Especifica este valor en la configuración de Kaspersky Security Center Linux y en la configuración del destinatario de su sistema SIEM.

- **Protocolo**

  Protocolo usado para transferir mensajes de Kaspersky Security Center Linux a su sistema SIEM. Especifica este valor en la configuración de Kaspersky Security Center Linux y en la configuración del destinatario de su sistema SIEM.

Acerca de la exportación de eventos

Kaspersky Security Center Linux le permite recibir información sobre los eventos de funcionamiento del Servidor de administración y las aplicaciones de Kaspersky instaladas en dispositivos administrados. La información sobre estos eventos se guarda en la base de datos del Servidor de administración.

La exportación de eventos puede utilizarse en sistemas centralizados que permiten atender a los problemas de seguridad en un nivel organizativo y técnico. Estos sistemas, denominados sistemas SIEM, brindan servicios para hacer un monitoreo de la seguridad y son capaces de integrar la información de distintas soluciones. Pueden analizar, en tiempo real, los eventos y las alertas de seguridad que generan las aplicaciones, el hardware de red y los centros de operaciones de seguridad (SOC).

Los sistemas SIEM reciben información de muchas fuentes, como redes, soluciones de seguridad, servidores, aplicaciones y bases de datos. Pueden integrar los datos que obtienen para reducir las probabilidades de que un evento crítico pase desapercibido. También pueden realizar análisis automatizados de alertas y eventos correlacionados para notificar a los administradores de cualquier problema de seguridad inmediato. Las alertas de estos sistemas se pueden comunicar a través de un panel o tablero, o se pueden enviar por correo electrónico u otra vía provista por un tercero.

El proceso de exportación de eventos desde Kaspersky Security Center Linux a sistemas SIEM externos involucra a dos partes: un remitente de eventos (Kaspersky Security Center Linux) y un destinatario para los eventos (el sistema SIEM). Para exportar eventos con éxito, debe configurar esto en su sistema SIEM y en Kaspersky Security Center Linux. No importa cuál de los dos lados se configura primero. Puede configurar la transmisión de eventos en Kaspersky Security Center Linux y luego configurar la recepción de estos por el sistema SIEM, o viceversa.

Métodos para enviar eventos desde Kaspersky Security Center Linux

Hay tres métodos para enviar eventos desde Kaspersky Security Center Linux a sistemas externos:

- El envío de eventos a través del protocolo de Syslog a cualquier sistema SIEM

  Mediante el protocolo Syslog, puede transmitir cualquier evento que ocurra en el Servidor de administración y en las aplicaciones de Kaspersky instaladas en los dispositivos administrados. El protocolo de Syslog es un protocolo de registro de mensajes estándares. Puede utilizarlo para exportar eventos a cualquier sistema SIEM.

  Para ello, debe marcar los eventos que desea transmitir al sistema SIEM. Puede marcar los eventos en Kaspersky Security Center Web Console. Solo los eventos marcados se transmitirán al sistema SIEM. Si no marcó nada, no se transmitirá ningún evento.

- Envío de eventos a través de los protocolos CEF y LEEF a sistemas de Kaspersky SIEM, QRadar, Splunk y ArcSight

Puede utilizar los protocolos CEF y LEEF para exportar eventos generales. Al exportar eventos a través de los protocolos CEF y LEEF, no tiene la posibilidad de seleccionar eventos específicos para exportarlos. En su lugar, se exportan todos los eventos generales. Para convertir eventos de Kaspersky Security Center Linux a eventos en formato CEF y LEEF, debe utilizar el archivo siem_conversion_rules.xml. Este archivo contiene la lista de atributos de eventos de Kaspersky Security Center Linux y los atributos correspondientes de eventos en formato CEF y LEEF. Además, el archivo siem_conversion_rules.xml contiene las reglas para generar mensajes correspondientes a eventos. Este archivo está incluido en el kit de distribución de Kaspersky Security Center Linux.

A diferencia del protocolo Syslog, los protocolos CEF y LEEF no son universales. CEF y LEEF están diseñados para los sistemas SIEM apropiados (Kaspersky SIEM, QRadar, Splunk y ArcSight). Por lo tanto, cuando elige exportar eventos sobre uno de estos protocolos, usa el analizador requerido en el sistema SIEM.

- Directamente desde la base de datos de Kaspersky Security Center Linux a cualquier sistema SIEM

  Este método de exportar eventos puede utilizarse para recibir eventos directamente de vistas públicas de la base de datos mediante consultas de SQL. Los resultados de una pregunta se guardan en un archivo de XML que se puede utilizar como datos de entrada para un sistema externo. Solo los eventos disponibles en vistas públicas se pueden exportar directamente desde la base de datos.

Recepción de eventos por parte del sistema SIEM

El sistema SIEM debe recibir y correctamente analizar eventos recibidos de Kaspersky Security Center Linux. Para lograrlo, debe configurar correctamente el sistema SIEM. El proceso de configuración depende del sistema SIEM que se utilice. Sin embargo, existen algunos pasos de configuración generales (como la configuración del receptor y el analizador) que son comunes a todos.

Acerca de la configuración de la exportación de eventos en un sistema SIEM

El proceso de exportación de eventos desde Kaspersky Security Center Linux a sistemas SIEM externos involucra a dos partes: un remitente de eventos (Kaspersky Security Center Linux) y un destinatario para los eventos (el sistema SIEM). Debe configurar la exportación de eventos en su sistema SIEM y en Kaspersky Security Center Linux.

Los ajustes que especifique en el sistema SIEM dependerán del sistema particular que esté utilizando. En general, para todo sistema SIEM, deberá configurar un receptor y, opcionalmente, un analizador que procese los eventos recibidos.

Configuración del receptor

Para recibir eventos enviados por Kaspersky Security Center Linux, debe configurar el destinatario en su sistema SIEM. Por lo general, deberá especificar los valores de los siguientes parámetros dentro del sistema SIEM:

- **Protocolo de exportación**

  Un protocolo de transferencia de mensajes, ya sea UDP, TCP o TLS sobre TCP. Este protocolo debe ser igual que el protocolo que especificó en Kaspersky Security Center Linux.

- **Puerto**

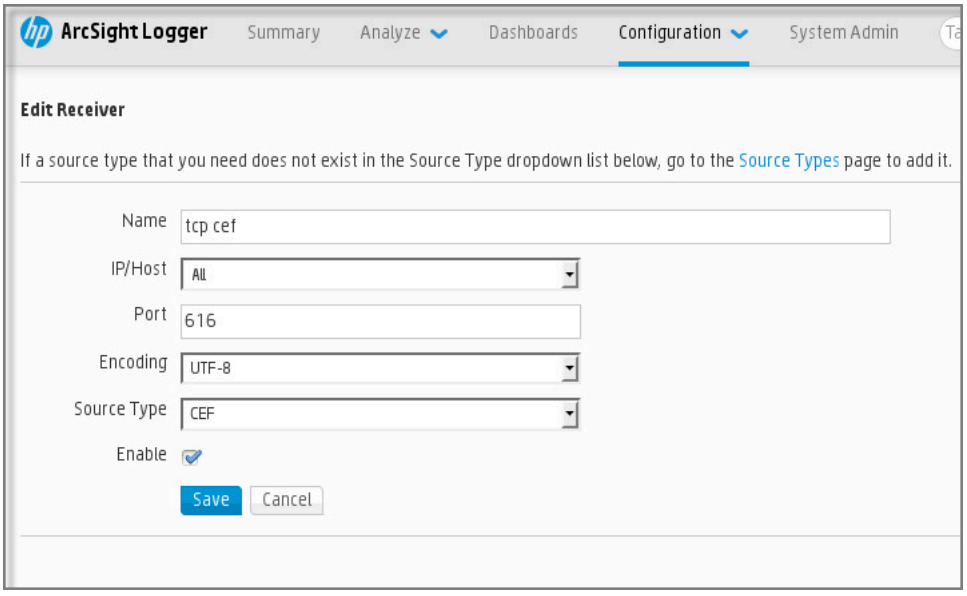
  Especifique el número de puerto utilizado para conectarse a Kaspersky Security Center Linux. Este puerto debe ser el mismo que el puerto que especifica en Kaspersky Security Center Linux durante la configuración con un sistema SIEM.

- **Formato de los datos**

  Especifique el formato Syslog, CEF o LEEF.

Según el sistema SIEM que utilice, debería especificar algunas configuraciones adicionales del destinatario.

La figura siguiente muestra la pantalla de configuración del destinatario en ArcSight.



Configuración del destinatario en ArcSight

Analizador sintáctico de mensajes

Los eventos exportados se transfieren al sistema SIEM en forma de mensajes. A continuación, se aplica un analizador sintáctico a estos mensajes para garantizar que el sistema SIEM pueda utilizar la información de los eventos. Un analizador sintáctico de mensajes forma parte del sistema SIEM; se utiliza para separar el contenido del mensaje en campos como el código del evento, la gravedad, la descripción y los parámetros. Esto permite al sistema SIEM procesar eventos recibidos de Kaspersky Security Center Linux, de modo que se puedan almacenar en la base de datos del sistema SIEM.

Acerca de la exportación de eventos en formato CEF o LEEF

Puede utilizar los formatos CEF y LEEF para exportar a sistemas SIEM los eventos generales, los eventos de cambio de directiva y los eventos que las aplicaciones de Kaspersky transfieren al Servidor de administración. El conjunto de eventos exportados se predefine, y no puede seleccionar los eventos que se exportarán. Antes de enviar eventos al sistema SIEM (Kaspersky SIEM, QRadar, ArcSight o Splunk), es necesario interpretar los eventos de Kaspersky Security Center Linux en eventos en formato CEF y LEEF utilizando las reglas especificadas en el archivo siem_conversion_rules.xml.

Según el sistema SIEM que utilice, deberá elegir uno u otro formato de exportación. La siguiente tabla muestra los formatos correspondientes a algunos sistemas SIEM.

Formatos de exportación de eventos por sistema SIEM

Sistema SIEM	Formato de exportación
Kaspersky SIEM	CEF
ArcSight	CEF
Splunk	CEF
QRadar	LEEF

- LEEF (Log Event Extended Format) es un formato de eventos especializado para el sistema SIEM IBM Security QRadar. QRadar puede recibir, identificar y procesar eventos transmitidos mediante el protocolo LEEF. Los eventos LEEF deben usar la codificación de caracteres UTF-8. Puede encontrar la información detallada del protocolo LEEF en el Centro de conocimientos de IBM.

- CEF (Formato de eventos comunes) es un estándar abierto para la gestión de registros que mejora la interoperabilidad de la información relacionada con la seguridad desde diferentes dispositivos y aplicaciones de red y seguridad. CEF le permite usar un formato de registros de eventos común de modo que los datos se puedan integrar y agregarse fácilmente para el análisis por un sistema de gestión de la empresa. Los eventos CEF deben usar la codificación de caracteres UTF-8.

La exportación automática significa que Kaspersky Security Center Linux envía eventos generales al sistema SIEM. La exportación automática de eventos se inicia inmediatamente después de que la habilita. Esta sección explica detalladamente cómo habilitar la exportación automática de eventos.

Conversión de eventos al formato CEF o LEEF

Antes de enviar eventos al sistema SIEM (Kaspersky SIEM, QRadar, ArcSight o Splunk), es necesario interpretar los eventos de Kaspersky Security Center Linux en eventos en formato CEF y LEEF utilizando las reglas especificadas en el archivo siem_conversion_rules.xml. Este archivo está incluido en el kit de distribución de Kaspersky Security Center Linux.

El archivo siem_conversion_rules.xml contiene las reglas de interpretación predefinidas para convertir eventos al formato CEF y LEEF. Si desea utilizar reglas de interpretación de eventos adicionales, puede agregarlas al archivo manualmente.

El archivo siem_conversion_rules.xml incluye las siguientes secciones:

- `<product name="SP_QRADAR" vendor="IBM">`

  Esta sección contiene reglas para generar eventos en formato LEEF, que se pueden exportar al sistema SIEM de QRadar.

- `<product name="SP_ARCSIGHT" vendor="HP">`.

  Esta sección contiene reglas para generar eventos en formato CEF, que se pueden exportar al sistema SIEM de ArcSight o Splunk.

- `<product name="Kaspersky SIEM" vendor="Kaspersky">`.

  Esta sección contiene reglas para generar eventos en formato CEF, que se pueden exportar a KUMA.

Cada sección tiene la subsección `<common>` donde se encuentran los atributos de eventos de Kaspersky Security Center Linux y los atributos correspondientes de los eventos en formato LEEF. Estos atributos comunes se utilizan para todos los tipos de eventos que se pueden exportar.

Además, cada sección tiene las subsecciones `<event>`. Cada subsección `<event>` contiene atributos adicionales que se agregan a los enumerados en la sección `<common>`.

Puede agregar una nueva regla de generación de eventos al archivo siem_conversion_rules.xml manualmente.

Para agregar una nueva regla de generación de eventos:

1. Agregue una nueva subsección `<event>` a la sección `<product name="SP_QRADAR" vendor="IBM">`, `<product name="SP_QRADAR" vendor="IBM">` o `<product name="Kaspersky SIEM" vendor="Kaspersky">` y, a continuación, especifique los atributos de evento adicionales, si es necesario.

2. Si un evento consta únicamente de atributos comunes, la subsección `<event>` estará vacía.

siem_conversion_rules.xml

```
<conversion_rules>
    <product name="SP_QRADAR" vendor="IBM">
        <common> <!-- Common Kaspersky Security Center Linux event attributes and corresponding LEEF event
attributes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="EVC_EV_DISP_HOST_NAME" type="AT_STRING" limit="255"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND"> <!-- Generation rule for the GNRL_EV_VIRUS_FOUND event with additional
attributes -->
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="EVC_EV_SHA256" type="AT_STRING" limit="255"/>
            </param>
            ...
        </event>
...
</product>
    <product name="SP_ARCSIGHT" vendor="HP">
        <common> <!-- Common Kaspersky Security Center Linux event attributes and corresponding LEEF event
attributes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="dhost" type="AT_STRING" limit="1023"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND">
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="cs4" type="AT_STRING" limit="255"/>
                <attr name="cs4Label" type="AT_STRING" val="SHA256"/>
            </param>
            ...
</product>
    <product name="Kaspersky SIEM" vendor="Kaspersky">
        <common> <!-- Common Kaspersky Security Center Linux event attributes and corresponding LEEF event
attributes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="dhost" type="AT_STRING" limit="1023"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND">
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="cs4" type="AT_STRING" limit="255"/>
                <attr name="cs4Label" type="AT_STRING" val="SHA256"/>
            </param>
            ...
</product>
</conversion_rules>
```

Marcar los eventos que se exportarán a un sistema SIEM en formato Syslog

Después de habilitar la exportación automática de eventos, debe seleccionar qué eventos se exportarán al sistema SIEM externo.

Para configurar la exportación de eventos en formato Syslog a un sistema externo, puede optar por una de estas vías:

- Marcar eventos generales. Si marca los eventos que desea exportar en la configuración de una directiva, en la configuración de los eventos o en la configuración del Servidor de administración, el sistema SIEM recibirá esos eventos cuando ocurran en cualquier aplicación sujeta a la directiva. Si los eventos exportados ya estaban seleccionados en la directiva, no podrá redefinirlos para una aplicación específica que esté administrada por esa directiva.

- Marcar eventos correspondientes a una aplicación administrada. Si marca eventos que correspondan a una aplicación administrada instalada en un dispositivo administrado, el sistema SIEM únicamente recibirá los eventos que ocurran en esa aplicación.

Para los eventos de cambio de directiva, solo puede habilitar o deshabilitar la exportación de todos esos eventos a un sistema SIEM.

Marcar eventos de una aplicación de Kaspersky para que se los exporte en formato Syslog

Si desea exportar los eventos ocurridos en una aplicación administrada específica instalada en los dispositivos administrados, marque los eventos para su exportación en la directiva de la aplicación. En este caso, los eventos marcados se exportan desde todos los dispositivos incluidos en el alcance de la directiva.

Para marcar los eventos que desea exportar en una aplicación administrada específica, haga lo siguiente:

1. En el menú principal, vaya a **Administración de activos** → **Directivas**.
2. Haga clic en la directiva de la aplicación para la que desea marcar los eventos.

   Se abre la ventana de configuración de la directiva.
3. Vaya a la sección **Configuración de eventos**.
4. marque las casillas ubicadas al lado de los eventos que quiera exportar a un sistema SIEM.
5. Haga clic en el botón **Marcar para exportar al sistema SIEM mediante Syslog**.

   También puede marcar un evento para exportarlo a un sistema SIEM en la sección **Registro de los eventos**, que se abre al hacer clic en el vínculo del evento.
6. Aparecerá una marca de verificación (✓) en la columna **Syslog** del evento (o los eventos) que haya elegido exportar al sistema SIEM.
7. Haga clic en el botón **Guardar**.

Los eventos marcados desde la aplicación administrada están listos para ser exportados a un sistema SIEM.

Puede marcar los eventos que desea exportar a un sistema SIEM para un dispositivo administrado específico. Si se marcaron eventos previamente exportados en una directiva de aplicación, no podrá redefinir los eventos marcados para un dispositivo administrado.

Para marcar los eventos que desea exportar a un dispositivo administrado, haga lo siguiente:

1. En el menú principal, vaya a **Administración de activos** → **Dispositivos administrados**.

   Se muestra la lista de dispositivos administrados.

2. En la lista de dispositivos administrados, haga clic en el vínculo con el nombre del dispositivo pertinente.

   Se muestra la ventana de propiedades del dispositivo seleccionado.

3. Vaya a la sección **Aplicaciones**.

4. En la lista de aplicaciones, haga clic en el vínculo con el nombre de la aplicación en cuestión.

5. Vaya a la sección **Configuración de eventos**.

6. marque las casillas ubicadas al lado de los eventos que quiera exportar a un sistema SIEM.

7. Haga clic en el botón **Marcar para exportar al sistema SIEM mediante Syslog**.

   También puede marcar un evento para exportarlo a un sistema SIEM en la sección **Registro de los eventos**, que se abre al hacer clic en el vínculo del evento.

8. Aparecerá una marca de verificación (✓) en la columna **Syslog** del evento (o los eventos) que haya elegido exportar al sistema SIEM.

En lo sucesivo, si la exportación a un sistema SIEM está configurada, el Servidor de administración enviará los eventos marcados a ese sistema SIEM.

Marcar eventos generales para que se los exporte en formato Syslog

Si lo desea, puede marcar eventos generales para que el Servidor de administración los exporte a sistemas SIEM en formato Syslog.

Para marcar eventos generales y exportarlos a un sistema SIEM:

1. En el menú principal, realice una de las siguientes acciones:

   - Haga clic en el nombre del Servidor de administración.
   - Vaya a **Administración de activos** → **Directivas** y, a continuación, haga clic en el vínculo de una directiva.

2. En la ventana que se abre, vaya a la pestaña **Configuración de eventos**.

3. Haga clic en **Marcar para exportar al sistema SIEM mediante Syslog**.

   También puede marcar un evento para exportarlo a un sistema SIEM en la sección **Registro de los eventos**, que se abre al hacer clic en el vínculo del evento.

4. Aparecerá una marca de verificación (✓) en la columna **Syslog** del evento (o los eventos) que haya elegido exportar al sistema SIEM.

En lo sucesivo, si la exportación a un sistema SIEM está configurada, el Servidor de administración enviará los eventos marcados a ese sistema SIEM.

Acerca de la exportación de eventos en formato Syslog

Los eventos del Servidor de administración y los eventos de las aplicaciones de Kaspersky que se encuentran instaladas en los dispositivos administrados se pueden exportar a un sistema SIEM en formato Syslog.

Syslog es un protocolo de registro de mensajes estándar. Permite que el software que genera los mensajes, el sistema que los almacena y el software que los reporta y analiza sean entidades separadas. Cada mensaje se etiqueta con un código numérico que indica el tipo de software que lo ha generado. A cada mensaje se le asigna, además, un nivel de gravedad.

La definición del formato Syslog se encuentra publicada en documentos RFC del Grupo de Trabajo de Ingeniería de Internet o IETF (estándares de Internet). El estándar RFC 5424 se utiliza para exportar los eventos desde Kaspersky Security Center Linux a sistemas externos.

En Kaspersky Security Center Linux, puede configurar la exportación de eventos a sistemas externos usando el formato Syslog.

El proceso de exportación consta de dos pasos:

1. Habilitar la exportación de eventos automática. En este paso, Kaspersky Security Center Linux se configura de modo que envíe eventos al sistema SIEM. Kaspersky Security Center Linux empieza a enviar eventos inmediatamente después de que habilita la exportación automática.

2. Seleccionar los eventos que se exportarán al sistema externo. Este paso consiste en indicar cuáles eventos deberán exportarse al sistema SIEM.

Configurar Kaspersky Security Center Linux para exportar eventos a un sistema SIEM

Si desea exportar eventos a un sistema SIEM, debe configurar el proceso de exportación en Kaspersky Security Center Linux.

Antes de enviar eventos al sistema SIEM (Kaspersky SIEM, QRadar, ArcSight o Splunk), es necesario interpretar los eventos de Kaspersky Security Center Linux en eventos en formato CEF y LEEF utilizando las reglas especificadas en el archivo siem_conversion_rules.xml.

Para configurar la exportación de eventos a un sistema SIEM en Kaspersky Security Center Web Console:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, seleccione la sección **Exportar a SIEM**.

3. Haga click en el enlace **Configurar conexión**.

   Se abre la sección **Exportar configuración**.

4. En la sección **Exportar configuración**, configure los siguientes ajustes:

- **Dirección del servidor del sistema SIEM**

  La dirección IP del servidor en el que está instalado el sistema SIEM. Encontrará este valor en la configuración del sistema SIEM.

- **Puerto del sistema SIEM**

  El número de puerto usado para establecer una conexión entre Kaspersky Security Center Linux y su servidor del sistema SIEM. Especifica este valor en la configuración de Kaspersky Security Center Linux y en la configuración del destinatario de su sistema SIEM.

- **Protocolo**

  Seleccione el protocolo que se utilizará para transferir mensajes al sistema SIEM. Puede seleccionar los protocolos TCP, UDP o TLS sobre TCP.

  Si selecciona el protocolo TLS sobre TCP, configure los siguientes ajustes:

  - **Autenticación del servidor**

    En el campo **Autenticación del servidor**, puede seleccionar los valores **Certificados de confianza** o **Huellas digitales SHA**:

    - **Certificados de confianza**. Puede obtener una cadena de certificados completa (incluido el certificado raíz) de una entidad de certificación (CA) de confianza y cargar ese archivo a Kaspersky Security Center Linux. Kaspersky Security Center Linux verifica si la cadena de certificados del servidor del sistema SIEM también está firmado por una CA de confianza o no.

      Para agregar un certificado de confianza, haga clic en el botón **Buscar archivo de certificados de CA** y, a continuación, cargue el certificado en cuestión.

    - **Huellas digitales SHA**. Puede especificar las huellas digitales SHA1 de la cadena de certificados completa del sistema SIEM (incluido el certificado raíz) en Kaspersky Security Center Linux. Para agregar una huella digital SHA1, cópiela en el campo **Huellas digitales** y haga clic en el botón **Agregar**.

    La opción **Agregar autenticación del cliente** permite generar un certificado para autenticar a Kaspersky Security Center Linux. Si utiliza esta opción, utilizará un certificado autofirmado emitido por Kaspersky Security Center Linux. En ese caso, podrá usar tanto un certificado de confianza como una huella digital SHA para autenticar al servidor del sistema SIEM.

  - **Agregar nombre del sujeto / nombre alternativo del sujeto**

    Se denomina "nombre del sujeto" al nombre de dominio para el que se ha obtenido un certificado. Para que Kaspersky Security Center Linux pueda conectarse al servidor del sistema SIEM, el nombre de dominio del servidor del sistema SIEM debe aparecer como nombre del sujeto en el certificado del servidor del sistema SIEM. El servidor del sistema SIEM puede cambiar de nombre de dominio si se modifica también el nombre del sujeto en el certificado. Si se presenta esta situación, utilice el campo **Agregar nombre del sujeto / nombre alternativo del sujeto** para especificar los nombres de sujeto pertinentes. Si alguno de los nombres de sujeto indicados en el campo coincide con el nombre de sujeto especificado en el certificado del sistema SIEM, Kaspersky Security Center Linux considerará que el certificado es válido.

  - **Agregar autenticación del cliente**

Para la autenticación del cliente, puede utilizar su propio certificado o puede generar uno en Kaspersky Security Center Linux.

- **Ingresar certificado**. Puede utilizar un certificado obtenido de cualquier fuente (por ejemplo, de una entidad de certificación de confianza). Deberá especificar el certificado y su clave privada. Puede usar, para ello, alguno de los siguientes tipos de certificado:

  - **PEM certificado X.509**. Use el campo **Archivo con certificado** para cargar el archivo que contenga el certificado y el campo **Archivo con clave** para cargar un archivo que contenga la clave privada. Los dos archivos son independientes entre sí. El orden en que se carguen los archivos no importa. Tras cargar los archivos, ingrese la contraseña para decodificar la clave privada en el campo **Verificación de certificado o contraseña**. Si la clave privada no está codificada, puede dejar la contraseña en blanco.

  - **PKCS12 certificado X.509**. Use el campo **Archivo con certificado** para cargar un único archivo que contenga tanto el certificado como su clave privada. Tras cargar el archivo, ingrese la contraseña para decodificar la clave privada en el campo **Verificación de certificado o contraseña**. Si la clave privada no está codificada, puede dejar la contraseña en blanco.

- **Generar clave**. Puede generar un certificado autofirmado dentro de Kaspersky Security Center Linux. El certificado autofirmado que se genere quedará almacenado en Kaspersky Security Center Linux, y usted podrá transferir la parte pública del certificado o su huella digital SHA-1 al sistema SIEM.

- **Formato de los datos**

  Puede seleccionar los formatos Kaspersky SIEM, IBM QRadar SIEM, ArcSight, Splunk o registro del sistema, según los requisitos del sistema SIEM.

  Si selecciona el formato de datos de registro del sistema, debe especificar **Tamaño máximo de mensaje, bytes**.

  Especifique el tamaño máximo (en bytes) de un mensaje transmitido al sistema SIEM. Cada evento se transmite en un mensaje. Si la duración real de un mensaje supera el valor especificado, el mensaje es truncado y los datos se pueden perder. El tamaño predeterminado es de 2048 bytes. Este campo solo está disponible si seleccionó el formato de System log en el campo **Protocolo**.

5. Si lo desea, puede exportar eventos que se encuentren archivados en la base de datos del Servidor de administración y definir la fecha a partir de la cual se iniciará la exportación de los eventos archivados:

   a. Haga clic en el enlace **Establezca la fecha de inicio de la exportación**.

   b. En la sección que se abre, especifique la fecha de inicio en el campo **Fecha para iniciar la exportación**.

   c. Haga clic en **Aceptar**.

6. Habilite la opción **Exportar eventos a SIEM**.

7. Para enviar eventos de cambio de directiva a SIEM, habilite la opción **Exportar eventos ampliados relacionados con cambios en las directivas al SIEM**. Se enviará un evento independiente a SIEM por cada configuración de directiva modificada.

8. Para comprobar que la conexión del sistema SIEM se haya configurado correctamente, haga clic en el botón **Comprobar conexión**.

   Se establece la conexión con el servidor del sistema SIEM y se envía un evento de prueba. Se mostrará el estado de la conexión.

9. Haga clic en el botón **Guardar**.

La exportación de eventos al sistema SIEM queda configurada. A partir de ahora, si configuró la recepción de eventos en un sistema SIEM, el Servidor de administración exportará los eventos marcados o los eventos de cambio de directiva a un sistema SIEM. Si definió una fecha de inicio para la exportación, el Servidor de administración también exportará los eventos marcados que se encuentren almacenados desde esa fecha en la base de datos del Servidor de administración.

Supervisión de cambios en directivas y perfiles de directiva

Cuando se cambia una configuración de directiva, se genera un evento de cambio de directiva que luego puede exportar a un sistema SIEM para supervisar los cambios en las directivas y generar alertas. Solo se puede acceder a los eventos de cambio de directiva a través de un sistema SIEM.

Los eventos de cambio de directiva no se almacenan en la base de datos del Servidor de administración después de generarse y no se pueden ver en la sección **Supervisión → Selecciones de eventos** de Kaspersky Security Center Web Console. Tampoco puede especificar la configuración de notificaciones ni la configuración de almacenamiento para estos eventos en la pestaña **Configuración de eventos**.

Cuando crea una directiva, se genera un evento de cambio de directiva para cada configuración de directiva. Cuando cambia una directiva, se genera un evento de cambio de directiva para cada configuración modificada de la directiva. La eliminación de una directiva genera un evento. Por ejemplo, la creación de una directiva de Kaspersky Security Center genera alrededor de 1000 eventos, y la creación de una directiva de Kaspersky Endpoint Security genera más de 7000 eventos.

Condiciones para generar eventos de cambio de directiva

Se genera un evento de cambio de directiva cada vez que un usuario realiza alguna de las siguientes acciones con una directiva o un perfil de directiva:

- Crear, editar o eliminar una directiva
- Crear, editar o eliminar un perfil de directiva
- Revertir la directiva a una revisión seleccionada
- Importar o copiar una directiva
- Importar o copiar un perfil de directiva
- Mover una directiva a otro grupo de administración

Se genera un evento de modificación de directiva cuando se cumplen las siguientes condiciones:

- Se modifican las directivas de las siguientes aplicaciones:
  - Agente de red de Kaspersky Security Center
  - Servidor de administración de Kaspersky Security Center
  - Kaspersky Endpoint Security para Windows 14.1 o posterior
  - Kaspersky Endpoint Security for Linux 12.5 o versiones posteriores
  - Kaspersky Endpoint Security for Linux 12.4 o versiones posteriores
  - Kaspersky Endpoint Security for Mac 12.2.1 o versiones posteriores
- La opción **Exportar eventos ampliados relacionados con cambios en las directivas al SIEM** en las propiedades del Servidor de administración está habilitada.
- La directiva se modifica manualmente a través de la interfaz de Kaspersky Security Center Web Console.

Los eventos de cambio de directiva no se crean en los siguientes casos:

- Se modifica la configuración general de la directiva.
- Se modifica la configuración de la directiva heredada de una directiva principal.
- La configuración de la directiva se modifica a través de Kaspersky Security Center OpenAPI.
- Se modifica la configuración de la aplicación de Kaspersky directamente en la aplicación.

Campos de eventos de cambio de directiva

La siguiente tabla muestra un conjunto de campos de eventos de cambio de directiva. La representación de estos campos depende del formato del evento de salida (por ejemplo, syslog, CEF o LEEF). Para conocer los nombres exactos de los campos y las plantillas de eventos, consulte el archivo siem_conversion_rules.xml. Los parámetros de eventos están disponibles solo en inglés.

Campo del evento	Tipo de datos	Descripción
`eventType`	cadena	Tipo de evento. Permite crear reglas de correlación para el tipo de evento específico. Valores posibles: "Directiva creada", "Directiva modificada", "Directiva eliminada".
`srvName`	cadena	Nombre del Servidor de administración.
`eventTime`	fecha y hora	Fecha y hora del evento (en UTC).
`eventGroupID`	int	ID del grupo de eventos de una modificación.
`objectID`	int	ID interno de un objeto.
`objectName`	cadena	Nombre para mostrar de la directiva.
`objectGroup`	cadena	Ruta completa y nombre del grupo de administración que contiene la directiva.
`user`	cadena	Nombre del usuario que realizó la modificación.

`operation`	cadena	Tipo de modificación del parámetro. Valores posibles: "Added", "Removed", "Changed".
`path`	cadena	Ruta del parámetro. Contiene la ruta al nodo primario del parámetro final. La ruta se crea según los nombres de las secciones y subsecciones de la directiva. La estructura de la ruta es idéntica a la que se describe en Configuración de la directiva del Agente de red, Configuración general de la directiva y Comparación de revisiones de directivas.
`parameter`	cadena	Nombre de la configuración de directiva modificada.
`oldValue`	cadena	Valor anterior del parámetro final.
`newValue`	cadena	Nuevo valor del parámetro final.

Exportación de eventos directamente desde la base de datos

Puede recuperar eventos directamente desde la base de datos de Kaspersky Security Center Linux sin necesidad de usar la interfaz de Kaspersky Security Center. Puede consultar directamente las vistas públicas y recuperar los datos del evento o crear su propia vista a partir de vistas públicas existentes y dirigirse a ellas para obtener los datos que necesita.

Vistas públicas

Para su conveniencia, un conjunto de vistas públicas se proporciona en la base de datos de Kaspersky Security Center Linux. Puede encontrar la descripción de estas vistas públicas en el documento klakdb.chm.

La vista pública v_akpub_ev_event contiene un conjunto de campos que representan los parámetros del evento en la base de datos. En el documento klakdb.chm, también puede encontrar información sobre las vistas públicas correspondiente a otras entidades de Kaspersky Security Center Linux; por ejemplo, dispositivos, aplicaciones o usuarios. Puede usar esta información en sus consultas.

Esta sección contiene instrucciones para ejecutar una consulta SQL mediante la utilidad klsql2 y un ejemplo de consulta.

Para crear consultas SQL o vistas de bases de datos, también puede utilizar cualquier otro programa para trabajar con bases de datos. En la sección correspondiente, se proporciona información sobre cómo ver los parámetros para conectar a la base de datos de Kaspersky Security Center Linux, como el nombre de la instancia y nombre de la base de datos.

Crear una consulta de SQL usando la utilidad klsql2

En este artículo, se describe cómo usar la utilidad klsql2 y cómo ejecutar una consulta SQL mediante esta utilidad. Utilice la versión de la utilidad klsql2 que se incluye en la versión de Kaspersky Security Center Linux instalada.

Para usar la utilidad klsql2:

1. Vaya al directorio donde está instalado el Servidor de Administración. La ruta de instalación predeterminada es /opt/kaspersky/ksc64/sbin.

2. En este directorio, cree un archivo en blanco con la extensión .sql.

3. Abra el archivo .sql creado en cualquier editor de texto.

4. En el archivo .sql, escriba la consulta SQL que desea y, luego, guarde el archivo.

5. En el dispositivo donde está instalado el Servidor de administración, en la línea de comandos, escriba el comando siguiente para ejecutar la consulta de SQL desde el archivo .sql y guardar los resultados en el archivo result.xml:

   ```
   sudo ./klsql2 -i src.sql -u <nombre de usuario> -p <contraseña> -o result.xml
   ```

   dónde `<nombre de usuario>` y `<contraseña>` son credenciales de la cuenta de usuario que tiene acceso a la base de datos.

6. Si es necesario, ingrese el nombre de usuario y la contraseña de la cuenta de usuario que tiene acceso a la base de datos.

7. Abra los archivos result.xml creados recientemente para ver los resultados de la consulta SQL.

Puede modificar el archivo .sql y crear cualquier consulta SQL para las vistas públicas. A continuación, desde la línea de comandos, ejecute su consulta y guarde los resultados en un archivo.

Ejemplo de una consulta de SQL usando la utilidad klsql2

Esta sección muestra un ejemplo de una consulta SQL, ejecutada por medio de la utilidad klsql2.

Los ejemplos siguientes ilustran la recuperación de eventos que ocurrieron en dispositivos durante los siete días anteriores, y muestran los eventos según la hora en la que se producen. Los eventos más recientes se muestran primero.

Ejemplo para PostgreSQL:

```
SELECT
  /* identificador del evento */
  "e"."nId",

  /* hora en que ocurrió el evento */
  "e"."tmRiseTime",

  /* nombre interno del tipo de evento */
  "e"."strEventType",

  /* nombre mostrado del evento */
  "e"."wstrEventTypeDisplayName",

  /* descripción mostrada del evento */
  "e"."wstrDescription",

  /* descripción mostrada del evento */
  "e"."wstrGroupName",

  /* nombre mostrado del dispositivo en el que ocurrió el evento */
  "h"."wstrDisplayName",
  (
    CAST((("h"."nIp" / 16777216 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 65536 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 256 )& 255 ) AS VARCHAR(4))  || '.'  ||

    /* Dirección IP del dispositivo en el que ocurrió el evento */
    CAST((("h"."nIp" )& 255 ) AS VARCHAR(4))
  )  AS "strIp"
FROM "v_akpub_ev_event"  AS "e"
  INNER JOIN  "v_akpub_host"  AS "h" ON "h"."nId" = "e"."nHostId"
WHERE "e"."tmRiseTime" >= NOW() AT TIME ZONE 'utc'  + make_interval(days => CAST(-7  AS INT))
ORDER BY "e"."tmRiseTime" DESC ;
```

Ejemplo para MySQL o MariaDB

```
SELECT

  /* identificador del evento */
  `e`.`nId`,

  /* hora en que ocurrió el evento */
  `e`.`tmRiseTime`,

  /* nombre interno del tipo de evento */
  `e`.`strEventType`,

  /* nombre mostrado del evento */
  `e`.`wstrEventTypeDisplayName`,

  /* descripción mostrada del evento */
  `e`.`wstrDescription`,

  /* nombre del grupo del dispositivo */
  `e`.`wstrGroupName`,

  /* nombre mostrado del dispositivo en el que ocurrió el evento */
  `h`.`wstrDisplayName`,
  CONCAT(
    LEFT(CAST(((`h`.`nIp`  DIV  1677721) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  65536) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  256) & 255) AS CHAR), 4), '.',

    /* Dirección IP del dispositivo en el que ocurrió el evento */
    LEFT(CAST(((`h`.`nIp`) & 255) AS CHAR), 4)
  )  AS `strIp`
FROM `v_akpub_ev_event`  AS `e`
  INNER JOIN  `v_akpub_host`  AS `h` ON `h`.`nId` = `e`.`nHostId`
WHERE `e`.`tmRiseTime` >= ADDDATE( UTC_TIMESTAMP( ) , INTERVAL -7  DAY)
ORDER BY `e`.`tmRiseTime` DESC ;
```

Visualización del nombre de la base de datos de Kaspersky Security Center Linux

Si desea acceder a la base de datos de Kaspersky Security Center Linux por medio de las herramientas de administración de bases de datos MySQL o MariaDB, debe conocer el nombre de la base de datos a fin de conectarse desde su editor de scripts de SQL.

Para ver el nombre de la base de datos de Kaspersky Security Center Linux:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, seleccione la sección **Detalles de la base de datos actual**.

   El nombre de la base de datos se especifica en el campo **Nombre de la base de datos**. Use el nombre de la base de datos para dirigirse a la base de datos en sus consultas de SQL.

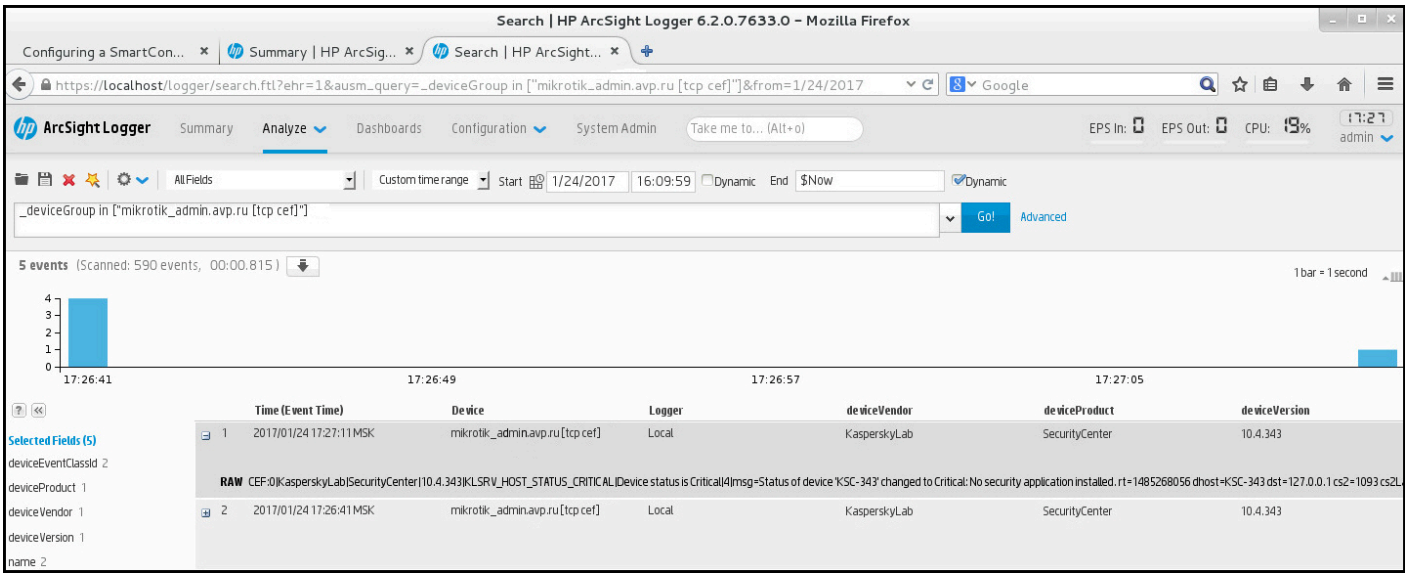
Ver los resultados de la exportación

Puede controlar si el procedimiento de exportación de eventos se ha completado debidamente. Para ello, verifique si el sistema SIEM recibe mensajes con los eventos exportados.

Si los eventos enviados desde Kaspersky Security Center Linux se reciben y analizan correctamente en su sistema SIEM, la configuración a ambos lados se realizó correctamente. De lo contrario, verifique la configuración que especificó en Kaspersky Security Center Linux en comparación con la configuración en su sistema SIEM.

La imagen de más abajo muestra los eventos exportados a ArcSight. El primero de ellos, *Device status is Critical*, es un evento crítico del Servidor de administración que se refiere al estado de un dispositivo.

La representación de los eventos exportados a un sistema SIEM varía según el sistema SIEM utilizado.



Ejemplo de eventos

Administración de revisiones de objetos

En esta sección encontrará información sobre la administración de revisiones de objetos.

La *revisión* es el estado de un objeto en un momento determinado. Cada vez que crea o modifica un objeto, se crea una nueva revisión de ese objeto. Cada revisión contiene toda la configuración del objeto tal como se encuentra en el momento en que se crea o se guarda la revisión.

Puede administrar revisiones de los siguientes objetos:

- Propiedades del Servidor de administración
- Directivas
- Tareas
- Grupos de administración
- Cuentas de usuario
- Paquetes de instalación

Puede realizar las siguientes acciones con las revisiones de los objetos:

- Ver una revisión seleccionada (disponible solo para directivas)
- Revertir los cambios realizados en un objeto a una revisión seleccionada
- Guardar revisiones como archivo JSON (disponible solo para directivas)

Todo objeto compatible con la administración de revisiones tiene una sección llamada **Historial de revisiones** en su ventana de propiedades. La sección contiene una lista de revisiones asociadas al objeto y los siguientes datos:

- **Revisión** número de revisión del objeto.
- **Hora** fecha y hora de modificación del objeto.
- **Usuario** nombre del usuario que modificó el objeto.
- **Dirección IP del dispositivo del usuario** dirección IP del dispositivo desde el que se modificó el objeto.
- **Dirección IP de Web Console** dirección IP de Kaspersky Security Center Web Console con la que se modificó el objeto.
- **Acción** acción realizada en el objeto.
- **Descripción** descripción de la revisión vinculada al cambio en la configuración del objeto.

  De forma predeterminada, la descripción de las revisiones está en blanco. Para agregar una descripción a una revisión, seleccione la revisión pertinente y haga clic en el botón **Editar descripción**. En la ventana abierta, ingrese un texto que describa la revisión.

Ver y guardar una revisión de una directiva

Una revisión de una directiva es un estado guardado de la directiva que se crea automáticamente cada vez que esta se modifica o se guarda. Una revisión contiene la configuración de la directiva, los perfiles y las reglas para activarlos, así como metadatos sobre la fecha de creación, el usuario que la creó y la dirección IP desde la que se creó. Kaspersky Security Center Linux le permite ver las revisiones de las directivas para realizar un seguimiento de los cambios en la configuración; también puede guardar una revisión en un archivo JSON.

Para que pueda ver y guardar la revisión de una directiva, el complemento web de administración correspondiente debe ofrecerle esta prestación.
Las opciones están disponibles para las directivas del Servidor de administración, del Agente de red, de Kaspersky Endpoint Security para Windows (a partir de la versión 14.0 del complemento web), de Kaspersky Endpoint Security for Linux (a partir de la versión 12.4 del complemento web) y de Kaspersky Endpoint Security for Mac (a partir de la versión 12.2.1 con el parche A del complemento web).

Para ver una revisión de una directiva:

1. En el menú principal, vaya a **Administración de activos** → **Directivas**.
2. Haga clic en la directiva a la que corresponda la revisión que desee ver y vaya a la sección **Historial de revisiones**.
3. En la lista de revisiones de la directiva, haga clic en el número de revisión que desee ver.

El informe que se muestra proporciona información sobre la configuración de la directiva, sus perfiles y las reglas para activarlos.

Si el tamaño de una revisión es superior a 10 MB, no podrá verla mediante Kaspersky Security Center Web Console. Se le pedirá que guarde la revisión seleccionada en un archivo JSON.

Si el tamaño de la revisión no supera los 10 MB, se mostrará un informe en formato HTML con la configuración de la revisión de directiva seleccionada. Dado que el informe se muestra en una ventana emergente, asegúrese de que las ventanas emergentes estén permitidas en su navegador.

Para las directivas de Kaspersky Endpoint Security para Windows y Kaspersky Endpoint Security for Mac, el informe no contendrá información acerca de los perfiles de directivas.

Para guardar la revisión de una directiva en un archivo JSON:

En la lista de revisiones de la directiva, seleccione la revisión que desee guardar y luego haga clic en **Guardar en archivo**.

La revisión se guardará en un archivo JSON.

Si es necesario, puede comparar las revisiones de la directiva.

Comparar las revisiones de una directiva

Puede comparar las revisiones anteriores de una directiva con su revisión actual, comparar las diferentes revisiones seleccionadas en la lista o comparar la revisión de una directiva con la revisión de otra directiva. Las opciones están disponibles para las directivas del Servidor de administración, el Agente de red, Kaspersky Endpoint Security para Windows (a partir de la versión 14.0 del complemento web) y Kaspersky Endpoint Security for Mac (a partir de la versión 12.2.1 Parche A del complemento web).

La comparación de revisiones de directivas está disponible si los complementos web de administración correspondientes admiten esta funcionalidad.

Para comparar las revisiones de una directiva:

1. En el menú principal, vaya a **Administración de activos** → **Directivas**.
2. Haga clic en la directiva cuyas revisiones desea comparar.

   Se abre la ventana de configuración de la directiva.
3. Vaya a la pestaña **Historial de revisiones** y luego seleccione las casillas junto a las revisiones que se van a comparar.

4. En la barra de herramientas, haga clic en el botón **Comparar** y, a continuación, seleccione una de las siguientes opciones:

   - **Con la revisión actual**, si desea comparar la revisión que seleccionó en el paso 3 con la última revisión guardada de la misma directiva.
   - **Revisiones seleccionadas**, si desea comparar las dos revisiones cuyas casillas seleccionó en el paso 3.

     El orden de selección de las casillas no afecta los resultados de la comparación. De manera predeterminada, la revisión más antigua de la seleccionada se compara con la revisión más reciente. Por ejemplo, si selecciona las casillas de verificación junto a las revisiones 5 y 1, la revisión 1 se compara con la revisión 5. El informe contendrá información sobre la configuración de la revisión 1 que se agregó, eliminó o modificó en comparación con la revisión 5.

   - **Con la revisión de otra directiva**, si desea comparar las revisiones de dos directivas diferentes.

     En el panel derecho que se abre, haga lo siguiente:

     a. En el campo **Nombre de la aplicación**, seleccione la directiva que desea comparar: la del Agente de red o la del Servidor de administración.

     b. En el campo **Nombre de la directiva**, especifique el nombre de la directiva cuya revisión desea comparar con la que seleccionó en el paso 3.

     Se muestra la lista de revisiones de la directiva.

     c. Seleccione revisión requerida y haga clic en el botón **Comparar**.

Se muestra un informe sobre la comparación de revisiones en formato HTML en una nueva pestaña de su navegador.

Si el resultado de la comparación supera los 10 MB, se muestra el cuadro de diálogo correspondiente. Puede hacer clic en el botón **Guardar en archivo** para guardar el informe como un archivo o cancelar la operación.

El informe se muestra en el idioma de la interfaz de Kaspersky Security Center Web Console. Puede expandir algunas secciones del informe haciendo clic en el ícono de flecha hacia abajo (▼) junto a la sección o contraer la sección haciendo clic en el ícono de flecha hacia arriba (▲).

El informe contiene la siguiente información:

- El logotipo de Kaspersky.
- El nombre del informe.
- La fecha y la hora de creación del informe.
- El nombre de la directiva, el Servidor de administración y el grupo de administración que incluye las directivas cuyas revisiones se compararon.
- El botón **Guardar como HTML**. Si hace clic en el botón, el informe se guardará en su computadora.

- La sección **Resumen** que muestra información general sobre las revisiones comparadas: nombre de las directivas, número de revisión, fecha y hora en que se guardó la revisión, el usuario que guardó la revisión y la descripción de la revisión.

  Para las directivas heredadas, no se muestra el usuario.

- Diferencias entre las revisiones comparadas. Las diferencias se muestran en las siguientes secciones:

  - **Parámetros agregados**
  - **Parámetros eliminados**
  - **Configuración modificada**
  - **Parámetros solo disponibles para el objeto 1** (si comparó las revisiones de dos directivas diferentes)
  - **Parámetros solo disponibles para el objeto 2** (si comparó las revisiones de dos directivas diferentes)

  Si una sección no tiene datos, no se muestra.

Devolver un objeto a una revisión anterior

Los cambios realizados en un objeto pueden revertirse. Por ejemplo, puede volver a dejar la configuración de una directiva tal como estaba en una fecha puntual.

Para revertir los cambios realizados en un objeto:

1. En la ventana de propiedades del objeto, abra la pestaña **Historial de revisiones**.
2. En la lista de revisiones de objeto, seleccione la revisión a la que quiere revertir los cambios.
3. Haga clic en el botón **Revertir**.
4. Haga clic en **Aceptar** para confirmar la operación.

   El objeto volverá a la revisión seleccionada. La lista de revisiones del objeto mostrará un registro de la acción que se tomó. En la descripción de la revisión, verá especificado el número de revisión a la que haya regresado el objeto.

La operación de revertir los cambios solo está disponible para objetos de directiva y tareas.

Amenazas activas

La información sobre los archivos no procesados que se detectaron en los dispositivos cliente se almacena en la sección **Repositorios**, subsección **Amenazas activas**.

El procesamiento y la desinfección pospuestos los lleva a cabo la aplicación de seguridad a petición o después de tener lugar un evento especificado. Puede configurar el procesamiento aplazado.

Desinfección de un archivo no procesado

Para iniciar la desinfección de un archivo no procesado:

1. En el menú principal, vaya a **Repositorios** → **Amenazas activas**.
2. Realice una de las siguientes acciones:
   - Marque la casilla ubicada junto a la regla que desee desinfectar.
   - Haga clic en el nombre del informe que desea desinfectar.
3. Haga clic en el botón **Desinfectar** para iniciar la desinfección del archivo.

   A continuación, se ejecuta el intento de desinfectar el archivo seleccionado.

Si el archivo se desinfecta, la aplicación de seguridad instalada en el dispositivo cliente lo restaura a su carpeta original. El registro del archivo se eliminará de la lista en la sección **Amenazas activas**. Si el archivo no se puede desinfectar, la aplicación de seguridad instalada en el dispositivo lo elimina desde ese dispositivo. El registro del archivo se eliminará de la lista en la sección **Amenazas activas**.

La capacidad de desinfección y eliminación de archivos puede variar según la aplicación de seguridad instalada, su versión y configuración.

Descarga de un archivo no procesado

Kaspersky Security Center Linux permite descargar copias de archivos no procesados detectados en dispositivos cliente. Esto se refiere a los archivos tratados o eliminados por la aplicación. Los archivos se descargan en el dispositivo donde está instalado Kaspersky Security Center Linux, en la carpeta que usted especifique.

Puede descargar copias de los archivos si los archivos se eliminaron o modificaron durante la desinfección y sus copias están almacenadas en el almacenamiento de Kaspersky Endpoint Security for Linux en el dispositivo administrado.

Para descargar una copia de un archivo no procesado:

1. En el menú principal, vaya a **Repositorios** → **Amenazas activas**.
2. Realice una de las siguientes acciones:
   - Seleccione la casilla al lado del archivo que desea descargar.
   - Haga clic en el nombre del archivo que desea descargar.
3. Para iniciar la descarga, haga clic en el botón **Descargar**.

La aplicación de seguridad instalada en el dispositivo cliente en que se detectó un archivo no procesado descarga una copia del archivo en la carpeta especificada.

Eliminar archivos desde la sección Amenazas activas

*Para eliminar un archivo de la sección **Amenazas activas**:*

1. En el menú principal, vaya a **Repositorios** → **Amenazas activas**.
2. Realice una de las siguientes acciones:
   - Marque la casilla ubicada junto al archivo que desee eliminar.
   - Haga clic en el nombre del archivo que desea eliminar.
3. Para eliminar los archivos, haga clic en el botón **Eliminar**.
4. En la ventana que se abre, haga clic en **Eliminar**.

   Las aplicaciones de seguridad que colocaron los archivos en repositorios de dispositivos cliente eliminarán los archivos desde estos repositorios. Los registros de los archivos se eliminarán de la lista en la sección **Amenazas activas**.

Eliminación de objetos

Esta sección proporciona información sobre cómo eliminar objetos.

Puede eliminar objetos como los siguientes:

- Directivas
- Tareas
- Paquetes de instalación
- Servidores de administración virtuales
- Usuarios
- Grupos de seguridad
- Grupos de administración

Para eliminar un objeto:

1. Abra la sección correspondiente de Kaspersky Security Center Web Console y luego seleccione el objeto.
2. En la barra de herramientas, haga clic en el botón **Eliminar**.
3. En la ventana que se abre, haga clic en **Aceptar** para confirmar su selección.

Se elimina el objeto seleccionado.

Cuando se elimina un objeto, se conserva información sobre el mismo en la base de datos. El plazo de almacenamiento para la información sobre los objetos eliminados es el mismo que el plazo de almacenamiento para las revisiones de objetos (el plazo recomendado es de 90 días). Puede cambiar el plazo de almacenamiento solo si tiene el permiso **Modificar** en el área de derechos **Objetos eliminados**.

Acercad de la eliminación de dispositivos cliente

Cuando elimina un dispositivo administrado de un grupo de administración, la aplicación mueve el dispositivo al grupo de Dispositivos no asignados. Después de eliminar el dispositivo, las aplicaciones de Kaspersky instaladas (Agente de red y cualquier aplicación de seguridad, por ejemplo, Kaspersky Endpoint Security) permanecen en el dispositivo.

Kaspersky Security Center Linux maneja los dispositivos del grupo Dispositivos no asignados según las siguientes reglas:

- Si configuró reglas de movimiento de dispositivos y un dispositivo cumple con los criterios de una regla de movimiento, el dispositivo se mueve automáticamente a un grupo de administración de acuerdo con la regla.
- El dispositivo se almacena en el grupo Dispositivos no asignados y se elimina automáticamente del grupo de acuerdo con las reglas de retención de dispositivos.

  Las reglas de retención de dispositivos no afectan a los dispositivos que tienen una o más unidades cifradas con cifrado de disco completo. Dichos dispositivos no se eliminan automáticamente, solo puede hacerlo de forma manual. Si necesita eliminar un dispositivo con una unidad cifrada, primero descifre la unidad y, luego, elimine el dispositivo.

  > Cuando elimina un dispositivo que tiene una unidad cifrada, también se eliminan los datos necesarios para descifrar la unidad. Si selecciona la casilla **Comprendo el riesgo y deseo eliminar los dispositivos seleccionados** en la ventana de confirmación que se abre cuando elimina dichos dispositivos (ya sea del grupo **Dispositivos no asignados** o **Dispositivos administrados**), significa que está al tanto de la subsecuente eliminación de datos.

  Para descifrar la unidad, se deben cumplir las siguientes condiciones:

  - El dispositivo se vuelve a conectar al Servidor de administración para restaurar los datos necesarios para descifrar la unidad.
  - El usuario del dispositivo recuerda la contraseña de descifrado.
  - La aplicación de seguridad que se usó para cifrar la unidad, por ejemplo, Kaspersky Endpoint Security para Windows, todavía está instalada en el dispositivo.

Si la tecnología Kaspersky Disk Encryption descifró la unidad, también puede intentar recuperar los datos con la utilidad de restauración FDERT.

En VDI, si tiene un dispositivo con unidades cifradas, la información de la unidad cifrada se elimina después de eliminar el dispositivo.

Cuando elimina manualmente un dispositivo del grupo de Dispositivos no asignados, la aplicación elimina el dispositivo de la lista. Después de eliminar el dispositivo, las aplicaciones de Kaspersky instaladas (si las hay) permanecen en el dispositivo. Después, si el dispositivo sigue estando visible para el Servidor de administración y se configuró un sondeo de red regular, Kaspersky Security Center Linux detecta el dispositivo durante el sondeo de red y lo agrega nuevamente al grupo Dispositivos no asignados. Por lo tanto, es razonable eliminar un dispositivo manualmente solo si el servidor de administración no puede ver el dispositivo.

Descarga y eliminación de archivos de Cuarentena y Copias de seguridad del archivo

Esta sección brinda información sobre cómo descargar y eliminar archivos de Cuarentena y Copias de seguridad del archivo en Kaspersky Security Center Web Console.

Descargar archivos de Cuarentena y Copia de seguridad de archivos

Los archivos almacenados en Cuarentena y en Copia de seguridad de archivos pueden descargarse si la opción **No desconectar del Servidor de administración** está habilitada en la configuración del dispositivo o si se está utilizando una puerta de enlace de conexión. Si no se cumple ninguna de estas condiciones, no podrá realizar la descarga.

Para guardar en el disco duro una copia de un archivo almacenado en Cuarentena o en Copias de seguridad del archivo:

1. Realice una de las siguientes acciones:

   - Si desea guardar una copia de un archivo que se encuentra en Cuarentena, en el menú principal vaya a **Operaciones → Repositorios → Cuarentena**.

   - Si desea guardar una copia de un archivo que se encuentra en Copia de seguridad, en el menú principal vaya a **Operaciones → Repositorios → Copias de seguridad del archivo**.

2. En la ventana que se abre, seleccione el archivo que desea descargar y haga clic en **Descargar**.

Comienza la descarga. La aplicación guarda, en la carpeta seleccionada, una copia del archivo almacenado en el repositorio Cuarentena del dispositivo cliente.

Acerca de la eliminación de objetos de los repositorios de Cuarentena, Copia de seguridad de archivos o Amenazas activas

Cuando las aplicaciones de seguridad de Kaspersky instaladas en los dispositivos cliente colocan objetos en los repositorios de Cuarentena, Copia de seguridad o Amenazas activas, envían la información sobre los objetos agregados a las secciones **Cuarentena**, **Copias de seguridad del archivo** o **Amenazas activas** en Kaspersky Security Center Linux. Al abrir una de estas secciones, podrá eliminar el objeto requerido.

En las secciones **Copias de seguridad del archivo** o **Amenazas activas**, seleccione un objeto de la lista y haga clic en el botón **Eliminar**.

En la sección **Cuarentena**, puede realizar una de las siguientes acciones:

- Seleccione la casilla que se encuentra junto al nombre del objeto que se eliminará y, a continuación, haga clic en el botón **Eliminar**, en la barra de herramientas.

- Haga clic en el nombre del objeto que se eliminará y, en la ventana de detalles que se abre, en la barra de herramientas, haga clic en el botón **Eliminar**.

  En este caso, el objeto se elimina, se muestra la notificación correspondiente en pantalla y se cierra la ventana de detalles.

Kaspersky Security Center Linux elimina el objeto seleccionado de la lista o elimina el objeto seleccionado del repositorio. La acción a realizar la define la aplicación de Kaspersky que colocó el objeto seleccionado en el repositorio. La aplicación de Kaspersky se especifica en el campo **Entrada agregada por**.

Para obtener más información sobre qué acción se debe realizar, consulte la documentación de la aplicación de Kaspersky.

Administrar la aplicación a través de SNMP

Esta sección describe cómo obtener información del Servidor de administración mediante SNMP (Protocolo simple de administración de redes) en Linux.

SNMP es un protocolo para administrar dispositivos de red.

Para trabajar con SNMP, Kaspersky Security Center Linux utiliza el servicio snmpd incluido en el sistema operativo y un agente SNMP para supervisar el rendimiento del Servidor de administración y enviar datos a las aplicaciones secundarias mediante el uso de OID. Kaspersky Security Center Linux puede enviar esta información en forma de estadísticas o capturas SNMP, que son notificaciones sobre eventos de la aplicación.

El SNMP le permite acceder a la siguiente información acerca de la aplicación:

- Información general
- Estadísticas de Kaspersky Security Center Linux desde la instalación de la aplicación
- Información acerca de los eventos de Kaspersky Security Center Linux

Se otorga acceso de solo lectura.

La información acerca de las trampas SNMP y las estadísticas enviadas a través de SNMP se almacena en el archivo adminkit.mib. De manera predeterminada, el archivo adminkit.mib se encuentra en la carpeta /opt/kaspersky/ksc64/share/snmp/.

El servicio snmpd local en cada nodo del clúster actúa como el servidor SNMP que recibe las estadísticas. No se admite la interacción con un servidor SNMP externo. Las capturas SNMP se pueden recibir utilizando el servicio snmptrapd localmente en cada nodo del clúster, o se pueden redirigir a un servidor externo.

Para las operaciones a través de SNMP, preconfigure el servicio snmpd en el sistema operativo en cada nodo del clúster.

Configuración del servicio snmpd en el sistema operativo

Antes de realizar la configuración, asegúrese de que el servicio snmpd esté instalado en su sistema operativo.

Creación de una cuenta de usuario para acceder a los datos

Antes de crear la cuenta, detenga el servicio snmpd ejecutando el siguiente comando:

```
bash
sudo systemctl stop snmpd
```

Para garantizar la seguridad del acceso a los datos a través de SNMPv3 con autenticación y cifrado, debe crear una cuenta de usuario en el lado del servicio snmpd con la siguiente información:

- Nombre de usuario (distingue entre mayúsculas y minúsculas)
- Algoritmo de autenticación (MD5 o SHA, se recomienda SHA)
- Contraseña de autenticación
- Algoritmo de cifrado (solo se admite AES)
- Contraseña de cifrado

Puede crear una cuenta de usuario de las siguientes maneras:

- Mediante la utilidad net-snmp-create-v3-user, si está disponible en el sistema operativo.
- Manualmente, agregando la directiva adecuada al archivo de configuración del servicio snmpd.

Para crear una cuenta de usuario con la utilidad net-snmp-create-v3-user, ejecute el siguiente comando:

```
net-snmp-create-v3-user -ro -a <algoritmo de autenticación> -x <algoritmo de cifrado> <nombre de usuario>
```

Las contraseñas de autenticación y cifrado se solicitan de forma interactiva.

Por ejemplo:

```
net-snmp-create-v3-user -ro -a SHA -x AES MonitoringUser
```

Para crear una cuenta usuario manualmente:

1. Cree el archivo de configuración /var/lib/snmp/snmpd.conf con el siguiente comando:

   ```
   touch /var/lib/snmp/snmpd.conf
   ```

2. Agregue las siguientes líneas al archivo de configuración:

   ```
   createUser <nombre de usuario> <algoritmo de autenticación> "<contraseña de autenticación>" <algoritmo de
   cifrado> "<contraseña de cifrado>"
   ```

   Por ejemplo:

   ```
   createUser MonitoringUser SHA "MonitoringAuthSecret" AES "MonitoringPrivSecret"
   ```

Creación de una cuenta de usuario para recibir capturas SNMP

Para recibir capturas SNMP a través de SNMPv3 con autenticación y cifrado, debe crear una cuenta en el sistema de supervisión en el contexto del servicio correspondiente (por lo general, el servicio snmptrapd).

La cuenta debe contener la siguiente información:

- Nombre de usuario.
- Algoritmo de autenticación
- Contraseña de autenticación

- Algoritmo de cifrado
- Contraseña de cifrado

Por motivos de seguridad, utilice cuentas de usuario independientes para acceder a los datos y recibir capturas SNMP.

Para obtener instrucciones sobre cómo crear una cuenta de usuario para recibir capturas de SNMP, consulte la documentación de su sistema de supervisión.

Configuración del servicio snmpd

La configuración del servicio snmpd se almacena en el archivo /etc/snmp/snmpd.conf. Puede agregar la información necesaria a un archivo de configuración existente o crear un nuevo archivo de configuración y agregar las líneas que se enumeran a continuación, en el orden indicado.

Si elige crear un nuevo archivo de configuración, asegúrese de que solo el superusuario tenga acceso a él. Si los permisos de acceso necesarios no están establecidos, configúrelos ejecutando los siguientes comandos en el orden especificado:

```
chown root:root /etc/snmp/snmpd.conf
chmod 600 /etc/snmp/snmpd.conf
```

Para configurar el servicio snmpd:

1. En el archivo de configuración, especifique el protocolo, la dirección de la interfaz de red y el número de puerto en el que el servicio snmpd debe escuchar las solicitudes entrantes.

   - Si desea escuchar solicitudes en todas las interfaces de red, agregue las siguientes líneas al archivo de configuración:

     ```
     agentAddress udp:161
     ```

   - Si desea escuchar solicitudes solo en la interfaz de red local, por ejemplo, si el sistema de supervisión está instalado en el mismo equipo, agregue las siguientes líneas al archivo de configuración:

     ```
     agentAddress udp:127.0.0.1:161
     ```

2. Configure la interacción entre Kaspersky Security Center Linux y el servicio snmpd. Puede utilizar un socket UNIX o un socket TCP.

   - Si utiliza un socket UNIX:

     a. Especifique la ruta y los permisos para el socket UNIX. Para ello, agregue las siguientes líneas al archivo de configuración:

     ```
     master agentx
     agentXSocket unix:/var/run/agentx-master.socket
     agentXPerms 770 770 kluser klusers
     ```

     b. Agregue el grupo klusers como grupo complementario para la cuenta {'KLSRV_UNATT_KLSVCUSER'}.

   - Si utiliza un socket TCP, especifique el puerto y la dirección del socket TCP. Para ello, agregue las siguientes líneas al archivo de configuración:

     ```
     master agentx
     agentXSocket tcp:127.0.0.1:705,tcp6:[::1]:705
     ```

3. Establezca el tiempo de espera de respuesta mínimo en al menos 30 segundos. Para ello, agregue las siguientes líneas al archivo de configuración:

   ```
   agentxTimeout 30
   ```

4. Si es necesario, puede proporcionar una descripción del servidor donde está configurado SNMP, la ubicación del sistema y la dirección de contacto del administrador. Para ello, agregue las siguientes líneas al archivo de configuración:

   ```
   sysDescr <descripción del servidor>
   sysLocation <ubicación del servidor>
   sysContact <dirección de contacto del administrador>
   sysServices 72
   ```

5. Especifique el alcance del árbol OID que desea que esté disponible para su sistema de supervisión a través del protocolo SNMP. Para ello, agregue las siguientes líneas al archivo de configuración:

   ```
   view monitoring included .1.3.6.1.4.1.23668.1093.1

   view systemonly included .1.3.6.1.4.1.23668.1093.1
   ```

6. Si es necesario, puede especificar adicionalmente el alcance del árbol de OID que contiene información acerca del sistema operativo que almacena el servicio snmpd. Este alcance estará disponible para su sistema de supervisión.

La información sobre el sistema operativo incluye, por ejemplo, información acerca del uso de CPU y RAM, espacio libre en las particiones del disco, carga de interfaces de red, una lista de software instalado, una lista de conexiones de red abiertas y una lista de procesos en ejecución. Parte de esta información puede ser confidencial.

- Si desea permitir el acceso solo a la información general del sistema y la información acerca del uso de RAM, CPU y dispositivos de disco, agregue las siguientes líneas al archivo de configuración:

```
# SNMPv2-MIB - Basic system information
view monitoring included .1.3.6.1.2.1.1
# HOST-RESOURCES-MIB - CPU, Memory, Filesystems
view monitoring included .1.3.6.1.2.1.25.1
view monitoring included .1.3.6.1.2.1.25.2
view monitoring included .1.3.6.1.2.1.25.3
view monitoring included .1.3.6.1.2.1.25.5
# UCD-SNMP-MIB - Memory and CPU usage
view monitoring included .1.3.6.1.4.1.2021.4
view monitoring included .1.3.6.1.4.1.2021.10
view monitoring included .1.3.6.1.4.1.2021.11
# UCD-SNMP-DISKIO-MIB - Block devices I/O statistics
view monitoring included .1.3.6.1.4.1.2021.13
# IF-MIB - Network interfaces I/O statistics
view monitoring included .1.3.6.1.2.1.2
view monitoring included .1.3.6.1.2.1.31
```

- Si desea permitir el acceso a toda la información del sistema, agregue las siguientes líneas al archivo de configuración:

```
view monitoring included .1
```

7. Especifique el modo de acceso y el alcance de la información para la cuenta de usuario creada. Para ello, agregue las siguientes líneas al archivo de configuración:

```
rouser <user name> priv -V monitoring
```

8. Para enviar capturas SNMP, especifique la dirección IP del sistema de supervisión y las credenciales de usuario para recibir capturas. Para ello, agregue las siguientes líneas al archivo de configuración:

```
trapsess -Ci -v3 -t0.1 -r1 -l authPriv -u <nombre de usuario para recibir capturas> -a <algoritmo de
autenticación> -A "<contraseña del usuario para recibir capturas>" -x <algoritmo de cifrado> -X "<contraseña de
cifrado>" udp:<dirección IP>:162
```

Se configura el servicio snmpd.

Para integrarse con múltiples sistemas de supervisión, cree una cuenta de usuario separada para cada sistema, especifique el alcance de la información disponible para cada cuenta de usuario (las directivas 'view' y 'rouser') y configure el envío de capturas SNMP (la directiva 'trapsess').

Iniciar el servicio snmpd con la nueva configuración

Para aplicar la nueva configuración:

1. Reinicie el servicio snmpd:

   ```
   systemctl restart snmpd
   ```

2. Verifique el estado del servicio snmpd:

   ```
   systemctl status snmpd
   ```

   El estado debe ser `running`.

3. Permita que el servicio se inicie automáticamente al iniciarse el sistema operativo:

   ```
   systemctl enable snmpd
   ```

4. Si está utilizando un firewall en su sistema operativo o equipo de red, agregue reglas para permitir el envío de los paquetes SNMP.

El servicio snmpd se está ejecutando.

Si el servicio klcssnmp se estaba ejecutando en el momento en que se configuró el servicio snmpd, reinicie también el servicio klcssnmp.

Comprobación del estado del servicio snmpd

Para probar el servicio snmpd, configure el uso de SNMP en Kaspersky Security Center Linux y solicite datos SNMP mediante la utilidad snmpwalk.

Para obtener los alcances de los datos SNMP proporcionados por Kaspersky Security Center Linux,

ejecute el siguiente comando:

```
snmpwalk -v3 -l authPriv -u <nombre de usuario> -a <algoritmo de autenticación> -A "<contraseña de autenticación>"
-x <algoritmo de cifrado> -X "<contraseña de cifrado>" <dirección IP> .1.3.6.1.4.1.23668.1093.1
```

Por ejemplo:

```
snmpwalk -v3 -l authPriv -u MonitoringUser -a SHA -A "MonitoringAuthSecret" -x AES -X "MonitoringPrivSecret"
127.0.0.1 .1.3.6.1.4.1.23668.1093.1
```

Habilitación y deshabilitación de las notificaciones mediante SNMP

Kaspersky Security Center Linux envía la notificación acerca de los eventos del Servidor de administración en forma de capturas SNMP.

De manera predeterminada, las notificaciones SNMP para eventos de Kaspersky Security Center Linux están deshabilitadas.

Para habilitar o deshabilitar las notificaciones de SNMP para eventos de Kaspersky Security Center Linux:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana **Propiedades del Servidor de administración**.

2. En la pestaña **Configuración de eventos** de la ventana de propiedades, haga clic en el tipo de evento para el que desea recibir notificaciones SNMP.

3. En el panel que se abre, habilite o deshabilite el botón de alternancia **Notificar por SNMP**.

   Esta opción solo está disponible si la opción **Enviar estadísticas a través del SNMP** está habilitada.

Las notificaciones SNMP para eventos de Kaspersky Security Center Linux se habilitan o deshabilitan según su selección.

Habilitación y deshabilitación de SNMP en Kaspersky Security Center Linux

De manera predeterminada, el envío de estadísticas a través de SNMP está activado. Para enviar capturas SNMP, configure el servicio snmpd.

Para habilitar o deshabilitar el envío de estadísticas a través de SNMP:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abre la ventana **Propiedades del Servidor de administración**.

2. En la pestaña **General**, seleccione la sección **SNMP**.

3. Habilite o deshabilite el botón de alternancia **Enviar estadísticas a través del SNMP**.

4. Haga clic en el botón **Guardar**.

El envío de estadísticas a través de SNMP se habilita o deshabilita según su selección.

Valores de identificadores de objetos para SNMP

La siguiente tabla muestra los valores y descripciones de los identificadores de objetos (también conocidos como DOI) que se utilizan para transferir información sobre el rendimiento del Servidor de administración a aplicaciones de terceros.

Valores y descripciones de DOI para SNMP

Valor del identificador de objeto	Tipo de datos numéricos	DOI	Descripción
`deploymentStatus`	`INTEGER { ok(0), info(1), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.1.1	Estado de despliegue. El estado puede ser uno de los siguientes: • **Información**. La licencia ya no es válida para N dispositivos. • **Advertencia**. Uno de los siguientes: Hay M equipos con aplicaciones de Kaspersky instaladas en un total de N dispositivos en grupos de Servidores de administración (N > M). La licencia L caducará en N dispositivos en M días. La tarea T de la instalación de aplicaciones se realizó correctamente en N dispositivos. Es necesario reiniciar M dispositivos. • **Crítico** La licencia caducó para N dispositivos. • **Entendido**. Ninguna de las anteriores.
`noAntivirusSoftware`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.1	`deploymentStatus` muestra que el grupo del Servidor de administración contiene demasiados dispositivos sin aplicaciones administradas. El valor será igual a 1 si se encontraron algunos dispositivos sin aplicaciones administradas. En caso contrario, el valor será igual a 0.
`remoteInstallTaskFailed`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.2	`deploymentStatus` muestra que la tarea de la instalación remota falló en algunos dispositivos. Puede obtener el número de esos dispositivos a través de `hostsRemoteInstallFailed`.
`licenceExpiring`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.3	`deploymentStatus` muestra que hay algunos dispositivos con una licencia que caduca en los próximos 7 días. Puede obtener el número de esos dispositivos a través de `hostsLicenseExpiring`.
`licenceExpired`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.4	`deploymentStatus` muestra que hay algunos dispositivos con licencia caducada. Puede obtener el número de esos dispositivos a través de `hostsLicenseExpired`.
`hostsInGroups`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.3	Número de dispositivos en los grupos del Servidor de administración.
`hostsWithAntivirus`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.4	Número de dispositivos en los grupos del Servidor de administración con aplicaciones administradas instaladas.
`hostsRemoteInstallFailed`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.5	Número de dispositivos en los que falló la tarea de instalación remota.
`licenceExpiringSerial`	`OCTET STRING`	.1.3.6.1.4.1.23668.1093.1.1.6	Identificación de una clave de licencia que caduca en menos de 7 días.
`licenceExpiredSerial`	`OCTET STRING`	.1.3.6.1.4.1.23668.1093.1.1.7	Identificación de la clave de licencia caducada.
`licenceExpiringDays`	`Unsigned32`	.1.3.6.1.4.1.23668.1093.1.1.8	Número de días antes de que caduque una licencia. Para este parámetro, el plazo de la licencia se considera caducado cuando quedan menos de siete días hasta la fecha de caducidad. Si restan más de siete días para la fecha de caducidad, el valor es 0.
`hostsLicenceExpiring`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.9	Número de dispositivos con una licencia que caduca pronto en menos de 7 días.

Valor del identificador de objeto	Tipo de datos numéricos	DOI	Descripción
hostsLicenceExpired	Counter32	.1.3.6.1.4.1.23668.1093.1.1.10	Número de dispositivos con licencia caducada.
updatesStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.2.1	Estado actual de la actualización de las bases antivirus. El estado puede ser uno de los siguientes: • **Información**. Las bases antivirus del Servidor de administración o de los dispositivos no se actualizan desde hace más de 1 día, y pasó menos de 1 día desde la instalación de la aplicación. • **Advertencia**. Las bases antivirus del Servidor de administración o de los dispositivos no se actualizan desde hace más de 3 días. Este valor se puede cambiar en la configuración de grupo. • **Crítico** Las bases antivirus del Servidor de administración o de los dispositivos no se actualizan desde hace más de 7 días. Este valor se puede cambiar en la configuración de grupo. • **Entendido**. Ninguna de las anteriores.
serverNotUpdated	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.2.2.1	El Servidor de administración no se ha actualizado en mucho tiempo. La cantidad de tiempo que se considera larga se especifica en updatesStatus.
notUpdatedHosts	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.2.2.2	Algunos dispositivos no se actualizaron durante mucho tiempo (de manera predeterminada, 7 días o más para el estado **Crítico** y 3 días para recibir una **Advertencia**). Puede obtener el número de esos dispositivos a través de hostsNotUpdated.
lastServerUpdateTime	Hex-STRING	.1.3.6.1.4.1.23668.1093.1.2.3	Última vez que se actualizaron las bases de antivirus en el Servidor de administración.
hostsNotUpdated	Counter32	.1.3.6.1.4.1.23668.1093.1.2.4	Número de dispositivos que contienen bases antivirus que no se han actualizado en mucho tiempo (de manera predeterminada, 7 días o más para el estado **Crítico** y 3 días para recibir una **Advertencia**). Si hay dispositivos con el estado de actualización **Crítico**, solo se cuentan estos dispositivos. Puede obtener el estado de la actualización a través de updatesStatus.
protectionStatus	INTEGER { ok(0), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.3.1	Estado de protección en tiempo real. Uno de los siguientes: • **Advertencia**. Uno de los siguientes: Se ha detectado una brecha de seguridad en un dispositivo que pertenece al grupo de Servidores de administración. Los errores de cifrado hicieron que algunos dispositivos cambiaran el estado de protección. El análisis completo no se ha realizado en mucho tiempo. • **Crítico** La protección antivirus no funciona en algunos dispositivos de los grupos del Servidor de administración. • **Entendido**. Ninguna de las anteriores.
antivirusNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.1	No se está ejecutando una aplicación de seguridad en algunos dispositivos. Puede obtener el número de esos dispositivos a través de hostsAntivirusNotRunning.
realtimeNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.2	La protección en tiempo real no se está ejecutando en algunos dispositivos. Puede obtener el número de esos dispositivos a través de hostsRealtimeNotRunning.
psRealtimeLevelChanged	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.3	El nivel de protección durante el tiempo de ejecución difiere del nivel que estableció el administrador en N equipos de los grupos de administración.
notCuredFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.4	Hay dispositivos que contienen objetos no desinfectados. Puede obtener el número de esos dispositivos a través de hostsNotCuredObject.

Valor del identificador de objeto	Tipo de datos numéricos	DOI	Descripción
tooManyThreats	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.5	Se han encontrado amenazas en algunos dispositivos. Puede obtener el número de esos dispositivos a través de hostsTooManyThreats.
virusOutbreak	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.6	El estado del brote de virus del sistema. El valor es igual a 1 si se encontró cierta cantidad de virus durante un determinado período de tiempo y 0 en caso contrario. La cantidad de virus y la cantidad de tiempo se especifican en el Servidor de administración mediante la configuración de ataque de virus.
psVulnerabilitiesFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.7	Se detectaron vulnerabilidades.
psEncryptionFaultsFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.8	Se detectaron errores de cifrado que cambiaron el estado de protección del dispositivo.
psVulnerableHostsFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.9	Se detectaron vulnerabilidades en algunos dispositivos.
psNotScannedLately	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.10	Se detectaron dispositivos sin un análisis completo durante un período prolongado.
psNagentsNotRunningUntilReboot	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.11	Dispositivos en los que el Agente de red se inicia solo después de que se detecta un reinicio.
hostsAntivirusNotRunning	Counter32	.1.3.6.1.4.1.23668.1093.1.3.3	Número de dispositivos con aplicaciones de seguridad que no se están ejecutando.
hostsRealtimeNotRunning	Counter32	.1.3.6.1.4.1.23668.1093.1.3.4	Número de dispositivos con protección en tiempo real que no se está ejecutando.
hostsRealtimeLevelChanged	Counter32	.1.3.6.1.4.1.23668.1093.1.3.5	Número de dispositivos con un nivel de protección en tiempo real inaceptable.
hostsNotCuredObject	Counter32	.1.3.6.1.4.1.23668.1093.1.3.6	Número de dispositivos que contienen objetos no desinfectados.
hostsTooManyThreats	Counter32	.1.3.6.1.4.1.23668.1093.1.3.7	Número de dispositivos que contienen amenazas.
fullscanStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.4.1	El estado del análisis antivirus completo es uno de los siguientes: • **Información**. Han pasado menos de 7 días desde el momento de la instalación de la aplicación. • **Advertencia**. El análisis completo del antivirus no se ha realizado durante más de 7 días desde el momento de la instalación de la aplicación. • **Crítico** El análisis completo del antivirus no se ha realizado durante más de 14 días desde el momento de la instalación de la aplicación. • **Entendido**. Ninguna de las anteriores.
notScannedLately	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.4.2.1	Algunos dispositivos no se han analizado durante un tiempo determinado. Puede obtener el número de esos dispositivos a través de hostsNotScannedLately. La cantidad de tiempo se especifica en fullScanStatus.
hostsNotScannedLately	Counter32	.1.3.6.1.4.1.23668.1093.1.4.3	Número de dispositivos que no se han analizado durante un tiempo determinado. La cantidad de tiempo se especifica en fullScanStatus.

Valor del identificador de objeto	Tipo de datos numéricos	DOI	Descripción
logicalNetworkStatus	INTEGER { ok(0), warning(1), critical(2) }	.1.3.6.1.4.1.23668.1093.1.5.1	Estado de la red lógica del Servidor de administración. Uno de los siguientes: • **Advertencia**. Si no se puede acceder al estado de advertencia de algún dispositivo o si hay dispositivos que no pertenecen a ningún grupo de Servidores de administración. • **Crítico** Si el Servidor de administración pierde control sobre algún dispositivo, o existen dispositivos en estado crítico a los que no se puede acceder. • **Entendido**. Ninguna de las anteriores.
notConnectedLongTime	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.5.2.1	Algunos dispositivos no han estado conectados al Servidor de administración durante mucho tiempo (7 días o más para un dispositivo en estado de **Advertencia** y 4 días para un dispositivo en estado **Crítico**). Puede obtener el número de esos dispositivos a través de hostsNotConnectedLongTime.
controlLost	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.5.2.2	El Servidor de administración ha perdido del control sobre algunos dispositivos. Puede obtener el número de esos dispositivos a través de hostsControlLost.
hostsFound	Counter32	.1.3.6.1.4.1.23668.1093.1.5.3	Número de dispositivos encontrados por el Servidor de administración que no pertenecen a ningún grupo del Servidor de administración.
groupsCount	Counter32	.1.3.6.1.4.1.23668.1093.1.5.4	Número de grupos de administración en el Servidor de administración.
hostsNotConnectedLongTime	Counter32	.1.3.6.1.4.1.23668.1093.1.5.5	Número de dispositivos que no se han conectado al Servidor de administración durante mucho tiempo. La cantidad de tiempo considerada larga se especifica en notConnectedLongTime.
hostsControlLost	Counter32	.1.3.6.1.4.1.23668.1093.1.5.6	Número de dispositivos que no están bajo el control del Servidor de administración.
eventsStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.6.1	El estado del subsistema de eventos es uno de los siguientes: • **Advertencia**. Uno de los siguientes: Los dispositivos del grupo de Servidores de administración no han buscado actualizaciones de Windows durante mucho tiempo. Hay dispositivos con problemas de estado. • **Crítico** Uno de los siguientes: Hay un evento "Crítico" en al menos un dispositivo. Hay un evento de "Error" en al menos un dispositivo. Hay un evento de tarea incompleta en al menos un dispositivo. Los dispositivos del grupo de Servidores de administración no han buscado actualizaciones de Windows durante mucho tiempo. Hay dispositivos con problemas de estado. • **Información** Uno de los siguientes: Pasó menos de una semana desde el último análisis antivirus completo en todos los dispositivos. Las tareas de instalación remota se completaron y no es necesario reiniciar los dispositivos. Pasó menos de una semana desde la última actualización del Servidor de administración. El Servidor de administración no se actualiza hace mucho tiempo, pero hay una actualización en curso. • **Entendido**. Ninguna de las anteriores.

Valor del identificador de objeto	Tipo de datos numéricos	DOI	Descripción
`criticalEventOccured`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.6.2.1	`eventsStatus` muestra que hay algunos eventos críticos en el Servidor de administración. Puede obtener el número de esas ocurrencias a través de `criticalEventsCount`. El valor es igual a 1 si hay al menos un evento crítico en algún dispositivo y 0 en caso contrario.
`criticalEventsCount`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.6.3	Número de eventos críticos en el Servidor de administración.

Trabajar con Kaspersky Security Center Linux con una licencia de Kaspersky Next XDR Optimum

Si compró una licencia para Kaspersky Next XDR Optimum como parte de la licencia de una aplicación EPP y una licencia de Kaspersky Security Center Linux, podrá usar la funcionalidad de Kaspersky Next XDR Optimum después de realizar la configuración inicial.

Si compró una licencia para Kaspersky Next XDR Optimum por separado como una extensión de una licencia comprada anteriormente después de instalar y activar las aplicaciones de Kaspersky en los dispositivos, deberá reactivar Kaspersky Security Center Linux en los dispositivos con el nuevo código de activación o archivo de clave según la forma en que haya adquirido la licencia de Kaspersky Next XDR Optimum. Después de eso, podrá realizar la configuración inicial.

Además, puede usar las funcionalidades de Kaspersky Next XDR Optimum en el modo de prueba. Para ello, primero debe agregar un Servidor de administración físico secundario y luego activarlo con la licencia de prueba de Kaspersky Next XDR Optimum. La funcionalidad de Kaspersky Next XDR Optimum estará disponible en el Servidor secundario durante el plazo de la licencia de prueba.

Después de activar el Servidor de administración con su licencia de Kaspersky Next XDR Optimum e implementar la clave de licencia en los dispositivos administrados mediante el Servidor de administración correspondiente, puede hacer lo siguiente:

- Responda a las amenazas mediante el uso de integraciones con Kaspersky Automated Security Awareness Platform, Kaspersky Threat Intelligence Portal Sandbox y Active Directory.
- Agrupación de alertas por atributos.

Para obtener más información acerca de las funciones habilitadas por la licencia de Kaspersky Next XDR Optimum, consulte la Ayuda de Kaspersky Endpoint Detection and Response Optimum.

Integraciones para responder a alertas

Si tiene la licencia de Kaspersky Next XDR Optimum, puede configurar integraciones con las siguientes soluciones para responder a las amenazas:

- Kaspersky Automated Security Awareness Platform
- Kaspersky Threat Intelligence Portal Sandbox
- Active Directory

Estas integraciones están disponibles si activó el Servidor de administración con una licencia de Kaspersky Next XDR Optimum.
Para realizar acciones de respuesta, debe implementar la clave de licencia de Kaspersky Next XDR Optimum en sus aplicaciones administradas.
Al utilizar la funcionalidad de Kaspersky Next XDR Optimum con una licencia de prueba, primero debe agregar un Servidor de administración secundario físico, activarlo con la licencia de prueba y luego implementar la clave de licencia en los dispositivos administrados mediante este Servidor de administración.

Si está utilizando la licencia de Kaspersky Next EDR Optimum, no es necesario que active las aplicaciones instaladas en sus dispositivos administrados con la licencia de Kaspersky Next XDR Optimum. Debe hacerlo solo para dispositivos nuevos, en caso de que los hubiera.

Como la licencia de Kaspersky Next XDR Optimum es compatible con el multiinquilinato, puede distribuir la clave de licencia de manera centralizada a las aplicaciones administradas. No se admite la distribución automática de la licencia a servidores de administración secundarios y virtuales.

Para configurar las integraciones, debe tener los derechos **Leer** y **Escribir** para el área funcional **Características generales: Integración de aplicaciones**.

Configurar la integración con Active Directory para realizar acciones de respuesta

La integración con Active Directory le permite realizar acciones de respuesta para los usuarios de Active Directory afectados o involucrados en la alerta.

Para configurar la integración con Active Directory para responder a las alertas, debe usar el Servidor de administración de Kaspersky Security Center Linux versión 15.4 o una versión posterior.

La integración con Active Directory para responder a las alertas y la configuración para analizar el controlador de dominio de Active Directory (la dirección y las credenciales de usuario del controlador de dominio) que especifica al configurar un sondeo de controlador de dominio son dos configuraciones diferentes. Dado que debe asegurarse de que el usuario para el que se va a realizar una acción de respuesta tenga una cuenta de Active Directory, debe configurar ambas integraciones: para el análisis y para la respuesta. El orden no es importante.

La configuración de integración no se hereda y se aplica solo al Servidor de administración (físico o virtual) en el que se configuran estas opciones.

Para configurar la integración con Active Directory para responder a las alertas:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abrirá la ventana de propiedades del Servidor de administración, con la pestaña **General** seleccionada.

2. Realice una de las siguientes acciones:

   - Seleccione la sección **Puntos de distribución**, haga clic en el nombre del punto de distribución requerido y, a continuación, en la ventana de propiedades que se abre, seleccione la sección **Active Directory**.
   - Seleccione la sección **Respuesta de Active Directory**.

3. En el panel derecho, habilite el botón de alternancia de la **Integración con Active Directory**.

   Más tarde, si desea desactivar la integración, solo puede hacerlo para todas las conexiones deshabilitando el botón de alternancia de la **Integración con Active Directory**. No se puede desactivar la integración para una conexión diferente. En su lugar, puede eliminar la conexión.

   > Cuando habilita o deshabilita el botón de alternancia de la **Integración con Active Directory**, la configuración se aplica tanto a la sección **Respuesta de Active Directory** como a la sección **Puntos de distribución**.

4. Cree una conexión al controlador de dominio de Active Directory haciendo clic en el botón **Agregar**.

5. En la ventana que se abrirá, defina los siguientes parámetros para la conexión:

   - **Dirección del controlador de dominio**

     Nombre del equipo, por ejemplo: `server.mycompany.com`.

     Puede especificar varias direcciones. Todos los controladores de dominio cuyas direcciones especifique deben pertenecer al mismo dominio.

   - **Nombre de dominio de Active Directory**

     Nombre de dominio completo DNS, por ejemplo: `mycompany.com`

     También puede especificar el nombre SAM o NetBIOS, por ejemplo: `mycompany`

     Utilice letras minúsculas. Si crea varias conexiones para el Servidor de administración o un punto de distribución, especifique nombres diferentes para cada conexión.

     > Para realizar acciones de respuesta, el nombre de dominio de Active Directory que especifique en este campo debe coincidir con el nombre de dominio de Active Directory especificado en la alerta.

   - **Nombre de usuario**

     Nombre de usuario de la cuenta de Active Directory con derechos de administrador con la cual se realizarán las acciones de respuesta.

   - **Contraseña**

     Contraseña de la cuenta de Active Directory con derechos de administrador con la cual se realizarán las acciones de respuesta.

6. Si desea verificar el estado de la conexión, haga clic en el botón **Comprobar conexión**.

   Si la conexión se establece correctamente, se muestra el estado **Conectado**. De lo contrario, el estado es **Error** y se muestra un mensaje de error con los controladores de dominio a los que no pudo conectarse.

Debe tener en cuenta cómo se realiza la conexión a Active Directory: **desde un dispositivo Linux o desde un dispositivo Windows**.

Conexión desde un dispositivo Linux

Por defecto, al conectarse y realizar la autenticación a un controlador de dominio desde un dispositivo Linux, la lógica es la siguiente:

1. El Servidor de administración o el punto de distribución intentan conectarse al controlador de dominio mediante el protocolo LDAPS.

   Se requiere una verificación estricta del certificado del servidor LDAP.

2. La parte pública del certificado del controlador de dominio se coloca en el repositorio de certificados del sistema para validar el certificado.

   Se usa la ruta de acceso a la autoridad de certificación (CA) del sistema, que depende del sistema operativo, para acceder a la cadena de certificados.

   Por ejemplo:

   - /etc/ssl/certs/ca-certificates.crt: ruta para sistemas operativos basados en Debian (Debian, Ubuntu, Astra).
   - /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem: ruta para CentOS o Red Hat.

3. Si la conexión LDAPS falla, se produce un error y no se utiliza ningún otro protocolo de conexión.

   En caso de problemas con LDAPS, puede comunicarse con el Soporte técnico de Kaspersky.

Si no desea instalar el certificado en el repositorio de certificados del sistema, puede usar el indicador KLNAG_LDAP_SSL_CACERT para establecer la ruta al certificado del controlador de dominio. Para hacerlo, ejecute el comando:

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "</path/to/domain-controller/cert>"
```

dónde `</path/to/domain-controller/cert>` es la ruta a la parte pública del certificado del controlador de dominio.

Por ejemplo, si la ruta es `"/var/opt/kaspersky/ldap_cert.crt"`, el comando es `klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "/var/opt/kaspersky/ldap_cert.crt"`

Conexión desde un dispositivo Windows

Al conectarse y realizar la autenticación a un controlador de dominio desde un dispositivo Windows, la configuración de la conexión la define el dominio.

Solo debe asegurarse de que:

- El LDAPS esté habilitado y el puerto 636 esté disponible en el dispositivo.
- Se permitan las conexiones al controlador de dominio a través de un firewall o un servidor proxy.

7. Haga clic en el botón **Guardar**.

La ventana se cierra y la conexión se muestra en la tabla de conexiones.

En la tabla de conexiones, puede hacer lo siguiente:

- Editar los parámetros de conexión.

  Para hacer esto, haga clic en el vínculo con el parámetro **Dirección del controlador de dominio** para la conexión requerida. En la ventana que se abre, cambie la configuración necesaria y, luego, haga clic en el botón **Guardar**.

  Solo puede editar los parámetros **Nombre de usuario** y **Contraseña**.

- Eliminar conexiones.

  Para hacer esto, seleccione la casilla que se encuentra junto a la conexión que desee eliminar, haga clic en el botón **Eliminar** en la barra de herramientas y luego confirme la eliminación de la conexión.

Configuración de la integración con Kaspersky Automated Security Awareness Platform

La integración con Kaspersky Automated Security Awareness Platform (en adelante, también denominada KASAP) le permite asignar cursos de aprendizaje KASAP a los usuarios asociados a las alertas.

La configuración de integración no se hereda y se aplica solo al Servidor de administración (físico o virtual) en el que se configuran estas opciones.

Antes de configurar una integración en Kaspersky Security Center Web Console, debe crear un token de autorización y obtener una URL para las solicitudes de API en KASAP.

Para configurar la integración con Kaspersky Automated Security Awareness Platform, siga estos pasos:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abrirá la ventana de propiedades del Servidor de administración, con la pestaña **General** seleccionada.

2. Elija la sección **KASAP**.
3. En el panel derecho, habilite el botón de alternancia de la **Integración con KASAP**.
4. Especifique la configuración que se utilizará para la conexión a KASAP:
   - **Token de API**: el token que creó para acceder a KASAP Open API.
   - **Dirección URL**: URL para las solicitudes de API que obtuvo al crear el token de API.

- **Usar un servidor proxy**: botón de alternancia que habilita el uso de un servidor proxy cuando se conecta a KASAP.

  El botón de alternancia está desactivado de forma predeterminada.

5. Si es necesario, verifique la configuración que especificó haciendo clic en el botón **Comprobar conexión**.

   Se muestra el estado de la conexión.

6. Haga clic en el botón **Guardar**.

La integración con Kaspersky Automated Security Awareness Platform está configurada.

Después de guardar la configuración de la integración con KASAP, puede ver la lista de grupos de aprendizaje de KASAP haciendo clic en el botón **Ver grupos**.

Si es necesario, cuando se muestra la lista de grupos, puede actualizarla haciendo clic en el botón **Actualizar grupos**.

No puede ocultar la lista después de abrirla. Si deshabilita el botón de alternancia de la **Integración con KASAP**, no se muestra la lista de grupos KASAP.

Configurar la integración con Kaspersky Threat Intelligence Portal Sandbox

La integración con Kaspersky Threat Intelligence Portal (en adelante también denominado Kaspersky TIP) le permite ejecutar los archivos movidos a la sección **Cuarentena** usando Kaspersky Sandbox: un entorno seguro aislado de su red corporativa.

La configuración de integración no se hereda y se aplica solo al Servidor de administración (físico o virtual) en el que se configuran estas opciones.

Antes de configurar la integración, debe obtener un token de autorización para las solicitudes de API en Kaspersky TIP.

Para configurar la integración con Kaspersky TIP Sandbox:

1. En el menú principal, haga clic en el nombre del Servidor de administración.

   Se abrirá la ventana de propiedades del Servidor de administración, con la pestaña **General** seleccionada.

2. Seleccione **Kaspersky TIP**.

3. En el panel derecho, habilite el botón de alternancia **Integración**.

   Se muestra la configuración para la conexión a Kaspersky TIP.

   Si después de configurar y guardar la configuración de integración deshabilita el botón de alternancia **Integración**, la configuración no se elimina, pero no se puede realizar la acción de respuesta.

4. Haga clic en el botón **Agregar token**, especifique en la ventana que aparece el token que obtuvo anteriormente de Kaspersky TIP y, a continuación, haga clic en el botón **Agregar**.

   La ventana se cierra y se agrega el token de API.

5. Si desea utilizar un servidor proxy al conectarse a Kaspersky TIP, habilite el botón de alternancia **Usar un servidor proxy**.

   El botón de alternancia está desactivado de forma predeterminada.

6. Haga clic en el botón **Guardar**.

La integración con Kaspersky TIP Sandbox está configurada.

Ahora puede enviar archivos desde la sección **Cuarentena** a Kaspersky TIP Sandbox para el análisis de amenazas. El tamaño máximo de un archivo es de 100 megabytes (MB).

Debido a que la licencia de Kaspersky Next XDR Optimum es compatible con el multiinquilinato, los archivos colocados en **Cuarentena** están divididos por inquilinos. Esta separación a nivel de inquilino también se aplica al enviar archivos a Kaspersky TIP Sandbox y ver los resultados si el administrador usa una cuenta de TIP dedicada y un token de API relacionado con cada inquilino. Sin embargo, la administración centralizada de la sección **Cuarentena** para todos los inquilinos no es posible, ya que la lista de cuarentena no muestra objetos de acuerdo con la jerarquía del servidor.

Agrupación de alertas por atributos

La combinación de alertas ayuda a identificar las alertas que pueden estar relacionadas con el mismo incidente, lo que simplifica el proceso de investigación.

Para habilitar la funcionalidad de combinación de alertas, debe hacer lo siguiente:

- Habilite la subsección **Alertas** en el menú principal.
- Active el Servidor de Administración con una licencia de Kaspersky Next XDR Optimum y, luego, implemente la clave de licencia de Kaspersky Next XDR Optimum en sus aplicaciones administradas.

  Al usar una funcionalidad de Kaspersky Next XDR Optimum con una licencia de prueba en el modo de prueba, primero debe agregar un Servidor de administración físico secundario y luego activar dicho servidor con esta licencia.

Si está utilizando la licencia de Kaspersky Next EDR Optimum, no es necesario que active las aplicaciones instaladas en sus dispositivos administrados con la licencia de Kaspersky Next XDR Optimum. Debe hacerlo solo para dispositivos nuevos, en caso de que los hubiera.
Como la licencia de Kaspersky Next XDR Optimum es compatible con el multiinquilinato, puede distribuir la clave de licencia de manera centralizada a las aplicaciones administradas. No se admite la distribución automática de la licencia a servidores de administración secundarios y virtuales.

Puede combinar alertas por nombre de dispositivo, cuenta o nombre de hash (SHA256).

> Las alertas se combinan por un atributo solo si ese atributo no está vacío.

Las alertas se combinan si comparten al menos un atributo y ocurren dentro de las 24 horas posteriores a cualquier otra alerta en el grupo.

Para combinar alertas por atributos:

1. En el menú principal, vaya a **Supervisión** → **Alertas**.
2. Realice una de las siguientes acciones:

   - Habilite el botón de alternancia de **Agregación de alertas** y, luego, seleccione uno o más atributos para combinar alertas de la siguiente manera:

     - **Nombre del dispositivo**
     - **Cuenta**
     - **Hash de archivo**Nombre de hash (SHA256)

     Los atributos **Nombre del dispositivo** y **Cuenta** están seleccionados de manera predeterminada.

   - Haga clic en el ícono de configuración (⚙). En el panel **Configuración de tabla** que se abre, vaya a la pestaña **Agrupación**. Seleccione **Id. del grupo de agregación** y haga clic en **Aplicar**.

   > Cuando la combinación está habilitada, las alertas se ordenan según la **Fecha y hora del evento**, del más reciente al más antiguo. No se admiten opciones de clasificación adicionales. Si selecciona una opción de agrupación diferente, se deshabilitará la combinación.

La tabla muestra las alertas combinadas por atributos. Las alertas no combinadas se muestran en la parte inferior de la tabla.

> Cada alerta se asigna a un solo grupo después de la combinación.

Integración entre Kaspersky Security Center Web Console y otras soluciones de Kaspersky

Esta sección describe cómo configurar el acceso desde Kaspersky Security Center Web Console a otra aplicación de Kaspersky, como Kaspersky Managed Detection and Response. Asimismo, esta sección describe cómo configurar la exportación a sistemas SIEM.

Establecer una conexión en segundo plano

Para configurar la interacción entre Kaspersky Security Center Linux y otra aplicación o solución de Kaspersky, como Kaspersky Managed Detection and Response (también denominada "MDR"), debe establecer una conexión en segundo plano entre Kaspersky Security Center Web Console y el Servidor de administración. Puede establecer esta conexión solo si su cuenta posee el derecho Modificar ACL de objeto del área funcional **Funciones generales: permisos de usuario**.

> Puede configurar la interacción solo entre Kaspersky Managed Detection and Response y la versión para Windows de Kaspersky Security Center.

Para establecer una conexión en segundo plano:

1. En el menú principal, vaya a **Configuración** → **Integración**.
2. Seleccione la pestaña **Configuración del servidor proxy de Web Console**.
3. En la sección **Integración**, establezca el botón de alternancia de la conexión en segundo plano en **Conexión en segundo plano para la integración Habilitada**.
4. En la sección **Habilitar una conexión en segundo plano** abierta, haga clic en el botón **Aceptar**.

Se establece la conexión en segundo plano entre Kaspersky Security Center Web Console y el Servidor de administración. El Servidor de administración crea una cuenta para la conexión en segundo plano; esta cuenta se utiliza como cuenta de servicio para mantener la interacción entre Kaspersky Security Center Linux y otra aplicación o solución de Kaspersky. El nombre de esta cuenta de servicio contiene el prefijo NWCSvcUser. Por seguridad, el Servidor de administración cambia la contraseña de la cuenta del servicio automáticamente cada 30 días. No puede eliminar la cuenta del servicio manualmente. El Servidor de administración elimina esta cuenta automáticamente si se deshabilita la conexión entre servicios. El Servidor de administración crea una única cuenta de servicio para cada instancia de Kaspersky Security Center Web Console y cada Consola de administración, y asigna todas las cuentas de servicio al grupo de seguridad llamado ServiceNwcGroup. El Servidor de administración crea este grupo de seguridad automáticamente durante la instalación de Kaspersky Security Center Linux. No se puede eliminar este grupo de seguridad manualmente.

Configuración de la conexión del servidor proxy

Para configurar una conexión de servidor proxy para Kaspersky Security Center Web Console y complementos web:

1. En el menú principal, vaya a **Configuración** → **Integración**.
2. Seleccione la pestaña **Configuración del servidor proxy de Web Console**.
3. Habilite la opción **Usar servidor proxy**.
4. Especifique la configuración de conexión del servidor proxy:
   - **Dirección del servidor proxy**
   - **Número de puerto**
   - **Autenticación del servidor proxy**
   - **Nombre de usuario** (se requiere si habilita la opción **Autenticación del servidor proxy**)
   - **Contraseña** (se requiere si habilita la opción **Autenticación del servidor proxy**)
5. Haga clic en **Guardar** para guardar la configuración de conexión del servidor proxy

Si tiene una jerarquía de Servidores de administración, la configuración de conexión del servidor proxy no se propaga a las Web Consoles que administran Servidores de administración secundarios. Debe configurar la conexión del servidor proxy por separado para cada Kaspersky Security Center Web Console.

Diagnóstico remoto de dispositivos cliente

Puede usar la función de diagnóstico remoto para realizar a distancia las siguientes operaciones en dispositivos cliente basados en Windows y Linux:

- Habilitar y deshabilitar la característica de seguimiento, cambiar el nivel de seguimiento y descargar el archivo de seguimiento
- Descargar información del sistema y los ajustes de las aplicaciones
- Descargar registros de eventos
- Crear un archivo de volcado para una aplicación
- Realizar un diagnóstico y descargar el informe de diagnóstico
- Iniciar, detener y reiniciar aplicaciones

Puede utilizar los registros de eventos y los informes de diagnóstico descargados de un dispositivo cliente para solucionar problemas por cuenta propia. Si se comunica con el servicio de soporte técnico de Kaspersky, los especialistas podrían pedirle que descargue archivos de seguimiento, archivos de volcado, registros de eventos e informes de diagnóstico del dispositivo cliente para que sean analizados en Kaspersky.

Abrir la ventana de diagnóstico remoto

Para realizar un diagnóstico remoto de dispositivos cliente basados en Windows y Linux, debe abrir la ventana de diagnóstico remoto.

Para abrir la ventana de diagnóstico remoto:

1. Realice una de las siguientes acciones para seleccionar el dispositivo para el que desee abrir la ventana de diagnóstico remoto:
   - Si el dispositivo pertenece a un grupo de administración, en el menú principal, vaya a **Administración de activos** → **Dispositivos administrados**.
   - Si el dispositivo pertenece al grupo Dispositivos no asignados, en el menú principal, vaya a **Administración de activos** → **Dispositivos no asignados**.
2. Haga clic en el nombre del dispositivo pertinente.
3. En la ventana que se abre, que contendrá las propiedades del dispositivo, elija la pestaña **Avanzado**.
4. En la pestaña **Avanzado**, haga clic en **Diagnóstico remoto**.

   Esto abre la ventana **Diagnóstico remoto** de un dispositivo cliente. Si no se establece la conexión entre el Servidor de administración y el dispositivo cliente, se muestra el mensaje de error.

Como alternativa, si necesita obtener toda la información de diagnóstico sobre un dispositivo cliente basado en Linux a la vez, puede ejecutar el script collect.sh en este dispositivo.

Habilitar y deshabilitar el seguimiento para las aplicaciones

Puede habilitar y deshabilitar el seguimiento para las aplicaciones, incluido el seguimiento con Xperf.

Habilitar y deshabilitar el seguimiento

Para habilitar o deshabilitar el seguimiento en un dispositivo remoto:

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnóstico remoto, seleccione la pestaña **Aplicaciones de Kaspersky**.

   En la sección **Administración de aplicaciones**, se muestra la lista de aplicaciones de Kaspersky instaladas en el dispositivo.
3. En la lista de aplicaciones, seleccione la aplicación para la que desee habilitar o deshabilitar el seguimiento.

   Se abre la lista de opciones de diagnóstico remoto.
4. Si desea habilitar el seguimiento, haga lo siguiente:

   a. En la sección **Seguimiento**, haga clic en **Habilitar seguimiento**.

   b. En la ventana **Modificar nivel de seguimiento**, recomendamos que mantenga los valores de configuración predeterminados. De ser necesario, un especialista del servicio de soporte técnico le indicará cómo modificar la configuración. Están disponibles las siguientes opciones:

   - **Nivel de seguimiento**

     El nivel de seguimiento determina qué tan detallado es el archivo de seguimiento.

   - **Seguimiento con rotación**

     La información de seguimiento se sobrescribe para que el archivo de seguimiento no aumente de tamaño desmedidamente. Especifique el número máximo de archivos que se utilizarán para almacenar la información de seguimiento y el tamaño máximo de cada archivo. Una vez que se haya guardado el número máximo de archivos de seguimiento, cada cual con su tamaño máximo, se eliminará el archivo de seguimiento más antiguo para que se pueda guardar un nuevo archivo de seguimiento.

     Esta opción solo está disponible para Kaspersky Endpoint Security.

   c. Haga clic en el botón **Guardar**.

Se habilita el seguimiento para la aplicación seleccionada. En algunos casos, para habilitar el seguimiento, deberá reiniciar la aplicación de seguridad y su tarea.

En dispositivos cliente basados en Linux, el seguimiento del componente Actualizador del Agente de red está regulado por la configuración del Agente de red. Por lo tanto, las opciones **Habilitar seguimiento** y **Modificar nivel de seguimiento** están deshabilitadas para este componente en dispositivos cliente que ejecutan Linux.

5. Para deshabilitar el seguimiento para la aplicación seleccionada, haga clic en el botón **Deshabilitar seguimiento**.

   Se deshabilita el seguimiento para la aplicación seleccionada.

Habilitar el seguimiento con Xperf

Si utiliza Kaspersky Endpoint Security, un especialista de nuestro servicio de soporte técnico podría pedirle que habilite el seguimiento con Xperf. Esta función permite obtener información sobre el rendimiento del sistema.

Para habilitar y configurar el seguimiento con Xperf o deshabilitarlo, siga los siguientes pasos:

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.

2. En la ventana de diagnóstico remoto, seleccione la pestaña **Aplicaciones de Kaspersky**.

   En la sección **Administración de aplicaciones**, se muestra la lista de aplicaciones de Kaspersky instaladas en el dispositivo.

3. En la lista de aplicaciones, seleccione Kaspersky Endpoint Security para Windows.

   Se muestra la lista de opciones de diagnóstico remoto para la app Kaspersky Endpoint Security para Windows.

4. En la sección **Seguimiento con Xperf**, haga clic en **Habilitar seguimiento con Xperf**.

   Si el seguimiento con Xperf ya está habilitado, verá, en cambio, el botón **Deshabilitar seguimiento con Xperf**. Haga clic en este botón si desea deshabilitar el seguimiento con Xperf para Kaspersky Endpoint Security para Windows.

5. Cuando se abra la ventana **Cambiar el nivel de seguimiento con Xperf**, dependiendo de lo que le haya pedido el especialista en soporte técnico, haga lo siguiente:

   a. Seleccione uno de los siguientes niveles de seguimiento:

   - **Nivel bajo**

     Un archivo de seguimiento de este tipo contiene una cantidad mínima de información sobre el sistema.

     Esta opción está seleccionada de forma predeterminada.

   - **Nivel profundo**

     Un archivo de seguimiento de este tipo contiene información más detallada que los archivos de seguimiento que se generan cuando se elige la opción *Nivel bajo*. El especialista en soporte técnico podría pedirle que elija este nivel si la información contenida en un archivo de nivel bajo no basta para evaluar el rendimiento del sistema. Un archivo de seguimiento de *Nivel profundo* contiene distintas clases de información técnica sobre el sistema: información sobre el hardware, el sistema operativo, la lista de procesos y programas iniciados y finalizados, los eventos utilizados para la evaluación del rendimiento, eventos de la Herramienta de evaluación del sistema de Windows y más.

b. Seleccione uno de los siguientes tipos de seguimiento con Xperf:

- **Tipo básico**

  La información de seguimiento se obtendrá mientras Kaspersky Endpoint Security esté en funcionamiento.

  Esta opción está seleccionada de forma predeterminada.

- **Tipo con reinicio**

  La información de seguimiento se obtendrá cuando se inicie el sistema operativo del dispositivo administrado. Este tipo de seguimiento es efectivo cuando el problema que afecta al rendimiento del sistema ocurre después de encender el dispositivo y antes de que se inicie Kaspersky Endpoint Security.

También podrían pedirle que habilite la opción **Tamaño de archivos de rotación, en MB** para evitar que el archivo de seguimiento aumente de tamaño desmedidamente. Si habilita esta opción, especifique el tamaño que el archivo de seguimiento podrá tener como máximo. Cuando el archivo alcance su máximo tamaño, la información de seguimiento más antigua comenzará a reemplazarse con información nueva.

c. Defina el tamaño del archivo de rotación.

d. Haga clic en el botón **Guardar**.

El seguimiento con Xperf queda configurado y habilitado.

6. Si desea deshabilitar el seguimiento con Xperf para Kaspersky Endpoint Security para Windows, haga clic en **Deshabilitar seguimiento con Xperf** en la sección **Seguimiento con Xperf**.

   Se deshabilita el seguimiento con Xperf.

Descargar los archivos de seguimiento de una aplicación

Para descargar un archivo de seguimiento de una aplicación:

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.

2. En la ventana de diagnóstico remoto, seleccione la pestaña **Aplicaciones de Kaspersky**.

   En la sección **Administración de aplicaciones**, se muestra la lista de aplicaciones de Kaspersky instaladas en el dispositivo.

3. En la lista de aplicaciones, seleccione la aplicación para la que desee descargar un archivo de seguimiento.

4. En la sección **Seguimiento**, haga clic en el botón **Archivos de seguimiento**.

   Se abre la ventana **Registros de seguimiento del dispositivo**, en la que se muestra una lista de archivos de seguimiento.

5. En la lista de archivos de seguimiento, seleccione el archivo que desee descargar.

6. Realice una de las siguientes acciones:

   - Si desea descargar el archivo seleccionado, haga clic en **Descargar**. Puede seleccionar uno o varios archivos para descargar.
   - Si desea descargar una parte del archivo seleccionado, haga lo siguiente:

     a. Haga clic en **Descargar una parte**.

     No puede descargar partes de varios archivos al mismo tiempo. Si selecciona más de un archivo de seguimiento, se deshabilita el botón **Descargar una parte**.

     b. En la ventana que se abre, indique el nombre y la parte del archivo que desee descargar.

     Para dispositivos basados en Linux, no está disponible la edición del nombre de la parte del archivo.

     c. Haga clic en **Descargar**.

El archivo seleccionado, o la parte seleccionada, se descargará en la ubicación que especifique.

Eliminar archivos de seguimiento

Puede eliminar los archivos de seguimiento que ya no necesite.

Para eliminar un archivo de seguimiento:

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnóstico remoto que se abre, seleccione la pestaña **Registros de eventos**.
3. En la sección **Archivos de seguimiento**, haga clic en **Registros de Windows Update** o en **Registros de instalación remota**, dependiendo de cuáles sean los archivos de seguimiento que desee eliminar.

   El vínculo **Registros de Windows Update** está disponible solo para dispositivos cliente basados en Windows.

   Se abre la ventana **Registros de seguimiento del dispositivo**, en la que se muestra una lista de archivos de seguimiento.
4. En la lista de archivos de seguimiento, seleccione uno o varios archivos que desee eliminar.
5. Haga clic en el botón **Eliminar**.

Los archivo de seguimiento seleccionados se eliminan.

Descargar la configuración de las aplicaciones

Para descargar la configuración de las aplicaciones instaladas en un dispositivo cliente:

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnóstico remoto, seleccione la pestaña **Aplicaciones de Kaspersky**.
3. En la sección **Configuración de las aplicaciones**, haga clic en el botón **Descargar** para descargar la información sobre la configuración de las aplicaciones instaladas en el dispositivo cliente.

En la ubicación especificada, se descarga el archivo ZIP con la información.

Descargar información del sistema desde un dispositivo cliente

Para descargar la información del sistema de un dispositivo cliente, siga los siguientes pasos:

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnóstico remoto, seleccione la pestaña **Información del sistema**.
3. Haga clic en el botón **Descargar** para descargar la información del sistema sobre el dispositivo cliente.

   Si obtiene información del sistema sobre un dispositivo basado en Linux, se agrega al archivo resultante un archivo de volcado para aplicaciones finalizadas de emergencia.

   El archivo comprimido puede contener datos confidenciales (por ejemplo, claves y contraseñas) en texto sin formato. Le recomendamos que revise los archivos incluidos en el archivo comprimido y elimine esos datos antes de enviarlo al servicio de Soporte técnico de Kaspersky.

En la ubicación especificada, se descarga el archivo con la información.

Descargar registros de eventos

Para descargar un registro de eventos de un dispositivo remoto:

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnóstico remoto, en la pestaña **Registros de eventos**, haga clic en **Todos los registros del dispositivo**.
3. En la ventana **Todos los registros del dispositivo**, seleccione uno o varios registros que desee descargar.

4. Realice una de las siguientes acciones:

   - Si desea descargar el archivo de registro seleccionado, haga clic en **Descargar archivo completo**.
   - Si desea descargar una parte del archivo de registro seleccionado, haga lo siguiente:

     a. Haga clic en **Descargar una parte**.

     No puede descargar partes de varios registros al mismo tiempo. Si selecciona más de un registro de eventos, se deshabilita el botón **Descargar una parte**.

     b. En la ventana que se abre, indique el nombre y la parte del registro que desee descargar.

     Para dispositivos basados en Linux, no está disponible la edición del nombre del registro.

     c. Haga clic en **Descargar**.

El registro de eventos seleccionado, o la parte seleccionada, se descarga en la ubicación especificada.

Iniciar, detener o reiniciar la aplicación

Puede iniciar, detener y reiniciar las aplicaciones instaladas en los dispositivos cliente.

Para iniciar, detener o reiniciar una aplicación:

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnóstico remoto, seleccione la pestaña **Aplicaciones de Kaspersky**.

   En la sección **Administración de aplicaciones**, se muestra la lista de aplicaciones de Kaspersky instaladas en el dispositivo.
3. En la lista de aplicaciones, seleccione la aplicación que desee iniciar, detener o reiniciar.
4. Haga clic en uno de los siguientes botones para realizar la acción correspondiente:

   - **Detener la aplicación**

     Este botón solo estará disponible si la aplicación se encuentra en ejecución.
   - **Reiniciar aplicación**

     Este botón solo estará disponible si la aplicación se encuentra en ejecución.
   - **Iniciar la aplicación**

     Este botón solo estará disponible si la aplicación no se encuentra en ejecución.

   Dependiendo de la acción que haya elegido, la aplicación seleccionada se iniciará, se detendrá o se reiniciará en el dispositivo cliente.

Si elige reiniciar el Agente de red, se le advertirá que la conexión entre el dispositivo y el Servidor de administración se cerrará.

Realizar un diagnóstico remoto del Agente de red de Kaspersky Security Center Linux y descargar los resultados

Para realizar un diagnóstico del Agente de red de Kaspersky Security Center Linux en un dispositivo remoto y descargar los resultados:

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnóstico remoto, seleccione la pestaña **Aplicaciones de Kaspersky**.

   En la sección **Administración de aplicaciones**, se muestra la lista de aplicaciones de Kaspersky instaladas en el dispositivo.
3. En la lista de aplicaciones, seleccione **Agente de red de Kaspersky Security Center Linux**.

   Se abre la lista de opciones de diagnóstico remoto.
4. En la sección **Informe de diagnóstico**, haga clic en el botón **Ejecutar diagnóstico**.

   Se iniciará el proceso de diagnóstico remoto y se generará un informe con el resultado. Cuando se complete el proceso, la aplicación le permitirá hacer clic en el botón **Descargar informe de diagnóstico**.
5. Haga clic en el botón **Descargar informe de diagnóstico** para descargar el informe.

En la ubicación especificada, se descarga el archivo.

Ejecutar una aplicación en un dispositivo cliente

Ocasionalmente, el personal técnico de Kaspersky puede pedirle que ejecute una aplicación en un dispositivo cliente. Si esto sucede, no es necesario que instale la aplicación en el dispositivo cliente.

Si desea ejecutar un script personalizado en el dispositivo cliente, puede utilizar la variable de entorno `KLACDT_SAVE_SETTING` para determinar la ruta donde se guardarán los resultados de la ejecución. Por ejemplo:

- Para un dispositivo Windows:

  ```
  @echo some result > %KLACDT_SAVE_SETTING%\res.log
  ```

- Para un dispositivo Linux:

  ```
  echo some result > $KLACDT_SAVE_SETTING/res.log
  ```

Para ejecutar una aplicación en un dispositivo cliente:

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnóstico remoto, seleccione la pestaña **Ejecución de una aplicación remota**.

3. En el campo **Tipo de objeto**, seleccione el tipo de objeto que desea cargar:

   - Seleccione **Archivo** para cargar el archivo ejecutable.
   - Seleccione **Carpeta** para cargar la carpeta que contiene la aplicación que desea ejecutar en el dispositivo cliente.

     Si selecciona este tipo de objeto, aparecerá el campo **Nombre del archivo ejecutable que debe ejecutarse**. En este campo, especifique el nombre del archivo ejecutable en la carpeta. También puede especificar la ruta relativa al archivo.
   - Seleccione **Archivo comprimido** para cargar el archivo ZIP que contiene la aplicación que desea ejecutar en el dispositivo cliente.

     Si selecciona este tipo de objeto, aparecerá el campo **Nombre del archivo ejecutable que debe ejecutarse**. En este campo, especifique el nombre del archivo ejecutable en la carpeta. También puede especificar la ruta relativa al archivo.

     El archivo ZIP debe incluir la carpeta de la utilidad. Esta carpeta contiene el archivo ejecutable que se ejecuta en un dispositivo remoto.

4. Para cargar el objeto, selecciónelo en la ventana del sistema o arrástrelo al campo de carga.
5. Si es necesario, en el campo **Argumentos para la línea de comandos**, especifique los argumentos de la línea de comando que se pasarán al ejecutar el archivo ejecutable.
6. Haga clic en el botón **Cargar y ejecutar** para ejecutar la aplicación seleccionada en un dispositivo cliente.
7. Una vez completada con éxito la ejecución de la aplicación, descargue los resultados haciendo clic en el botón **Descargar los resultados de la ejecución de la aplicación**.

   Los resultados de la ejecución de la aplicación se almacenan hasta que ejecute un nuevo diagnóstico o cierre la ventana.

Se completó el diagnóstico remoto del dispositivo cliente mediante la aplicación.

Ejecución de diagnósticos remotos en un dispositivo cliente basado en Linux

Kaspersky Security Center Linux le permite descargar la información de diagnóstico básica desde un dispositivo cliente. Como alternativa, puede obtener información de diagnóstico sobre un dispositivo basado en Linux utilizando el script collect.sh de Kaspersky. Este script debe ejecutarse en el dispositivo cliente basado en Linux que necesita ser diagnosticado. A continuación, se crea un archivo con información de diagnóstico, información del sistema del dispositivo, archivos de seguimiento de la aplicación, registros de eventos del dispositivo y un archivo de volcado de fallos y procesos terminados.

Le recomendamos que utilice el script collect.sh para obtener toda la información de diagnóstico sobre el dispositivo cliente basado en Linux a la vez. Si descarga la información de diagnóstico de forma remota a través de Kaspersky Security Center Linux, deberá revisar todas las secciones de la interfaz de diagnóstico remoto. Además, es probable que la información de diagnóstico de un dispositivo basado en Linux no se obtenga por completo.

Si necesita enviar el archivo generado con la información de diagnóstico al Servicio de soporte técnico de Kaspersky, elimine toda la información confidencial antes de enviar el archivo.

Para descargar la información de diagnóstico desde un dispositivo cliente basado en Linux mediante el script collect.sh:

1. Descargue el script collect.sh comprimido en el archivo collect.tar.gz.
2. Copie el archivo descargado en el dispositivo cliente basado en Linux que necesita ser diagnosticado.
3. Ejecute el siguiente comando para descomprimir el archivo collect.tar.gz:

   ```
   # tar -xzf collect.tar.gz
   ```

4. Ejecute el siguiente comando para especificar los derechos de ejecución del script:

   ```
   # chmod +x collect.sh
   ```

5. Ejecute el script collect.sh utilizando una cuenta con derechos de administrador:

   ```
   # ./collect.sh
   ```

Se genera un archivo con la información de diagnóstico y se guarda en la carpeta /tmp/$HOST_NAME-collect.tar.gz.

Administrar aplicaciones y archivos ejecutables en dispositivos cliente

En esta sección se describen las funciones de Kaspersky Security Center Linux relacionadas con la administración de aplicaciones y archivos ejecutables de terceros que se ejecuten en dispositivos cliente.

Uso de Control de aplicaciones para administrar archivos ejecutables

Puede utilizar el componente Control de aplicaciones para permitir o bloquear el inicio de archivos ejecutables en los dispositivos del usuario. El componente Control de aplicaciones es compatible con sistemas operativos Windows y Linux.

El componente Control de aplicaciones para sistemas operativos basados en Linux está disponible a partir de Kaspersky Endpoint Security 11.2 for Linux.

Requisitos previos

- Kaspersky Security Center Linux se implementó en su organización.
- Se ha creado y activado una directiva para Kaspersky Endpoint Security for Linux o Kaspersky Endpoint Security para Windows. El componente Control de aplicaciones está habilitado en la directiva.

Etapas

El procedimiento de uso de Control de aplicaciones consta de etapas:

1. **Crear y ver la lista de archivos ejecutables almacenados en los dispositivos cliente**

   En esta etapa, podrá descubrir qué archivos ejecutables se encuentran guardados en los dispositivos administrados. Revise la lista de archivos ejecutables y compárela con las listas de archivos ejecutables permitidos y prohibidos. Las restricciones sobre el uso de archivos ejecutables pueden estar vinculadas a las políticas de seguridad de la información de su organización.

   Instrucciones: Obtener y ver una lista de archivos ejecutables instalados en los dispositivos cliente

2. **Creación de categorías para archivos ejecutables utilizados en la organización**

   Analice las listas de aplicaciones y archivos ejecutables almacenados en los dispositivos administrados. Cree las categorías para archivos ejecutables en función del análisis. Recomendamos crear una categoría llamada "Aplicaciones de trabajo" que cubra los archivos ejecutables estándar que se utilicen en la organización. Luego, si tiene grupos de seguridad diferentes que trabajan con sus propios archivos ejecutables, puede crear una categoría independiente para cada grupo de seguridad.

El inicio de archivos ejecutables cuya configuración no coincide con ninguna de las reglas de Control de aplicaciones está regulado por el modo de funcionamiento seleccionado del componente:

- *Lista de rechazados*. En este modo, se permite la ejecución de cualquier archivo ejecutable, excepto los que se especifican en las reglas de bloqueo. Este modo está seleccionado de forma predeterminada.
- *Lista de admitidos*. En este modo, se impide la ejecución de todos los archivos ejecutables, excepto los que se especifican en las reglas de autorización.

Las reglas de Control de aplicaciones se implementan en todas las categorías de archivos ejecutables. En Kaspersky Security Center Linux, hay tres tipos de categorías de archivos ejecutables:

- Categorías con contenido agregado de forma manual. Para sumar archivos ejecutables a una categoría de este tipo, deberá definir distintas condiciones: metadatos del archivo, código hash del archivo, certificado del archivo, ruta de acceso al archivo, etc.
- Categoría que incluye los archivos ejecutables de los dispositivos seleccionados. Para crear una categoría de este tipo, deberá seleccionar un dispositivo. Los archivos ejecutables de ese dispositivo se agregarán a la categoría automáticamente.
- Categoría que incluye archivos ejecutables de la carpeta seleccionada. Especifica una carpeta cuyos archivos ejecutables se incluirán automáticamente dentro de la categoría.

3 Configurar Control de aplicaciones en la directiva de Kaspersky Endpoint Security

Configure el componente Control de aplicaciones en la directiva de Kaspersky Endpoint Security for Linux utilizando las categorías que creó en la etapa anterior.

Instrucciones: Configurar Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows

4 Activar el componente Control de aplicaciones en modo de prueba

Las reglas de Control de aplicaciones no deben bloquear los archivos ejecutables que los usuarios necesiten para trabajar. Para asegurarse de que esto sea así, cuando cree nuevas reglas de Control de aplicaciones, recomendamos que habilite un modo de prueba y analice el funcionamiento de las reglas. Mientras este modo esté habilitado, Kaspersky Endpoint Security para Windows no bloqueará los archivos ejecutables que las reglas de Control de aplicaciones no permitan iniciar, sino que simplemente notificará al Servidor de administración que tales archivos se iniciaron.

Para probar las reglas de Control de aplicaciones, recomendamos que haga lo siguiente:

- Defina la duración del período de prueba. El período de prueba puede durar de varios días a dos meses.
- Examine los eventos que surjan de probar el funcionamiento de Control de aplicaciones.

Instrucciones para Kaspersky Security Center Web Console: Configuración del componente Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows. Siga estas instrucciones y habilite la opción **Modo de prueba** en el proceso de configuración.

5 Cambiar la configuración del componente Control de aplicaciones

De ser necesario, modifique la configuración de Control de aplicaciones. Con los resultados de las pruebas, puede crear una categoría con contenido agregado manualmente que incluya los archivos ejecutables vinculados a los eventos de Control de aplicaciones.

Instrucciones: Kaspersky Security Center Web Console: Agregar archivos ejecutables vinculados a eventos a una categoría de aplicaciones

6. **Aplicar las reglas de Control de aplicaciones en modo de funcionamiento normal**

   Después de probar las reglas de Control de aplicaciones y completar la configuración de las categorías, podrá aplicar las reglas de Control de aplicaciones en el modo de operación.

   Instrucciones para Kaspersky Security Center Web Console: Configuración del componente Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows. Siga estas instrucciones y deshabilite la opción **Modo de prueba** en el proceso de configuración.

7. **Verificar la configuración de Control de aplicaciones**

   Asegúrese de haber hecho lo siguiente:

   - Categorías de archivos ejecutables creadas.
   - Configuración de Control de aplicaciones con las categorías.
   - Aplicar las reglas de Control de aplicaciones en el modo de operación.

Resultados

Al concluir este escenario, el inicio de archivos ejecutables en los dispositivos administrados estará bajo su control. Los usuarios pueden iniciar solo aquellos archivos ejecutables que están permitidos en su organización y no pueden iniciar los que están prohibidos.

Para obtener información detallada sobre Control de aplicaciones, consulte la Ayuda de Kaspersky Endpoint Security for Linux y la Ayuda de Kaspersky Endpoint Security para Windows.

Obtención y visualización de una lista de archivos ejecutables almacenados en los dispositivos cliente

Puede obtener la lista de archivos ejecutables almacenados en los dispositivos cliente de una de las siguientes maneras:

- Habilitando las notificaciones sobre el inicio de aplicaciones en la directiva de Kaspersky Endpoint Security.
- Creando una tarea de inventario.

Habilitando las notificaciones sobre el inicio de aplicaciones en la directiva de Kaspersky Endpoint Security

Para habilitar las notificaciones sobre la ejecución de aplicaciones:

1. Abra la configuración de la directiva de Kaspersky Endpoint Security y luego vaya a **Configuración general** → **Informes y almacenamiento**.
2. En el grupo de configuración **Transferencia de datos al servidor de administración**, seleccione la casilla de verificación **Acerca de las aplicaciones iniciadas** y guarde los cambios.

Cuando un usuario intenta iniciar archivos ejecutables, la información sobre estos archivos se añade a la lista de archivos ejecutables en el dispositivo cliente. Kaspersky Endpoint Security envía esta información al Agente de red, que a su vez la envía al Servidor de administración.

Crear una tarea de inventario

En Kaspersky Endpoint Security for Linux, la función de inventariado de archivos ejecutables está disponible desde la versión 11.2.

Puede reducir la carga a la que se somete la base de datos cuando se obtiene información sobre las aplicaciones instaladas. Para ahorrar espacio en la base de datos, recomendamos que ejecute una tarea de inventario en los dispositivos de referencia que tengan instalada una selección de aplicaciones estándar. El número preferible de dispositivos es de 1 a 3.

Para crear una tarea que haga un inventario de los archivos ejecutables instalados en los dispositivos cliente:

1. En el menú principal, vaya a **Tareas**.

   Se muestra la lista de tareas.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Siga los pasos del asistente.
3. En la página **Configuración de tarea nueva**, abra la lista desplegable **Aplicación** y seleccione Kaspersky Endpoint Security for Linux o Kaspersky Endpoint Security para Windows, dependiendo del sistema operativo instalado en los dispositivos cliente.
4. En la lista desplegable **Tipo de tarea**, seleccione **Inventario**.
5. En la página **Finalizar la creación de la tarea**, haga clic en el botón **Finalizar**.

Una vez que finalice el Asistente para crear nueva tarea, se creará y configurará la tarea **Inventario**. Si lo desea, puede cambiar la configuración de la tarea creada. Encontrará la nueva tarea en la lista de tareas.

Para obtener una descripción detallada de la tarea de inventario, consulte la Ayuda de Kaspersky Endpoint Security for Linux y la Ayuda de Kaspersky Endpoint Security para Windows.

Una vez efectuada la tarea **Inventario**, se crea la lista de archivos ejecutables almacenados en los dispositivos administrados para que pueda verla.

Durante el inventario, se pueden detectar archivos ejecutables en los siguientes formatos (dependiendo de la opción que seleccione en las propiedades de la tarea de inventario): MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR y HTML.

Consultar las listas de archivos ejecutables almacenados en los dispositivos administrados

Para visualizar la lista de los archivos ejecutables almacenados en los dispositivos cliente, haga lo siguiente:

En el menú principal, vaya a **Administración de software** → **Aplicaciones de terceros** → **Archivos ejecutables**.

La página muestra la lista de los archivos ejecutables almacenados en los dispositivos cliente.

Si es necesario, puede enviar el archivo ejecutable del dispositivo administrado al dispositivo donde está abierta su Kaspersky Security Center Web Console.

Para enviar un archivo ejecutable:

1. En el menú principal, vaya a **Administración de software** → **Aplicaciones de terceros** → **Archivos ejecutables**.
2. Haga clic en el enlace del archivo ejecutable que desea enviar.
3. En la ventana que se abre, vaya a **Dispositivos** y seleccione la casilla del dispositivo administrado desde el que desea enviar el archivo ejecutable.

   Antes de enviar el archivo ejecutable, asegúrese de que el dispositivo administrado tiene una conexión directa con el Servidor de administración, seleccionando la casilla de verificación **No desconectar del Servidor de administración**.

4. Haga clic en el botón **Enviar**.

   El archivo ejecutable seleccionado se descarga para su posterior envío al dispositivo donde está abierta Kaspersky Security Center Web Console.

Creación de una categoría de aplicaciones con contenido agregado manualmente

Puede especificar un conjunto de criterios que sean comunes a los archivos ejecutables que los usuarios podrán o no podrán iniciar en su organización. Puede agregar los archivos que respondan a estos criterios a una nueva categoría de aplicaciones. Más tarde, podrá usar esa nueva categoría para configurar el componente Control de aplicaciones.

Para crear una categoría de aplicaciones con contenido agregado manualmente:

1. En el menú principal, vaya a **Administración de software → Aplicaciones de terceros → Categorías de aplicaciones**.

   Se muestra una página con una lista de categorías de aplicaciones.

2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva categoría. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

3. En el paso **Seleccione un método para crear la categoría**, especifique el nombre de la categoría de aplicaciones y seleccione la opción **Categoría con contenido agregado de forma manual. Los datos de los archivos ejecutables se agregan de forma manual a la categoría**.

4. En el paso **Condiciones**, haga clic en el botón **Agregar** para agregar un criterio de condición e incluir archivos en la categoría de creación.

5. En el paso **Criterios de la condición**, haga lo siguiente:

   a. Seleccione un tipo de regla para la creación de la categoría:

   - **De la categoría KL**

     Seleccione esta opción si, como condición para agregar aplicaciones a la categoría personalizada, desea elegir una categoría de aplicaciones de Kaspersky. Las aplicaciones que pertenezcan a la categoría de Kaspersky elegida se agregarán a la categoría de aplicaciones personalizada.

   - **Seleccionar el certificado del repositorio**

     Seleccione esta opción para elegir certificados almacenados en el repositorio. La condición de la categoría solo coincide con los archivos ejecutables que están firmados por el certificado especificado.

     Los certificados se agregan al repositorio si creó e inició una tarea de inventario o marcó la casilla **Acerca de las aplicaciones iniciadas** en la directiva de Kaspersky Endpoint Security. Puede realizar ambas acciones.

     > La información sobre certificados solo se puede extraer de archivos ejecutables en formato PE (.exe, .dll, .sys).

   - **Especificar la ruta a la aplicación (se pueden usar máscaras)**

     Seleccione esta opción para especificar la ruta a una carpeta del dispositivo cliente que contenga los archivos ejecutables que quiera agregar a la categoría de aplicaciones personalizada.

   - **Unidad extraíble**

     Seleccione esta opción para especificar el tipo de soporte (unidad extraíble o cualquier tipo de unidad) desde el que se ejecuta la aplicación. Las aplicaciones que se inicien desde el tipo de unidad seleccionado se agregarán a la categoría de aplicaciones personalizada.

   - **Hash, metadatos o certificado**:

     - **Seleccionar de la lista de archivos ejecutables**

       Seleccione esta opción si desea elegir las aplicaciones que se agregarán a la categoría de la lista de archivos ejecutables almacenados en el dispositivo cliente.

- **Seleccionar del registro de aplicaciones**

  Si selecciona esta opción, se abrirá el registro de aplicaciones. Después de seleccionar una aplicación del registro, se abre la ventana con los parámetros llenos de metadatos de la aplicación que seleccionó:

  - Nombre del archivo.
  - Versión del archivo. Puede indicar el número de versión exacto o introducir una condición, como "superior a 5.0".
  - Nombre de la aplicación.
  - Versión de la aplicación. Puede indicar el número de versión exacto o introducir una condición, como "superior a 5.0".
  - Proveedor.

  Tenga en cuenta que solo se bloquea la ejecución de archivos ejecutables que cumplan con los parámetros especificados, no la ejecución de la aplicación que seleccione. Si los metadatos de la aplicación seleccionada coinciden con el del archivo ejecutable que se ejecuta al iniciar la aplicación, puede continuar con el siguiente paso. De lo contrario, debe cambiar los valores manualmente para que coincidan con los metadatos del archivo ejecutable.

- **Especificar manualmente**

  Selecciona esta opción para especificar los metadatos, el certificado o el hash de archivo que se tomarán como condición para agregar aplicaciones a la categoría personalizada.

  Hash de archivo

  Según la versión de la aplicación de seguridad instalada en los dispositivos en su red, debe seleccionar un algoritmo para que Kaspersky Security Center Linux calcule el valor de hash para archivos en esta categoría. La información sobre los valores hash calculados por las funciones hash se almacena en la base de datos del Servidor de administración.

  SHA256 es una función de hash criptográfica. En la actualidad, se la considera la más confiable en su clase, pues no se encontró vulnerabilidad alguna en su algoritmo. Kaspersky Endpoint Security for Linux es compatible con la computación SHA256.

  Seleccione cualquiera de las opciones de evaluación del valor de hash de Kaspersky Security Center Linux para archivos en la categoría:

  - Si todas las instancias de aplicaciones de seguridad instaladas en su red son Kaspersky Endpoint Security para Linux o versiones posteriores, marque la casilla **SHA256**.
  - Marque la casilla **Hash MD5** solo si utiliza Kaspersky Endpoint Security para Windows. Kaspersky Endpoint Security para Linux no admite una función hash MD5.

  Metadatos

  Seleccione esta opción si desea especificar los metadatos de los archivos (nombre, versión, proveedor, etc.). La condición de la categoría solo coincide con los archivos ejecutables que tienen los mismos metadatos.

  Certificado

  Seleccione esta opción para elegir certificados almacenados en el repositorio. La condición de la categoría solo coincide con los archivos ejecutables que están firmados por el certificado especificado.

  Los certificados se agregan al repositorio si creó e inició una tarea de inventario o marcó la casilla **Acerca de las aplicaciones iniciadas** en la directiva de Kaspersky Endpoint Security. Puede realizar ambas acciones.

- **De la carpeta comprimida**

  Si se selecciona esta opción, puede especificar un archivo de una carpeta archivada y luego seleccionar qué condición desea usar para agregar aplicaciones a la categoría de usuario. La carpeta archivada se descomprime y las condiciones que seleccione se aplican a los archivos de la carpeta. Puede seleccionar una de las siguientes opciones como condición:

  - **Hash de archivo**

    Usted selecciona qué función hash (MD5 o SHA256) desea usar para calcular los valores hash. Las aplicaciones que tienen los mismos hashes que los archivos en la carpeta especificada se agregan a la categoría de aplicaciones del usuario.

    Seleccione una función hash MD5 solo si utiliza Kaspersky Endpoint Security para Windows. Kaspersky Endpoint Security para Linux no admite una función hash MD5.

  - **Metadatos**

    Usted selecciona qué metadatos desea utilizar como criterio. Los archivos ejecutables que contienen los mismos metadatos se agregarán a la categoría de aplicaciones del usuario.

  - **Certificado**

    Seleccione qué propiedades del certificado (asunto del certificado, huella digital o emisor) desea utilizar como criterio. Los archivos ejecutables que se hayan firmado conforme a esos certificados se agregarán a la categoría personalizada.

  Los criterios de los **Metadatos** y **Certificado** deben especificarse manualmente después de cargar un archivo o una carpeta comprimida si desea usar estos criterios.

Si se selecciona esta opción, puede especificar un archivo de una carpeta archivada y luego seleccionar qué condición desea usar para agregar aplicaciones a la categoría de usuario. La carpeta archivada se descomprime y las condiciones que seleccione se aplican a los archivos de la carpeta. Puede seleccionar una de las siguientes opciones como condición:

- **Hash de archivo**

  Usted selecciona qué función hash (MD5 o SHA256) desea usar para calcular los valores hash. Las aplicaciones que tienen los mismos hashes que los archivos en la carpeta especificada se agregan a la categoría de aplicaciones del usuario.

  Seleccione una función hash MD5 solo si utiliza Kaspersky Endpoint Security para Windows. Kaspersky Endpoint Security para Linux no admite una función hash MD5.

- **Metadatos**

  Usted selecciona qué metadatos desea utilizar como criterio. Los archivos ejecutables que contienen los mismos metadatos se agregarán a la categoría de aplicaciones del usuario.

- **Certificado**

  Seleccione qué propiedades del certificado (asunto del certificado, huella digital o emisor) desea utilizar como criterio. Los archivos ejecutables que se hayan firmado conforme a esos certificados se agregarán a la categoría personalizada.

Los criterios de los **Metadatos** y**Certificado** deben especificarse manualmente después de cargar un archivo o una carpeta comprimida si desea usar estos criterios.

b. Si es necesario, agregue un comentario en el campo **Descripción**. El número de símbolos no puede exceder los 1000.

Más adelante, podrá editar o eliminar el comentario. Para hacerlo, en las propiedades de la categoría de aplicaciones, abra la pestaña **Condiciones** y, en la columna **Criterio de la condición**, haga clic en el vínculo de la condición cuyo comentario desea editar o eliminar.

> Cuando selecciona el tipo de regla **De la categoría KL**, puede agregar un comentario para todas las condiciones que se crearán en función de este tipo de regla. Puede editar o eliminar el comentario para cada condición por separado.

El criterio seleccionado se agrega a la lista de condiciones.

Puede agregar tantos criterios como necesite para la categoría de aplicaciones que se está creando.

6. En el paso **Exclusiones**, haga clic en el botón **Agregar** para agregar un criterio de condición excluyente que permita excluir archivos de la nueva categoría.

   Si es necesario, puede agregar un comentario en el campo **Descripción**. El número de símbolos no puede exceder los 1000.

   Más adelante, podrá editar o eliminar el comentario. Para hacerlo, en las propiedades de la categoría de aplicaciones, abra la pestaña **Exclusiones** y, en la columna **Criterio de la condición**, haga clic en el vínculo de la condición cuyo comentario desea editar o eliminar.

7. En el paso **Criterios de la condición**, seleccione un tipo de regla tal como lo hizo al elegir un tipo de regla para crear la categoría.

Cuando finaliza el asistente, la categoría de aplicaciones se crea y se muestra en la lista de categorías de aplicaciones. Podrá usar la nueva categoría cuando configure Control de aplicaciones.

Para obtener información detallada sobre Control de aplicaciones, consulte la Ayuda de Kaspersky Endpoint Security for Linux y la Ayuda de Kaspersky Endpoint Security para Windows.

Crear una categoría de aplicaciones con archivos ejecutables de dispositivos específicos

Puede usar archivos ejecutables almacenados en ciertos dispositivos puntuales como modelo de los archivos ejecutables que quiera permitir o bloquear. Los archivos ejecutables de estos dispositivos pueden servirle de base para crear una categoría de aplicaciones, que luego podrá usar en la configuración del componente Control de aplicaciones.

Asegúrese de que se cumplan los siguientes requisitos previos:

- El componente Control de aplicaciones está habilitado en la directiva de Kaspersky Endpoint Security.
- Se obtuvo una lista de los archivos ejecutables almacenados en los dispositivos administrados.

Para crear una categoría de aplicaciones que incluya archivos ejecutables de dispositivos seleccionados:

1. En el menú principal, vaya a **Administración de software → Aplicaciones de terceros → Categorías de aplicaciones**.

   Se muestra una página con la lista de categorías de archivos ejecutables.

2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva categoría. Utilice el botón **Next** para avanzar a un nuevo paso del asistente.

3. En el paso **Seleccione un método para crear la categoría**, especifique el nombre de la categoría y seleccione la opción **Categoría que incluye los archivos ejecutables de los dispositivos seleccionados. Estos archivos ejecutables se procesan de forma automática y sus métricas se agregan a la categoría**.

4. Haga clic en **Agregar**.

5. En la ventana que se abre, seleccione el dispositivo que contenga los archivos ejecutables que desee usar para crear la categoría de aplicaciones. Puede seleccionar más de un dispositivo.

6. Configure los siguientes ajustes:

   - **Algoritmo de evaluación del valor de hash**

     Según la versión de la aplicación de seguridad instalada en los dispositivos en su red, debe seleccionar un algoritmo para que Kaspersky Security Center Linux calcule el valor de hash para archivos en esta categoría. La información sobre los valores hash calculados por las funciones hash se almacena en la base de datos del Servidor de administración.

     SHA256 es una función de hash criptográfica. En la actualidad, se la considera la más confiable en su clase, pues no se encontró vulnerabilidad alguna en su algoritmo. Kaspersky Endpoint Security for Linux es compatible con la computación SHA256.

     Seleccione cualquiera de las opciones de evaluación del valor de hash de Kaspersky Security Center Linux para archivos en la categoría:

     - Si todas las instancias de aplicaciones de seguridad instaladas en su red son Kaspersky Endpoint Security para Linux o versiones posteriores, marque la casilla **SHA256**.

     Marque la casilla **Hash MD5** solo si utiliza Kaspersky Endpoint Security para Windows. Kaspersky Endpoint Security para Linux no admite una función hash MD5.

     La casilla **Calcular SHA256 para los archivos de esta categoría (compatible con Kaspersky Endpoint Security 10 Service Pack 2 para Windows y versiones posteriores)** está activada de manera predeterminada.

     De manera predeterminada, la casilla **Calcular MD5 para los archivos de esta categoría (compatible con versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows)** está desactivada.

   - **Sincronizar datos con el repositorio del Servidor de administración**

     Seleccione esta opción si desea que el Servidor de administración verifique periódicamente si ha habido cambios en la(s) carpeta(s) especificada(s).

     Esta opción está deshabilitada de forma predeterminada.

     Si habilita esta opción, indique la frecuencia (en horas) con la que se llevará a cabo la verificación. Por defecto, se realiza una búsqueda de cambios cada veinticuatro horas.

   - **Tipo de archivo**

     Utilice esta sección para especificar qué clase de archivos se usarán para crear la categoría de aplicaciones.

     Todos los archivos. Para crear la categoría, se tendrán en cuenta todos los archivos. Esta opción está seleccionada de forma predeterminada.

     Solo archivos fuera de las categorías de aplicaciones. Para crear la categoría, solo se tendrán en cuenta los archivos que no estén incluidos en las categorías de aplicaciones.

- **Carpetas**

  Utilice esta sección para elegir las carpetas del dispositivo (o de los dispositivos) que contengan los archivos que se usarán para crear la categoría de aplicaciones.

  Todas las carpetas. Para crear la categoría, se tendrán en cuenta todas las carpetas. Esta opción está seleccionada de forma predeterminada.

  Carpeta especificada: Para crear la categoría, solo se tendrá en cuenta la carpeta especificada. Si selecciona esta opción, deberá especificar la ruta a la carpeta.

Cuando finaliza el asistente, se crea la categoría de archivos ejecutables y se muestra en la lista de categorías. Podrá usar la categoría creada cuando configure Control de aplicaciones.

Creación de una categoría de aplicaciones que incluya archivos ejecutables de una carpeta seleccionada

Puede usar archivos ejecutables de una carpeta seleccionada como el estándar de archivos ejecutables que desea permitir o bloquear en su organización. Sobre la base de los archivos ejecutables de la carpeta seleccionada, puede crear una categoría de aplicaciones y usarla en la configuración del componente Control de aplicaciones.

Para crear una categoría que incluya archivos ejecutables de la carpeta seleccionada, haga lo siguiente:

1. En el menú principal, vaya a **Administración de software → Aplicaciones de terceros → Categorías de aplicaciones**.

   Se muestra una página con una lista de categorías.

2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva categoría. Utilice el botón **Next** para avanzar a un nuevo paso del asistente.

3. En el paso **Seleccione un método para crear la categoría**, especifique el nombre de la categoría y seleccione la opción **Categoría con los archivos ejecutables de una carpeta específica. Los archivos ejecutables de aplicaciones presentes en la carpeta especificada se procesan automáticamente y sus métricas se agregan a la categoría**.

4. Especifique la carpeta con los archivos ejecutables que se utilizarán para crear la categoría.

5. Configure los siguientes parámetros:

   - **Incluir DLL en esta categoría**

     La categoría de aplicaciones incluye bibliotecas de enlace dinámico (archivos en el formato de DLL) y el componente Control de aplicaciones registra las acciones de esas bibliotecas que se ejecutan en el sistema. Incluir archivos DLL en la categoría podría reducir el rendimiento de Kaspersky Security Center Linux.

     Esta casilla está desactivada por defecto.

   - **Incluir datos de scripts en esta categoría**

     La categoría de aplicaciones incluye datos sobre scripts, y los scripts no son bloqueados por el componente Protección contra amenazas web. Incluir los datos del script en la categoría podría reducir el rendimiento de Kaspersky Security Center Linux.

     Esta casilla está desactivada por defecto.

- **Algoritmo de evaluación del valor de hash**: **Calcular SHA256 para los archivos de esta categoría/Calcular hashes MD5 para los archivos de esta categoría**

  Según la versión de la aplicación de seguridad instalada en los dispositivos en su red, debe seleccionar un algoritmo para que Kaspersky Security Center Linux calcule el valor de hash para archivos en esta categoría. La información sobre los valores hash calculados por las funciones hash se almacena en la base de datos del Servidor de administración.

  SHA256 es una función de hash criptográfica. En la actualidad, se la considera la más confiable en su clase, pues no se encontró vulnerabilidad alguna en su algoritmo. Kaspersky Endpoint Security for Linux es compatible con la computación SHA256.

  Seleccione cualquiera de las opciones de evaluación del valor de hash de Kaspersky Security Center Linux para archivos en la categoría:

  - Si todas las instancias de aplicaciones de seguridad instaladas en su red son Kaspersky Endpoint Security para Linux o versiones posteriores, marque la casilla **SHA256**.

  Marque la casilla **Hash MD5** solo si utiliza Kaspersky Endpoint Security para Windows. Kaspersky Endpoint Security para Linux no admite una función hash MD5.

  La casilla **Calcular SHA256 para los archivos de esta categoría (compatible con Kaspersky Endpoint Security 10 Service Pack 2 para Windows y versiones posteriores)** está activada de manera predeterminada.

  De manera predeterminada, la casilla **Calcular MD5 para los archivos de esta categoría (compatible con versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows)** está desactivada.

- **Forzar análisis de cambios en carpeta**

  Si se habilita esta opción, la aplicación buscará con frecuencia cambios en la carpeta de incorporación de contenido de categorías. Puede especificar la frecuencia de las búsquedas (en horas) en el campo de entrada que se encuentra al lado de la casilla de verificación. De forma predeterminada, el intervalo entre búsquedas forzadas es de 24 horas.

  Si se deshabilita esta opción, la aplicación no forzará la búsqueda en la carpeta. El servidor intenta acceder a los archivos si se modificaron, agregaron o eliminaron.

  Esta opción está deshabilitada de forma predeterminada.

Cuando finaliza el asistente, se crea la categoría de archivos ejecutables y se muestra en la lista de categorías. Puede usar la categoría en la configuración de Control de aplicaciones.

Para obtener información detallada sobre Control de aplicaciones, consulte la Ayuda de Kaspersky Endpoint Security for Linux y la Ayuda de Kaspersky Endpoint Security para Windows.

Visualización de la lista de categorías de aplicaciones

Puede ver la lista de las categorías configuradas de los archivos ejecutables y la configuración de cada una.

Para ver la lista de categorías de aplicaciones:

En el menú principal, vaya a **Administración de software → Aplicaciones de terceros → Categorías de aplicaciones**.

Se muestra una página con una lista de categorías.

Para ver las propiedades de una categoría de aplicaciones:

Haga clic en el nombre de la categoría.

Se muestra la ventana de propiedades de la categoría. Las propiedades se agrupan en varias pestañas.

Agregar archivos ejecutables vinculados a eventos a una categoría de aplicaciones

Una vez que configure el componente Control de aplicaciones en las directivas de Kaspersky Endpoint Security, encontrará los siguientes eventos en la lista de eventos:

- **Inicio de aplicación prohibido** (evento de nivel *Crítico*). Este evento se muestra si Control de aplicaciones se ha configurado para hacer cumplir sus reglas.
- **Inicio de aplicación prohibido en el modo de prueba** (evento de nivel *Información*). Este evento se muestra si Control de aplicaciones se ha configurado para aplicar sus reglas en modo de prueba.
- **Mensaje para el administrador sobre la prohibición de inicio de la aplicación** (evento de *Advertencia*). Este evento aparece si Control de aplicaciones se ha configurado para hacer cumplir sus reglas y un usuario ha solicitado acceso a una aplicación que no tiene permitido ejecutar.

Recomendamos crear selecciones de eventos para ver los eventos relacionados con el funcionamiento de Control de aplicaciones.

Puede agregar los archivos ejecutables vinculados a los eventos de Control de aplicaciones a una categoría de aplicaciones nueva o existente. En cualquiera de los dos casos, la categoría debe ser una categoría de aplicaciones con contenido agregado manualmente.

Para agregar archivos ejecutables vinculados a los eventos de Control de aplicaciones a una categoría de aplicaciones:

1. En el menú principal, vaya a **Supervisión** → **Selecciones de eventos**.

   Se muestra la lista de selecciones de eventos.

2. Elija y genere una selección de eventos que le permita ver los eventos relacionados con Control de aplicaciones.

   Si no creó una selección de eventos relacionada con Control de aplicaciones, puede seleccionar y generar una de las selecciones predefinidas (por ejemplo, **Eventos recientes**).

   Se muestra la lista de eventos.

3. Seleccione los eventos asociados a los archivos ejecutables que desee agregar a la categoría de aplicaciones. A continuación, haga clic en el botón **Asignar a categoría**.

   Se inicia el Asistente para crear nueva categoría. Utilice el botón **Next** para avanzar a un nuevo paso del asistente.

4. En la página del asistente, configure los ajustes pertinentes:

- En la sección **Acción sobre archivo ejecutable relacionado con el evento**, seleccione una de las siguientes opciones:

  - **Agregar a una nueva categoría de aplicación**

    Seleccione esta opción si desea crear una nueva categoría de aplicaciones basada en los archivos ejecutables vinculados a los eventos.

    Esta opción está seleccionada de forma predeterminada.

    Si selecciona esta opción, escriba el nombre que tendrá la nueva categoría.

  - **Agregar a una categoría de aplicación existente**

    Seleccione esta opción si desea agregar los archivos ejecutables vinculados a los eventos a una categoría de aplicaciones existente.

    Esta opción no está seleccionada de manera predeterminada.

    Si selecciona esta opción, elija la categoría de aplicaciones con contenido agregado manualmente a la que desee agregar los archivos ejecutables.

- En la sección **Tipo de reglas**, seleccione una de las siguientes opciones:

  - **Reglas para agregar a inclusiones**

  - **Reglas para agregar a exclusiones**

- En la sección **Parámetro utilizado como condición**, seleccione una de las siguientes opciones:

  - **Detalles del certificado (o hashes SHA256 para archivos sin certificado)**

    Los archivos pueden estar firmados con un certificado. Cada certificado puede utilizarse para firmar más de un archivo. Un mismo certificado puede usarse para firmar distintas versiones de una misma aplicación, por ejemplo, o distintas aplicaciones de un mismo proveedor. Cuando seleccione un certificado, podría suceder que la categoría termine con varias versiones de una misma aplicación o con varias aplicaciones de un mismo proveedor.

    Cada archivo tiene su propia función hash SHA256. Si selecciona una función hash SHA256, solo se agregará a la categoría el archivo específico que se corresponda con ese hash (por ejemplo, la versión especificada de la aplicación).

    Seleccione esta opción si desea agregar los detalles del certificado de un archivo ejecutable (o la función hash SHA256 de los archivos sin certificado) a las reglas de la categoría.

    Esta opción está seleccionada de forma predeterminada.

  - **Detalles del certificado (los archivos sin certificado se omitirán)**

    Los archivos pueden estar firmados con un certificado. Cada certificado puede utilizarse para firmar más de un archivo. Un mismo certificado puede usarse para firmar distintas versiones de una misma aplicación, por ejemplo, o distintas aplicaciones de un mismo proveedor. Cuando seleccione un certificado, podría suceder que la categoría termine con varias versiones de una misma aplicación o con varias aplicaciones de un mismo proveedor.

    Seleccione esta opción si desea agregar los detalles del certificado de un archivo ejecutable a las reglas de la categoría. Si el archivo ejecutable no tiene certificado, el archivo se omitirá. No se agregará información sobre ese archivo a la categoría.

- **Solo SHA256 (los archivos sin hash se omitirán)**

  Cada archivo tiene su propia función hash SHA256. Si selecciona una función hash SHA256, solo se agregará a la categoría el archivo específico que se corresponda con ese hash (por ejemplo, la versión especificada de la aplicación).

  Seleccione esta opción si solo desea agregar los detalles de la función hash SHA256 del archivo ejecutable.

- **Solo hashes MD5**

  Seleccione esta opción solo si utiliza Kaspersky Endpoint Security para Windows. Kaspersky Endpoint Security para Linux no admite una función hash MD5.

  Cada archivo tiene su propia función hash MD5. Si selecciona una función hash MD5, solo se agregará a la categoría el archivo específico que se corresponda con ese hash (por ejemplo, la versión especificada de la aplicación).

5. Haga clic en **Aceptar**.

Cuando finaliza el asistente, los archivos ejecutables vinculados a los eventos de Control de aplicaciones se agregan a la categoría de aplicaciones nueva o existente. Puede ver la configuración de la categoría de aplicaciones creada o modificada.

Para obtener información detallada sobre Control de aplicaciones, consulte la Ayuda de Kaspersky Endpoint Security for Linux y la Ayuda de Kaspersky Endpoint Security para Windows.

Configurar Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows

Tras crear las categorías de Control de aplicaciones, puede utilizarlas para configurar el componente en las directivas de Kaspersky Endpoint Security para Windows.

Para configurar Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows:

1. En el menú principal, vaya a **Administración de activos** → **Directivas**.

   Se muestra una página con una lista de directivas.

2. Haga clic en la directiva de **Kaspersky Endpoint Security para Windows**.

   Se abre la ventana de configuración de la directiva.

3. Vaya a **Configuración de la aplicación** → **Controles de seguridad** → **Control de aplicaciones**.

   Se abre la ventana **Control de aplicaciones**, en la que encontrará los ajustes de Control de aplicaciones.

4. La opción **Control de aplicaciones** está habilitada de manera predeterminada. Pase el interruptor a **Control de aplicaciones DESHABILITADO** para deshabilitar la opción.

5. En el bloque de opciones **Configuración de Control de aplicaciones**, habilite el modo de funcionamiento pertinente para aplicar las reglas de Control de aplicaciones y permitir que Kaspersky Endpoint Security para Windows bloquee el inicio de aplicaciones.

   Si desea probar las reglas de Control de aplicaciones, en la sección **Configuración de Control de aplicaciones**, habilite el modo de prueba. Cuando el modo de prueba está habilitado, Kaspersky Endpoint Security para Windows no bloquea el inicio de las aplicaciones, pero registra información sobre las reglas activadas en el informe. Haga clic en el vínculo **Ver informe** para ver esa información.

6. Habilite la opción **Controlar la carga de módulos DLL** si desea que Kaspersky Endpoint Security para Windows monitoree la carga de módulos DLL cuando los usuarios inicien aplicaciones.

   Se guardará un informe con datos sobre los módulos y sobre las aplicaciones que carguen esos módulos.

   Kaspersky Endpoint Security para Windows únicamente atenderá a los módulos DLL y controladores que se carguen después de que habilite la opción **Controlar la carga de módulos DLL**. Reinicie el dispositivo después de habilitar la opción **Controlar la carga de módulos DLL** si desea que Kaspersky Endpoint Security para Windows supervise la carga de todos los módulos DLL y controladores, incluidos aquellos que se carguen antes de la ejecución de Kaspersky Endpoint Security para Windows.

7. (Opcional). En el bloque **Plantillas de mensajes**, modifique la plantilla del mensaje que se le muestra al usuario cuando se le impide iniciar una aplicación y la plantilla del correo electrónico que el usuario le puede enviar a usted.

8. En el bloque de opciones **Modo de Control de aplicaciones**, seleccione el modo **Lista de rechazados** o el modo **Lista de admitidos**.

   De forma predeterminada, está seleccionado el modo **Lista de rechazados**.

9. Haga clic en el vínculo **Configuración de las listas de reglas**.

   Se abre la ventana **Listas de rechazados y admitidos** que permite agregar una categoría de aplicaciones. De manera predeterminada, la pestaña **Lista de rechazados** está seleccionada si se selecciona el modo **Lista de rechazados**, o la pestaña **Lista de admitidos** si se selecciona el modo **Lista de admitidos**.

10. En la ventana **Listas de rechazados y admitidos**, haga clic en el botón **Agregar**.

    Se abre la ventana **Regla de Control de aplicaciones**.

11. Haga clic en el vínculo **Debe elegir una categoría**.

    Se abre la ventana **Categoría de aplicaciones**.

12. Agregue la categoría de aplicaciones (o las categorías de aplicaciones) que creó anteriormente.

    Si desea modificar la configuración de una categoría que creó, haga clic en el botón **Editar**.

    Si desea crear una nueva categoría, haga clic en el botón **Agregar**.

    Si desea eliminar una categoría de la lista, haga clic en el botón **Eliminar**.

13. Una vez que la lista de categorías de aplicaciones esté completa, haga clic en el botón **Aceptar**.

    Se cierra la ventana **Categoría de aplicaciones**.

14. En la ventana de la regla de **Control de aplicaciones**, en la sección **Usuarios y sus derechos**, cree una lista con los usuarios y grupos de usuarios a los que se aplicará la regla de Control de aplicaciones.

15. Haga clic en el botón **Aceptar** para guardar la configuración y cerrar la ventana **Regla de Control de aplicaciones**.

16. Haga clic en el botón **Aceptar** para guardar la configuración y cerrar la ventana **Listas de rechazados y admitidos**.

17. Haga clic en el botón **Aceptar** para guardar la configuración y cerrar la ventana **Control de aplicaciones**.

18. Cierre la ventana con la configuración de la directiva de Kaspersky Endpoint Security para Windows.

    Se guarda la configuración de Control de aplicaciones. Una vez que la directiva se propague a los dispositivos cliente, el inicio de archivos ejecutables estará bajo su control.

Para obtener información detallada sobre Control de aplicaciones, consulte la Ayuda de Kaspersky Endpoint Security for Linux y la Ayuda de Kaspersky Endpoint Security para Windows.

Obtener y ver una lista de aplicaciones instaladas en los dispositivos cliente

Kaspersky Security Center Linux hace un inventario de todo el software instalado en los dispositivos cliente administrados que ejecutan Linux y Windows.

El Agente de red elabora una lista de las aplicaciones instaladas en un dispositivo y luego transmite la lista al Servidor de administración. El Agente de red tarda entre 10 y 15 minutos en actualizar la lista de aplicaciones.

Para los dispositivos cliente basados en Windows, el Agente de red recibe la mayor parte de la información sobre las aplicaciones instaladas del registro de Windows. Para los dispositivos cliente basados en Linux, los administradores de paquetes brindan información al Agente de red sobre las aplicaciones instaladas.

Para ver la lista de las aplicaciones instaladas en los dispositivos administrados:

1. En el menú principal, vaya a **Administración de software** → **Aplicaciones de terceros** → **Registro de aplicaciones**.

   La página muestra una tabla con las aplicaciones que están instaladas en los dispositivos administrados. Seleccione una aplicación para ver sus propiedades (por ejemplo, el nombre del proveedor, el número de versión, la lista de archivos ejecutables y la lista de dispositivos en los que la aplicación está instalada).

2. Puede agrupar y filtrar los datos de la tabla con las aplicaciones instaladas de la siguiente manera:

   - Haga clic en el icono de configuración ( ) en la esquina superior derecha de la tabla.

     En el menú invocado **Configuración de las columnas**, seleccione las columnas que se mostrarán en la tabla. Para ver el tipo de sistema operativo de los dispositivos cliente en los que está instalada la aplicación, seleccione la columna **Tipo de SO**.

   - Haga clic en el icono de filtro ( ) en la esquina superior derecha de la tabla y luego especifique y aplique el criterio de filtro en el menú invocado.

     Se muestra la tabla filtrada de aplicaciones instaladas.

Para visualizar la lista de aplicaciones instaladas en un dispositivo administrado en particular, haga lo siguiente:

En el menú principal, vaya a **Administración de activos** → **Dispositivos administrados** → **nombre del dispositivo** → **Avanzado** → **Registro de aplicaciones**. En este menú, puede exportar la lista de aplicaciones a un archivo CSV o TXT.

Para obtener información detallada sobre Control de aplicaciones, consulte la Ayuda de Kaspersky Endpoint Security for Linux y la Ayuda de Kaspersky Endpoint Security para Windows.

Acerca de las aplicaciones de terceros

Kaspersky Security Center Linux puede ayudarlo a actualizar y corregir las vulnerabilidades del software de terceros instalado en los dispositivos cliente. Kaspersky Security Center Linux puede actualizar software de terceros de la versión instalada a la versión más reciente únicamente.

> La lista de software de terceros puede cambiar y se actualiza dinámicamente. Para comprobar si puede actualizar el software de terceros instalado en los dispositivos de los usuarios con Kaspersky Security Center Linux, consulte la lista de actualizaciones disponibles en Kaspersky Security Center Web Console.

El procedimiento que se describe a continuación está destinado únicamente a ver la lista de software de terceros que se puede actualizar con Kaspersky Security Center Linux. Se siguen los pasos para acceder a la información relevante sin iniciar ninguna tarea.

Para ver la lista de software de terceros que puede actualizar con Kaspersky Security Center Linux, haga lo siguiente:

1. En el menú principal, vaya a **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.
3. En el paso **Configuración de tarea nueva** del asistente, especifique estos ajustes:
   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Security Center Linux**.
   b. En el campo **Tipo de tarea**, seleccione **Instalar actualizaciones requeridas y reparar vulnerabilidades**.
4. En el paso **Alcance de la tarea** del asistente, seleccione la opción **Dispositivos administrados**.
5. En el paso del asistente **Elija las reglas de instalación de actualizaciones**, haga clic en el botón **Agregar**.

   Se inicia el Asistente de creación de reglas. Avance por el asistente utilizando el botón **Siguiente**.
6. En el paso del asistente **Seleccionar tipo de regla**, seleccione **Regla para actualizaciones de terceros**.
7. En el paso del asistente **Criterios generales**, seleccione la opción **Instalar todas las actualizaciones (excepto las rechazadas)** y, luego, haga clic en **Siguiente**.

Se muestra la lista de software de terceros.

Instalación de actualizaciones para software de terceros

Kaspersky Security Center Linux le permite administrar las actualizaciones del software de terceros instaladas en los dispositivos administrados y reparar las vulnerabilidades de dicho software mediante la instalación de las actualizaciones necesarias.

Kaspersky Security Center Linux busca actualizaciones a través de la tarea *Buscar vulnerabilidades y actualizaciones requeridas*. Cuando se completa esta tarea, el Servidor de administración recibe listas en las que se detallan las vulnerabilidades detectadas y las actualizaciones requeridas para el software de terceros con el que cuentan los dispositivos indicados en las propiedades de la tarea. Tras revisarse la información de las actualizaciones disponibles, se las puede instalar en los dispositivos.

Para actualizar algunas aplicaciones, Kaspersky Security Center Linux elimina la versión anterior de la aplicación e instala la versión nueva.

Para actualizar una aplicación de terceros o reparar una vulnerabilidad en una aplicación de terceros instalada en un dispositivo administrado, podría necesitarse la colaboración del usuario. Si la aplicación está abierta, por ejemplo, podría tener que pedírsele al usuario que la cierre.

Por seguridad, cada actualización de software de terceros que se instala con la función Administración de vulnerabilidades y parches se somete a un análisis antimalware automático con las tecnologías de Kaspersky Estas tecnologías revisan automáticamente los archivos utilizando técnicas de análisis antivirus, análisis estático, análisis dinámico, análisis de comportamiento en un entorno de pruebas y aprendizaje automático, entre otras.

Los expertos de Kaspersky no realizan análisis manuales de las actualizaciones de software de terceros que puedan instalarse mediante la función Administración de vulnerabilidades y parches. Tampoco buscan vulnerabilidades (conocidas o desconocidas) o funciones no documentadas en las actualizaciones ni las analizan de modos que no se hayan indicado en el párrafo anterior

Una vez que los metadatos de las actualizaciones de software de terceros se descargan en el repositorio, las actualizaciones se pueden instalar en los dispositivos cliente mediante la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*.

> La tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* se puede crear únicamente si se cuenta con una licencia para la función Administración de vulnerabilidades y parches.

Cuando se completa esta tarea, las actualizaciones se instalan en los dispositivos administrados automáticamente. Cuando se descargan metadatos de nuevas actualizaciones en el repositorio del Servidor de administración, Kaspersky Security Center Linux verifica si las actualizaciones cumplen con los criterios especificados en las reglas de actualización. Las actualizaciones nuevas que cumplen con los criterios se descargan e instalan en forma automática cuando la tarea se ejecuta nuevamente.

Procedimiento: Actualización de software de terceros

En esta sección, se describe un procedimiento para actualizar el software de terceros instalado en dispositivos cliente. El término "software de terceros" comprende aplicaciones desarrolladas por otros proveedores de software.

Requisitos previos

El Servidor de administración debe estar conectado a Internet para instalar actualizaciones de software de terceros.

Etapas

El proceso para actualizar aplicaciones de terceros se divide en etapas:

1. **Buscar las actualizaciones requeridas**

   Para buscar las actualizaciones que se requieren para el software de terceros de los dispositivos administrados, ejecute la tarea *Buscar vulnerabilidades y actualizaciones requeridas*. Cuando se completa esta tarea, Kaspersky Security Center Linux recibe las listas de vulnerabilidades detectadas y las actualizaciones requeridas para el software de terceros instalado en los dispositivos que especificó en las propiedades de la tarea.

   La tarea *Buscar vulnerabilidades y actualizaciones requeridas* se crea automáticamente al utilizar el Asistente de inicio rápido del Servidor de administración. Si no ejecutó el asistente, hágalo ahora o cree la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

   > Puede crear la tarea *Buscar vulnerabilidades y actualizaciones requeridas* solo para dispositivos Windows. No puede crear esta tarea para dispositivos que ejecutan otros sistemas operativos.

2. **Ver la lista de actualizaciones encontradas**

   Consulte información sobre las actualizaciones de software de terceros disponibles y decida qué actualizaciones desea instalar. Para obtener información detallada sobre una actualización, haga clic en el nombre de la misma en la lista. Para cada actualización de la lista, también puede ver las estadísticas sobre su instalación en los dispositivos cliente.

3. **Configurar la instalación de actualizaciones**

   Una vez que Kaspersky Security Center Linux cuente con la lista de actualizaciones de software de terceros, cree la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* para instalar las actualizaciones en los dispositivos cliente.

   > Solo puede crear la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* para dispositivos Windows. No puede crear esta tarea para dispositivos que ejecuten otros sistemas operativos.

   La tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* se utiliza para instalar actualizaciones para aplicaciones de Microsoft (incluidas las actualizaciones que proporciona el servicio Windows Update) y actualizaciones para software de otros proveedores. Tenga en cuenta que solo se puede crear la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* si tiene la licencia para la función Administración de vulnerabilidades y parches.

   Para instalar algunas actualizaciones de software, deberá aceptar el Contrato de licencia de usuario final (EULA) para el software de instalación. Si rechaza el EULA, no se instalará la actualización de software correspondiente.

   Puede iniciar una tarea de instalación de actualizaciones según una programación. Si elige configurar una programación, asegúrese de que la tarea de instalación de actualizaciones se ejecute luego de que finalice la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

4. **Programar las tareas**

   Para asegurarse de que la lista de actualizaciones siempre esté actualizada, defina una programación que haga que la tarea *Buscar vulnerabilidades y actualizaciones requeridas* se ejecute automáticamente de tanto en tanto. De manera predeterminada, la tarea *Buscar vulnerabilidades y actualizaciones requeridas* está configurada para iniciarse de forma manual.

   Si creó la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, puede programarla para que se ejecute con igual o menor frecuencia que la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

Cuando programe las tareas, asegúrese de que la tarea de instalación de actualizaciones se inicie después de que la tarea *Buscar vulnerabilidades y actualizaciones requeridas* haya finalizado.

5. **Aprobar y rechazar actualizaciones de software de terceros (opcional)**

   Si creó la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, en la ventana de propiedades de la tarea, puede definir reglas que controlen la instalación de las actualizaciones.

   Para cada regla, puede definir las actualizaciones que se instalarán según el estado de la actualización: *Sin definir*, *Aprobada* o *Rechazada*. Así, si crea una tarea específica para sus servidores, por ejemplo, podría definir una regla que únicamente permita la instalación de aquellas actualizaciones que tengan el estado *Aprobada*. Tras ello, podría asignar manualmente el estado *Aprobada* a las actualizaciones que desee instalar. Las actualizaciones que tengan el estado *Sin definir* o *Rechazada* no se instalarán en los servidores especificados en la tarea.

   Puede usar el estado *Aprobada* para administrar la instalación de una cantidad de actualizaciones modesta. Cuando necesite instalar muchas actualizaciones, utilice en cambio las reglas que puede configurar en la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*. Asigne el estado *Aprobada* únicamente a las actualizaciones específicas que no cumplan con los criterios indicados en las reglas. Cuando se aprueba manualmente una gran cantidad de actualizaciones, el rendimiento del Servidor de administración disminuye, y este puede sobrecargarse.

   De forma predeterminada, las actualizaciones de software descargadas tienen el estado *Sin definir*. Puede cambiar el estado a *Aprobada* o *Rechazada* en la lista **Actualizaciones de software** (**Administración de software** → **Administración de parches** → **Actualizaciones de software**).

   Para obtener más información, consulte las instrucciones sobre cómo aprobar y rechazar actualizaciones de software de terceros.

6. **Ejecutar la tarea de instalación de actualizaciones**

   Inicie la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*. Al hacerlo, se descargarán las actualizaciones y se las instalará en los dispositivos administrados. Cuando se complete la tarea, verifique que su estado en la lista de tareas sea *Completada correctamente*.

7. **Generar un informe sobre los resultados de la instalación de las actualizaciones (opcional)**

   Para ver estadísticas detalladas sobre la instalación de las actualizaciones, genere el Informe sobre los resultados de la instalación de actualizaciones de software de terceros.

Resultados

Si creó y configuró la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, las actualizaciones se instalarán automáticamente en los dispositivos administrados. Cuando se descarguen nuevas actualizaciones en el repositorio del Servidor de administración, Kaspersky Security Center Linux verificará si cumplen con los criterios especificados en las reglas de actualización. Las actualizaciones nuevas que cumplan con los criterios se instalarán automáticamente la siguiente vez que se ejecute la tarea.

Opciones para instalar actualizaciones de software de terceros

Puede instalar actualizaciones de software de terceros y actualizaciones de Windows Update en dispositivos administrados mediante la creación y ejecución de la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*. La tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* se puede crear únicamente si tiene la licencia para la función Administración de vulnerabilidades y parches. Puede utilizar esta tarea para instalar las actualizaciones de software de otros proveedores.

Para actualizar una aplicación de terceros o reparar una vulnerabilidad en una aplicación de terceros instalada en un dispositivo administrado, podría necesitarse la colaboración del usuario. Si la aplicación está abierta, por ejemplo, podría tener que pedirle al usuario que la cierre.

Como alternativa, para crear una tarea que instale las actualizaciones requeridas, puede optar por estos métodos:

- Abra la lista de actualizaciones y, luego, elija las actualizaciones que se deban instalar.

  Como resultado, se creará una nueva tarea para instalar las actualizaciones seleccionadas. Si lo prefiere, puede agregar las actualizaciones seleccionadas a una tarea existente.

- Utilice el Asistente de instalación de actualizaciones.

  Para usar el Asistente de instalación de actualizaciones, debe tener una licencia de Administración de vulnerabilidades y parches.

  El asistente simplifica la creación y configuración de tareas de instalación de actualizaciones. También evita que se creen tareas redundantes, que tengan las mismas actualizaciones para instalar.

Instalación de actualizaciones de software de terceros desde la lista de actualizaciones

Para instalar actualizaciones de software de terceros desde la lista de actualizaciones:

1. Siga alguna de las siguientes rutas para abrir la lista de actualizaciones:

   - **Administración de software** → **Administración de parches** → **Actualizaciones de software**.
   - **Administración de activos** → **Dispositivos administrados** → <nombre del dispositivo> → **Avanzado** → **Actualizaciones disponibles**.
   - **Administración de software** → **Aplicaciones de terceros** → **Registro de aplicaciones** → <nombre de la aplicación> → **Actualizaciones disponibles**.

   Se mostrará una lista con las actualizaciones disponibles.

2. Marque las casillas de verificación ubicadas junto a las actualizaciones que desee instalar.

3. Haga clic en el botón **Instalar actualizaciones**. Si este botón no está visible, haga clic en el botón de puntos suspensivos y luego seleccione **Instalar actualizaciones** en la lista desplegable.

   Para instalar algunas actualizaciones de software, deberá aceptar el contrato de licencia de usuario final (EULA). Si rechaza el EULA, no se instalará la actualización de software correspondiente.

4. Seleccione una de las siguientes opciones:

   - **Nueva tarea**

     Se inicia el Asistente para crear nueva tarea. Si tiene la licencia de la Administración de vulnerabilidades y parches, la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* estará preseleccionada. Siga los pasos del asistente para completar la creación de la tarea.

   - **Instalar actualización (agregar regla a la tarea especificada)**

     Seleccione una tarea a la que desee agregar las actualizaciones seleccionadas. Si tiene la licencia de Administración de vulnerabilidades y parches, seleccione la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*. Una nueva regla para instalar las actualizaciones seleccionadas se agrega automáticamente a la tarea seleccionada. Las actualizaciones seleccionadas se agregan a las propiedades de la tarea.

     Se abrirá la ventana de propiedades de la tarea. Haga clic en **Guardar** para guardar los cambios.

   Si optó por crear una tarea, se la creará y se la agregará a la lista de tareas disponible en **Tareas**. Si eligió agregar las actualizaciones a una tarea existente, se agregarán las actualizaciones a las propiedades de la tarea que haya seleccionado.

Para instalar las actualizaciones de software de terceros, deberá iniciar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*. Para iniciar esta tarea, haga clic en el botón **Iniciar** en la lista de tareas o configure su programación en las propiedades de la tarea que se iniciará. Si elige configurar una programación, asegúrese de que la tarea de instalación de actualizaciones se ejecute luego de que finalice la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

Instalación de actualizaciones de software de terceros mediante el Asistente de instalación de actualizaciones

Para usar el Asistente de instalación de actualizaciones, debe tener una licencia de Administración de vulnerabilidades y parches.

Para crear una tarea para instalar actualizaciones de software de terceros con el Asistente de instalación de actualizaciones:

1. En el menú principal, vaya a **Administración de software → Administración de parches → Actualizaciones de software**.

   Se mostrará una lista con las actualizaciones disponibles.

2. Marque la casilla ubicada junto a la actualización que desee instalar.

3. Haga clic en el botón **Ejecutar el Asistente de instalación de actualizaciones**.

Se iniciará el Asistente de instalación de actualizaciones. En la página **Seleccione una tarea de instalación de actualizaciones**, verá una lista con todas las tareas existentes de los siguientes tipos:

- *Instalar actualizaciones requeridas y reparar vulnerabilidades*
- *Reparar vulnerabilidades*

4. Si desea que el asistente solamente le muestre las tareas que permitan instalar la actualización seleccionada, habilite la opción **Mostrar solo las tareas que permitan instalar esta actualización**.

5. Elija lo que desea hacer:

   - Para iniciar una tarea existente, marque la casilla junto a la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* y, luego, haga clic en el botón **Iniciar**.

     La tarea se completará en segundo plano. No se requieren más acciones.

   - Para agregar una nueva regla a una tarea existente, haga lo siguiente:

     a. Marque la casilla ubicada junto al nombre de la tarea pertinente y haga clic en el botón **Agregar regla**.

     > El botón **Agregar regla** estará deshabilitado si selecciona más de una tarea.

     No es posible agregar reglas a una tarea *Reparar vulnerabilidades*. Si selecciona una tarea *Reparar vulnerabilidades*, se mostrará la siguiente notificación: "*Para instalar actualizaciones, use la tarea 'Instalar actualizaciones requeridas y reparar vulnerabilidades'".*

     b. En el paso **Crear una regla de instalación de actualizaciones** del asistente, configure la nueva regla:

     - **Regla de instalación para actualizaciones de este nivel de importancia**

       Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

       Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al nivel de gravedad de la actualización seleccionada. Los niveles posibles son **Medio**, **Alto** y **Crítico**. Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

       Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

       Esta opción está deshabilitada de forma predeterminada.

       Esta regla no se muestra si el nivel de importancia de la actualización seleccionada es *Desconocido*.

     - **Regla de instalación para actualizaciones de este nivel de importancia conforme a MSRC**

       Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

       Si esta opción (que solo está disponible para actualizaciones de Windows Update) está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que el Centro de respuestas de seguridad de Microsoft (MSRC) haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Bajo**, **Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

Esta opción está deshabilitada de forma predeterminada.

Esta regla solo se muestra para las actualizaciones del software de Microsoft. No se muestra si el nivel de importancia de la actualización seleccionada es *Desconocido*.

- **Regla de instalación para actualizaciones de este proveedor**

  Esta opción solo está disponible para actualizaciones de aplicaciones de terceros. Kaspersky Security Center Linux instala solo las actualizaciones relacionadas con las aplicaciones desarrolladas por el mismo proveedor que la actualización seleccionada. No se instalarán actualizaciones rechazadas ni actualizaciones para software de otros proveedores.

  Esta opción está deshabilitada de forma predeterminada.

  Esta regla solo se muestra para actualizaciones de software de terceros.

- **Regla de instalación para actualizaciones del tipo**

- **Regla de instalación para actualizaciones de la aplicación seleccionada**

  Esta regla solo se muestra para actualizaciones de software de terceros.

- **Regla de instalación para la actualización seleccionada**

- **Aprobar actualizaciones seleccionadas**

  Se aprobará la instalación de la actualización seleccionada. Habilite esta opción si ha aplicado reglas de instalación de actualizaciones que solo permitan instalar actualizaciones aprobadas.

  Esta opción está deshabilitada de forma predeterminada.

- **Instalar automáticamente todas las actualizaciones de software que antecedan a las seleccionadas y se requieran para instalarlas**

  Mantenga habilitada esta opción si está de acuerdo en que, para instalar las actualizaciones seleccionadas, se instalen versiones intermedias de las aplicaciones.

  Si deshabilita esta opción, se instalarán únicamente las versiones de las aplicaciones que haya seleccionado. Deshabilite esta opción si quiere que las aplicaciones se actualicen en forma directa, sin que se trate de instalar versiones intermedias. Cuando las actualizaciones seleccionadas no se puedan instalar sin que antes se instalen versiones más antiguas de las aplicaciones, el proceso de actualización no se completará.

  A modo de ejemplo, imagine que un dispositivo tiene instalada la versión 3 de una aplicación. Quiere actualizar esa versión a la 5, pero la versión 5 solo se puede instalar sobre la versión 4. Si esta opción está habilitada, el software instalará primero la versión 4 y luego la versión 5. Si esta opción está deshabilitada, el software no podrá actualizar la aplicación.

  Esta opción está activada de forma predeterminada.

c. Haga clic en **Agregar**.

Se abrirá la ventana de propiedades de la tarea. Encontrará la nueva regla en las propiedades de la tarea. Si lo desea, vea y modifique la regla o los otros ajustes de la tarea. Haga clic en **Guardar** para guardar los cambios.

- Para crear una tarea:

  a. Haga clic en el botón **Nueva tarea**.

  b. En el paso **Crear una regla de instalación de actualizaciones** del asistente, configure la nueva regla:

  - **Regla de instalación para actualizaciones de este nivel de importancia**

    Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

    Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al nivel de gravedad de la actualización seleccionada. Los niveles posibles son **Medio**, **Alto** y **Crítico**. Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

    Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

    Esta opción está deshabilitada de forma predeterminada.

    Esta regla no se muestra si el nivel de importancia de la actualización seleccionada es *Desconocido*.

  - **Regla de instalación para actualizaciones de este nivel de importancia conforme a MSRC**

    Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

    Si esta opción (que solo está disponible para actualizaciones de Windows Update) está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que el Centro de respuestas de seguridad de Microsoft (MSRC) haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Bajo**, **Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

    Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

    Esta opción está deshabilitada de forma predeterminada.

    Esta regla solo se muestra para las actualizaciones del software de Microsoft. No se muestra si el nivel de importancia de la actualización seleccionada es *Desconocido*.

  - **Regla de instalación para actualizaciones de este proveedor**

    Esta opción solo está disponible para actualizaciones de aplicaciones de terceros.
    Kaspersky Security Center Linux instala solo las actualizaciones relacionadas con las aplicaciones desarrolladas por el mismo proveedor que la actualización seleccionada. No se instalarán actualizaciones rechazadas ni actualizaciones para software de otros proveedores.

    Esta opción está deshabilitada de forma predeterminada.

    Esta regla solo se muestra para actualizaciones de software de terceros.

  - **Regla de instalación para actualizaciones del tipo**

  - **Regla de instalación para actualizaciones de la aplicación seleccionada**

    Esta regla solo se muestra para actualizaciones de software de terceros.

  - **Regla de instalación para la actualización seleccionada**

- **Aprobar actualizaciones seleccionadas**

  Se aprobará la instalación de la actualización seleccionada. Habilite esta opción si ha aplicado reglas de instalación de actualizaciones que solo permitan instalar actualizaciones aprobadas.

  Esta opción está deshabilitada de forma predeterminada.

- **Instalar automáticamente todas las actualizaciones de software que antecedan a las seleccionadas y se requieran para instalarlas**

  Mantenga habilitada esta opción si está de acuerdo en que, para instalar las actualizaciones seleccionadas, se instalen versiones intermedias de las aplicaciones.

  Si deshabilita esta opción, se instalarán únicamente las versiones de las aplicaciones que haya seleccionado. Deshabilite esta opción si quiere que las aplicaciones se actualicen en forma directa, sin que se trate de instalar versiones intermedias. Cuando las actualizaciones seleccionadas no se puedan instalar sin que antes se instalen versiones más antiguas de las aplicaciones, el proceso de actualización no se completará.

  A modo de ejemplo, imagine que un dispositivo tiene instalada la versión 3 de una aplicación. Quiere actualizar esa versión a la 5, pero la versión 5 solo se puede instalar sobre la versión 4. Si esta opción está habilitada, el software instalará primero la versión 4 y luego la versión 5. Si esta opción está deshabilitada, el software no podrá actualizar la aplicación.

  Esta opción está activada de forma predeterminada.

c. Haga clic en **Agregar**.

En el Asistente para crear nueva tarea, continúe con la creación de la tarea. La regla agregada en el Asistente de instalación de actualizaciones se mostrará en el Asistente para crear nueva tarea. Cuando llegue al final del asistente, la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* se agregará a la lista de tareas.

Configuración de la tarea Buscar vulnerabilidades y actualizaciones requeridas

La tarea *Buscar vulnerabilidades y actualizaciones requeridas* se crea automáticamente cuando se ejecuta el asistente de inicio rápido. Si no ejecutó este asistente, puede crear la tarea de forma manual.

A continuación, se describen los ajustes que puede configurar para la tarea *Buscar vulnerabilidades y actualizaciones requeridas* (junto con sus ajustes generales) ya sea al momento de crear la tarea o, si la tarea ya existe, a través de sus propiedades:

- **Buscar vulnerabilidades y actualizaciones catalogadas por Microsoft**

  Al buscar vulnerabilidades y actualizaciones, Kaspersky Security Center Linux utiliza la información sobre las actualizaciones de Microsoft aplicables desde la fuente de actualizaciones de Microsoft, las cuales están disponibles en este momento.

  Podría deshabilitar esta opción si, por ejemplo, ha creado tareas diferentes (con configuraciones diferentes) para las actualizaciones de Microsoft y para las actualizaciones de aplicaciones de terceros.

  Esta opción está activada de forma predeterminada.

  La información sobre las actualizaciones opcionales de Microsoft Windows no se envía al Servidor de administración.

- **Conectarse al servidor de actualizaciones para actualizar los datos**

  El Agente de Windows Update del dispositivo administrado se conectará al origen de actualizaciones de Microsoft. Los siguientes servidores pueden actuar como orígenes de actualizaciones de Microsoft:

  - Un servidor Windows Server con Microsoft Windows Server Update Services (WSUS) que se encuentre instalado en la red de su organización
  - Los servidores de actualizaciones de Microsoft

  Cuando esta opción está habilitada, el Agente de Windows Update del dispositivo administrado se conecta al origen de actualizaciones de Microsoft para obtener información actualizada sobre las actualizaciones de Microsoft Windows aplicables.

  Cuando esta opción está deshabilitada, el Agente de actualización de Windows del dispositivo administrado usa la información sobre las actualizaciones de Microsoft Windows aplicables que el origen de actualizaciones brindó en un momento anterior.

  Conectarse al origen de actualizaciones de Microsoft puede consumir muchos recursos. Podría deshabilitar esta opción si ha configurado un esquema de conexión periódica a este origen en otra tarea o en la sección **Actualizaciones y vulnerabilidades de software** de las propiedades de la directiva del Agente de red. Si no quiere deshabilitar esta opción, para intentar que el Servidor de administración no se sobrecargue, modifique la programación de la tarea para que se la inicie en un punto aleatorio de un intervalo de 360 minutos.

  Esta opción está activada de forma predeterminada.

  El modo de obtener las actualizaciones deriva de combinar las siguientes opciones de configuración de la directiva del Agente de red:

  - El Agente de actualización de Windows de un dispositivo administrado se conecta al servidor de actualizaciones para recibir actualizaciones solo si la opción **Conectarse al servidor de actualizaciones para actualizar los datos** está habilitada en las propiedades de la tarea *Buscar vulnerabilidades y actualizaciones requeridas* y el **Modo de búsqueda de Windows Update** está configurado como **Activo** en la configuración de la directiva del Agente de red.
  - Si no necesita el Agente de red para iniciar una conexión al origen de actualizaciones de Microsoft Windows ni para descargar actualizaciones al realizar la tarea *Análisis de vulnerabilidades*, puede seleccionar la opción **Pasivo** en **Modo de búsqueda de Windows Update**, pero la opción **Conectarse al servidor de actualizaciones para actualizar los datos** debe permanecer habilitada. Así podrá ahorrar recursos y usar las actualizaciones de Windows antes recibidas para analizar las vulnerabilidades. Puede usar el modo pasivo si configura la recepción de actualizaciones de Microsoft Windows de otra manera. Si la recepción de actualizaciones de Microsoft Windows no está configurada de otra manera, no seleccione la opción **Pasivo** en **Modo de búsqueda de Windows Update** porque, en este caso, nunca recibirá información sobre las actualizaciones.
  - Independientemente del estado de la opción **Conectarse al servidor de actualizaciones para actualizar los datos** (habilitado o deshabilitado), si se selecciona la opción **Modo de búsqueda de Windows Update** en **Deshabilitado**, Kaspersky Security Center Linux no solicita ninguna información sobre actualizaciones.

Si en la red de la organización se utiliza el servidor WSUS (servidor WSUS local) y desea usarlo junto con el Servidor de administración de Kaspersky Security Center, primero debe asegurarse de que el Servidor de administración de Kaspersky Security Center no se use como un servidor WSUS y, luego, hacer lo siguiente:

1. En los dispositivos administrados que ejecutan Windows, especifique el servidor WSUS local para el servicio Windows Update. Puede hacerlo de forma manual desde el Registro de Windows o con una directiva de grupo de Windows.

2. En el servidor WSUS local, especifique las clasificaciones necesarias para las actualizaciones y las aplicaciones donde se distribuirán las actualizaciones.

3. Sincronice el servidor WSUS con el servidor que lo precede (puede ser un servidor WSUS de Microsoft u otro servidor WSUS local anterior).

Luego de ejecutar la tarea *Buscar vulnerabilidades y actualizaciones requeridas* en el dispositivo, el Agente de red usa el servicio Windows Update para enviar una solicitud de las actualizaciones de Windows correspondientes al dispositivo. El servicio Windows Update obtiene la dirección del servidor WSUS externo del registro y busca actualizaciones directamente desde dicho servidor WSUS externo. Luego, el servicio Windows Update reenvía esta lista al Servidor de administración a través del Agente de red. Por lo tanto, el Servidor de administración tendrá una base de datos actualizada.

- **Buscar vulnerabilidades y actualizaciones catalogadas por Kaspersky para software de terceros**

  Si esta opción está habilitada, Kaspersky Security Center Linux busca vulnerabilidades y actualizaciones requeridas para aplicaciones de terceros (aplicaciones creadas por proveedores de software distintos de Kaspersky y Microsoft) en el Registro de Windows y en las carpetas especificadas en **Especifique las rutas para la búsqueda avanzada de aplicaciones en el sistema de archivos**. Kaspersky determina el alcance de la lista de aplicaciones de terceros compatibles.

  Si esta opción está deshabilitada, Kaspersky Security Center Linux no busca vulnerabilidades ni actualizaciones requeridas para aplicaciones de terceros. Puede que quiera deshabilitar esta opción si utiliza tareas diferentes, con configuraciones diferentes, para las actualizaciones de Microsoft Windows y para las actualizaciones de aplicaciones de terceros.

  Esta opción está activada de forma predeterminada.

- **Especifique las rutas para la búsqueda avanzada de aplicaciones en el sistema de archivos**

  Carpetas en las que Kaspersky Security Center Linux buscará aplicaciones de terceros que requieran la instalación de actualizaciones o que tengan vulnerabilidades que deban repararse. Puede utilizar variables del sistema.

  Especifique las carpetas en las que se instalan las aplicaciones. De forma predeterminada, la lista contiene carpetas del sistema en las que se instalan la mayoría de las aplicaciones.

- **Habilitar diagnóstico avanzado**

  Si esta función está habilitada, el Agente de red escribe archivos de seguimiento incluso si el seguimiento está desactivado para el Agente de red en la Utilidad de diagnóstico remoto de Kaspersky Security Center Linux. Los datos de seguimiento se guardan en dos archivos sucesivamente; el tamaño total de ambos archivos está determinado por el valor de la opción **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**. Cuando los archivos alcanzan su límite de tamaño, el Agente de red comienza a sobrescribirlos. Los archivos de seguimiento se almacenan en la carpeta %WINDIR%\Temp. Puede usar la utilidad de diagnóstico remoto para acceder a estos archivos, descargarlos y eliminarlos.

  Si esta función está deshabilitada, el Agente de red escribe datos de seguimiento de acuerdo con la configuración de la Utilidad de diagnóstico remoto de Kaspersky Security Center Linux. No se guardará ningún otro dato de seguimiento.

No es necesario que habilite la característica de diagnóstico avanzado al momento de crear una tarea. Es posible que desee utilizar esta función más adelante si, por ejemplo, una ejecución de tarea falla en algunos de los dispositivos y desea recopilar información adicional durante otra ejecución de tarea.

Esta opción está deshabilitada de forma predeterminada.

- **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**

  El valor predeterminado es 100 MB, y los valores disponibles están entre 1 MB y 2048 MB. Los especialistas en soporte técnico de Kaspersky podrían pedirle que cambie el valor predeterminado si, para solucionar un problema, les remite archivos de diagnóstico avanzado con información insuficiente.

Recomendaciones para programar la tarea

Al programar la tarea *Buscar vulnerabilidades y actualizaciones requeridas*, asegúrese de que las opciones **Ejecutar tareas no realizadas** y **Utilizar retardo aleatorio automático para el inicio de la tarea** estén habilitadas.

De manera predeterminada, la tarea *Buscar vulnerabilidades y actualizaciones requeridas* está configurada para iniciarse de forma manual. Si las reglas del lugar de trabajo de la organización especifican el cierre de todos los dispositivos a esta hora, la tarea *Buscar vulnerabilidades y actualizaciones requeridas* se ejecutará después de que los dispositivos se vuelvan a encender; es decir, a la mañana siguiente. Esto puede ser inconveniente porque los análisis de vulnerabilidades pueden hacer que aumente la carga en los subsistemas de disco y CPU. Debe buscar que la programación de la tarea se adecue a las reglas dispuestas por su organización.

Crear la tarea Buscar vulnerabilidades y actualizaciones requeridas

Mediante la tarea *Buscar vulnerabilidades y actualizaciones requeridas*, Kaspersky Security Center Linux recibe las listas de las vulnerabilidades detectadas y las actualizaciones requeridas para el software de terceros instalado en los dispositivos administrados.

Puede crear la tarea *Buscar vulnerabilidades y actualizaciones requeridas* solo para dispositivos Windows. No puede crear esta tarea para dispositivos que ejecutan otros sistemas operativos.

La tarea *Buscar vulnerabilidades y actualizaciones requeridas* se crea automáticamente cuando se ejecuta el asistente de inicio rápido. Si no ha ejecutado este asistente, puede crear la tarea de forma manual.

Para crear una tarea del tipo Buscar vulnerabilidades y actualizaciones requeridas:

1. En el menú principal, vaya a **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.
3. Para la aplicación de Kaspersky Security Center, seleccione el tipo de tarea **Buscar vulnerabilidades y actualizaciones requeridas**.
4. Escriba un nombre para la tarea que está creando. El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).

5. Seleccione los dispositivos a los que se asignará la tarea.

6. Especifique qué métodos se usarán para detectar aplicaciones que tengan vulnerabilidades o que deban actualizarse:

   - **Buscar vulnerabilidades y actualizaciones catalogadas por Microsoft**

     Al buscar vulnerabilidades y actualizaciones, Kaspersky Security Center Linux utiliza la información sobre las actualizaciones de Microsoft aplicables desde la fuente de actualizaciones de Microsoft, las cuales están disponibles en este momento.

     Podría deshabilitar esta opción si, por ejemplo, ha creado tareas diferentes (con configuraciones diferentes) para las actualizaciones de Microsoft y para las actualizaciones de aplicaciones de terceros.

     Esta opción está activada de forma predeterminada.

     La información sobre las actualizaciones opcionales de Microsoft Windows no se envía al Servidor de administración.

     - **Conectarse al servidor de actualizaciones para actualizar los datos**

       El Agente de Windows Update del dispositivo administrado se conectará al origen de actualizaciones de Microsoft. Los siguientes servidores pueden actuar como orígenes de actualizaciones de Microsoft:

       - Un servidor Windows Server con Microsoft Windows Server Update Services (WSUS) que se encuentre instalado en la red de su organización
       - Los servidores de actualizaciones de Microsoft

       Cuando esta opción está habilitada, el Agente de Windows Update del dispositivo administrado se conecta al origen de actualizaciones de Microsoft para obtener información actualizada sobre las actualizaciones de Microsoft Windows aplicables.

       Cuando esta opción está deshabilitada, el Agente de actualización de Windows del dispositivo administrado usa la información sobre las actualizaciones de Microsoft Windows aplicables que el origen de actualizaciones brindó en un momento anterior.

       Conectarse al origen de actualizaciones de Microsoft puede consumir muchos recursos. Podría deshabilitar esta opción si ha configurado un esquema de conexión periódica a este origen en otra tarea o en la sección **Actualizaciones y vulnerabilidades de software** de las propiedades de la directiva del Agente de red. Si no quiere deshabilitar esta opción, para intentar que el Servidor de administración no se sobrecargue, modifique la programación de la tarea para que se la inicie en un punto aleatorio de un intervalo de 360 minutos.

       Esta opción está activada de forma predeterminada.

El modo de obtener las actualizaciones deriva de combinar las siguientes opciones de configuración de la directiva del Agente de red:

- El Agente de actualización de Windows de un dispositivo administrado se conecta al servidor de actualizaciones para recibir actualizaciones solo si la opción **Conectarse al servidor de actualizaciones para actualizar los datos** está habilitada en las propiedades de la tarea *Buscar vulnerabilidades y actualizaciones requeridas* y el **Modo de búsqueda de Windows Update** está configurado como **Activo** en la configuración de la directiva del Agente de red.

- Si no necesita el Agente de red para iniciar una conexión al origen de actualizaciones de Microsoft Windows ni para descargar actualizaciones al realizar la tarea *Análisis de vulnerabilidades*, puede seleccionar la opción **Pasivo** en **Modo de búsqueda de Windows Update**, pero la opción **Conectarse al servidor de actualizaciones para actualizar los datos** debe permanecer habilitada. Así podrá ahorrar recursos y usar las actualizaciones de Windows antes recibidas para analizar las vulnerabilidades. Puede usar el modo pasivo si configura la recepción de actualizaciones de Microsoft Windows de otra manera. Si la recepción de actualizaciones de Microsoft Windows no está configurada de otra manera, no seleccione la opción **Pasivo** en **Modo de búsqueda de Windows Update** porque, en este caso, nunca recibirá información sobre las actualizaciones.

- Independientemente del estado de la opción **Conectarse al servidor de actualizaciones para actualizar los datos** (habilitado o deshabilitado), si se selecciona la opción **Modo de búsqueda de Windows Update** en **Deshabilitado**, Kaspersky Security Center Linux no solicita ninguna información sobre actualizaciones.

Si en la red de la organización se utiliza el servidor WSUS (servidor WSUS local) y desea usarlo junto con el Servidor de administración de Kaspersky Security Center, primero debe asegurarse de que el Servidor de administración de Kaspersky Security Center no se use como un servidor WSUS y, luego, hacer lo siguiente:

1. En los dispositivos administrados que ejecutan Windows, especifique el servidor WSUS local para el servicio Windows Update. Puede hacerlo de forma manual desde el Registro de Windows o con una directiva de grupo de Windows.

2. En el servidor WSUS local, especifique las clasificaciones necesarias para las actualizaciones y las aplicaciones donde se distribuirán las actualizaciones.

3. Sincronice el servidor WSUS con el servidor que lo precede (puede ser un servidor WSUS de Microsoft u otro servidor WSUS local anterior).

Luego de ejecutar la tarea *Buscar vulnerabilidades y actualizaciones requeridas* en el dispositivo, el Agente de red usa el servicio Windows Update para enviar una solicitud de las actualizaciones de Windows correspondientes al dispositivo. El servicio Windows Update obtiene la dirección del servidor WSUS externo del registro y busca actualizaciones directamente desde dicho servidor WSUS externo. Luego, el servicio Windows Update reenvía esta lista al Servidor de administración a través del Agente de red. Por lo tanto, el Servidor de administración tendrá una base de datos actualizada.

- **Buscar vulnerabilidades y actualizaciones catalogadas por Kaspersky para software de terceros**

Si esta opción está habilitada, Kaspersky Security Center Linux busca vulnerabilidades y actualizaciones requeridas para aplicaciones de terceros (aplicaciones creadas por proveedores de software distintos de Kaspersky y Microsoft) en el Registro de Windows y en las carpetas especificadas en **Especifique las rutas para la búsqueda avanzada de aplicaciones en el sistema de archivos**. Kaspersky determina el alcance de la lista de aplicaciones de terceros compatibles.

Si esta opción está deshabilitada, Kaspersky Security Center Linux no busca vulnerabilidades ni actualizaciones requeridas para aplicaciones de terceros. Puede que quiera deshabilitar esta opción si utiliza tareas diferentes, con configuraciones diferentes, para las actualizaciones de Microsoft Windows y para las actualizaciones de aplicaciones de terceros.

Esta opción está activada de forma predeterminada.

Puede deshabilitar estas opciones después de crear la tarea en la pestaña **Configuración de la aplicación** de la ventana de propiedades de la tarea.

7. **Especifique las rutas para la búsqueda avanzada de aplicaciones en el sistema de archivos**

   Carpetas en las que Kaspersky Security Center Linux buscará aplicaciones de terceros que requieran la instalación de actualizaciones o que tengan vulnerabilidades que deban repararse. Puede utilizar variables del sistema.

   Especifique las carpetas en las que se instalan las aplicaciones. De forma predeterminada, la lista contiene carpetas del sistema en las que se instalan la mayoría de las aplicaciones.

   Puede cambiar las rutas especificadas después de crear la tarea en la pestaña **Configuración de la aplicación** de la ventana de propiedades de la tarea.

8. Si es necesario, **Habilitar diagnóstico avanzado**.

   Si esta función está habilitada, el Agente de red escribe archivos de seguimiento incluso si el seguimiento está desactivado para el Agente de red en la Utilidad de diagnóstico remoto de Kaspersky Security Center Linux. Los datos de seguimiento se guardan en dos archivos sucesivamente; el tamaño total de ambos archivos está determinado por el valor de la opción **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**. Cuando los archivos alcanzan su límite de tamaño, el Agente de red comienza a sobrescribirlos. Los archivos de seguimiento se almacenan en la carpeta %WINDIR%\Temp. Puede usar la utilidad de diagnóstico remoto para acceder a estos archivos, descargarlos y eliminarlos.

   Si esta función está deshabilitada, el Agente de red escribe datos de seguimiento de acuerdo con la configuración de la Utilidad de diagnóstico remoto de Kaspersky Security Center Linux. No se guardará ningún otro dato de seguimiento.

   No es necesario que habilite la característica de diagnóstico avanzado al momento de crear una tarea. Es posible que desee utilizar esta función más adelante si, por ejemplo, una ejecución de tarea falla en algunos de los dispositivos y desea recopilar información adicional durante otra ejecución de tarea.

   Esta opción está deshabilitada de forma predeterminada.

   Puede deshabilitar esta opción después de crear la tarea en la pestaña **Configuración de la aplicación** de la ventana de propiedades de la tarea.

9. Especifique el **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**

   El valor predeterminado es 100 MB, y los valores disponibles están entre 1 MB y 2048 MB. Los especialistas en soporte técnico de Kaspersky podrían pedirle que cambie el valor predeterminado si, para solucionar un problema, les remite archivos de diagnóstico avanzado con información insuficiente.

   Debe especificar el valor si habilitó el diagnóstico avanzado en el paso anterior. Puede cambiar este valor después de crear la tarea en la pestaña **Configuración de la aplicación** de la ventana de propiedades de la tarea.

10. Si desea modificar la configuración predeterminada de la tarea, habilite la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de la tarea**. Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Puede cambiar la configuración por defecto más tarde, en cualquier momento.

11. Haga clic en el botón **Finalizar**.

El asistente creará la tarea. Si habilitó la opción **Abrir los detalles de la tarea cuando se complete la creación**, se abrirá automáticamente la ventana de propiedades de la tarea. En esta ventana, puede definir la configuración general de la tarea y, si es necesario, cambiar los ajustes establecidos durante la creación de la tarea.

También puede abrir la ventana de propiedades de la tarea haciendo clic en el nombre de la tarea creada en la lista de tareas.

La tarea queda creada y configurada. Para ejecutar la tarea, selecciónela en la lista de tareas y haga clic en el botón **Iniciar**.

Recomendaciones para programar la tarea

Al programar la tarea *Buscar vulnerabilidades y actualizaciones requeridas*, asegúrese de que las opciones **Ejecutar tareas no realizadas** y **Utilizar retardo aleatorio automático para el inicio de la tarea** estén habilitadas.

De manera predeterminada, la tarea *Buscar vulnerabilidades y actualizaciones requeridas* está configurada para iniciarse de forma manual.

También puede programar la tarea *Buscar vulnerabilidades y actualizaciones requeridas* para que se inicie en un momento determinado. Por ejemplo, puede elegir el inicio programado **Cada N horas** en la lista desplegable **Iniciar tarea**, en la pestaña **Programación** de la ventana de propiedades de la tarea. En este caso, tenga en cuenta que, si las reglas del lugar de trabajo de la organización especifican el cierre de todos los dispositivos a esta hora, la tarea *Buscar vulnerabilidades y actualizaciones requeridas* se ejecutará después de que los dispositivos se vuelvan a encender. Esto puede ser inconveniente porque los análisis de vulnerabilidades pueden hacer que aumente la carga en los subsistemas de disco y CPU. Debe buscar que la programación de la tarea se adecue a las reglas dispuestas por su organización.

Para obtener una descripción detallada de la configuración de inicio programado, vea la configuración general de la tarea.

Ver información sobre las actualizaciones disponibles para el software de terceros

Puede ver la lista de actualizaciones disponibles para las aplicaciones de terceros instaladas en los dispositivos cliente (incluidas las aplicaciones de Microsoft).

Para ver una lista de las actualizaciones disponibles para las aplicaciones de terceros instaladas en los dispositivos cliente:

En el menú principal, vaya a **Administración de software** → **Administración de parches** → **Actualizaciones de software**.

Se mostrará una lista con las actualizaciones disponibles.

Puede aplicar un filtro a la lista de actualizaciones de software mostrada. Para definir el filtro, haga clic en el ícono **Filtrar** ( ) de la lista de actualizaciones de software. También puede elegir un filtro preestablecido en la lista desplegable **Filtros preestablecidos**, que se encuentra sobre la lista de vulnerabilidades de software.

Para ver las propiedades de una actualización:

1. Haga clic en el nombre de la actualización de software que sea de su interés.
2. Se abre la ventana de propiedades de la actualización, que consta de las siguientes pestañas con información:

- **General**

  Esta pestaña contiene los detalles generales de la actualización seleccionada:

  - Estado de aprobación de la actualización (si desea cambiar este estado, puede elegir uno diferente en la lista desplegable)
  - Fecha y hora en que se registró la actualización
  - Fecha y hora en que se creó la actualización
  - Nivel de importancia de la actualización
  - Requisitos de instalación impuestos por la actualización
  - Familia de aplicaciones a la que pertenece la actualización
  - Aplicación a la que corresponde la actualización
  - Número de revisión de la actualización

- **Atributos**

  Esta pestaña muestra una serie de atributos que permiten buscar más información sobre la actualización seleccionada. Los atributos disponibles dependen de si la actualización fue publicada por Microsoft o por otro desarrollador.

  Cuando una actualización proviene de Microsoft, la información disponible en la pestaña es la siguiente:

  - Nivel de importancia asignado a la actualización por el Centro de respuestas de seguridad de Microsoft (MSRC)
  - Vínculo al artículo de Microsoft Knowledge Base en el que se describe la actualización
  - Vínculo al artículo del boletín de seguridad de Microsoft en el que se describe la actualización
  - Identificador (id.) de la actualización

  Cuando una actualización proviene de otro desarrollador, la información disponible en la pestaña es la siguiente:

  - Indicador de si la actualización es un parche o un paquete de distribución completo
  - Idioma de localización de la actualización
  - Indicador de si la actualización se instaló de forma manual o automática
  - Indicador de si la actualización se revocó tras ser instalada
  - Vínculo de descarga de la actualización

- **Dispositivos**

  Esta pestaña contiene la lista de dispositivos en los que se encuentra instalada la actualización elegida.

- **Vulnerabilidades reparadas**

  Esta pestaña contiene la lista de vulnerabilidades que pueden repararse con la actualización seleccionada.

- **Cruce de actualizaciones**

  Esta pestaña muestra cualquier "cruce" que pueda existir entre las actualizaciones publicadas para una misma aplicación; en otras palabras, aquí se indica si la actualización seleccionada puede reemplazar a otras actualizaciones o si, por el contrario, puede ser reemplazada por otras. Esta información solo está disponible para actualizaciones de Microsoft.

- **Tareas para instalar esta actualización**

  Esta pestaña contiene una lista de tareas que, por su alcance, pueden usarse para instalar la actualización seleccionada. Desde aquí también se puede crear una nueva tarea de instalación remota para la actualización.

Para ver las estadísticas de instalación de una actualización:

1. Marque la casilla ubicada junto a la actualización de software que sea de su interés.

2. Haga clic en el botón **Estadísticas de los estados de instalación de la actualización**.

Se muestra un diagrama con los estados de instalación de la actualización. Si hace clic en un estado, se abrirá una lista con los dispositivos que tengan ese estado en particular.

Puede ver información sobre las actualizaciones de software disponibles para el software de terceros (incluido el software de Microsoft) instalado en un dispositivo con Windows en particular.

Para ver la lista de las actualizaciones disponibles para el software de terceros instalado en un dispositivo administrado específico:

1. En el menú principal, vaya a **Administración de activos** → **Dispositivos administrados**.

   Se muestra la lista de dispositivos administrados.

2. En la lista de dispositivos administrados, haga clic en el vínculo con el nombre del dispositivo sobre el que quiera información.

   Se muestra la ventana de propiedades del dispositivo seleccionado.

3. En la ventana de propiedades del dispositivo seleccionado, elija la pestaña **Avanzado**.

4. En el panel de la izquierda, elija la sección **Actualizaciones disponibles**. Si solo desea ver las actualizaciones instaladas, seleccione la opción **Mostrar actualizaciones instaladas**.

Se muestra la lista de actualizaciones de software de terceros disponibles para el dispositivo seleccionado.

Exportar la lista de actualizaciones de software disponibles a un archivo

Puede exportar a un archivo CSV o TXT la lista de actualizaciones disponibles para las aplicaciones de terceros (incluidas las de Microsoft). Una vez que tenga este archivo, podrá almacenarlo para fines estadísticos o enviaserlo a la persona que esté a cargo de la seguridad de la información.

Para exportar a un archivo de texto la lista de actualizaciones disponibles para el software de terceros instalado en todos los dispositivos administrados:

1. En el menú principal, vaya a **Operaciones** → **Administración de parches** → **Actualizaciones de software**.

   Se mostrará una lista con las actualizaciones disponibles.

   Si desea exportar la lista completa de actualizaciones de software, tenga en cuenta que solo se exportarán las actualizaciones que aparezcan en la página que esté viendo.

   Si desea exportar solo algunas actualizaciones, seleccione las casillas junto a las actualizaciones que desee visualizar en la lista.

2. Haga clic en el botón **Exportar a TXT** o en el botón **Exportar a CSV**, dependiendo del formato de exportación que prefiera. Si no ve alguno de estos botones, haga clic en el botón de los puntos suspensivos y, luego, seleccione la opción que desee de la lista desplegable.

El archivo que contiene la lista de actualizaciones disponibles para el software de terceros, incluido el software de Microsoft, se descarga en el dispositivo que esté usando.

Para exportar a un archivo de texto la lista de actualizaciones disponibles para el software de terceros instalado en un dispositivo administrado específico:

1. Abra la lista de actualizaciones de software de terceros disponibles para el dispositivo administrado pertinente.

   Se mostrará una lista con las actualizaciones disponibles.

   Si desea exportar la lista completa de actualizaciones de software, tenga en cuenta que solo se exportarán las actualizaciones que aparezcan en la página que esté viendo.

   Si desea exportar solo algunas actualizaciones, marque las casillas ubicadas junto a las actualizaciones que desee ver en la lista.

   Si desea exportar solo las actualizaciones instaladas, marque la casilla **Mostrar actualizaciones instaladas**.

2. Haga clic en el botón **Exportar a TXT** o en el botón **Exportar a CSV**, dependiendo del formato de exportación que prefiera. Si no ve alguno de estos botones, haga clic en el botón de los puntos suspensivos y, luego, seleccione la opción que desee de la lista desplegable.

En el dispositivo que esté usando, se guardará el archivo con la lista de actualizaciones disponibles para el software de terceros (incluido el software de Microsoft) instalado en el dispositivo administrado seleccionado.

Aprobar y rechazar actualizaciones de software de terceros

Al configurar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, puede crear una regla que exija que las actualizaciones que se deban instalar tengan un estado específico. Una regla de actualización puede permitir, por ejemplo, la instalación de estas actualizaciones:

- Solo las actualizaciones aprobadas
- Solo las actualizaciones aprobadas o sin estado definido
- Todas las actualizaciones, independientemente de su estado

Puede aprobar las actualizaciones que deban instalarse y rechazar las que no deban instalarse.

Puede usar el estado *Aprobada* para administrar la instalación de una cantidad de actualizaciones modesta. Cuando necesite instalar muchas actualizaciones, utilice, en cambio, las reglas que puede configurar en las propiedades de la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*. Asigne el estado *Aprobada* únicamente a las actualizaciones específicas que no cumplan con los criterios indicados en las reglas. Cuando aprueba manualmente una gran cantidad de actualizaciones, el rendimiento del Servidor de administración disminuye, lo que puede provocar su sobrecarga.

Para aprobar o rechazar una o más actualizaciones:

1. En el menú principal, vaya a **Administración de software → Administración de parches → Actualizaciones de software**.

   Se mostrará una lista con las actualizaciones disponibles.

2. Seleccione las actualizaciones que desee aprobar o rechazar.

3. Haga clic en el botón **Aprobar** para aprobar las actualizaciones seleccionadas o en el botón **Rechazar** para rechazarlas. Si no ve alguno de estos botones, haga clic en el botón de los puntos suspensivos y, luego, seleccione la opción que desee de la lista desplegable.

   El estado predeterminado de una actualización es *Sin definir*.

Los estados de las actualizaciones seleccionadas cambian a los que ha elegido.

Como alternativa, puede cambiar el estado de aprobación en las propiedades de una actualización específica.

Para aprobar o rechazar una actualización desde sus propiedades:

1. En el menú principal, vaya a **Administración de software → Administración de parches → Actualizaciones de software**.

   Se mostrará una lista con las actualizaciones disponibles.

2. Haga clic en el nombre de la actualización que desee aprobar o rechazar.

   Se abre la ventana de propiedades de la actualización.

3. En la sección **General**, seleccione el estado de la actualización en la lista desplegable **Estado de aprobación de la actualización**. Puede seleccionar los estados *Aprobada*, *Rechazada* o *Sin definir*.

4. Haga clic en **Guardar** para guardar los cambios.

El estado de la actualización seleccionada cambia al que ha elegido.

Si configura el estado *Rechazada* para las actualizaciones de software de terceros, estas actualizaciones no se instalarán en los dispositivos cuya instalación se haya planeado pero aún no se haya realizado. Las actualizaciones no se eliminarán de los dispositivos en los que ya se encuentren instaladas. Si es necesario, puede eliminarlas manualmente de forma local.

Crear la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades

Para utilizar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, debe tener una licencia de Administración de vulnerabilidades y parches.

Utilice la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* para aplicar actualizaciones y reparar vulnerabilidades en las aplicaciones de terceros instaladas en los dispositivos administrados. Esta tarea le permite aplicar diversas múltiples actualizaciones y reparar múltiples vulnerabilidades siguiendo un conjunto de con las reglas, indicadas que especifica en la configuración de la tarea.

Si desea usar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* para instalar actualizaciones o reparar vulnerabilidades, realice alguna de las siguientes acciones:

- Ejecute el Asistente de instalación de actualizaciones o el Asistente de reparación de vulnerabilidades.
- Cree una tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*.
- Agregue una regla de instalación de actualizaciones a una tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* existente.

Para crear la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades:

1. En el menú principal, vaya a **Tareas**.

2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

3. En la lista desplegable **Aplicación**, seleccione Kaspersky Security Center Linux.

4. En la lista **Tipo de tarea**, seleccione el tipo de tarea **Instalar actualizaciones requeridas y reparar vulnerabilidades**.

   Si no ve esta la tarea, no aparece, asegúrese de que la cuenta tenga los derechos de **Lectura**, **Escritura** y **Ejecución** para el área funcional **Administración del sistema**: **Administración de vulnerabilidades y parches**. Sin estos derechos de acceso, no podrá crear ni configurar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*.

5. En el campo **Nombre de la tarea**, ingrese el nombre de la tarea nueva.

   El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).

6. Seleccione los dispositivos a los que se asignará la tarea.

7. Agregue las reglas de instalación de actualizaciones en el paso **Elija las reglas de instalación de actualizaciones** del asistente.

   Estas reglas se aplican a la instalación de actualizaciones en dispositivos cliente. Si no se especifican las reglas, la tarea no tiene nada que realizar. Para obtener información sobre las operaciones con reglas, consulte Reglas para la instalación de actualizaciones.

   Estas reglas se aplican a la instalación de actualizaciones en dispositivos cliente. Si no especifica ninguna regla, la tarea se omitirá.

8. Configure los siguientes ajustes:

   - **Comenzar la instalación cuando se esté por reiniciar o apagar el dispositivo**

     Si esta opción está habilitada, las actualizaciones se instalarán en el momento en el que los dispositivos se reinicien o se apaguen. De lo contrario, las actualizaciones se instalarán siguiendo la programación que se defina.

     Utilice esta opción si la instalación de las actualizaciones podría afectar el rendimiento de los dispositivos.

     Esta opción está deshabilitada de forma predeterminada.

   - **Instalar los componentes generales obligatorios del sistema**

     Si esta opción está habilitada, antes de que se instale una actualización, la aplicación instalará automáticamente todos los componentes generales del sistema que la actualización requiera para instalarse (los llamados "requisitos previos"). Una actualización podría requerir, por ejemplo, que esté instalada cierta actualización del sistema operativo.

     Si esta opción está deshabilitada, posiblemente tenga que instalar los requisitos previos manualmente.

     Esta opción está deshabilitada de forma predeterminada.

   - **Permitir que se instalen versiones nuevas de las aplicaciones durante la actualización**

     Si esta opción está habilitada, las actualizaciones podrán cambiar la versión del software actualizado por una más reciente.

     Si esta opción está deshabilitada, los cambios de versión no estarán permitidos. Para instalar una versión más reciente de una aplicación, deberá usar una tarea diferente o proceder en forma manual. Podría usar esta opción si, por ejemplo, desea evaluar el cambio de versión en una infraestructura de prueba o si sabe que la versión más reciente no es compatible con la infraestructura de su empresa.

     Esta opción está activada de forma predeterminada.

     > Los cambios de versión pueden ocasionar problemas de funcionamiento en las aplicaciones dependientes instaladas en los dispositivos cliente.

   - **Descargar las actualizaciones en el dispositivo sin instalarlas**

     Si esta opción está habilitada, la aplicación descargará las actualizaciones disponibles en los dispositivos, pero no las instalará automáticamente. Podrá instalar las actualizaciones descargadas manualmente.

Las actualizaciones de Microsoft se descargan en el sistema de almacenamiento de Windows. Las actualizaciones para aplicaciones de terceros (aplicaciones creadas por proveedores de software que no son ni Kaspersky ni Microsoft) se descargan en la carpeta especificada en el campo **Descargar actualizaciones en**.

Si esta opción está deshabilitada, las actualizaciones se instalarán en los dispositivos automáticamente.

Esta opción está deshabilitada de forma predeterminada.

- **Descargar actualizaciones en**

  Esta carpeta se utiliza para descargar las actualizaciones para aplicaciones de terceros (aplicaciones creadas por proveedores de software que no son ni Kaspersky ni Microsoft).

- **Habilitar diagnóstico avanzado**

  Si esta función está habilitada, el Agente de red escribe archivos de seguimiento incluso si el seguimiento está desactivado para el Agente de red en la Utilidad de diagnóstico remoto de Kaspersky Security Center Linux. Los datos de seguimiento se guardan en dos archivos sucesivamente; el tamaño total de ambos archivos está determinado por el valor de la opción **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**. Cuando los archivos alcanzan su límite de tamaño, el Agente de red comienza a sobrescribirlos. Los archivos de seguimiento se almacenan en la carpeta %WINDIR%\Temp. Puede usar la utilidad de diagnóstico remoto para acceder a estos archivos, descargarlos y eliminarlos.

  Si esta función está deshabilitada, el Agente de red escribe datos de seguimiento de acuerdo con la configuración de la Utilidad de diagnóstico remoto de Kaspersky Security Center Linux. No se guardará ningún otro dato de seguimiento.

  No es necesario que habilite la característica de diagnóstico avanzado al momento de crear una tarea. Es posible que desee utilizar esta función más adelante si, por ejemplo, una ejecución de tarea falla en algunos de los dispositivos y desea recopilar información adicional durante otra ejecución de tarea.

  Esta opción está deshabilitada de forma predeterminada.

  - **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**

    El valor predeterminado es 100 MB, y los valores disponibles están entre 1 MB y 2048 MB. Los especialistas en soporte técnico de Kaspersky podrían pedirle que cambie el valor predeterminado si, para solucionar un problema, les remite archivos de diagnóstico avanzado con información insuficiente.

Avance al siguiente paso del asistente.

9. Defina las opciones de reinicio del sistema operativo:

   - **No reiniciar el dispositivo**

     Cuando termine la operación, los dispositivos cliente no se reiniciarán automáticamente. Para que la operación se complete, deberá reiniciar los dispositivos en forma manual o mediante, por ejemplo, una tarea de administración de dispositivos. Los resultados de la tarea y el estado de cada dispositivo darán cuenta de que hay un reinicio pendiente. Esta opción es útil cuando la tarea va a ejecutarse en servidores y dispositivos que deben operar continuamente.

   - **Reiniciar el dispositivo**

     Los dispositivos cliente se reiniciarán automáticamente siempre que resulte necesario para completar la operación. Esta opción es útil cuando la tarea se realiza en dispositivos que admiten una breve interrupción para apagarse o reiniciarse.

- **Solicitar al usuario una acción**

  A través de un recordatorio en pantalla, se le pedirá a cada usuario que reinicie su dispositivo manualmente. Puede configurar algunos ajustes avanzados para esta opción: el texto del mensaje que se le muestra al usuario, la frecuencia con la que se muestra este mensaje y el tiempo que se espera antes de reiniciar el dispositivo por la fuerza (sin que el usuario confirme el reinicio). Esta opción es la más adecuada para estaciones de trabajo en las que los usuarios deben poder seleccionar el momento más conveniente para reiniciar.

  Esta opción está seleccionada de forma predeterminada.

- **Repetir solicitud cada (min)**

  Si habilita esta opción, la aplicación le solicitará al usuario que reinicie su sistema operativo con la frecuencia especificada.

  Esta opción está activada de forma predeterminada. El intervalo por defecto es de 5 minutos. Los valores disponibles van de 1 a 1440 minutos.

  Si no habilita esta opción, la solicitud se mostrará una sola vez.

- **Reiniciar después de (min)**

  Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

  Esta opción está activada de forma predeterminada. El tiempo de espera por defecto es de 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Tiempo de espera antes del cierre forzado de aplicaciones en sesiones bloqueadas (min)**

  Las aplicaciones se cerrarán por la fuerza cuando el dispositivo del usuario se bloquee (sea manualmente o en forma automática tras un tiempo de inactividad).

  Si esta opción está habilitada, las aplicaciones del dispositivo bloqueado se cerrarán por la fuerza luego de transcurra el intervalo especificado en el campo de entrada.

  Si esta opción está deshabilitada, las aplicaciones del dispositivo bloqueado no se cerrarán.

  Esta opción está deshabilitada de forma predeterminada.

10. En el paso **Finalizar la creación de la tarea** del asistente, habilite la opción **Abrir los detalles de la tarea cuando se complete la creación** para modificar la configuración predeterminada de la tarea.

    Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Podrá modificarla más adelante.

11. Haga clic en el botón **Finalizar**.

    El Asistente para crear nueva tarea creará la tarea. Si habilitó la opción **Abrir los detalles de la tarea cuando se complete la creación**, se abrirá automáticamente la ventana de propiedades de la tarea. En esta ventana, puede definir la configuración general de la tarea y, si es necesario, cambiar los ajustes establecidos durante la creación de la tarea.

    > También puede abrir la ventana de propiedades de la tarea haciendo clic en el nombre de la tarea creada en la lista de tareas.

    La tarea se creará, configurará y se mostrará en la lista de tareas.

12. Para ejecutar la tarea, selecciónela en la lista de tareas y haga clic en el botón **Iniciar**.

    También puede programar el inicio de la tarea en la pestaña **Programación**, en la ventana de propiedades de la tarea.

Para obtener una descripción detallada de la configuración de inicio programado, vea la configuración general de la tarea.

Una vez completada la tarea, se instalan las actualizaciones necesarias y se reparan las vulnerabilidades.

Si en la red de la organización se utiliza el servidor WSUS (servidor WSUS local) y desea usarlo junto con el Servidor de administración, primero debe asegurarse de que el Servidor de administración no se use como servidor WSUS y, luego, hacer lo siguiente:

a. En los dispositivos administrados que ejecutan Windows, especifique el servidor WSUS local para el servicio Windows Update. Puede hacerlo de forma manual desde el Registro de Windows o con una directiva de grupo de Windows.

b. En el servidor WSUS local, especifique las clasificaciones necesarias para las actualizaciones y las aplicaciones donde se distribuirán las actualizaciones.

c. Sincronice el servidor WSUS con el servidor que lo precede (puede ser un servidor WSUS de Microsoft u otro servidor WSUS local anterior).

Después de que se ejecute la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* en el dispositivo, el Agente de red utiliza el servicio de Windows Update para instalar las actualizaciones de Windows. El servicio Windows Update obtiene la dirección del servidor WSUS externo del registro y descarga las actualizaciones directamente desde dicho servidor WSUS externo.

Agregar reglas de instalación de actualizaciones

Esta función solo está disponible con una licencia de Administración de vulnerabilidades y parches.

Si desea utilizar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* para instalar actualizaciones de software o reparar vulnerabilidades en sus aplicaciones, debe definir reglas de instalación de actualizaciones. Estas reglas determinan qué actualizaciones se deben instalar y qué vulnerabilidades se deben reparar.

La configuración exacta depende de si la regla se creará para todas las actualizaciones, para actualizaciones de Windows Update o para actualizaciones publicadas para aplicaciones de terceros (aplicaciones creadas por proveedores de software que no sean ni Kaspersky ni Microsoft). Cuando agregue una regla para actualizaciones de Windows Update o para actualizaciones de aplicaciones de terceros, podrá seleccionar las aplicaciones específicas (y las versiones puntuales de esas aplicaciones) para las que desee instalar actualizaciones. Cuando agregue una regla para todas las actualizaciones, podrá seleccionar las actualizaciones específicas que desee instalar y las vulnerabilidades puntuales que desee reparar mediante la instalación de actualizaciones.

Para agregar una regla de instalación de actualizaciones, puede optar por cualquiera de estos métodos:

- Al agregar una regla al crear una nueva tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*.
- Agregue la regla en la pestaña **Configuración de la aplicación** de la ventana de propiedades de una tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* existente.
- Utilice el Asistente de instalación de actualizaciones o el Asistente de reparación de vulnerabilidades.

Agregar reglas para todas las actualizaciones

Para agregar una nueva regla para todas las actualizaciones, haga lo siguiente:

1. Haga clic en **Agregar**.

   Se inicia el Asistente de creación de reglas. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

2. En el paso **Seleccionar tipo de regla** del asistente, elija **Regla para todas las actualizaciones**.

3. En el paso **Criterios generales** del asistente, defina los siguientes ajustes:

   - **Conjunto de actualizaciones que se instalarán**

     Seleccione las actualizaciones que deban instalarse en los dispositivos cliente:

     - **Instalar las actualizaciones aprobadas únicamente**. Solo se instalarán las actualizaciones que estén aprobadas.
     - **Instalar todas las actualizaciones (excepto las rechazadas)**. Se instalarán las actualizaciones que tengan el estado de aprobación *Aprobada* o *Sin definir*.
     - **Instalar todas las actualizaciones (incluidas las rechazadas)**. Se instalarán todas las actualizaciones, sin importar su estado de aprobación. Tenga cuidado al utilizar esta opción. Selecciónela si, por ejemplo, quiere usar una infraestructura de prueba para evaluar la instalación de algunas actualizaciones rechazadas.

   - **Reparar vulnerabilidades que tengan o superen este nivel de gravedad**

     Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

     Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Medio**, **Alto** o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

     Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

     Esta opción está deshabilitada de forma predeterminada.

   Avance al siguiente paso del asistente.

4. Seleccione las actualizaciones que se instalarán:

   - **Instalar todas las actualizaciones adecuadas**

     Instalar todas las actualizaciones de software que cumplan con los criterios especificados en la página **Criterios generales** del asistente. Esta es la opción seleccionada por defecto.

   - **Instalar solo las actualizaciones de la lista**

     Se instalarán únicamente las actualizaciones de software que seleccione manualmente en la lista. La lista contiene todas las actualizaciones de software disponibles.

Existen situaciones en las que querrá elegir manualmente las actualizaciones que se instalarán: podría suceder, por ejemplo, que quiera evaluar ciertas actualizaciones en un entorno de prueba, que quiera actualizar solo las aplicaciones que considere importantes o que necesite actualizar solo algunas aplicaciones puntuales.

- **Instalar automáticamente todas las actualizaciones de software que antecedan a las seleccionadas y se requieran para instalarlas**

  Mantenga habilitada esta opción si está de acuerdo en que, para instalar las actualizaciones seleccionadas, se instalen versiones intermedias de las aplicaciones.

  Si deshabilita esta opción, se instalarán únicamente las versiones de las aplicaciones que haya seleccionado. Deshabilite esta opción si quiere que las aplicaciones se actualicen en forma directa, sin que se trate de instalar versiones intermedias. Cuando las actualizaciones seleccionadas no se puedan instalar sin que antes se instalen versiones más antiguas de las aplicaciones, el proceso de actualización no se completará.

  A modo de ejemplo, imagine que un dispositivo tiene instalada la versión 3 de una aplicación. Quiere actualizar esa versión a la 5, pero la versión 5 solo se puede instalar sobre la versión 4. Si esta opción está habilitada, el software instalará primero la versión 4 y luego la versión 5. Si esta opción está deshabilitada, el software no podrá actualizar la aplicación.

  Esta opción está activada de forma predeterminada.

Avance al siguiente paso del asistente.

5. Seleccione las vulnerabilidades que se repararán al instalar las actualizaciones seleccionadas:

   - **Reparar todas las vulnerabilidades que coincidan con otros criterios**

     Reparar todas las vulnerabilidades que cumplan con los criterios especificados en la página **Criterios generales** del asistente. Esta es la opción seleccionada por defecto.

   - **Reparar solo las vulnerabilidades de la lista**

     Se repararán únicamente las vulnerabilidades que seleccione manualmente en la lista. La lista contiene todas las vulnerabilidades detectadas.

     Existen situaciones en las que querrá elegir manualmente las vulnerabilidades que se repararán: podría suceder, por ejemplo, que quiera verificar en un entorno de prueba que las vulnerabilidades se puedan reparar, que quiera reparar las vulnerabilidades solo en las aplicaciones que considere importantes o que prefiera reparar las vulnerabilidades solo en ciertas aplicaciones puntuales.

   Avance al siguiente paso del asistente.

6. Escriba el nombre de la regla que está agregando. Podrá cambiar este nombre más tarde en la pestaña **Configuración de la aplicación** de la ventana de propiedades de la tarea creada.

La nueva regla se creará y configurará, y aparecerá en la tabla de reglas del Asistente para crear nueva tarea.

Agregar reglas para actualizaciones de Windows Update

Para agregar una nueva regla para actualizaciones de Windows Update, haga lo siguiente:

1. Haga clic en **Agregar**.

   Se inicia el Asistente de creación de reglas. Avance por el asistente utilizando el botón **Siguiente**.

2. Seleccione **Regla para Windows Update**.

   Avance al siguiente paso del asistente.

3. En el paso **Criterios generales** del asistente, defina los siguientes ajustes:

   - **Conjunto de actualizaciones que se instalarán**

     Seleccione las actualizaciones que deban instalarse en los dispositivos cliente:

     - **Instalar las actualizaciones aprobadas únicamente**. Solo se instalarán las actualizaciones que estén aprobadas.
     - **Instalar todas las actualizaciones (excepto las rechazadas)**. Se instalarán las actualizaciones que tengan el estado de aprobación *Aprobada* o *Sin definir*.
     - **Instalar todas las actualizaciones (incluidas las rechazadas)**. Se instalarán todas las actualizaciones, sin importar su estado de aprobación. Tenga cuidado al utilizar esta opción. Selecciónela si, por ejemplo, quiere usar una infraestructura de prueba para evaluar la instalación de algunas actualizaciones rechazadas.

   - **Reparar vulnerabilidades que tengan o superen este nivel de gravedad**

     Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

     Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Medio**, **Alto** o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

     Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

     Esta opción está deshabilitada de forma predeterminada.

   - **Reparar vulnerabilidades con un nivel de gravedad de MSRC igual o mayor que**

     Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

     Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que el Centro de respuestas de seguridad de Microsoft (MSRC) haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Bajo**, **Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

     Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

     Esta opción está deshabilitada de forma predeterminada.

4. En la página **Aplicaciones**, seleccione las aplicaciones y las versiones de las aplicaciones para las que desee instalar actualizaciones. Por defecto, están seleccionadas todas las aplicaciones.

5. En la página **Categorías de actualizaciones**, seleccione las categorías de actualizaciones que se instalarán. Las categorías son las mismas que se usan en el Catálogo de Microsoft Update. Por defecto, están seleccionadas todas las categorías.

6. En la página **Nombre**, escriba un nombre para la regla que está agregando. Podrá cambiar este nombre más tarde, en la sección **Configuración** de la ventana de propiedades de la tarea creada.

Cuando el Asistente de creación de reglas llegue a su fin, se agregará la nueva regla. La encontrará en la lista de

reglas del Asistente para crear nueva tarea o en las propiedades de la tarea.

Agregar reglas para actualizaciones de aplicaciones de terceros

Para agregar una nueva regla para actualizaciones de aplicaciones de terceros, haga lo siguiente:

1. Haga clic en **Agregar**.

   Se inicia el Asistente de creación de reglas. Avance por el asistente utilizando el botón **Siguiente**.

2. En el paso **Seleccionar tipo de regla** del asistente, elija **Regla para las actualizaciones de terceros**.

3. En el paso **Criterios generales** del asistente, defina los siguientes ajustes:

   - **Conjunto de actualizaciones que se instalarán**

     Seleccione las actualizaciones que deban instalarse en los dispositivos cliente:

     - **Instalar las actualizaciones aprobadas únicamente**. Solo se instalarán las actualizaciones que estén aprobadas.
     - **Instalar todas las actualizaciones (excepto las rechazadas)**. Se instalarán las actualizaciones que tengan el estado de aprobación *Aprobada* o *Sin definir*.
     - **Instalar todas las actualizaciones (incluidas las rechazadas)**. Se instalarán todas las actualizaciones, sin importar su estado de aprobación. Tenga cuidado al utilizar esta opción. Selecciónela si, por ejemplo, quiere usar una infraestructura de prueba para evaluar la instalación de algunas actualizaciones rechazadas.

   - **Reparar vulnerabilidades que tengan o superen este nivel de gravedad**

     Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

     Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Medio**, **Alto** o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

     Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

     Esta opción está deshabilitada de forma predeterminada.

   Avance al siguiente paso del asistente.

4. Seleccione las aplicaciones y las versiones de las aplicaciones para las que desee instalar actualizaciones.

   Por defecto, están seleccionadas todas las aplicaciones.

   Avance al siguiente paso del asistente.

5. Escriba el nombre de la regla que está agregando. Podrá cambiar este nombre más tarde en la pestaña **Configuración de la aplicación** de la ventana de propiedades de la tarea creada.

La nueva regla se creará y configurará, y aparecerá en la tabla de reglas del Asistente para crear nueva tarea.

Configuración de la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades especificada después de su creación

Después de crear la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, puede definir los siguientes ajustes de configuración en la pestaña **Configuración de la aplicación** de la ventana de propiedades de la tarea:

- En la sección **Instalación de prueba**:
  - **No analizar**. Seleccione esta opción si no desea realizar una instalación de prueba de las actualizaciones.
  - **Ejecutar análisis en los dispositivos seleccionados**. Seleccione esta opción si desea probar la instalación de actualizaciones en dispositivos seleccionados. Haga clic en el botón **Agregar** y, luego, seleccione los dispositivos en los que desee realizar una instalación de prueba de las actualizaciones.
  - **Ejecutar análisis en los dispositivos del grupo especificado**. Seleccione esta opción si desea probar la instalación de actualizaciones en un grupo de dispositivos. En el campo **Especifique un grupo de prueba**, indique un grupo de dispositivos en el que desee realizar una instalación de prueba.
  - **Ejecutar análisis en el porcentaje de dispositivos especificado**. Seleccione esta opción si desea probar la instalación de actualizaciones en un porcentaje de dispositivos. En el campo **Porcentaje de dispositivos de prueba en relación con todos los dispositivos de destino**, indique el porcentaje de dispositivos en el que desee realizar una instalación de prueba de las actualizaciones.

  Una vez que haya seleccionado cualquier opción excepto **No analizar**, en el campo **Cantidad de tiempo para tomar la decisión de si se debe continuar la instalación, en horas**, indique la cantidad de horas que deberán transcurrir desde la instalación de prueba de las actualizaciones hasta el inicio de la instalación de las actualizaciones en todos los dispositivos.
- En la sección **Actualizaciones para instalar**, puede ver la lista de actualizaciones instaladas por la tarea. Solo se muestran las actualizaciones que coinciden con la configuración de la tarea aplicada.

Para obtener una descripción completa de los ajustes de configuración de la tarea, vea los ajustes de configuración generales de la tarea.

Actualización automática de aplicaciones de terceros

Algunas aplicaciones de terceros se pueden actualizar automáticamente. Quien determina si una aplicación es compatible con la función de actualización automática es su desarrollador o proveedor. Si una aplicación de terceros instalada en un dispositivo administrado se puede actualizar automáticamente, podrá configurar el ajuste de actualización automática en las propiedades de esa aplicación. Luego de que modifique este ajuste, las instancias del Agente de red implementarán el nuevo valor en cada dispositivo administrado que tenga instalada esa aplicación.

El ajuste de actualización automática es independiente de los demás objetos y ajustes de la característica Administración de vulnerabilidades y parches. Este ajuste, por ejemplo, no se ve afectado por los estados de aprobación de las actualizaciones ni por las distintas tareas de instalación de actualizaciones, como *Instalar actualizaciones requeridas y reparar vulnerabilidades* y *Reparar vulnerabilidades*.

Para configurar el ajuste de actualización automática para una aplicación creada por un tercero:

1. En la ventana principal de la aplicación, vaya a la sección **Administración de software → Aplicaciones de terceros → Registro de aplicaciones**.

2. Haga clic en el nombre de la aplicación para la que desee modificar el ajuste de actualización automática.

   Puede usar las columnas **Estado de las actualizaciones automáticas** y **Administrar actualizaciones automáticas** para filtrar la lista y simplificar la búsqueda.

   Se abrirá la ventana de propiedades de la aplicación.

3. En la sección **General**, seleccione un valor para la siguiente función:

   Estado de las actualizaciones automáticas

   Seleccione una de las siguientes opciones:

   - **Sin definir**

     Se deshabilitará la función de actualización automática. Kaspersky Security Center Linux instala actualizaciones de aplicaciones de terceros mediante las siguientes tareas: *Instalar actualizaciones requeridas y reparar vulnerabilidades* y *Reparar vulnerabilidades*.

   - **Permitido**

     Las actualizaciones que el proveedor publique para la aplicación se instalarán automáticamente en los dispositivos administrados. No se requerirá ninguna otra acción.

   - **Bloqueado**

     Las actualizaciones para la aplicación no se instalarán automáticamente. Kaspersky Security Center Linux instala actualizaciones de aplicaciones de terceros mediante las siguientes tareas: *Instalar actualizaciones requeridas y reparar vulnerabilidades* y *Reparar vulnerabilidades*.

4. Haga clic en **Guardar** para guardar los cambios.

El valor definido para el ajuste de actualización automática se implementa en la aplicación seleccionada.

Reparación de vulnerabilidades en el software de terceros

En esta sección, se describen las características de Kaspersky Security Center Linux relacionadas con la reparación de vulnerabilidades en el software instalado en dispositivos administrados.

Acerca de la búsqueda y reparación de vulnerabilidades de software

Kaspersky Security Center Linux detecta y repara vulnerabilidades de software en dispositivos administrados que ejecutan sistemas operativos Microsoft Windows. La solución puede detectar vulnerabilidades tanto en el sistema operativo como en aplicaciones desarrolladas por Microsoft y otros terceros.

La función de actualizaciones (incluido el suministro de actualizaciones para las firmas antivirus y la base de código) y la función de KSN pueden dejar de estar disponibles en el software en el territorio de EE. UU.

Búsqueda de vulnerabilidades de software

Para encontrar vulnerabilidades de software, Kaspersky Security Center Linux utiliza funciones de una base de datos de vulnerabilidades conocidas. Esta base de datos fue creada y es mantenida por lo especialistas de Kaspersky. Contiene datos de diverso tipo sobre cada vulnerabilidad: la descripción de la vulnerabilidad, su fecha de detección y su nivel de gravedad. Puede ver los detalles de las vulnerabilidades de software en el sitio web de Kaspersky.

Kaspersky Security Center Linux usa la tarea *Buscar vulnerabilidades y actualizaciones requeridas* para encontrar vulnerabilidades de software.

Reparación de vulnerabilidades de software

Para reparar vulnerabilidades de software, Kaspersky Security Center Linux utiliza las actualizaciones de software que publican los proveedores de software. Los metadatos de estas actualizaciones se copian al repositorio del Servidor de administración cuando se ejecuta la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*. Esta tarea tiene como objetivo descargar metadatos de actualizaciones para software de Kaspersky y de terceros. La tarea se crea automáticamente cuando se utiliza el asistente de inicio rápido de Kaspersky Security Center Linux. De ser necesario, también se puede crear la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* de forma manual.

Las actualizaciones de software con las que se corrigen las vulnerabilidades pueden ser paquetes de distribución completos o parches. Las actualizaciones de software diseñadas para corregir vulnerabilidades de software se denominan *reparaciones*. Las *correcciones recomendadas* son aquellas que los especialistas de Kaspersky sugieren instalar. Las *correcciones de usuario* son aquellas que los usuarios eligen instalar manualmente. Para instalar una corrección de usuario, se debe crear un paquete de instalación que contenga esta reparación.

Si tiene una licencia de Kaspersky Security Center Linux con la función de Administración de vulnerabilidades y parches, puede usar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*. La tarea repara múltiples vulnerabilidades automáticamente instalando las reparaciones recomendadas. Si utiliza esta tarea, puede configurar manualmente ciertas reglas para la reparación de distintas vulnerabilidades.

Si no tiene una licencia de Kaspersky Security Center Linux con la función Administración de vulnerabilidades y parches, puede usar la tarea *Reparar vulnerabilidades*. Con esta tarea, puede corregir vulnerabilidades instalando reparaciones recomendadas para el software de Microsoft y reparaciones de usuario para el software de otros proveedores.

Por seguridad, cada actualización de software de terceros que se instala con la función Administración de vulnerabilidades y parches se somete a un análisis antimalware automático con las tecnologías de Kaspersky. Estas tecnologías revisan automáticamente los archivos utilizando técnicas de análisis antivirus, análisis estático, análisis dinámico, análisis de comportamiento en un entorno de pruebas y aprendizaje automático, entre otras.

Los expertos de Kaspersky no realizan análisis manuales de las actualizaciones de software de terceros que puedan instalarse mediante la función Administración de vulnerabilidades y parches. Tampoco buscan vulnerabilidades (conocidas o desconocidas) o funciones no documentadas en las actualizaciones ni las analizan de modos que no se hayan indicado en el párrafo anterior.

Para actualizar una aplicación de terceros o reparar una vulnerabilidad en una aplicación de terceros instalada en un dispositivo administrado, podría necesitarse la colaboración del usuario. Si la aplicación está abierta, por ejemplo, podría tener que pedirle al usuario que la cierre.

Para reparar algunas vulnerabilidades de software, deberá aceptar un contrato de licencia de usuario final (EULA) que lo faculte a instalar el software. Si se le solicita aceptar el EULA, hágalo. Si rechaza el EULA, la vulnerabilidad de software correspondiente no se reparará.

Procedimiento: búsqueda y reparación de vulnerabilidades de software de terceros

En esta sección, se describe un escenario para buscar y reparar vulnerabilidades en dispositivos administrados que utilizan el sistema operativo Windows. Puede detectar y reparar vulnerabilidades en el sistema operativo y en las aplicaciones de terceros, incluidas las de Microsoft.

Requisitos previos

- Kaspersky Security Center Linux se implementó en su organización.
- Hay dispositivos administrados que ejecutan Windows en su organización.
- Existe una conexión a Internet que le permita al Servidor de administración realizar las siguientes tareas:
  - Hacer una lista de reparaciones recomendadas para vulnerabilidades en el software de Microsoft. Los especialistas de Kaspersky crean y actualizan periódicamente esta lista.
  - Reparar vulnerabilidades en software de terceros que no sean Microsoft.

Etapas

El proceso para buscar y reparar vulnerabilidades de software se divide en etapas:

1. **Análisis en busca de vulnerabilidades en el software instalado en los dispositivos administrados**

Para encontrar vulnerabilidades en el software instalado en los dispositivos administrados, ejecute la tarea *Buscar vulnerabilidades y actualizaciones requeridas*. Cuando se completa esta tarea, Kaspersky Security Center Linux recibe una lista con las vulnerabilidades detectadas y las actualizaciones necesarias para el software de terceros instalado en los dispositivos indicados en las propiedades de la tarea.

La tarea *Buscar vulnerabilidades y actualizaciones requeridas* se crea automáticamente con el asistente de inicio rápido de Kaspersky Security Center Linux. Si no ejecutó el asistente de inicio rápido, puede hacerlo en este momento o puede crear la tarea manualmente.

Puede crear la tarea *Buscar vulnerabilidades y actualizaciones requeridas* solo para dispositivos Windows. No puede crear esta tarea para dispositivos que ejecutan otros sistemas operativos.

2 Ver la lista de vulnerabilidades de software detectadas

Abra la lista **Vulnerabilidades de software** y decida qué vulnerabilidades desea reparar. Para ver información detallada sobre una vulnerabilidad, haga clic en el nombre de la misma en la lista. La aplicación le da acceso a estadísticas sobre el estado de cada vulnerabilidad en los dispositivos administrados.

3 Configurar la reparación de vulnerabilidades

Tras detectarse las vulnerabilidades de software, puede corregir las que estén presentes en los dispositivos administrados utilizando la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* o la tarea *Reparar vulnerabilidades*.

Utilice la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* para aplicar actualizaciones y reparar vulnerabilidades en las aplicaciones de terceros (incluidas las de Microsoft) instaladas en los dispositivos administrados. Puede usar esta tarea para instalar múltiples actualizaciones y reparar múltiples vulnerabilidades utilizando un conjunto de reglas. Tenga en cuenta que esta tarea se puede crear únicamente si se cuenta con una licencia para la función Administración de vulnerabilidades y parches. Para corregir las vulnerabilidades que se detecten en las aplicaciones, la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* usará las actualizaciones de software recomendadas.

La tarea *Reparar vulnerabilidades* no requiere la opción de licencia correspondiente a la función Administración de vulnerabilidades y parches. Para utilizar esta tarea, se deben indicar manualmente las soluciones de usuario que se usarán para reparar las vulnerabilidades en el software de terceros que figuren en la configuración de la tarea La tarea *Reparar vulnerabilidades* utiliza las actualizaciones recomendadas para el software de Microsoft y las actualizaciones indicadas por el usuario para el software de terceros.

Las tareas *Instalar actualizaciones requeridas y reparar vulnerabilidades* y *Reparar vulnerabilidades* únicamente se pueden crear para dispositivos Windows. No puede crear estas tareas para dispositivos que se ejecutan en otros sistemas operativos.

Puede crear estas tareas en forma manual o a través del Asistente de reparación de vulnerabilidades, que las crea en forma automática.

Si creó y configuró la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, las vulnerabilidades se repararán en los dispositivos administrados automáticamente. Cuando se ejecute la tarea creada, la lista de actualizaciones de software disponibles se comparará con las reglas especificadas en la configuración de la tarea. Las actualizaciones de software que cumplan con los criterios de las reglas se descargarán en el repositorio del Servidor de administración y se instalarán a fin de reparar las vulnerabilidades de software.

Si creó la tarea *Reparar vulnerabilidades*, solo se corregirán las vulnerabilidades presentes en el software de Microsoft.

4 Programar las tareas

Programe la tarea *Buscar vulnerabilidades y actualizaciones requeridas* para que se ejecute automáticamente de forma periódica a fin de mantener actualizada la lista de vulnerabilidades. Se recomienda una frecuencia promedio de una vez a la semana.

Si creó la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, puede programarla para que se ejecute con igual o menor frecuencia que la tarea *Buscar vulnerabilidades y actualizaciones requeridas*. Aunque puede definir una programación para la tarea *Reparar vulnerabilidades*, tenga en cuenta que, cada vez que esta se inicie, deberá seleccionar los parches que se aplicarán al software de Microsoft o de otros desarrolladores.

Cuando programe las tareas, asegúrese de que la tarea para reparar las vulnerabilidades se inicie después de que finalice la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

5. **Ignorar vulnerabilidades de software (opcional)**

   Puede ignorar determinadas vulnerabilidades de software en todos los dispositivos administrados o solo en los dispositivos administrados que usted seleccione.

6. **Ejecutar la tarea de reparación de vulnerabilidades**

   Inicie la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* o la tarea *Reparar vulnerabilidades*. Cuando se complete la tarea, asegúrese de que su estado en la lista de tareas sea *Completada correctamente*.

7. **Crear el informe sobre los resultados de la reparación de vulnerabilidades de software (opcional)**

   Para ver estadísticas detalladas sobre la reparación de vulnerabilidades, genere el "Informe de vulnerabilidades". El informe le indicará qué vulnerabilidades de software no se corrigieron. Así, podrá identificar y abordar las vulnerabilidades presentes en el software de terceros, (incluido el de Microsoft) que se utilice en su organización.

8. **Revisar la configuración de la búsqueda y reparación de vulnerabilidades en el software de terceros**

   Asegúrese de haber hecho lo siguiente:

   - Obtuvo y revisó la lista de vulnerabilidades de software detectadas en los dispositivos administrados.
   - Ignoró determinadas vulnerabilidades de software, de ser necesario.
   - Configuró la tarea de reparación de vulnerabilidades.
   - Programó las tareas de búsqueda y reparación de vulnerabilidades de software de manera tal que comiencen secuencialmente.
   - Verificó que se haya iniciado la tarea para reparar vulnerabilidades de software.

Reparación de vulnerabilidades en el software de terceros

Para encontrar vulnerabilidades en el software de terceros, puede crear y ejecutar la tarea *Buscar vulnerabilidades y actualizaciones requeridas*, y recibir una lista de vulnerabilidades de software. Una vez que tenga la lista de vulnerabilidades de software, puede reparar las que se hayan encontrado en los dispositivos Windows administrados.

Para reparar vulnerabilidades de software en el sistema operativo y en las aplicaciones creadas por terceros (incluido Microsoft), cree y ejecute la tarea Reparar vulnerabilidades o la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades.

Para actualizar una aplicación de terceros o reparar una vulnerabilidad en una aplicación de terceros instalada en un dispositivo administrado, podría necesitarse la colaboración del usuario. Si la aplicación afectada está abierta, por ejemplo, podría tener que pedirle al usuario que la cierre.

Como alternativa, para crear una tarea para reparar vulnerabilidades de software, puede optar por estas vías:

- Abra la lista de vulnerabilidades y seleccione las vulnerabilidades que desee reparar.

  Como resultado, se creará una nueva tarea para reparar las vulnerabilidades de software seleccionadas. Si lo prefiere, puede agregar las vulnerabilidades seleccionadas a una tarea existente.

- Utilice el Asistente de reparación de vulnerabilidades.

  > El Asistente de reparación de vulnerabilidades solo está disponible si se cuenta con una licencia de Administración de vulnerabilidades y parches.

  Este asistente simplifica la creación y configuración de tareas de reparación de vulnerabilidad y evita que se creen tareas redundantes.

Reparar vulnerabilidades de software a través de la lista de vulnerabilidades

Para reparar vulnerabilidades de software a través de la lista de vulnerabilidades:

1. Realice una de las siguientes acciones para abrir la lista de vulnerabilidades:

   - En el menú principal, vaya a **Administración de software** → **Administración de parches** → **Vulnerabilidades de software**.
   - En el menú principal, vaya a **Administración de activos** → **Dispositivos administrados** → <nombre del dispositivo> → **Avanzado** → **Vulnerabilidades de software**.
   - En la ventana principal de la aplicación, vaya a la sección **Administración de software** → **Aplicaciones de terceros** → **Registro de aplicaciones** → <nombre de la aplicación> → **Vulnerabilidades**.

   Se mostrará una tabla con una lista de las vulnerabilidades detectadas en el software de terceros instalado en los dispositivos administrados.

2. En la lista de vulnerabilidades, marque las casillas junto a las vulnerabilidades que desee reparar y, luego, haga clic en el botón **Reparar vulnerabilidad**.

   Si no se cuenta con la actualización de software recomendada para reparar alguna de las vulnerabilidades seleccionadas, se mostrará un mensaje informativo.

   Para reparar algunas vulnerabilidades de software, se le solicita al usuario que acepte un contrato de licencia de usuario final (EULA) para instalar el software. Deberá aceptar el EULA. Si rechaza el EULA, no se reparará la vulnerabilidad de software correspondiente.

3. Seleccione una de las siguientes opciones:

   - **Nueva tarea**

     Se inicia el Asistente para crear nueva tarea. Si tiene una licencia de Administración de vulnerabilidades y parches, la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades aparecerá marcada. Si no cuenta con esta licencia, el tipo de tarea Reparar vulnerabilidades estará preseleccionada. Siga los pasos del asistente para completar la creación de la tarea.

   - **Reparar vulnerabilidad (agregar regla a la tarea especificada)**

Seleccione la tarea a la que desee agregar las vulnerabilidades seleccionadas. Si tiene una licencia de Administración de vulnerabilidades y parches, seleccione la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades. Se agregará automáticamente a la tarea elegida una nueva regla para corregir las vulnerabilidades seleccionadas. Si no tiene esta licencia, seleccione la tarea Reparar vulnerabilidades. Las vulnerabilidades seleccionadas se agregarán a las propiedades de la tarea.

Se abrirá la ventana de propiedades de la tarea. Haga clic en **Guardar** para guardar los cambios.

Si optó por crear una tarea, se la creará y se la agregará a la lista de tareas disponible en **Tareas**. Si optó por agregar las vulnerabilidades a una tarea existente, las vulnerabilidades se guardarán en las propiedades de la tarea que haya elegido.

Para reparar las vulnerabilidades en el software de terceros, inicie la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades o la tarea Reparar vulnerabilidades. Si la tarea que creó es Reparar vulnerabilidades, deberá definir las actualizaciones de software manualmente en la configuración de la tarea.

Reparar vulnerabilidades de software con el Asistente de reparación de vulnerabilidades

El Asistente de reparación de vulnerabilidades solo está disponible con la licencia de la Administración de vulnerabilidades y parches.

Para reparar vulnerabilidades de software a través del Asistente de reparación de vulnerabilidades:

1. En el menú principal, vaya a **Administración de software → Administración de parches → Vulnerabilidades de software**.

   Se muestra una tabla con una lista de las vulnerabilidades detectadas en el software de terceros instalado en los dispositivos administrados.

2. Marque la casilla ubicada junto a la vulnerabilidad que desee reparar.

3. Haga clic en el botón **Ejecutar el Asistente de reparación de vulnerabilidades**.

   Este botón estará deshabilitado si selecciona más de una vulnerabilidad.

   Se iniciará el Asistente de reparación de vulnerabilidades. Se mostrará la lista de tareas existentes. La lista puede incluir los siguientes tipos de tareas:

   - Instalar actualizaciones requeridas y reparar vulnerabilidades
   - Reparar vulnerabilidades

   No se puede modificar la tarea Reparar vulnerabilidades para instalar nuevas actualizaciones. Para instalar nuevas actualizaciones, solo puede utilizar la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades.

4. Si desea que el asistente muestre solo las tareas que permitan reparar la vulnerabilidad seleccionada, habilite la opción **Mostrar solo las tareas que permitan reparar esta vulnerabilidad**.

5. Realice una de las siguientes acciones:

- Para iniciar una tarea, marque la casilla ubicada junto al nombre de la tarea en cuestión y haga clic en el botón **Iniciar**.

  No se requieren más acciones. En este punto, puede cerrar el asistente. La tarea se completará en segundo plano.

- Para agregar una nueva regla a una tarea Instalar actualizaciones requeridas y reparar vulnerabilidades:

  a. Marque la casilla ubicada junto al nombre de la tarea pertinente y haga clic en el botón **Agregar regla**.

  > El botón **Agregar regla** estará deshabilitado si selecciona más de una tarea.

  No puede agregar una regla a una tarea Reparar vulnerabilidades. Si selecciona una tarea Reparar vulnerabilidades, se mostrará la siguiente notificación: "Para instalar actualizaciones, use la tarea 'Instalar actualizaciones requeridas y reparar vulnerabilidades'".

  b. En la página que se abrirá, configure la nueva regla:

  - **Regla para reparar vulnerabilidades de este nivel de gravedad**

    Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

    Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al nivel de gravedad de la actualización seleccionada. Los niveles posibles son **Medio**, **Alto** y **Crítico**. Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

    Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

    Esta opción está deshabilitada de forma predeterminada.

  - **Regla para reparar vulnerabilidades por medio de actualizaciones del mismo tipo que la actualización definida como recomendada para la vulnerabilidad seleccionada**

    Esta regla solo se muestra para las vulnerabilidades en el software de Microsoft.

  - **Regla para reparar vulnerabilidades en las aplicaciones del proveedor seleccionado**

    Esta regla solo se muestra para vulnerabilidades en el software de terceros.

  - **Regla para reparar una vulnerabilidad en todas las versiones de la aplicación seleccionada**

    Esta regla solo se muestra para vulnerabilidades de software de terceros.

  - **Regla para reparar la vulnerabilidad seleccionada**

  - **Aprobar actualizaciones que reparen esta vulnerabilidad**

    Se aprobará la instalación de la actualización seleccionada. Habilite esta opción si ha aplicado reglas de instalación de actualizaciones que solo permitan instalar actualizaciones aprobadas.

    Esta opción está deshabilitada de forma predeterminada.

c. Haga clic en **Agregar**.

Se abrirá la ventana de propiedades de la tarea. Encontrará la nueva regla en las propiedades de la tarea. Si lo desea, vea y modifique la regla o los otros ajustes de la tarea. Haga clic en **Guardar** para guardar los cambios.

- Para crear una tarea:

a. Haga clic en el botón **Nueva tarea**.

b. En la página que se abrirá, configure la nueva regla:

- **Regla para reparar vulnerabilidades de este nivel de gravedad**

  Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

  Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al nivel de gravedad de la actualización seleccionada. Los niveles posibles son **Medio**, **Alto** y **Crítico**. Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

  Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

  Esta opción está deshabilitada de forma predeterminada.

- **Regla para reparar vulnerabilidades por medio de actualizaciones del mismo tipo que la actualización definida como recomendada para la vulnerabilidad seleccionada**

  Esta regla solo se muestra para las vulnerabilidades en el software de Microsoft.

- **Regla para reparar vulnerabilidades en las aplicaciones del proveedor seleccionado**

  Esta regla solo se muestra para vulnerabilidades en el software de terceros.

- **Regla para reparar una vulnerabilidad en todas las versiones de la aplicación seleccionada**

  Esta regla solo se muestra para vulnerabilidades de software de terceros.

- **Regla para reparar la vulnerabilidad seleccionada**

- **Aprobar actualizaciones que reparen esta vulnerabilidad**

  Se aprobará la instalación de la actualización seleccionada. Habilite esta opción si ha aplicado reglas de instalación de actualizaciones que solo permitan instalar actualizaciones aprobadas.

  Esta opción está deshabilitada de forma predeterminada.

c. Haga clic en **Agregar**.

d. En el Asistente para crear nueva tarea, continúe con la creación de la tarea.

La nueva regla que agregó en el Asistente de reparación de vulnerabilidades se mostrará en el paso **Elija las reglas de instalación de actualizaciones** del Asistente para crear nueva tarea. Cuando haya completado el asistente, la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades se agregará a la lista de tareas.

Crear la tarea Reparar vulnerabilidades

La tarea *Reparar vulnerabilidades* se utiliza para reparar vulnerabilidades de software en dispositivos administrados. Puede reparar vulnerabilidades de software en software de terceros, incluido el software de Microsoft.

Solo puede crear la tarea *Reparar vulnerabilidades* para dispositivos Windows. No puede crear esta tarea para dispositivos que ejecuten otros sistemas operativos.

Puede crear una nueva tarea *Reparar vulnerabilidades* solo si tiene la licencia de Administración de vulnerabilidades y parches.

Para reparar vulnerabilidades nuevas, puede agregarlas a una tarea de *Reparar vulnerabilidades* existente. Sin embargo, recomendamos que utilice la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* en lugar de la tarea *Reparar vulnerabilidades*. La tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* le permitirá instalar múltiples actualizaciones y reparar múltiples vulnerabilidades simultánea y automáticamente utilizando un conjunto de reglas.

Para actualizar una aplicación de terceros o reparar una vulnerabilidad en una aplicación de terceros instalada en un dispositivo administrado, podría necesitarse la colaboración del usuario. Si la aplicación está abierta, por ejemplo, podría tener que pedirle al usuario que la cierre.

Para crear la tarea Reparar vulnerabilidades:

1. En el menú principal, vaya a **Tareas**.

   También puede crear esta tarea en la ventana de propiedades del dispositivo en la pestaña **Tareas**.

2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

3. En la lista desplegable **Aplicación**, seleccione Kaspersky Security Center.

4. En la lista **Tipo de tarea**, seleccione el tipo de tarea **Reparar vulnerabilidades**.

5. En el campo **Nombre de la tarea**, ingrese el nombre de la tarea nueva.

   El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).

6. Seleccione los dispositivos a los que se asignará la tarea.

   Avance al siguiente paso del asistente.

7. Haga clic en **Agregar**.

   Se abre la lista de vulnerabilidades.

8. En la lista de vulnerabilidades, marque las casillas ubicadas junto a las vulnerabilidades que desee reparar y luego haga clic en el botón **Aceptar**.

Las vulnerabilidades de software de Microsoft suelen tener correcciones recomendadas. No se requieren acciones adicionales.

Para vulnerabilidades en el software de otros proveedores, primero tendrá que especificar una corrección de usuario para cada vulnerabilidad que desee reparar. Después de eso, podrá agregar esas vulnerabilidades a la tarea *Reparar vulnerabilidades*.

Avance al siguiente paso del asistente.

9. Defina las opciones de reinicio del sistema operativo:

- **No reiniciar el dispositivo**

  Cuando termine la operación, los dispositivos cliente no se reiniciarán automáticamente. Para que la operación se complete, deberá reiniciar los dispositivos en forma manual o mediante, por ejemplo, una tarea de administración de dispositivos. Los resultados de la tarea y el estado de cada dispositivo darán cuenta de que hay un reinicio pendiente. Esta opción es útil cuando la tarea va a ejecutarse en servidores y dispositivos que deben operar continuamente.

- **Reiniciar el dispositivo**

  Los dispositivos cliente se reiniciarán automáticamente siempre que resulte necesario para completar la operación. Esta opción es útil cuando la tarea se realiza en dispositivos que admiten una breve interrupción para apagarse o reiniciarse.

- **Solicitar al usuario una acción**

  A través de un recordatorio en pantalla, se le pedirá a cada usuario que reinicie su dispositivo manualmente. Puede configurar algunos ajustes avanzados para esta opción: el texto del mensaje que se le muestra al usuario, la frecuencia con la que se muestra este mensaje y el tiempo que se espera antes de reiniciar el dispositivo por la fuerza (sin que el usuario confirme el reinicio). Esta opción es la más adecuada para estaciones de trabajo en las que los usuarios deben poder seleccionar el momento más conveniente para reiniciar.

  Esta opción está seleccionada de forma predeterminada.

- **Repetir solicitud cada (min)**

  Si habilita esta opción, la aplicación le solicitará al usuario que reinicie su sistema operativo con la frecuencia especificada.

  Esta opción está activada de forma predeterminada. El intervalo por defecto es de 5 minutos. Los valores disponibles van de 1 a 1440 minutos.

  Si no habilita esta opción, la solicitud se mostrará una sola vez.

- **Reiniciar después de (min)**

  Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

  Esta opción está activada de forma predeterminada. El tiempo de espera por defecto es de 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Forzar el cierre de aplicaciones en sesiones bloqueadas**

  Las aplicaciones abiertas en el dispositivo cliente podrían impedir que se lo reinicie. Si el usuario está editando un documento en un procesador de textos, por ejemplo, y no ha guardado el archivo, el procesador de textos no permitirá que el dispositivo se reinicie.

  Si habilita esta opción, las aplicaciones que se estén ejecutando en un dispositivo bloqueado se cerrarán por la fuerza y, tras ello, el dispositivo se reiniciará. Los usuarios podrían perder los cambios que no hayan guardado.

Si no habilita esta opción, los dispositivos bloqueados no se reiniciarán. El estado de la tarea en tales dispositivos indicará que hay un reinicio pendiente. Los usuarios tendrán que cerrar manualmente todas las aplicaciones abiertas para luego reiniciar sus dispositivos.

Esta opción está deshabilitada de forma predeterminada.

Avance al siguiente paso del asistente.

10. Configure los ajustes relativos a la cuenta:

- **Cuenta predeterminada**

  La tarea se ejecutará utilizando la misma cuenta que la aplicación que realizará la tarea.

  Esta opción está seleccionada de forma predeterminada.

- **Especificar cuenta**

  Complete los campos **Cuenta** y **Contraseña** para especificar los detalles de la cuenta con la que se ejecutará la tarea. La cuenta debe tener los derechos necesarios para realizar la tarea.

- **Cuenta**

  Cuenta con la que se ejecutará la tarea.

- **Contraseña**

  Contraseña de la cuenta con la que se ejecutará la tarea.

11. En el paso **Finalizar la creación de la tarea** del asistente, habilite la opción **Abrir los detalles de la tarea cuando se complete la creación** para modificar la configuración predeterminada de la tarea.

    Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Podrá modificarla más adelante.

12. Haga clic en el botón **Finalizar**.

    El asistente creará la tarea. Si habilitó la opción **Abrir los detalles de la tarea cuando se complete la creación**, se abrirá automáticamente la ventana de propiedades de la tarea. En esta ventana, puede definir la configuración general de la tarea y, si es necesario, cambiar los ajustes establecidos durante la creación de la tarea.

    > También puede abrir la ventana de propiedades de la tarea haciendo clic en el nombre de la tarea creada en la lista de tareas.

    La tarea se crea, configura y muestra en la lista de tareas en **Tareas**.

13. Para ejecutar la tarea, selecciónela en la lista de tareas y haga clic en el botón **Iniciar**.

    También puede programar el inicio de la tarea en la pestaña **Programación**, en la ventana de propiedades de la tarea.

    Para obtener una descripción detallada de la configuración de inicio programado, vea la configuración general de la tarea.

Al completarse la tarea, se reparan las vulnerabilidades seleccionadas.

Selección de soluciones de usuario para vulnerabilidades de software de terceros

Para usar la tarea *Reparar vulnerabilidades*, debe especificar manualmente las actualizaciones de software para reparar las vulnerabilidades en el software de terceros que se detalla en la configuración de la tarea. La tarea *Reparar vulnerabilidades* utiliza reparaciones recomendadas para el software de Microsoft y reparaciones de usuario para otro software de terceros.

Las *reparaciones de usuario* son actualizaciones de software que el administrador especifica de forma manual para su instalación a fin de reparar vulnerabilidades.

Para seleccionar reparaciones de usuario para vulnerabilidades en software de terceros, realice lo siguiente:

1. En el menú principal, vaya a **Administración de software → Administración de parches → Vulnerabilidades de software**.

   Se mostrará una tabla con una lista de las vulnerabilidades detectadas en el software de terceros instalado en los dispositivos administrados.

2. En la lista de vulnerabilidades de software, haga clic en el vínculo con el nombre de la vulnerabilidad de software para la que desea especificar una reparación del usuario.

   Se abrirá la ventana de propiedades de la vulnerabilidad seleccionada.

3. En el panel de la izquierda, seleccione la sección **Correcciones del usuario y otras correcciones**.

   Se muestra la lista de reparaciones del usuario para la vulnerabilidad de software seleccionada.

4. Haga clic en **Agregar**.

   Se muestra una lista de paquetes de instalación disponibles. La lista de paquetes de instalación que se muestran corresponde a la lista de la carpeta **Administración de software → Paquetes de instalación**.

   Si no creó un paquete de instalación que contenga una corrección de usuario para la vulnerabilidad seleccionada, puede crearlo ahora haciendo clic en el botón **Nuevo** y siguiendo los pasos del Asistente de nuevo paquete.

5. Seleccione uno o más paquetes de instalación que contengan una o más reparaciones del usuario para la vulnerabilidad seleccionada.

6. Haga clic en el botón **Guardar**.

Como resultado, quedan especificados los paquetes de instalación que contengan correcciones de usuario para la vulnerabilidad de software. Cuando se inicie la tarea *Reparar vulnerabilidades*, se instalará el paquete de instalación y se reparará la vulnerabilidad de software.

Ver información sobre las vulnerabilidades de software detectadas en todos los dispositivos administrados

Si ya analizó el software de los dispositivos administrados en busca de vulnerabilidades, puede ver la lista de vulnerabilidades de software detectadas. Si ejecuta la tarea para la jerarquía de Servidores de administración, puede ver la lista de dispositivos administrados en los que se hayan detectado vulnerabilidades y que correspondan únicamente al Servidor de administración seleccionado.

También puede generar y ver un informe de vulnerabilidades.

Para ver la lista de vulnerabilidades de software detectadas en todos los dispositivos administrados:

En el menú principal, vaya a **Operaciones** → **Administración de parches** → **Vulnerabilidades de software**.

Se muestra la lista de vulnerabilidades de software detectadas en los dispositivos cliente.

Para ajustar la lista de vulnerabilidades de software:

Haga clic en el ícono **Filtrar** () ubicado en la esquina superior derecha de la lista de vulnerabilidades de software y, luego, seleccione los filtros que necesite. También puede elegir un filtro preestablecido en la lista desplegable **Filtros preestablecidos**, que se encuentra sobre la lista de vulnerabilidades de software.

Si lo desea, puede obtener información detallada sobre cualquiera de las vulnerabilidades de la lista.

Para obtener información sobre una vulnerabilidad de software:

En la lista de vulnerabilidades de software, haga clic en el vínculo con el nombre de la vulnerabilidad de su interés.

Se abre la ventana de propiedades de la vulnerabilidad de software.

Ver información sobre las vulnerabilidades de software detectadas en un dispositivo administrado específico

Puede ver información sobre las vulnerabilidades de software detectadas en un dispositivo administrado específico que ejecute Windows.

Para ver la lista de las vulnerabilidades de software detectadas en el dispositivo administrado seleccionado:

1. En el menú principal, vaya a **Administración de activos** → **Dispositivos administrados**.

   Se muestra la lista de dispositivos administrados.

2. En la lista de dispositivos administrados, haga clic en el vínculo con el nombre del dispositivo para el que desee ver las vulnerabilidades de software detectadas.

   Se muestra la ventana de propiedades del dispositivo seleccionado.

3. En la ventana de propiedades del dispositivo seleccionado, elija la pestaña **Avanzado**.

4. En el panel izquierdo, seleccione la sección **Vulnerabilidades de software**.

Se muestra la lista de vulnerabilidades de software detectadas en el dispositivo administrado que seleccionó.

Para ver las propiedades de una vulnerabilidad de software específica:

En la lista de vulnerabilidades de software, haga clic en el vínculo con el nombre de la vulnerabilidad de software que sea de su interés.

Se muestra la ventana de propiedades de la vulnerabilidad de software seleccionada.

Ver estadísticas de las vulnerabilidades presentes en los dispositivos administrados

Puede ver estadísticas sobre cada vulnerabilidad de software detectada en los dispositivos administrados. Las estadísticas se presentan en forma de diagrama. El diagrama muestra la cantidad de dispositivos con los siguientes estados:

- *Ignorada en: <cantidad de dispositivos>*. Este estado se asigna cuando la vulnerabilidad se desestima manualmente a través de sus propiedades.
- *Reparada en: <cantidad de dispositivos>*. Este estado se asigna cuando la tarea para reparar la vulnerabilidad se completa correctamente.
- *Reparación programada para: <cantidad de dispositivos>*. Este estado se asigna cuando ya se ha creado una tarea para reparar la vulnerabilidad, pero aún no se la ha ejecutado.
- *Parche aplicado en: <cantidad de dispositivos>*. Este estado se asigna cuando se seleccionó manualmente una actualización de software que debía, pero no pudo, reparar la vulnerabilidad.
- *Es necesario realizar un arreglo en: <cantidad de dispositivos>*. Este estado se asigna cuando la vulnerabilidad se ha reparado solo en algunos dispositivos administrados y aún debe repararse en más dispositivos administrados.

Para ver las estadísticas de una vulnerabilidad en los dispositivos administrados:

1. En el menú principal, vaya a **Operaciones** → **Administración de parches** → **Vulnerabilidades de software**.

   La página muestra una lista de las vulnerabilidades detectadas en las aplicaciones de los dispositivos administrados.

2. Marque la casilla ubicada junto a una vulnerabilidad.
3. Haga clic en el botón **Estadísticas de la vulnerabilidad en los dispositivos**.

   El botón **Estadísticas de la vulnerabilidad en los dispositivos** se deshabilita si selecciona más de una vulnerabilidad.

Se muestra un diagrama con los estados de la vulnerabilidad. Para ver los dispositivos en los que la vulnerabilidad tenga un estado en particular, haga clic en ese estado.

Exportar la lista de vulnerabilidades de software a un archivo

Puede descargar la lista de vulnerabilidades como un archivo CSV o TXT. Puede enviar estos archivos a la persona que esté a cargo de la seguridad de la información o almacenarlos con fines estadísticos.

Para exportar a un archivo de texto la lista de vulnerabilidades de software detectadas en todos los dispositivos administrados:

1. En el menú principal, vaya a **Operaciones → Administración de parches → Vulnerabilidades de software**.

   Se muestra una lista de vulnerabilidades de software en las aplicaciones detectadas en los dispositivos administrados.

   De forma predeterminada, solo se exportan las vulnerabilidades que se visualizan en la página actual.

   Si solo desea exportar vulnerabilidades específicas, marque las casillas ubicadas junto a las vulnerabilidades que desee ver.

2. Haga clic en el botón **Exportar a TXT** o en el botón **Exportar a CSV**, dependiendo del formato de exportación que prefiera. Si no ve alguno de estos botones, haga clic en el botón de los puntos suspensivos y, luego, seleccione la opción que desee de la lista desplegable.

En su dispositivo, se descargará un archivo con la lista de vulnerabilidades de software.

Para ver la lista de las vulnerabilidades de software detectadas en el dispositivo administrado seleccionado:

1. En el menú principal, vaya a **Administración de activos → Dispositivos administrados**.

   Se muestra la lista de dispositivos administrados.

2. En la lista de dispositivos administrados, haga clic en el vínculo con el nombre del dispositivo para el que desee ver las vulnerabilidades de software detectadas.

   Se muestra la ventana de propiedades del dispositivo seleccionado.

3. En la ventana de propiedades del dispositivo seleccionado, elija la pestaña **Avanzado**.

4. En el panel izquierdo, seleccione la sección **Vulnerabilidades de software**.

Se muestra la lista de vulnerabilidades de software detectadas en el dispositivo administrado que seleccionó.

De forma predeterminada, solo se exportan las vulnerabilidades que se visualizan en la página actual.

Si solo desea exportar vulnerabilidades específicas, marque las casillas ubicadas junto a las vulnerabilidades que desee ver.

1. Haga clic en el botón **Exportar a TXT** o en el botón **Exportar a CSV**, dependiendo del formato de exportación que prefiera. Si no ve alguno de estos botones, haga clic en el botón de los puntos suspensivos y, luego, seleccione la opción que desee de la lista desplegable.

En su dispositivo, se descargará un archivo con la lista de vulnerabilidades de software.

Ignorar vulnerabilidades de software

Puede ignorar las vulnerabilidades de software que no desee reparar. Hay distintos motivos para ignorar una vulnerabilidad de software, por ejemplo:

- no considera que la vulnerabilidad de software sea de extrema importancia para su organización;
- entiende que, al reparar la vulnerabilidad, se pondrían en riesgo los datos vinculados al software vulnerable;
- sabe que la vulnerabilidad de software no es un riesgo para la red de su organización porque utiliza otras medidas para proteger sus dispositivos administrados.

Puede ignorar una vulnerabilidad de software en todos los dispositivos administrados o solo en los dispositivos administrados que usted seleccione.

Para ignorar una vulnerabilidad de software en todos los dispositivos administrados:

1. En el menú principal, vaya a **Operaciones → Administración de parches → Vulnerabilidades de software**.

   Se muestra una lista de las vulnerabilidades de software detectadas en las aplicaciones de los dispositivos administrados.

2. En la lista de vulnerabilidades de software, haga clic en el vínculo con el nombre de la vulnerabilidad de software que desee ignorar.

   Se abre la ventana de propiedades de la vulnerabilidad de software.

3. En la pestaña **General**, habilite la opción **Ignorar vulnerabilidad**.

4. Haga clic en el botón **Guardar**.

   Se cierra la ventana de propiedades de vulnerabilidad de software.

La vulnerabilidad de software se ignorará en todos los dispositivos administrados.

Para ignorar una vulnerabilidad de software en un dispositivo administrado específico:

1. En el menú principal, vaya a **Administración de activos → Dispositivos administrados**.

   Se muestra la lista de dispositivos administrados.

2. En la lista de dispositivos administrados, haga clic en el vínculo con el nombre del dispositivo en el que desee ignorar la vulnerabilidad de software.

   Se abre la ventana de propiedades del dispositivo.

3. En la ventana de propiedades del dispositivo, seleccione la pestaña **Avanzado**.

4. En el panel izquierdo, seleccione la sección **Vulnerabilidades de software**.

   Se muestra la lista de vulnerabilidades de software detectadas en el dispositivo.

5. En la lista de vulnerabilidades de software, seleccione la vulnerabilidad que desee ignorar en el dispositivo seleccionado.

   Se abre la ventana de propiedades de la vulnerabilidad de software.

6. En la ventana de propiedades de vulnerabilidades de software, en la pestaña **General**, habilite la opción **Ignorar vulnerabilidad**.

7. Haga clic en el botón **Guardar**.

   Se cierra la ventana de propiedades de vulnerabilidad de software.

8. Cierre la ventana de propiedades del dispositivo.

La vulnerabilidad de software se ignorará en el dispositivo seleccionado.

Cuando se completen las tareas *Reparar vulnerabilidades* o *Instalar actualizaciones requeridas y reparar vulnerabilidades*, las vulnerabilidades de software ignoradas no se repararán. Las vulnerabilidades ignoradas pueden excluirse de la lista de vulnerabilidades utilizando un filtro.

Crear un paquete de instalación para una aplicación de terceros usando la base de datos de Kaspersky

Kaspersky Security Center Web Console permite instalar aplicaciones de terceros en forma remota utilizando paquetes de instalación. Las aplicaciones de terceros se incluyen en una base de datos dedicada de Kaspersky. Esta base de datos se crea automáticamente cuando se ejecuta por primera vez la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*.

Para crear un paquete de instalación para una aplicación de terceros utilizando la base de datos de Kaspersky, debe contar con una licencia de Administración de vulnerabilidades y parches.

Para crear un paquete de instalación de una aplicación de terceros desde la base de datos de Kaspersky, haga lo siguiente:

1. En el menú principal, vaya a la sección **Administración de software → Paquetes de instalación**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente de nuevo paquete. Realice las acciones que le indica el asistente usando el botón **Siguiente**.
3. Elija la opción **Seleccionar una aplicación de la base de datos de Kaspersky para crear un paquete de instalación**.

   Esta opción solo está disponible si cuenta con una licencia de la Administración de vulnerabilidades y parches.

   Avance al siguiente paso del asistente.
4. Seleccione la aplicación para la que desee crear el paquete de instalación.

   Avance al siguiente paso del asistente.
5. Seleccione el idioma de localización pertinente en la lista desplegable y, luego, haga clic en Siguiente.

   Este paso solo se muestra si la aplicación brinda varias opciones de idioma.
6. Si se le solicita que acepte un Contrato de licencia para la instalación, en el paso **Contratos de licencia y Políticas de privacidad** del asistente, haga lo siguiente:

   a. Haga clic en el vínculo **Mostrar** para leer el Contrato de licencia en el sitio web del proveedor o ver las actualizaciones de la licencia.

   b. Marque la casilla **Confirmo que he leído completamente, entiendo y acepto los términos y las condiciones de este Contrato de licencia de usuario final**.

   c. Haga clic en el botón **Aceptar todos** para aceptar todos los contratos de licencia y las políticas de privacidad que se muestran en la lista.

7. En el paso **Nombre del nuevo paquete de instalación** del asistente, en el campo **Nombre del paquete**, ingrese el nombre del paquete de instalación y haga clic en **Siguiente**.

   El nuevo paquete de instalación se carga en el Servidor de administración. El Asistente de nuevo paquete muestra un mensaje para informar que el paquete de instalación se creó correctamente.

8. Haga clic en el botón **Finalizar**.

El nuevo paquete de instalación aparecerá en la lista de paquetes de instalación. Puede seleccionar este paquete al crear o reconfigurar la tarea Instalar aplicación de forma remota.

Para crear y reconfigurar la tarea Instalar aplicación de forma remota con un paquete de instalación de una aplicación de terceros incluida en la base de datos de Kaspersky, debe contar con una licencia de Administración de vulnerabilidades y parches.

Ver y modificar la configuración de un paquete de instalación de una aplicación de terceros desde la base de datos de Kaspersky

Si creó un paquete de instalación para algunas de las aplicaciones de terceros incluidas en la base de datos de Kaspersky, puede ver y modificar posteriormente la configuración de esto paquete.

Para modificar la configuración de un paquete de instalación de una aplicación de terceros incluida en la base de datos de Kaspersky, debe tener una licencia de Administración de vulnerabilidades y parches.

Para ver y modificar la configuración de un paquete de instalación de una aplicación de terceros incluida en la base de datos de Kaspersky:

1. En el menú principal, vaya a **Administración de software** → **Paquetes de instalación**.
2. En la lista de paquetes de instalación que se abre, haga clic en el nombre del paquete pertinente.

   Se abre la ventana de propiedades.

3. Ajuste la configuración si es necesario.
4. Haga clic en el botón **Guardar**.

Se guarda la configuración modificada.

Configurar el paquete de instalación de una aplicación de terceros incluida en la base de datos de Kaspersky

Los ajustes de configuración correspondientes al paquete de instalación de una aplicación de terceros se agrupan en las siguientes pestañas:

No todos los ajustes enumerados a continuación se muestran de forma predeterminada. Si necesita agregar columnas, haga clic en el botón **Filtrar** y, luego, seleccione en la lista los nombres de las columnas que precise.

- Pestaña **General**:
  - Campo de entrada que contiene el nombre del paquete de instalación y que se puede editar manualmente
  - **Aplicación**

    El nombre de la aplicación de terceros para la que se creó el paquete de instalación.
  - **Versión**

    El número de versión de la aplicación de terceros para la que se creó el paquete de instalación.
  - **Tamaño**

    El tamaño del paquete de instalación de terceros (en kilobytes).
  - **Creado**

    La fecha y la hora en que se creó el paquete de instalación de terceros.
  - **Ruta**

    La ruta a la carpeta de red donde se almacena el paquete de instalación de terceros.
- Pestaña **Procedimiento de instalación**:
  - **Instalar los componentes generales obligatorios del sistema**

    Si esta opción está habilitada, antes de que se instale una actualización, la aplicación instalará automáticamente todos los componentes generales del sistema que la actualización requiera para instalarse (los llamados "requisitos previos"). Una actualización podría requerir, por ejemplo, que esté instalada cierta actualización del sistema operativo.

    Si esta opción está deshabilitada, posiblemente tenga que instalar los requisitos previos manualmente.

    Esta opción está deshabilitada de forma predeterminada.
  - Tabla que muestra las propiedades de la actualización y contiene las siguientes columnas:
    - **Nombre**

      Nombre de la actualización.

- **Descripción**

  Descripción de la actualización.

- **Origen**

  El origen de la actualización, es decir, si fue publicada por Microsoft o por un desarrollador externo diferente.

- **Tipo**

  El tipo de actualización, es decir, si la actualización está destinada a un controlador o una aplicación.

- **Categoría**

  La categoría de Windows Server Update Services (WSUS) que se muestra para las actualizaciones de Microsoft (Actualizaciones críticas, Actualizaciones de las definiciones, Controladores, Paquetes de características, Actualizaciones de seguridad, Service Packs, Herramientas, Paquetes acumulativos de actualizaciones, Actualizaciones o Upgrade).

- **Nivel de importancia conforme a MSRC**

  El nivel de importancia de la actualización definido por el Centro de respuesta de seguridad de Microsoft (MSRC).

- **Nivel de importancia**

  El nivel de importancia de la actualización definido por Kaspersky.

- **Nivel de importancia del parche**

  El nivel de importancia del parche si está destinado a una aplicación de Kaspersky.

- **Artículo**

  El identificador (id.) del artículo de la Base de conocimientos que describe la actualización.

- **Boletín**

  El id. del boletín de seguridad que describe la actualización.

- **Instalación no asignada (nueva versión)**

  Muestra si la actualización tiene el estado Instalación no asignada.

- **Por instalarse**

  Muestra si la actualización tiene el estado Por instalarse.

- **Instalándose**

  Muestra si la actualización tiene el estado Instalándose.

- **Instalada**

  Muestra si la actualización tiene el estado Instalada.

- **Error**

  Muestra si la actualización tiene el estado Error.

- **Se debe reiniciar el dispositivo**

  Muestra si la actualización tiene el estado Se debe reiniciar el dispositivo.

- **Registrada**

  Muestra la fecha y hora en que se registró la actualización.

- **Instalada en modo interactivo**

  Muestra si la actualización solicita la intervención del usuario durante la instalación.

- **Estado de aprobación de la actualización**

  Muestra si la instalación de la actualización está aprobada.

- **Revisión**

  Muestra el número de revisión actual de la actualización.

- **Id. de actualización**

  Muestra el id. de la actualización.

- **Versión de la aplicación**

  Muestra el número de versión a la que se actualizará la aplicación.

- **Reemplazada**

  Muestra otras actualizaciones que pueden reemplazar a la actualización.

- **Reemplaza**

  Muestra otras actualizaciones que pueden ser reemplazadas por la actualización.

- **Debe aceptar los términos del Contrato de licencia**

  Muestra si la actualización solicita aceptar los términos de un contrato de licencia de usuario final (EULA).

- **Dirección URL de descripción**

  Muestra el nombre del proveedor de la actualización.

- **Familia de aplicaciones**

  Muestra el nombre de la familia de aplicaciones a las que pertenece la actualización.

- **Aplicación**

  Muestra el nombre de la aplicación a la que pertenece la actualización.

- **Idioma de localización**

  Muestra el idioma de localización de la actualización.

- **Instalación no asignada (nueva versión)**

  Muestra si la actualización tiene el estado Instalación no asignada (nueva versión).

- **Requiere instalación de requisitos previos**

  Muestra si la actualización tiene el estado Requiere instalación de requisitos previos.

- **Modo de descarga**

  Muestra el modo de descarga de la actualización.

- **Es un parche**

  Muestra si la actualización es un parche.

- **Sin instalar**

  Muestra si la actualización tiene el estado Sin instalar.

- **Creado**

- Pestaña **Configuración** que muestra los ajustes del paquete de instalación (con sus nombres, descripciones y valores) que se utilizan como parámetros de línea de comandos durante la instalación. Si el paquete no proporciona tales ajustes, se muestra un mensaje al respecto. Puede modificar estos ajustes de configuración.

- Pestaña **Historial de revisiones**, que muestra las revisiones del paquete de instalación y contiene las siguientes columnas:

  - **Revisión**: muestra el número de revisión de los paquetes de instalación.

  - **Hora**: fecha y hora en que se modificó la configuración del paquete de instalación.

  - **Usuario**: nombre del usuario que modificó la configuración del paquete de instalación.

  - **Dirección IP del dispositivo del usuario**: dirección IP del dispositivo desde el que se modificó el objeto.

  - **Dirección IP de Web Console**: dirección IP de la copia de Kaspersky Security Center Web Console con la que se modificó el objeto.

  - **Acción**: acción realizada sobre el paquete de instalación dentro de la revisión.

  - **Descripción**: descripción de la revisión vinculada al cambio realizado en la configuración del paquete de instalación.

    De manera predeterminada, la descripción de las revisiones está en blanco. Para agregar una descripción a una revisión, seleccione la revisión pertinente y haga clic en el botón **Editar descripción**. En la ventana abierta, ingrese un texto que describa la revisión.

Corrección de vulnerabilidades en una red aislada

En esta sección, se describen los pasos que le permitirán reparar vulnerabilidades de software de terceros en dispositivos administrados que se encuentren conectados a servidores de administración sin acceso a Internet.

Procedimiento: reparar vulnerabilidades en el software de terceros

Puede instalar actualizaciones y corregir vulnerabilidades en el software de terceros instalado en los dispositivos administrados de una red aislada. En una red aislada, los dispositivos administrados (y el Servidor de administración a los que esos dispositivos están conectados) no tienen acceso a Internet. Para reparar vulnerabilidades en una red de este tipo, se necesita contar con un Servidor de administración que tenga conexión a Internet. El Servidor de administración con acceso a Internet se utiliza para descargar parches (actualizaciones requeridas) y, luego, enviarlos a los servidores de administración aislados.

Kaspersky Security Center no puede descargar actualizaciones para el software de Microsoft instalado en servidores de administración aislados; solo puede descargar actualizaciones para software de otros terceros, que hayan sido publicadas por los desarrolladores de esas aplicaciones.

Para obtener más información sobre el proceso de reparación de vulnerabilidades en una red aislada, consulte la descripción y el esquema del proceso.

Requisitos previos

Antes de comenzar, haga lo siguiente:

1. Asigne un dispositivo para conectarse a Internet y descargar parches. Este dispositivo se considerará el Servidor de administración con acceso a Internet.
2. Instale Kaspersky Security Center Linux (versión 15.1 como mínimo) en los siguientes dispositivos:
   - El dispositivo del primer punto, que actuará como Servidor de administración con acceso a Internet
   - Los dispositivos aislados, que actuarán como servidores de administración aislados de Internet (en adelante, se usará el término "servidores de administración aislados" para referirse a estos dispositivos)
3. Asegúrese de que cada Servidor de administración tenga suficiente espacio en disco para descargar y almacenar actualizaciones y parches.

Etapas

La instalación de actualizaciones y la reparación de vulnerabilidades de software de terceros en dispositivos administrados conectados a servidores de administración aislados abarca las siguientes etapas:

1. **Configuración del Servidor de administración con acceso a Internet**

   Prepare el Servidor de administración con acceso a Internet para que atienda las solicitudes de actualizaciones de software de terceros requeridas y descargar los parches.

2. **Configuración de los servidores de administración aislados**

   Prepare los servidores de administración aislados para que, de manera periódica, generen listas con las actualizaciones que requieran y para que puedan procesar los parches que descargue el Servidor de administración con acceso a Internet. Una vez configurados, los servidores de administración aislados ya no intentarán descargar parches de Internet. En cambio, obtendrán sus actualizaciones de los parches.

3. **Transferencia de los parches e instalación de las actualizaciones en los servidores de administración aislados**

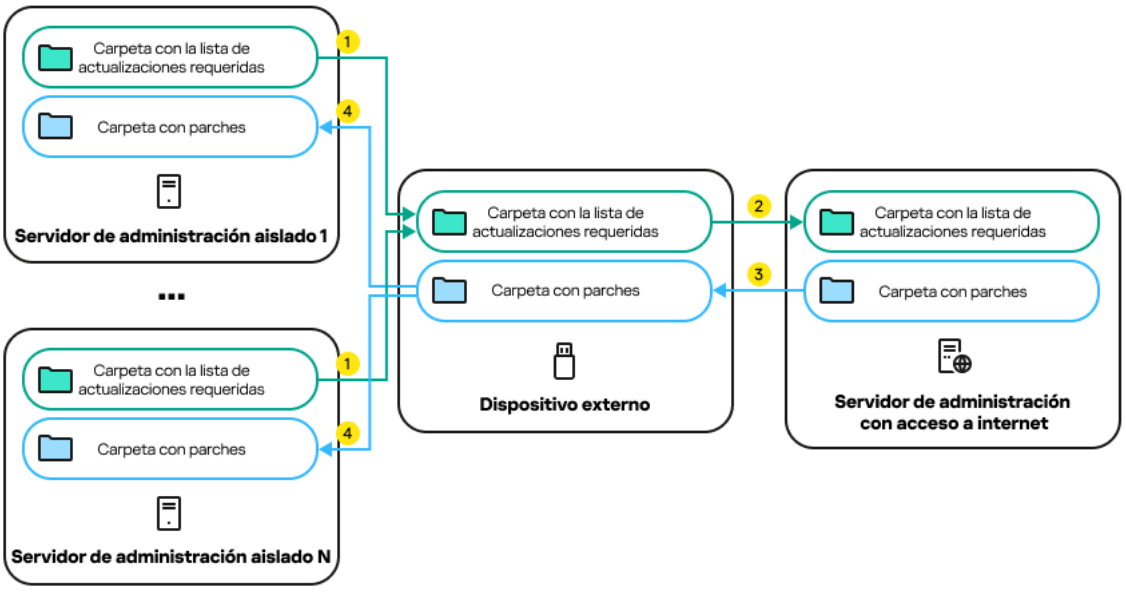
   Una vez que los servidores de administración estén configurados, podrá transmitir las listas de actualizaciones requeridas y los parches correspondientes entre el Servidor de administración con acceso a Internet y los servidores de administración aislados. Completado este intercambio, las actualizaciones contenidas en los parches se instalarán en los dispositivos administrados mediante la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*.

Resultados

Como resultado, las actualizaciones para el software de terceros se transmitirán a los servidores de administración aislados y se instalarán en los dispositivos administrados conectados a ellos a través de Kaspersky Security Center Linux. Solo tendrá que configurar los servidores de administración una vez. Tras completar la configuración, podrá obtener las actualizaciones requeridas con la frecuencia que resulte necesaria (por ejemplo, una vez al día o varias veces al día).

Acerca de la reparación de vulnerabilidades en el software de terceros en una red aislada

En la siguiente imagen, se describe el proceso que permite reparar vulnerabilidades de software de terceros en una red aislada. Este proceso puede llevarse a cabo periódicamente.



Transmisión de parches y de la lista de actualizaciones requeridas entre los servidores de administración aislados y el Servidor de administración con acceso a Internet

Cada Servidor de administración que se encuentra aislado de Internet (denominado, en lo sucesivo, "Servidor de administración aislado") genera una lista con las actualizaciones que deben instalarse en los dispositivos administrados que están conectados a él. Esta lista de actualizaciones se almacena en una carpeta específica como un conjunto de archivos binarios, cada uno con el nombre del identificador del parche que contiene la actualización necesaria. Por lo tanto, cada archivo de la lista se corresponde con un parche específico.

La lista de las actualizaciones requeridas se transfiere mediante un dispositivo externo del Servidor de administración aislado al Servidor de administración designado que tiene acceso a Internet. Completada la transferencia, el Servidor de administración designado obtiene los parches necesarios de Internet y los pone en la carpeta indicada.

Cuando todos los parches se han descargado y copiado a la carpeta indicada, se los vuelve a transferir a cada Servidor de administración aislado del cual se haya obtenido una lista de actualizaciones requeridas. Los parches se guardan en una carpeta creada específicamente para ellos en cada Servidor de administración aislado.

Luego de esto, se ejecuta la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* para instalar los parches y las actualizaciones en los dispositivos administrados conectados a los servidores de administración aislados.

Configurar el Servidor de administración con acceso a Internet para reparar vulnerabilidades en una red aislada

Como preparativo para reparar vulnerabilidades y transmitir parches dentro de una red aislada, primero debe configurar el Servidor de administración con acceso a Internet y, luego, los servidores de administración aislados.

Para configurar el Servidor de administración con acceso a Internet:

1. Cree dos carpetas en el disco en el que esté instalado el Servidor de administración:

   - Una carpeta para almacenar la lista de actualizaciones requeridas
   - Una carpeta para los parches

   Puede dar a estas carpetas el nombre que desee.

2. Otorgue el derecho **Modificar** al grupo KLAdmins para las carpetas que acaba de crear. Utilice para ello las herramientas administrativas que vienen incluidas en el sistema operativo.

3. Utilice la utilidad klscflag para especificar las rutas a las carpetas en las propiedades del Servidor de administración.

   Ejecute el símbolo del sistema de Windows usando derechos de administrador y, a continuación, cambie su directorio actual al directorio con la utilidad klscflag. La utilidad klscflag se encuentra en la carpeta donde está instalado el Servidor de administración. La ruta de instalación predeterminada: <Disk>:\Archivos de programa (x86)\Kaspersky Lab\Kaspersky Security Center.

4. Ejecute los siguientes comandos en la línea de comandos:

   - Para establecer la ruta a la carpeta de parches, ingrese lo siguiente:
     `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "<ruta a la carpeta>"`
   - Para establecer la ruta a la carpeta para la lista de actualizaciones requeridas, ingrese lo siguiente:
     `klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v "<ruta a la carpeta>"`

Ejemplo: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "/Carpeta para parches"`

5. Si es necesario, use la utilidad klscflag para especificar la frecuencia con la que el Servidor de administración deberá buscar nuevas solicitudes de parches:
   `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v <valor en segundos>`

   La configuración predeterminada es de 120 segundos.

   Ejemplo: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v 120`

6. Cree la tarea *Buscar vulnerabilidades y actualizaciones requeridas* a fin de obtener información sobre los parches para el software de terceros instalado en los dispositivos administrados. A continuación, programe la tarea.

7. Cree la tarea *Reparar vulnerabilidades* a fin de indicar qué parches se utilizarán para reparar vulnerabilidades en el software de terceros. A continuación, programe la tarea.

   Ejecute las tareas de forma manual si no quiere esperar al siguiente inicio programado. El orden en que se inician las tareas es importante. La tarea *Reparar vulnerabilidades* debe ejecutarse después de finalizada la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

8. Reinicie el servicio del Servidor de administración.

El Servidor de administración con acceso a Internet queda listo para descargar y transmitir actualizaciones a los servidores de administración aislados. Antes de comenzar a reparar vulnerabilidades, deberá configurar los servidores de administración aislados.

Configuración de servidores de administración aislados para corregir vulnerabilidades en una red aislada

Después de configurar el Servidor de administración con acceso a Internet, realice en cada Servidor de administración aislado de la red los siguientes preparativos, que le permitirán reparar vulnerabilidades e instalar actualizaciones en los dispositivos administrados conectados a ellos.

Para configurar sus servidores de administración aislados, siga estos pasos para cada Servidor de administración:

1. Active una clave de licencia para la función Administración de vulnerabilidades y parches (VAPM).

2. Cree dos carpetas en el disco en el que esté instalado el Servidor de administración:

   - Una carpeta para almacenar la lista de actualizaciones requeridas
   - Una carpeta para los parches

   Puede dar a estas carpetas el nombre que desee.

3. Otorgue el derecho **Modificar** al grupo KLAdmins para las carpetas que acaba de crear. Utilice para ello las herramientas administrativas que vienen incluidas en el sistema operativo.

4. Utilice la utilidad klscflag para especificar las rutas a las carpetas en las propiedades del Servidor de administración.

   Ejecute el símbolo del sistema de Windows usando derechos de administrador y, a continuación, cambie su directorio actual al directorio con la utilidad klscflag. La utilidad klscflag se encuentra en la carpeta donde está instalado el Servidor de administración. La ruta de instalación predeterminada: <Disk>:\Archivos de programa (x86)\Kaspersky Lab\Kaspersky Security Center.

5. Ejecute los siguientes comandos en la línea de comandos:

   - Para establecer la ruta a la carpeta de parches, ingrese lo siguiente:
     `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "<ruta a la carpeta>"`
   - Para establecer la ruta a la carpeta para la lista de actualizaciones requeridas, ingrese lo siguiente:
     `klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v "<ruta a la carpeta>"`

   Ejemplo: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "/FolderForPatches"`

6. Si es necesario, use la utilidad klscflag para especificar la frecuencia con la que el Servidor de administración aislado buscará nuevos parches:
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v <valor en segundos>`

   La configuración predeterminada es de 120 segundos.

   Ejemplo: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v 120`

7. Si es necesario, use la utilidad klscflag para calcular los hashes SHA256 de los parches:
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_VERIFY_HASH -t d -v 1`

   Al ejecutar este comando, sabrá si los parches sufrieron cambios al transferirse al Servidor de administración aislado. El comando también le dará la certeza de que los parches con actualizaciones requeridas que se reciban son los correctos.

   De manera predeterminada, Kaspersky Security Center Linux no calcula los hashes SHA256 de los parches. Si habilita esta opción, cuando el Servidor de administración aislado reciba parches, Kaspersky Security Center Linux calculará sus hashes y comparará el resultado con los valores hash almacenados en la base de datos del Servidor de administración. Si los hashes calculados no coinciden con los de la base de datos, verá un error y deberá reemplazar los parches problemáticos.

8. Cree la tarea *Buscar vulnerabilidades y actualizaciones requeridas* a fin de obtener información sobre los parches para el software de terceros instalado en los dispositivos administrados y, a continuación, programe la tarea.

9. Cree la tarea *Reparar vulnerabilidades* a fin de indicar qué parches se utilizarán para reparar vulnerabilidades en el software de terceros. A continuación, programe la tarea.

   Ejecute las tareas de forma manual si no quiere esperar al siguiente inicio programado. El orden en que se inician las tareas es importante. La tarea *Reparar vulnerabilidades* debe ejecutarse después de finalizada la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

10. Reinicie el servicio del Servidor de administración.

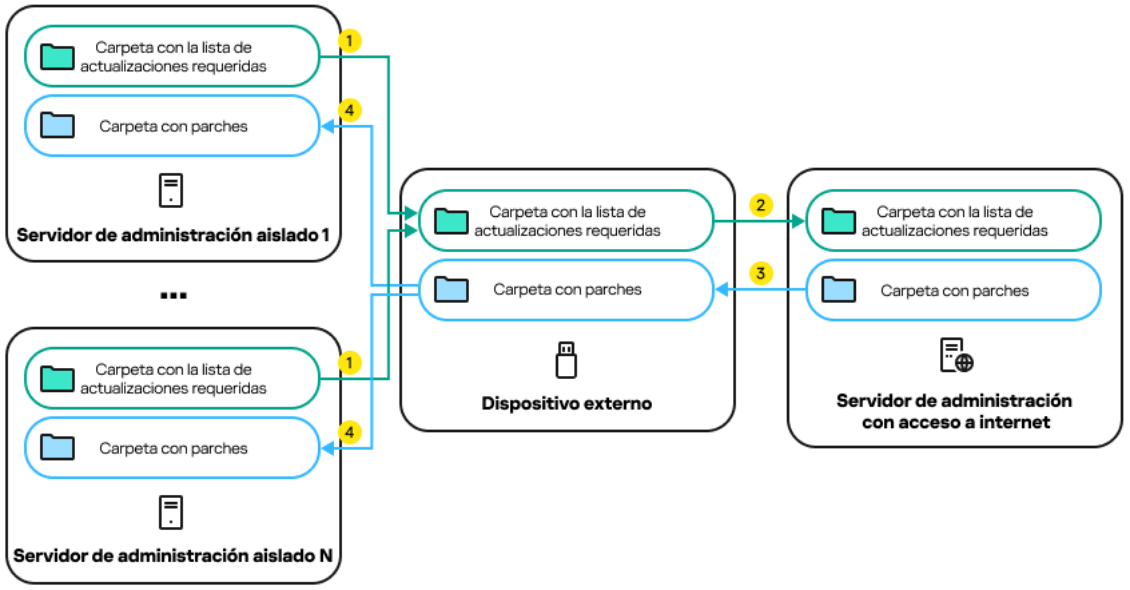
Una vez que haya configurado todos los servidores de administración, podrá transmitir los parches y las listas de actualizaciones que se requieran y reparar vulnerabilidades de software de terceros en los dispositivos administrados de su red aislada.

Transmitir parches e instalar actualizaciones en una red aislada

Una vez que haya configurado los servidores de administración, podrá transferir los parches que contengan las actualizaciones requeridas del Servidor de administración con acceso a Internet a los servidores de administración aislados. Las actualizaciones pueden transmitirse e instalarse con la frecuencia que se necesite (por ejemplo, una o más veces al día).

Para transferir los parches y la lista de actualizaciones requeridas entre sus servidores de administración, necesitará un dispositivo externo (por ejemplo, una unidad de almacenamiento extraíble). Asegúrese de que este dispositivo tenga espacio libre suficiente para almacenar los parches descargados.

En la siguiente imagen, se describe el proceso según el cual se transmiten los parches y la lista de actualizaciones requeridas:



Transmisión de parches y de la lista de actualizaciones requeridas entre los servidores de administración aislados y el Servidor de administración con acceso a Internet

Para instalar actualizaciones y reparar vulnerabilidades en dispositivos administrados conectados a servidores de administración aislados, haga lo siguiente:

1. Inicie la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* si no se encuentra en ejecución.
2. Conecte el dispositivo externo a cualquier Servidor de administración aislado.
3. Cree dos carpetas en el dispositivo externo: una para la lista de actualizaciones requeridas y otra para los parches. Puede dar a estas carpetas el nombre que desee.

   Si ya había creado estas carpetas, vacíelas.
4. Copie la lista de actualizaciones requeridas de cada Servidor de administración aislado y péguela en el dispositivo externo, en la carpeta que creó para la lista de actualizaciones requeridas.

   Debe juntar las listas de todos los servidores de administración aislados en una sola carpeta. Cuando termine con este paso, la carpeta contendrá archivos binarios con los identificadores de los parches requeridos por todos los servidores de administración aislados.

5. Conecte el dispositivo externo al Servidor de administración con acceso a Internet.

6. Copie la lista de actualizaciones requeridas del dispositivo externo y péguela en la carpeta que creó para la lista de actualizaciones requeridas en el Servidor de administración con acceso a Internet.

   Los parches necesarios se descargarán de Internet automáticamente y se guardarán en la carpeta de parches del Servidor de administración. El proceso puede llevar varias horas.

7. Asegúrese de descargar todos los parches necesarios. Para ello, puede realizar una de las acciones siguientes:

   - Revise la carpeta y busque los parches en el Servidor de administración con acceso a Internet. Verifique que todos los parches nombrados en la lista de actualizaciones requeridas se hayan descargado a la carpeta necesaria. Esto es más conveniente si la cantidad de parches requerida es pequeña.

   - Prepare un script especial, por ejemplo, un script de shell. Si obtiene una gran cantidad de parches, será difícil comprobar por sí mismo que se descargaron todos los parches. En casos así, es mejor automatizar la comprobación.

8. Copie los parches del Servidor de administración con acceso a Internet y péguelos en la carpeta que creó para tal fin en el dispositivo externo.

9. Transfiera los parches a todos los servidores de administración aislados. Coloque los parches en una carpeta creada para ellos.

Como resultado de estas instrucciones, cada Servidor de administración aislado creará una lista con las actualizaciones requeridas por los dispositivos administrados que a él se encuentren conectados. Cuando el Servidor de administración con acceso a Internet reciba la lista de actualizaciones requeridas, descargará los parches correspondientes de Internet. Cuando estos parches aparezcan en los servidores de administración aislados, serán procesados por la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*. Con ello, se instalarán las actualizaciones pertinentes en los dispositivos administrados y se repararán las vulnerabilidades presentes en el software de terceros.

No reinicie el dispositivo en el que esté instalado el Servidor de administración mientras se esté ejecutando la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*. Tampoco inicie la tarea *Copia de seguridad de los datos del Servidor de administración*, pues esta dará lugar a un reinicio. Si se reinicia el dispositivo, la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* se interrumpirá y las actualizaciones no se instalarán. Si esta tarea se detiene, ejecútela otra vez manualmente o aguarde a que ocurra el siguiente inicio programado.

Deshabilitar la transmisión de parches y la instalación de actualizaciones en una red aislada

Puede deshabilitar la transmisión de parches a aquellos servidores de administración aislados que, por ejemplo, ya no planee tener en una red aislada. De esta forma, puede reducir la cantidad de parches y el tiempo que toma descargarlos.

Para deshabilitar la transmisión de parches a servidores de administración aislados, haga lo siguiente:

1. Si desea dar de baja todos los servidores de administración aislados, en las propiedades del Servidor de administración con acceso a Internet, elimine las rutas a las carpetas utilizadas para los parches y para la lista de actualizaciones requeridas. Si piensa conservar algunos servidores de administración en una red aislada, omita este paso.

Ejecute el símbolo del sistema de Windows usando derechos de administrador y, a continuación, cambie su directorio actual al directorio con la utilidad klscflag. La utilidad klscflag se encuentra en la carpeta donde está instalado el Servidor de administración. La ruta de instalación predeterminada: <Disk>:\Archivos de programa (x86)\Kaspersky Lab\Kaspersky Security Center.

Ejecute los siguientes comandos en la línea de comandos:

- Para eliminar la ruta a la carpeta utilizada para los parches:
  `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v ""`
- Para eliminar la ruta a la carpeta utilizada para la lista de actualizaciones requeridas:
  `klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v ""`

2. Si eliminó las rutas a las carpetas, reinicie el servicio en el Servidor de administración con acceso a Internet.

3. En las propiedades de cada Servidor de administración aislado que desee quitar de la red aislada, elimine las rutas a las carpetas utilizadas para los parches y para la lista de actualizaciones requeridas.

   Ejecute los siguientes comandos en la línea de comandos utilizando una cuenta con privilegios de root:

   - Para eliminar la ruta a la carpeta utilizada para los parches:
     `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v ""`
   - Para eliminar la ruta a la carpeta utilizada para la lista de actualizaciones requeridas:
     `klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v ""`

4. Reinicie el servicio de cada Servidor de administración en el que realice la eliminación de rutas.

Si modificó la configuración del Servidor de administración con acceso a Internet, los parches ya no se transmitirán a través de Kaspersky Security Center Linux.

Si solo modificó la configuración de algunos servidores de administración específicos y los quitó de la red aislada, estos ya no recibirán parches a través de Kaspersky Security Center Linux. Solo los servidores de administración que permanezcan en la red aislada continuarán recibiendo parches.

Si posteriormente necesitara reparar vulnerabilidades en los servidores aislados que dio de baja, deberá volver a configurar tanto esos servidores de administración como el Servidor de administración con acceso a Internet.

Guía de referencia de API

Esta guía de referencia de OpenAPI de Kaspersky Security Center está diseñada para ayudar en las siguientes tareas:

- Automatización y personalización. Puede automatizar las tareas que no quiera manejar manualmente. Por ejemplo, como administrador, puede utilizar OpenAPI de Kaspersky Security Center para crear y ejecutar scripts que faciliten el desarrollo de la estructura de los grupos de administración y mantengan dicha estructura actualizada.

- Desarrollo personalizado. Con OpenAPI, puede desarrollar una aplicación cliente.

Puede utilizar el campo de búsqueda en la parte derecha de la pantalla para localizar la información que necesita en la guía de referencia de OpenAPI.

GUÍA DE REFERENCIA DE OPENAPI

Muestras de scripts

La guía de referencia de OpenAPI contiene muestras de los scripts de Python que se enumeran en la siguiente tabla. Los ejemplos muestran cómo se puede llamar a los métodos de OpenAPI para realizar diversas tareas de protección de su red en forma automática (por ejemplo, crear una jerarquía primario-secundario, ejecutar tareas en Kaspersky Security Center Linux o asignar puntos de distribución). Puede ejecutar los ejemplos o crear sus propios scripts basados en los ejemplos.

Para llamar a los métodos OpenAPI y ejecutar scripts,

Instale el paquete KlAkOAPI del archivo KlAkOAPI.tar.gz en un dispositivo donde esté instalado el Servidor de administración.

El paquete KlAkOAPI incluye un conjunto de muestras que realizan operaciones típicas. Puede llamar a los métodos de OpenAPI, ejecutar las muestras y sus propios scripts solo en dispositivos donde estén instalados el Servidor de administración y el paquete KlAkOAPI. El archivo KlAkOAPI.tar.gz que contiene este paquete se encuentra en la carpeta de instalación de Kaspersky Security Center Linux.

Coincidencia entre procedimientos de usuario y ejemplos de métodos OpenAPI de Kaspersky Security Center

Ejemplo	Propuesta del ejemplo	Procedimiento
Registro KlAkParams	Puede extraer y procesar datos usando la estructura de datos `KlAkParams`. La muestra indica cómo trabajar con esta estructura de datos. La salida de la muestra se puede presentar de diferentes maneras. Puede obtener los datos para enviar un método HTTP o para usarlo en su código.	Supervisión e informes
Crear y eliminar una jerarquía "principal/secundario"	Puede agregar un Servidor de administración secundario para establecer una jerarquía "principal/secundario". Alternativamente, puede desconectar de la jerarquía el Servidor de administración secundario.	Crear una jerarquía de Servidores de administración, agregar un Servidor de administración secundario y eliminar una jerarquía de Servidores de administración
Descargar archivos de lista de red a través de la puerta de enlace de conexión al host especificado	Puede conectarse al agente de red en el dispositivo necesario utilizando una pasarela de conexión y luego descargar un archivo con la lista de red a su dispositivo.	Ajuste de puntos de distribución y puertas de enlace de conexión

Ejemplo	Propuesta del ejemplo	Procedimiento
Instalar una clave de licencia almacenada en el repositorio del Servidor de administración principal en los servidores de administración secundarios	Puede conectarse al Servidor de administración principal, descargar desde allí la clave de licencia necesaria y transmitirla a todos los Servidores de administración secundarios incluidos en una jerarquía.	Licencias de aplicaciones administradas
Crear un informe de derechos de usuario efectivos	Puede crear diferentes informes Por ejemplo, puede generar el informe de derechos de usuario efectivos utilizando esta muestra. Este informe describe los derechos que tiene un usuario, dependiendo de su grupo y papel. Puede descargar el informe en formato HTML, PDF o Excel.	Generar y ver un informe
Iniciar la tarea del dispositivo	Puede conectarse al Agente de red en el dispositivo necesario utilizando una pasarela de conexión y luego ejecutar la tarea necesaria.	Iniciar una tarea manualmente
Registrar puntos de distribución para los dispositivos de un grupo	Puede asignar dispositivos administrados como puntos de distribución (antes conocidos como agentes de actualización).	Actualización de las bases de datos y las aplicaciones de Kaspersky
Enumerar todos los grupos	Puede realizar varias acciones en los grupos de administración: El ejemplo muestra cómo hacer lo siguiente: • Obtener un identificador del grupo raíz "Dispositivos administrados" • Moverse a través de la jerarquía de grupo • Recuperar la jerarquía completa y ampliada de los grupos, junto con sus nombres y nivel de anidación	Configuración del Servidor de administración
Enumerar las tareas, consultar las estadísticas de las tareas y ejecutar una tarea	Puede averiguar la siguiente información: • Historial de progreso de la tarea • Estado de la tarea actual • Número de tareas en diferentes estados También puedes ejecutar una tarea. De forma predeterminada, la muestra ejecuta una tarea después de emitir sus estadísticas.	Administración de tareas
Crear y ejecutar una tarea	Puede crear una tarea Especifique los siguientes parámetros de la tarea en la muestra: • Tipo • Método de ejecución • Perfiles • Grupo de dispositivos para el cual se utilizará la tarea De forma predeterminada, la muestra crea una tarea con el tipo "Mostrar mensaje". Puede ejecutar esta tarea para todos los dispositivos administrados del Servidor de administración. Si es necesario, puede especificar sus propios parámetros de tarea .	Crear una tarea
Enumerar las claves de licencia	Puede obtener una lista de todas las claves de licencia activas para aplicaciones Kaspersky instaladas en dispositivos administrados de Administration Server. La lista contiene datos detallados sobre cada clave de licencia, como un nombre, tipo o fecha de vencimiento.	Visualización de información sobre las claves de licencia en uso
Crear y encontrar un usuario interno	Puede crear una cuenta para un trabajo adicional.	Agregar una cuenta de un usuario interno
Crear una categoría personalizada	Puede crear la categoría de aplicación con los parámetros necesarios.	Creación de una categoría de aplicaciones con contenido agregado manualmente
Enumerar los usuarios mediante SrvView	Puede usar la clase SrvView para solicitar información detallada al Servidor de administración. Por ejemplo, puede obtener una lista de usuarios utilizando esta muestra.	Administración de usuarios y roles de usuarios
Crear usuarios internos, crear un paquete de instalación de Android y enviarlo por correo electrónico	Puede crear usuarios internos con la clase SecurityPolicy , crear un paquete de instalación de Android y enviarlo a los usuarios por correo electrónico.	Agregar una cuenta de un usuario interno

Aplicaciones que interactúan con Kaspersky Security Center Linux a través de OpenAPI

Algunas aplicaciones interactúan con Kaspersky Security Center Linux a través de OpenAPI. Entre estas aplicaciones se encuentran, por ejemplo, Kaspersky Anti Targeted Attack Platform o Kaspersky Security for Virtualization. También puede ser una aplicación cliente personalizada que puede desarrollar con OpenAPI.

Las aplicaciones que interactúan con Kaspersky Security Center Linux a través de OpenAPI se conectan al Servidor de administración. Si ha configurado una lista de direcciones IP autorizadas a conectarse al Servidor de administración, agregue las direcciones IP de los dispositivos en los que estén instaladas las aplicaciones que utilicen la interfaz OpenAPI de Kaspersky Security Center Linux. Para saber si una aplicación utiliza OpenAPI, consulte la ayuda de esa aplicación.

Prácticas recomendadas para proveedores de servicios

Esta sección proporciona información sobre cómo configurar y usar Kaspersky Security Center Linux.

Esta sección contiene recomendaciones para instalar, configurar y usar la aplicación. También describe modos de resolver problemas habituales en el funcionamiento de la aplicación.

Planificación del despliegue de Kaspersky Security Center Linux

Al planificar la implementación de los componentes de Kaspersky Security Center Linux en la red de una organización, considere el tamaño y el alcance del proyecto, en particular los siguientes factores:

- Número total de dispositivos.
- Número de clientes MSP.

Un Servidor de administración puede admitir un máximo de 50 000 dispositivos. Cuando el número total de dispositivos en la red de la organización supera los 50 000, hay que instalar varios Servidores de administración en la infraestructura del proveedor de servicios y combinarlos en una jerarquía para facilitar la administración centralizada.

Se pueden crear hasta 500 servidores virtuales en un solo Servidor de administración, por lo que se requiere un Servidor de administración particular por cada 500 clientes MSP.

En la etapa de planificación del despliegue, es necesario tener en cuenta la asignación del certificado especial X.509 al Servidor de administración. La asignación del certificado X.509 al Servidor de administración puede ser útil en los casos siguientes (lista parcial):

- Para la inspección del tráfico de la capa de sockets seguros (SSL) mediante un de terminación SSL
- Para especificar los valores requeridos de los campos del certificado
- Para proporcionar la solidez de cifrado deseada del certificado

Suministro de acceso a Internet al Servidor de administración

Para permitir que los dispositivos en la red del cliente accedan al Servidor de administración mediante Internet, debe abrir los siguientes puertos del Servidor de administración:

- 13000 TCP: puerto TLS del Servidor de administración para conectar Agentes de red instalados en la red del cliente
- 8061 TCP: puerto HTTPS para publicar paquetes independientes usando herramientas de Kaspersky Security Center Web Console

- 8060 TCP: puerto HTTP para publicar paquetes independientes usando herramientas de Kaspersky Security Center Web Console
- 13292 TCP: puerto de TLS solo requerido si hay dispositivos móviles que se deban administrar
- 8080 TCP: Puerto HTTPS para Kaspersky Security Center Web Console

Configuración estándar de Kaspersky Security Center Linux

Uno o varios Servidores de administración están instalados en los servidores del MSP. El número de Servidores de administración puede seleccionarse según el hardware disponible, el número total de clientes MSP o el número total de dispositivos administrados.

Un Servidor de administración puede admitir un máximo de 50 000 dispositivos. Debe considerar la posibilidad de aumentar el número de dispositivos administrados en el futuro próximo: puede ser útil conectar un número levemente menor de dispositivos a un solo Servidor de administración.

Se pueden crear hasta 500 servidores virtuales en un solo Servidor de administración, por lo que se requiere un Servidor de administración particular por cada 500 clientes MSP.

Si se utilizan varios servidores, se recomienda que los combine en una jerarquía. La utilización de una jerarquía de Servidores de administración le permite evitar directivas y tareas duplicadas, gestionar el conjunto completo de dispositivos administrados, como si fueran administrados por un solo Servidor de administración; por ejemplo, buscar dispositivos, crear selecciones de dispositivos y crear informes.

En cada servidor virtual que corresponda a un cliente MSP, debe asignar uno o varios puntos de distribución. Si los clientes MSP y el Servidor de administración se vinculan por Internet, puede ser útil crear una tarea *Descargar actualizaciones a los repositorios de puntos de distribución* para los puntos de distribución, de modo que descarguen las actualizaciones directamente desde los servidores de Kaspersky, no desde el Servidor de administración.

Si algunos dispositivos en la red del cliente MSP no tienen acceso directo a Internet, debe cambiar los puntos de distribución al modo de puerta de enlace de conexión. En este caso, los Agentes de red en los dispositivos en la red del cliente MSP se conectarán, para mayor sincronización, al Servidor de administración, pero mediante la puerta de enlace, no de manera directa.

Como es muy probable que el Servidor de administración no pueda sondear la red cliente MSP, puede ser útil transferir esta función a un punto de distribución.

El Servidor de administración no podrá enviar notificaciones al puerto UDP 15000 a dispositivos administrados ubicados detrás de la NAT en la red del cliente MSP. Para resolver este problema, puede ser útil activar el modo de conexión continua con el Servidor de administración en las propiedades de los dispositivos que funcionan como puntos de distribución y se ejecutan en el modo de Puerta de enlace de conexión (opción **No desconectar del Servidor de administración**). El modo de conexión continua está disponible si el número total de puntos de distribución no supera los 300.

Es posible que un cliente MSP quiera administrar los dispositivos Android y iOS de los empleados. El Servidor de administración administra los dispositivos móviles mediante TLS, puerto TCP 13292.

Acerca de los puntos de distribución

Los dispositivos que tengan instalado el Agente de red pueden utilizarse como punto de distribución. En este modo, el Agente de red puede realizar las funciones siguientes:

- Transferir archivos a dispositivos cliente, incluidos:
  - Actualizaciones de las bases de datos y módulos de software de Kaspersky

    Las actualizaciones se pueden recibir desde el Servidor de administración o desde los servidores de actualización de Kaspersky. En este último caso, se debe crear *la tarea Descargar actualizaciones a los repositorios de puntos de distribución* para el dispositivo que sirve como punto de distribución.
  - Actualizaciones para el software de terceros
  - Paquetes de instalación
- Instalar software (incluido el Agente de red, durante el despliegue inicial) en otros dispositivos.
- Sondear la red para detectar nuevos dispositivos y actualizar la información disponible sobre los dispositivos de los que ya se tenía conocimiento. Un punto de distribución puede aplicar los mismos métodos de descubrimiento de dispositivos que el Servidor de administración.

El despliegue de puntos de distribución en la red de una organización cumple los siguientes objetivos:

- Reducir la carga en el Servidor de administración si funciona como la fuente de actualizaciones.
- Optimizar el tráfico de Internet ya que, en este caso, no es necesario que cada dispositivo de la red del cliente MSP tenga acceso a servidores de Kaspersky o el Servidor de administración para descargar actualizaciones.
- Proporcionar al Servidor de administración acceso a dispositivos detrás de NAT (con relación al Servidor de administración) de la red del cliente MSP, lo que permite que el Servidor de administración realice las acciones siguientes:
  - Envíe notificaciones a dispositivos mediante UDP en la red IPv4 o IPv6.
  - Sondee la red IPv4 o IPv6.
  - Realizar el despliegue inicial.
  - Actuar como un servidor push.

Un punto de distribución se asigna a un grupo de administración. En este caso, la cobertura del punto de distribución incluye todos los dispositivos dentro del grupo de administración y todos sus subgrupos. Sin embargo, el dispositivo que actúa como punto de distribución no se puede incluir en el grupo de administración al cual se ha asignado.

Puede hacer que un punto de distribución funcione como una puerta de enlace de conexión. En este caso, los dispositivos en el alcance del punto de distribución se conectarán al Servidor de administración a través de la puerta de enlace, no directamente. Puede usar este modo en situaciones que no permitan el establecimiento de una conexión directa entre dispositivos con el Agente de red y un Servidor de administración.

Los dispositivos designados como puntos de distribución deben protegerse contra el acceso no autorizado por medios virtuales y físicos.

Jerarquía de Servidores de administración

Algunas empresas cliente (por ejemplo, los MSP) pueden tener varios servidores de administración en funcionamiento. Puede ser poco conveniente administrar varios Servidores de administración independientes, por lo que se puede aplicar una jerarquía. En una jerarquía, un Servidor de administración instalado en Linux puede funcionar como servidor principal o como servidor secundario. Un Servidor de administración principal instalado en Linux puede administrar servidores secundarios instalados tanto en Linux como en Windows. Un servidor principal basado en Windows puede administrar un servidor secundario basado en Linux.

La configuración "principal/secundario" de dos Servidores de administración proporciona las opciones siguientes:

- El Servidor de administración secundario hereda directivas, tareas, roles de usuario y paquetes de instalación del Servidor de administración principal. De esta forma, se evita la duplicación de configuraciones.
- Las selecciones de dispositivos en el Servidor de administración principal pueden incluir dispositivos desde los Servidores de administración secundarios.
- Los informes sobre el Servidor de administración principal pueden contener datos (incluida información detallada) de los Servidores de administración secundarios.
- El Servidor de administración principal puede actuar como origen de actualizaciones del Servidor de administración secundario.

El Servidor de administración principal solo recibe datos de Servidores de administración secundarios no virtuales dentro del alcance de las opciones antes enumeradas. Esta limitación no se aplica a los Servidores de administración virtuales, que comparten la base de datos con su Servidor de administración principal.

La jerarquía de los Servidores de administración es compatible con el modo de multiinquilinato. Este modo permite que un administrador principal administre varios clientes de forma centralizada e independiente. Cada organización u oficina cliente está aislada de las demás y se denomina inquilino. Puede asignar varios dispositivos administrados junto con sus datos, configuraciones, directivas y tareas asociados a un inquilino, y configurar los derechos de usuario por inquilino.

Un Servidor de administración principal, instalado en la infraestructura de la organización principal, actúa como inquilino principal. El Servidor de administración principal permite que los Servidores de administración secundarios o virtuales (sus inquilinos aislados) reciban y procesen de forma independiente sus propios eventos y trabajen con sus propios recursos, servicios y configuraciones.

Un proveedor de servicios que tenga varias organizaciones cliente puede proporcionar las funcionalidades de Kaspersky Security Center Linux, incluida la combinación de alertas y las acciones de respuesta, a cada organización cliente de forma independiente. Para lograr esto, el proveedor de servicios conecta Servidores de administración secundarios o virtuales como inquilinos para cada organización cliente. El proveedor de servicios brinda servicios utilizando su propio personal y recursos.

Servidores de administración virtuales

Sobre la base de un Servidor de administración físico, se pueden crear varios Servidores de administración virtual, los que serán similares a los Servidores de administración secundarios. En comparación con el modelo de acceso discrecional, que se basa en listas de control de acceso (ACL), el modelo del Servidor de administración virtual es más funcional y proporciona un mayor nivel de aislamiento. Además de una estructura dedicada de grupos de administración para dispositivos asignados con directivas y tareas, cada Servidor de administración virtual presenta su propio grupo de dispositivos no asignados, sus propios conjuntos de informes, dispositivos seleccionados y eventos, paquetes de instalación, reglas de traslado, etc. Para el aislamiento mutuo máximo de clientes MSP, recomendamos que elija Servidores de administración virtuales como la funcionalidad que se utilizará. Asimismo, la creación de un Servidor de administración virtual para cada cliente MSP le permite proporcionar a clientes opciones básicas de administración de la red mediante Kaspersky Security Center Web Console.

Los Servidores de administración virtual son muy similares a los Servidores de administración secundarios, pero con las distinciones siguientes:

- Un Servidor de administración virtual carece de la mayoría de las configuraciones globales y sus propios puertos TCP.
- Un Servidor de administración virtual no tiene Servidores de administración secundarios.
- Un Servidor de administración virtual no tiene otros Servidores de administración virtuales.
- En un Servidor de administración físico se ven los dispositivos, grupos, eventos y objetos de los dispositivos administrados (elementos en Cuarentena, registro de aplicaciones, etc.) de todos sus Servidores de administración virtuales.
- Un Servidor de administración virtual solo puede analizar la red con puntos de distribución conectados.

Despliegue y configuración inicial

Kaspersky Security Center Linux es una aplicación distribuida. Kaspersky Security Center Linux incluye las siguientes aplicaciones:

- Servidor de administración: El componente principal, diseñado para administrar los dispositivos de una organización y almacenar datos en un DBMS.
- Kaspersky Security Center Web Console: Una interfaz web para el Servidor de administración diseñada para las operaciones básicas. Puede instalar este componente en cualquier dispositivo que cumpla requisitos de software y hardware.
- Agente de red: diseñado para administrar la aplicación de seguridad instalada en un dispositivo, así como para recopilar información sobre ese dispositivo. Los agentes de red se instalan en dispositivos de una organización.

El despliegue de Kaspersky Security Center Linux en la red de una organización se realiza de la siguiente manera:

- Instalación de un Servidor de administración.
- Instalación de Kaspersky Security Center Web Console.
- Instalación del Agente de red y aplicación de seguridad en dispositivos de la empresa.

Recomendaciones sobre la instalación del Servidor de administración

Esta sección contiene recomendaciones sobre cómo para instalar el Servidor de administración. Esta sección también proporciona situaciones sobre cómo usar una carpeta compartida en el dispositivo del Servidor de administración a fin de instalar el Agente de red en los dispositivos cliente.

Creación de cuentas para los servicios del Servidor de administración en un clúster de conmutación por error

Antes de comenzar el despliegue de Kaspersky Security Center Linux en un clúster de conmutación por error, debe crear cuentas para los servicios de Kaspersky Security Center Linux.

Para ello, siga estos pasos en el nodo activo, el nodo pasivo y el servidor de archivos:

1. Cree un grupo llamado "kladmins" y asigne el mismo GID a los tres grupos.
2. Cree una cuenta de usuario llamada "ksc" y asigne el mismo UID a las tres cuentas de usuario. Defina "kladmins" como grupo principal para las cuentas creadas.
3. Cree una cuenta de usuario llamada "rightless" y asigne el mismo UID a las tres cuentas de usuario. Defina "kladmins" como grupo principal de las cuentas creadas.

Selección de un DBMS

La siguiente tabla enumera las opciones de DBMS válidas, así como las recomendaciones y las restricciones en su uso.

Recomendaciones y restricciones en DBMS

DBMS	Recomendaciones y restricciones
MySQL (ver versiones compatibles)	Utilice este DBMS si planea ejecutar un solo Servidor de administración para menos de 20 000 dispositivos.
MariaDB (ver versiones compatibles)	Utilice este DBMS si planea ejecutar un solo Servidor de administración para menos de 20 000 dispositivos.

PostgreSQL, Postgres Pro (ver versiones compatibles)	Utilice este DBMS si planea ejecutar un solo Servidor de administración para menos de 50 000 dispositivos.
Tantor (consulte las versiones compatibles)	Utilice este DBMS si planea ejecutar un solo Servidor de administración para menos de 50 000 dispositivos. El DBMS de Tantor solo es compatible con Astra Linux Special Edition RUSB.10015-01 (actualización operativa 1.8).

Para obtener información sobre cómo instalar el DBMS seleccionado, consulte su documentación.

Se recomienda deshabilitar la Tarea del inventario del software y deshabilitar (en la configuración de directivas de Kaspersky Endpoint Security) las notificaciones del Servidor de administración en las aplicaciones iniciadas.

Si decide instalar PostgreSQL o Postgres Pro, asegúrese de especificar la contraseña del superusuario. Si no especifica esta contraseña, es posible que el Servidor de administración no pueda conectarse a la base de datos.

Si instala MySQL, MariaDB, PostgreSQL, o Postgres Pro, use la configuración recomendada para garantizar que el DBMS funcione correctamente.

Si usa un DBMS PostgreSQL, MariaDB o MySQL, la pestaña **Eventos** puede mostrar una lista incompleta de eventos para el dispositivo cliente seleccionado. Esto ocurre cuando el DBMS almacena una gran cantidad de eventos. Realice una de las siguientes acciones si desea aumentar la cantidad de eventos mostrados:

- Eliminación de eventos innecesarios.
- Reducción del plazo de almacenamiento para eventos innecesarios.

Para ver una lista completa de eventos registrados en el Servidor de administración para el dispositivo, use Informes.

Especificación de la dirección del Servidor de administración

Al instalar el Servidor de Administración, debe especificar el nombre DNS o la dirección IP estática del Servidor de administración. Esta dirección se utilizará como dirección predeterminada al crear paquetes de instalación del Agente de red. Después de esto, podrá cambiar la dirección del equipo host del Servidor de administración usando herramientas de Kaspersky Security Center Web Console; la dirección no cambiará automáticamente en los paquetes de instalación del Agente de red que ya se hayan creado.

Mantener conexiones inactivas

Le recomendamos que configure los siguientes parámetros de estado activo en los dispositivos de la puerta de enlace de conexión para mejorar la estabilidad de la conexión:

- `net.ipv4.tcp_keepalive_intvl` especifica la frecuencia con la que se deben enviar mensajes keepalive después del primero. Establezca el valor de este parámetro en `1`.
- `net.ipv4.tcp_keepalive_probes` especifica cuántos mensajes keepalive se pueden enviar sin una respuesta antes de que la conexión se considere inactiva. Establezca el valor de este parámetro en `10`.
- `net.ipv4.tcp_keepalive_time` especifica cuánto tiempo esperar después del último paquete de datos antes de enviar el primer mensaje keepalive. Establezca el valor de este parámetro en `900`.

Para configurar los parámetros de keepalive:

1. Abra el archivo /etc/sysctl.conf.
2. Agregue los siguientes valores de parámetro:

```
net.ipv4.tcp_keepalive_intvl = 1
net.ipv4.tcp_keepalive_probes = 10
net.ipv4.tcp_keepalive_time = 900
```

3. Ejecute el siguiente comando para realizar la actualización de los parámetros de keepalive:

```
sudo sysctl -p /etc/sysctl.conf
```

4. Ejecute los siguientes comandos para asegurarse de que se hayan aplicado los valores de los parámetros:

```
sudo sysctl net.ipv4.tcp_keepalive_intvl
sudo sysctl net.ipv4.tcp_keepalive_probes
sudo sysctl net.ipv4.tcp_keepalive_time
```

Desplegar el Agente de red y las aplicaciones de seguridad

Para administrar los dispositivos de una organización y protegerlos contra amenazas de seguridad, es necesario instalar el Agente de red y una aplicación de seguridad de Kaspersky en cada dispositivo administrado.

Para obtener información sobre el despliegue de la protección, consulte la sección Despliegue del agente de red y la aplicación de seguridad.

Para obtener información sobre la protección de dispositivos móviles, consulte la sección Administración de dispositivos móviles.

En Microsoft Windows XP, el Agente de red podría no realizar las siguientes operaciones correctamente: descargar actualizaciones directamente desde los servidores de Kaspersky (como un punto de distribución); funcionar como servidor proxy de KSN (como un punto de distribución); detectar vulnerabilidades de terceros (si se usa la Administración de vulnerabilidades y parches).

Configuración de protección en la red de una organización cliente

Una vez finalizada la instalación del Servidor de Administración, Kaspersky Security Center Web Console se inicia y le solicita que realice la configuración inicial a través del asistente correspondiente. Cuando el Asistente de inicio rápido se está ejecutando, las siguientes directivas y tareas se crean en el grupo de administración original:

- Directiva de Kaspersky Endpoint Security.
- Tarea de grupo para actualizar Kaspersky Endpoint Security.
- Tarea de grupo para analizar un dispositivo con Kaspersky Endpoint Security.
- Directiva del Agente de red.
- Tarea de análisis de vulnerabilidades (tarea del Agente de red).
- Tarea de instalación de actualizaciones y reparación de vulnerabilidades (tarea del Agente de red).

Las directivas y las tareas se crean con las configuraciones predeterminadas, que pueden resultar ser subóptimas o incluso inadmisibles para la organización. Por lo tanto, debe comprobar las propiedades de objetos que se han creado y modificarlos manualmente, si es necesario.

Esta sección contiene la información sobre la configuración manual de directivas, tareas y otras configuraciones del Servidor de administración e información sobre el punto de distribución, lo que crea una estructura del grupo de administración y la jerarquía de tareas, y otra configuración.

Configuración manual de la directiva de Kaspersky Endpoint Security

Esta sección proporciona recomendaciones sobre cómo configurar la directiva de Kaspersky Endpoint Security creada por el Asistente de inicio rápido. Puede realizar la configuración en la ventana de propiedades de la directiva.

Al editar una configuración, tenga en cuenta que puede bloquear o desbloquear la configuración para prohibir o permitir la edición de su valor en una estación de trabajo.

Configuración de la directiva en la sección Protección avanzada contra amenazas

Para obtener una descripción completa de los ajustes disponibles en esta sección, consulte la documentación de Kaspersky Endpoint Security para Windows.

En la sección **Protección avanzada contra amenazas**, puede configurar el uso de Kaspersky Security Network para Kaspersky Endpoint Security para Windows. También puede configurar Kaspersky Endpoint Security para Windows, como detección de comportamiento, prevención de exploits, Prevención de intrusiones en el host y motor de reparación.

En la subsección **Kaspersky Security Network**, le recomendamos que active la opción **Kaspersky Security Network**. Esta función ayuda a redistribuir y optimizar el tráfico de la red. Si la opción **Kaspersky Security Network** está deshabilitada, puede habilitar el uso directo de servidores KSN.

Configuración de la directiva en la sección Protección básica contra amenazas

Para obtener una descripción completa de los ajustes disponibles en esta sección, consulte la documentación de Kaspersky Endpoint Security para Windows.

En la sección **Protección básica contra amenazas** de la ventana de propiedades de la directiva, le recomendamos que especifique configuraciones adicionales en las subsecciones **Firewall** y **Protección contra amenazas de archivo**.

La subsección **Firewall** contiene ajustes que le permiten controlar la actividad de red de las aplicaciones en los dispositivos cliente. Un dispositivo cliente utiliza una red a la que se le ha asignado alguno de estos estados: pública, local o de confianza. Kaspersky Endpoint Security puede permitir o bloquear el tráfico de red en un dispositivo basándose en el estado de la red. Cuando agregue una nueva red a su organización, deberá asignarle un estado de red adecuado. Si el dispositivo cliente es, por ejemplo, una computadora portátil, recomendamos que el dispositivo use una red pública o de confianza, ya que la computadora portátil no siempre está conectada a la red local. En la subsección **Firewall** puede verificar si ha asignado correctamente estados a las redes utilizadas en su organización.

Para revisar la lista de redes:

1. En las propiedades de la directiva, vaya a **Protección básica contra amenazas** → **Firewall**.
2. En la sección **Redes disponibles**, haga clic en el botón **Configuración**.
3. En la ventana **Firewall** que se abre, vaya a la pestaña **Redes** para ver la lista de redes.

En la subsección **Protección contra amenazas de archivo** puede desactivar el análisis de las unidades de red. El análisis de unidades de red puede tener un impacto pronunciado en las unidades. Es preferible realizar análisis indirectos en los servidores de archivos.

Para deshabilitar el análisis de unidades de red:

1. En las propiedades de la directiva, vaya a **Protección básica contra amenazas → Protección contra amenazas de archivo**.
2. En la sección **Nivel de seguridad**, haga clic en el botón **Configuración**.
3. En la ventana **Protección contra amenazas de archivo** que se abre, en la ficha **General**, desmarque la casilla **Todas las unidades de red**.

Configuración de la directiva en la sección Configuración general

Para obtener la descripción completa de la configuración disponible en esta sección, consulte la documentación de Kaspersky Endpoint Security.

A continuación, se describen algunas acciones de configuración adicionales que recomendamos realizar en la ventana de propiedades de la directiva de Kaspersky Endpoint Security, en la sección **Configuración general**.

Sección Configuración general, subsección Informes y almacenamiento

En la sección **Transferencia de datos al Servidor de administración**, encontrará la casilla **Acerca de las aplicaciones iniciadas**. Cuando esta casilla está seleccionada, la base de datos del Servidor de administración guarda la información acerca de todas las versiones de todos los módulos de software en los dispositivos en red. Esta información puede ocupar una gran cantidad de espacio en la base de datos de Kaspersky Security Center Linux (docenas de gigabytes). Por lo tanto, si la casilla **Acerca de las aplicaciones iniciadas** aún está seleccionada en la directiva de alto nivel, se debe desmarcar.

Sección Configuración general, subsección Interfaz

Si la protección de amenazas en la red de la organización se debe administrar en el modo centralizado a través de Kaspersky Security Center Web Console, debe deshabilitar la visualización de la interfaz de usuario de Kaspersky Endpoint Security en las estaciones de trabajo (desactive la casilla **Mostrar interfaz de la aplicación** en la sección **Interacción con el usuario**) y habilitar la protección con contraseña (marque la casilla **Habilitar protección con contraseña** en la sección **Protección con contraseña**).

Configuración de la directiva en la sección Configuración de eventos

En la sección **Configuración de eventos**, debe deshabilitar el almacenamiento de cualquier evento en el Servidor de administración, excepto los siguientes:

- En la pestaña **Crítico**:
  - *La ejecución automática de la aplicación está deshabilitada*
  - *Acceso denegado*
  - *Inicio de aplicación prohibido*
  - *No se puede desinfectar*
  - *Contrato de licencia de usuario final infringido*

- *No se pudo cargar el módulo de cifrado*
- *No se pueden iniciar dos tareas al mismo tiempo*
- *Se detectó una amenaza activa; ejecute la Desinfección avanzada*
- *Ataque de red detectado*
- *No se actualizaron todos los componentes*
- *Error de activación*
- *Error al habilitar el modo portátil*
- *Error de interacción con Kaspersky Security Center*
- *Error al deshabilitar el modo portátil*
- *Error al cambiar los componentes de la aplicación*
- *Error al implementar las reglas de cifrado o descifrado de archivos*
- *No se puede aplicar la directiva*
- *Proceso finalizado*
- *Actividad de red bloqueada*

- En la pestaña **Error funcional**: *La configuración de la tarea no es válida y no se aplicó*
- En la pestaña **Advertencia**:
  - *Autoprotección deshabilitada*
  - *Clave de reserva incorrecta*
  - *El usuario optó por no implementar la directiva de cifrado*
- En la ficha **Información**: *Inicio de aplicación prohibido en el modo de prueba*

Configuración manual de la tarea de grupo para actualizar Kaspersky Endpoint Security

Si el Servidor de administración actúa como origen de actualización, la opción de programación óptima y recomendada para Kaspersky Endpoint Security es **Cuando se descargan nuevas actualizaciones en el repositorio** con la casilla **Usar retardo aleatorio automático para el inicio de tareas** marcada.

Si se crea una tarea local para descargar actualizaciones de servidores de Kaspersky al repositorio en cada punto de distribución, la programación periódica será óptima y recomendada para la tarea de actualización del grupo de Kaspersky Endpoint Security. En este caso, el valor del intervalo de aleatorización debería configurarse en 1 hora.

Instalación manual de la tarea de grupo para analizar un dispositivo con Kaspersky Endpoint Security

El Asistente de inicio rápido crea una tarea de grupo para analizar un dispositivo. Si la programación especificada automáticamente de la tarea de análisis de grupo no es adecuada para su organización, debe configurar de forma manual la programación más conveniente para esta tarea según las reglas del lugar de trabajo adoptadas en la organización.

Por ejemplo, la tarea tiene asignada la programación **Ejecutar los viernes a las 7:00 p. m.** con aleatorización automática y la casilla de verificación **Ejecutar tareas no realizadas** no está marcada. Esto significa que si los dispositivos de la organización se apagan, por ejemplo, los viernes a las 6:30 p.m., la tarea de análisis de los dispositivos nunca se ejecutará. En este caso, debe configurar la tarea de análisis de grupo manualmente.

Programación de la tarea Buscar vulnerabilidades y actualizaciones requeridas

El Asistente de inicio rápido crea la tarea *Buscar vulnerabilidades y actualizaciones requeridas* para el Agente de red. De forma predeterminada, se asigna a la tarea la programación **Ejecutar los martes a las 7:00 p. m.** con aleatorización automática, y la casilla **Ejecutar tareas no realizadas** está marcada.

Si las reglas del lugar de trabajo de la organización especifican el cierre de todos los dispositivos a esta hora, la tarea *Buscar vulnerabilidades y actualizaciones requeridas* se ejecutará después de que los dispositivos se vuelvan a encender; es decir, el miércoles por la mañana. Esto puede ser inconveniente porque los análisis de vulnerabilidades pueden hacer que aumente la carga en los subsistemas de disco y CPU. Debe buscar que la programación de la tarea se adecue a las reglas dispuestas por su organización.

Configuración manual de la tarea de grupo para la instalación de actualizaciones y la reparación de vulnerabilidades

El Asistente de inicio rápido crea una tarea de grupo para la instalación de actualizaciones y la reparación de vulnerabilidades para el Agente de red. De forma predeterminada, la tarea está configurada para ejecutarse todos los días a la 1:00 a. m. con una demora definida al azar automáticamente, y la opción **Ejecutar tareas no realizadas** no debe estar habilitada.

Si las reglas del lugar de trabajo de la organización especifican el cierre de dispositivos durante la noche, la instalación de actualizaciones nunca se ejecutará. Debe configurar la programación más cómoda para esta tarea de análisis de vulnerabilidades según las reglas del lugar de trabajo adoptadas en la organización. También es importante tener en cuenta que la instalación de actualizaciones puede requerir reiniciar el dispositivo.

Creación de una estructura de grupos de administración y asignación de puntos de distribución

Una estructura de grupos de administración en Kaspersky Security Center Linux realiza las funciones siguientes:

- Define el alcance de las directivas

  Existe otra forma de aplicar ajustes pertinentes al dispositivos: mediante el uso de perfiles de directiva. En este caso, el alcance de las directivas se establece, por ejemplo, mediante etiquetas de dispositivos o funciones de usuario.

- Define el alcance de las tareas de grupo

  Existe un modo de definir el alcance de las tareas de grupo que no depende de una jerarquía de grupos de administración: el uso de tareas para selecciones de dispositivos y de tareas para dispositivos específicos.

- Regula la capacidad de acceder a los distintos dispositivos, Servidores de administración secundarios y Servidores de administración virtuales

- Asigna puntos de distribución

Al momento de crear la estructura de grupos de administración, para que la asignación de puntos de distribución sea óptima, es necesario tener en cuenta la topología de la red de la organización. La distribución óptima de puntos de distribución le permite ahorrar tráfico en la red de la organización.

Según el organigrama de la empresa y la topología de red adoptada por el cliente MSP, pueden aplicarse las siguientes configuraciones estándares a la estructura de grupos de administración:

- Oficina única

- Varias oficinas remotas pequeñas

Configuración estándar de un cliente MSP: oficina única

En una configuración estándar de "oficina única", todos los dispositivos se encuentran en la red de la organización y tienen la capacidad de "verse" los unos a los otros. La red de la organización puede constar de varias partes independientes (redes o segmentos de red) vinculadas por canales estrechos.

Los siguientes métodos pueden emplearse para armar la estructura de grupos de administración:

- Armar la estructura de grupos de administración tomando en cuenta la topología de la red. No es necesario que la estructura de grupos de administración refleje con absoluta precisión la topología de la red. Es suficiente con que haya coincidencia entre las partes independientes de la red y ciertos grupos de administración. Puede usar la asignación automática de puntos de distribución o asignarlos manualmente.

- Armar la estructura de grupos de administración sin tener en cuenta la topología de la red. En este caso, debe deshabilitar la asignación automática de puntos de distribución y luego asignar uno o varios dispositivos para que actúen como puntos de distribución para un grupo de administración original en cada una de las partes independientes de la red; por ejemplo, para el grupo **Dispositivos administrados**. Todos los puntos de distribución estarán al mismo nivel y presentarán el mismo alcance en todos los dispositivos en la red de la organización. En este caso, cada Agente de red se conectará al punto de distribución que tenga la ruta más corta. Puede rastrear la ruta hasta un punto de distribución con la utilidad tracert o traceroute.

Configuración estándar de un cliente MSP: varias pequeñas oficinas remotas

Esta configuración estándar contempla la existencia de varias pequeñas oficinas remotas, que pueden comunicarse con una oficina central a través de Internet. Cada oficina remota está ubicada detrás de una pasarela NAT; debido a ello, las oficinas remotas están aisladas las unas de las otras y no se pueden conectar entre sí.

La configuración se debe ver reflejada en la estructura de grupos de administración: debe crearse un grupo de administración independiente para cada oficina remota (los grupos **Oficina 1** y **Oficina 2** en la siguiente imagen).



Oficinas remotas incluidas en la estructura de grupos de administración

Cada grupo de administración correspondiente a una oficina debe tener asignados uno o más puntos de distribución. Los puntos de distribución deben ser dispositivos que se encuentren en la oficina remota y deben tener una cantidad suficiente de espacio libre en disco. Los dispositivos incluidos en el grupo **Oficina 1** accederán a los puntos de distribución asignados al grupo de administración **Oficina 1**, por ejemplo.

Cuando hay usuarios que utilizan una computadora portátil para trabajar físicamente en más de una oficina, resulta necesario designar, junto con los puntos de distribución existentes, dos o más dispositivos en cada oficina remota para que actúen como puntos de distribución de un grupo de administración ubicado en un nivel superior (el grupo llamado **Grupo para oficinas** en la imagen anterior).

Ejemplo: Una computadora portátil incluida en el grupo de administración **Oficina 1** se traslada físicamente a la oficina que corresponde al grupo de administración **Oficina 2**. Luego del traslado, el Agente de red de la computadora portátil intenta acceder a los puntos de distribución asignados al grupo **Oficina 1**, pero esos puntos de distribución no están disponibles. Tras ello, el Agente de red intenta acceder a los puntos de distribución asignados al **Grupo para oficinas**. Como las oficinas remotas están aisladas entre sí, los intentos de acceder a los puntos de distribución asignados al grupo de administración **Grupo para oficinas** solo tendrán éxito cuando el Agente de red intente acceder a los puntos de distribución del grupo **Oficina 2**. Así, la computadora portátil permanecerá en el grupo de administración correspondiente a su oficina inicial, pero usará el punto de distribución de la oficina en la que se encuentre físicamente.

Jerarquía de directivas, usando perfiles de directivas

En esta sección se proporciona información sobre cómo aplicar directivas a los dispositivos en los grupos de administración. Esta sección también proporciona información sobre los perfiles de directivas.

Jerarquía de directivas

En Kaspersky Security Center Linux, usa directivas para definir un solo conjunto de ajustes para varios dispositivos. Por ejemplo, el alcance de la directiva de la aplicación P definido para el grupo de administración G incluye los dispositivos administrados que tienen la aplicación P instalada y que se han agregado al grupo G o a cualquiera de sus subgrupos, excepto los subgrupos donde la casilla **Heredar del grupo primario** está desmarcada en las propiedades.

Una directiva se diferencia de cualquier parámetro local por los candados (🔒) que aparecen al lado de su configuración. Si una configuración (o un grupo de configuraciones) está bloqueada en las propiedades de la directiva, debe usar, en primer lugar, esta configuración (o grupo de configuraciones) al crear la configuración vigente y, en segundo lugar, debe escribir la configuración o el grupo de configuraciones en la directiva descendente.

La creación de la configuración vigente en un dispositivo se puede describir de la forma siguiente: los valores de toda la configuración que no se hayan bloqueado se toman desde la directiva, a continuación se sobrescriben con los valores de la configuración local, y luego la recolección resultante se sobrescribe con los valores de la configuración bloqueada tomada desde la directiva.

Las directivas de la misma aplicación se afectan mutuamente a través de la jerarquía de grupos de administración: la configuración bloqueada desde la directiva descendente sobrescribe la misma configuración desde la directiva descendente.

Hay una directiva especial para los usuarios fuera de la oficina. Esta directiva entra en vigor en un dispositivo cuando el dispositivo cambia al modo fuera de la oficina. Las directivas fuera de la oficina no afectan a otras directivas a través de la jerarquía de grupos de administración.

Perfiles de directivas

En muchas circunstancias, puede ser inconveniente aplicar directivas a dispositivos solo mediante la jerarquía de grupos de administración. Puede ser necesario crear varias instancias de una sola directiva que se diferencien en una o dos configuraciones para grupos de administración diferentes, y sincronizar los contenidos de esas directivas en el futuro.

Para ayudarle a prevenir tales problemas, Kaspersky Security Center Linux admite *perfiles de directivas*. Un perfil de directiva es un subconjunto nominado de los valores de configuración definidos en una directiva. Este subconjunto de valores, que se distribuye a los dispositivos de destino junto con la propia directiva, entra en vigor cuando se presenta una condición específica, llamada *condición de activación del perfil*. Los perfiles solo contienen configuraciones que se diferencian de la directiva "básica" que está activa en el dispositivo cliente (equipo o dispositivo móvil). Al activarse un perfil se modifica la configuración de directiva que se encontraba activa en el dispositivo antes de que se activara el perfil. La configuración toma los valores especificados en el perfil.

Las restricciones siguientes se imponen actualmente en los perfiles de directivas:

- Una directiva puede incluir un máximo de 100 perfiles.
- Un perfil de directivas no puede contener otros perfiles.
- Un perfil de directivas no puede contener una configuración de notificaciones.

Contenido de un perfil

Un perfil de directivas contiene las siguientes partes:

- Perfiles de nombre con nombres idénticos que se afectan mutuamente a través de la jerarquía de grupos de administración con reglas comunes.
- Subconjunto de configuración de la directiva. A diferencia de la directiva, que contiene todas las configuraciones, un perfil solo contiene configuraciones que realmente se requieren (configuraciones bloqueadas).

- La condición de activación es una expresión lógica con propiedades del dispositivo. Un perfil está activo (complementa a la directiva) solo cuando la condiciones de activación del perfil se hace verdadera. En todos los otros casos, el perfil está inactivo y es ignorado. Las propiedades del dispositivo siguientes se pueden incluir en esa expresión lógica:
  - Estado de modo fuera de la oficina.
  - Propiedades del entorno de la red; nombre de la regla activa para conexión con el Agente de red.
  - Presencia o ausencia de etiquetas específicas en el dispositivo.
  - El hecho de que el dispositivo pertenezca a una unidad de Active Directory, sea esta relación de pertenencia explícita (el dispositivo se encuentra en la unidad organizativa especificada) o implícita (el dispositivo está en una unidad organizativa que se encuentra dentro de la unidad especificada, sin importar el nivel de anidamiento).
  - Membrecía del dispositivo en un grupo de seguridad de Active Directory (explícita o implícita).
  - Membrecía del propietario del dispositivo en un grupo de seguridad de Active Directory (explícita o implícita).
- Casilla de deshabilitación del Perfil. Los perfiles deshabilitados siempre se ignoran y sus condiciones de activación respectivas no se verifican.
- Prioridad del Perfil. Las condiciones de activación de perfiles diferentes son independientes, por lo tanto varios perfiles se pueden activar simultáneamente. Si los perfiles activos contienen recolecciones no superpuestas de configuraciones, no se producirá ningún problema. Sin embargo, si dos perfiles activos contienen valores diferentes de la misma configuración, una ambigüedad ocurrirá. Esta ambigüedad se debe evitar a través de prioridades del perfil: El valor de la variable ambigua se tomará desde el perfil que tiene la prioridad más alta (el que se califica más alto en la lista de perfiles).

Comportamiento de los perfiles cuando las directivas se afectan mutuamente a través de la jerarquía

Los perfiles con el mismo nombre se fusionan según las reglas de fusión de directivas. Los perfiles de una directiva ascendente tienen una prioridad más alta que los perfiles de una directiva descendente. Si la edición de la configuración se prohíbe en la directiva ascendente (está bloqueada), la directiva descendente usa las condiciones de activación del perfil de la ascendente. Si la edición de la configuración está permitida en la directiva ascendente, las condiciones de activación del perfil desde la directiva descendente se utilizan.

Como un perfil de directivas puede contener la propiedad **El dispositivo no tiene conexión** en su condición de activación, los perfiles reemplazan completamente la función de las directivas para los usuarios fuera de la oficina, que ya no se admitirán.

Una directiva para usuarios fuera de la oficina puede contener perfiles, pero sus perfiles solo se pueden activar después de que el dispositivo cambie al modo fuera de la oficina.

Tareas

Para administrar las aplicaciones de seguridad de Kaspersky instaladas en los dispositivos a través de Kaspersky Security Center Linux, es necesario crear y ejecutar *tareas*. Las tareas son el medio que se utiliza para instalar, iniciar y detener aplicaciones, analizar archivos, actualizar bases de datos y módulos de software y realizar otras acciones en las aplicaciones.

Las tareas para una aplicación específica solo se pueden crear si el complemento de administración para esa aplicación está instalado.

Una tarea se puede ejecutar en el Servidor de administración o en un dispositivo.

Las siguientes tareas se realizan en el Servidor de administración:

- Distribución automática de informes
- Descarga de actualizaciones en el repositorio del Servidor de administración
- Copia de seguridad de los datos del Servidor de administración
- Mantenimiento de la base de datos

Los siguientes tipos de tareas se ejecutan en los dispositivos:

- *Tareas locales*. Son tareas que se ejecutan en un dispositivo específico.

  Las tareas locales pueden ser modificadas por el administrador (mediante Kaspersky Security Center Web Console) o por el usuario de un dispositivo remoto (mediante la interfaz de su aplicación de seguridad, por ejemplo). Si el administrador y el usuario del dispositivo administrado modifican una tarea local al mismo tiempo, los cambios realizados por el administrador se consideran prioritarios y son los que entran en vigor.

- *Tareas de grupo*. Son tareas que se ejecutan en todos los dispositivos de un grupo específico.

  A menos que se especifique lo contrario en las propiedades de la tarea, una tarea de grupo también afecta a todos los subgrupos del grupo seleccionado. Una tarea de grupo también afecta (opcionalmente) a los dispositivos que se han conectado a Servidores de administración secundarios y virtuales incluidos en el grupo o en cualquiera de sus subgrupos.

- *Tareas globales*. Son tareas que se ejecutan en un conjunto de dispositivos que pueden o no pertenecer a un grupo.

Para cada aplicación, puede crear cualquier número de tareas de grupo, tareas globales o tareas locales.

Puede copiar, importar, exportar y eliminar tareas, consultar el progreso de su ejecución y modificar su configuración.

Para que una tarea se inicie en un dispositivo, la aplicación para la que se la ha creado debe estar en ejecución.

Los resultados de las tareas se guardan en el registro de eventos y en el registro de eventos de Kaspersky Security Center Linux, tanto centralmente en el Servidor de administración como localmente en cada dispositivo.

No incluya datos privados en la configuración de las tareas. Por ejemplo, evite especificar la contraseña del administrador del dominio.

Reglas de movimiento de dispositivos

Recomendamos que automatice la asignación de dispositivos a grupos de administración a través de las *reglas de movimiento de dispositivos*. Una regla de movimiento de dispositivos consta de tres partes principales: nombre, condición de ejecución (expresión lógica con atributos del dispositivo) y grupo de administración de destino. Una regla mueve un dispositivo al grupo de administración de destino si los atributos del dispositivo cumplen la condición de ejecución de la regla.

Toda regla de movimiento de dispositivos tiene una prioridad. El Servidor de administración comprueba los atributos del dispositivo en cuanto a si cumplen con la condición de ejecución de cada regla, en orden ascendente de prioridad. Si los atributos del dispositivo cumplen con la condición de ejecución de una regla, el dispositivo se mueve al grupo de destino, y con esto cesa el procesamiento de la regla en este dispositivo. Si los atributos de dispositivo cumplen con las condiciones de varias reglas, el dispositivo se mueve al grupo de destino de la regla con la prioridad más alta (es decir, la que tiene la clasificación más alta en la lista de reglas).

Las reglas de movimiento de dispositivos se pueden crear implícitamente. Por ejemplo, en las propiedades de un paquete de instalación o una tarea de instalación remota, puede especificar el grupo de administración al cual el dispositivo se debe mover después de que Agente de red se instala en este. Además, las reglas de movimiento de dispositivos pueden ser creadas explícitamente por el administrador de Kaspersky Security Center Linux, en la sección **Administración de activos → Reglas de movimiento**.

La regla de movimiento predeterminada está diseñada para la asignación inicial de dispositivos a grupos de administración, que se ejecuta una sola vez. La regla mueve dispositivos desde el grupo de Dispositivos no asignados solo una vez. Si un dispositivo se movió una vez mediante esta regla, la regla no lo volverá a mover, incluso si devuelve el dispositivo al grupo de dispositivos no asignados manualmente. Este es el modo recomendado de aplicar las reglas de movimiento.

Puede mover dispositivos que ya se han asignado a algunos grupos de administración. Para hacer esto, en las propiedades de una regla, borre la casilla de verificación **Solo mover dispositivos que no pertenezcan a un grupo de administración**.

Aplicar reglas de movimiento a dispositivos que ya se han asignado a algunos grupos de administración aumenta considerablemente la carga en el Servidor de administración.

La casilla **Solo mover dispositivos que no pertenezcan a un grupo de administración** está bloqueada en las propiedades de las reglas de movimiento creadas automáticamente. Esas reglas se crean cuando agrega la tarea *Instalar la aplicación de forma remota* o crea un paquete de instalación independiente.

Puede crear una regla móvil que afectaría a un dispositivo solo repetidamente.

Recomendamos encarecidamente no mueva un solo dispositivo desde un grupo al otro repetidamente (por ejemplo, a fin de aplicar una directiva especial a ese dispositivo, ejecutar una tarea de grupo especial o actualizar el dispositivo a través de un punto de distribución específico).

Tales situaciones no se admiten, porque aumentan la carga en el Servidor de administración y el tráfico de red a un grado extremo. Estas situaciones también entran en conflicto con los principios operativos de Kaspersky Security Center Linux (en particular en el área de derechos de acceso, eventos e informes). Se debe encontrar otra solución; por ejemplo, a través del uso de perfiles de directivas, tareas para selecciones de dispositivos, asignación de Agentes de red según el escenario estándar, entre otras cosas.

Categorización del software

La herramienta principal para supervisar la ejecución de aplicaciones son las *categorías de Kaspersky* (en adelante también conocidas como *categorías KL*). Las categorías de KL ayudan a los administradores de Kaspersky Security Center Linux a simplificar la asistencia de la clasificación del software y minimizan el tráfico hacia los dispositivos administrados.

Las categorías de usuario solo se deben crear para aplicaciones que no se pueden clasificar en ninguna de las categorías KL existentes (por ejemplo, para el software personalizado). Las categorías de usuario se crean sobre la base de un paquete de instalación de la aplicación (MSI) o una carpeta con paquetes de instalación.

Si está disponible una colección grande de software que no se ha clasificado a través de categorías KL, puede ser útil crear una categoría actualizada automáticamente. Las sumas de control de archivos ejecutables automáticamente se agregarán a esta categoría en cada modificación de la carpeta que contiene paquetes de distribución.

Copia de seguridad y restauración de la configuración del Servidor de administración

La copia de seguridad de la configuración del Servidor de administración y su base de datos se realiza a través de la tarea de copia de seguridad y la utilidad klbackup. Una copia de seguridad incluye toda la configuración principal y objetos que pertenecen al Servidor de administración, por ejemplo, certificados, claves maestras para el cifrado de unidades en dispositivos administrados, claves para varias licencias, estructura de grupos de administración con todos sus contenidos, tareas, directivas, etc. Con una copia de seguridad puede recuperar la operación de un Servidor de administración cuanto antes, lo que puede demorar de una docena de minutos a un par de horas.

Si ninguna copia de seguridad está disponible, un error puede llevar a una pérdida irrevocable de certificados y toda la configuración del Servidor de administración. Esto requerirá a volver a configurar Kaspersky Security Center Linux desde el principio y volver a realizar la distribución inicial del Agente de red en la red de la organización. Todas las claves principales para el cifrado de unidades en dispositivos administrados también se perderán, arriesgando la pérdida irrevocable de datos cifrados en dispositivos con Kaspersky Endpoint Security. Por ese motivo, no debe descuidar las copias de seguridad habituales del Servidor de administración usando la tarea de copia de seguridad estándar.

El asistente de inicio rápido crea una tarea de copia de seguridad de la configuración del Servidor de administración que se inicia todos los días a las 4:00 a.m. Las copias de seguridad se guardan de forma predeterminada en la carpeta /var/opt/kaspersky/KSC_Backups*.

Como una copia de seguridad contiene datos importantes, la tarea de copia de seguridad y la utilidad klbackup aseguran la protección con contraseña de copias de seguridad. De forma predeterminada, la tarea de copia de seguridad se crea con una contraseña en blanco. Debe configurar una contraseña en las propiedades de la tarea de copia de seguridad. Descuidar este requisito causa una situación donde todas las claves de certificados del Servidor de administración, las claves para licencias y las claves principales para el cifrado de unidades en dispositivos administrados permanecen no cifradas.

Además de la copia de seguridad habitual, también debe crear una copia de seguridad antes de cada cambio significativo, incluida la instalación de actualizaciones del Servidor de administración y los parches.

Para restaurar una copia de seguridad, deberá utilizar la utilidad klbackup en una instancia del Servidor de administración que se acabe de instalar, que esté en funcionamiento y que sea de la misma versión para la que se haya creado la copia de seguridad (o de una versión más reciente).

La instancia del Servidor de Administración en la que se va a realizar la restauración debe utilizar un DBMS del mismo tipo y de la misma versión, o posteriores. La versión del Servidor de administración puede ser igual (con un parche idéntico o posterior) o posterior.

Esta sección describe situaciones estándares para restaurar la configuración y objetos del Servidor de administración.

Un dispositivo con el Servidor de administración es inoperable

Si un dispositivo con el Servidor de administración es inoperable debido a un error, se recomiendan realizar las siguientes acciones:

- El nuevo Servidor de administración debe tener asignado el mismo nombre DNS.

  Si se estableció una dirección IP estática en el paquete de instalación del Agente de red cuando se implementaron los Agentes de red, también debe asignar la misma dirección IP al nuevo Servidor de administración. También puede usar la dirección de conexión que define a qué Servidor de administración se conecta el Agente de administración (puede averiguar esta dirección en los dispositivos administrados mediante la utilidad klnagchk).

- En el archivo de configuración de IAM `var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml` , para `server_iam.ksc_address`, establezca exactamente la misma dirección del Servidor de administración que se especifica en el nombre alternativo del sujeto (SAN) del certificado del Servidor de administración aplicado anteriormente. Consulte el siguiente artículo para obtener más información: Cómo agregar la dirección del Servidor de administración a la configuración del Servidor de IAM.

- Instalar el Servidor de administración usando un DBMS del mismo tipo, de la misma versión (o una posterior). Puede instalar la misma versión del Servidor con el mismo parche (o uno posterior), o una versión posterior. Después de la instalación, no realice la instalación inicial a través del Asistente.

- Ejecute la utilidad klbackup y realice la restauración. Vuelva a instalar Web Console después de una restauración exitosa.

La configuración del Servidor de administración o la base de datos es corrupta

Si el Servidor de administración es inoperable debido a configuración o la base de datos corruptas (por ejemplo, después de una sobrecarga eléctrica), se recomienda usar la siguiente situación de restauración:

1. Analice el sistema de archivos en el dispositivo dañado.

2. Desinstale la versión inoperable del Servidor de administración.

3. Reinstale el Servidor de administración usando un DBMS del mismo tipo y de la misma versión (o una posterior). Puede instalar la misma versión del Servidor con el mismo parche (o uno posterior), o una versión posterior. Después de la instalación, no realice la instalación inicial a través del Asistente.

4. Ejecute la utilidad klbackup y realice la restauración.

Se prohíbe restaurar el Servidor de administración de cualquier modo diferente de a través de la utilidad klbackup.

Cualquier intento de restaurar el Servidor de administración a través de un software de terceros llevará inevitablemente a la desincronización de datos en los nodos de Kaspersky Security Center Linux de la aplicación distribuida y, por consiguiente, al funcionamiento inadecuado de la aplicación.

Acerca de los perfiles de conexión para los usuarios fuera de la oficina

Los usuarios de computadoras portátiles fuera de la oficina (más adelante también llamadas "dispositivos") tal vez tengan que cambiar el método de conexión a un Servidor de administración o entre Servidores de administración, según la ubicación actual del dispositivo en la red de la empresa.

Utilización de direcciones diferentes de un Servidor de administración solo

Los dispositivos con Agente de red instalado pueden conectarse al Servidor de administración desde la red interna de la organización o desde Internet. Esta situación puede requerir que el Agente de red use direcciones diferentes para la conexión con el Servidor de administración: dirección externa del Servidor de administración para conexión a Internet y dirección interna del Servidor de administración para la conexión a la red interna.

Para hacer esto, debe agregar un perfil (para la conexión con el Servidor de administración desde Internet) a la directiva del Agente de red. Añada el perfil en las propiedades de la directiva (sección **Conectividad**, subsección **Perfiles de conexión**). En la ventana de creación de perfil, debe deshabilitar la opción **Usar para recibir actualizaciones solamente** y seleccionar la opción **Sincronizar configuración de conexión con la configuración del Servidor de administración especificada en este perfil**. Si usa una puerta de enlace de conexión para acceder al Servidor de administración (por ejemplo, en una configuración de Kaspersky Security Center Linux como la que se describe en Acceso a Internet: Agente de red como puerta de enlace de conexión en una DMZ), debe especificar la dirección de la puerta de enlace de conexión en el campo correspondiente del perfil de conexión.

Conmutación entre Servidores de administración según la red actual

Si la organización tiene varias oficinas con Servidores de administración diferentes y algunos dispositivos con Agentes de red instalados se transfieren entre ellos, necesita un Agente de red para conectarse al Servidor de administración de la red local en la oficina donde el dispositivo se localiza actualmente.

En este caso, debe crear un perfil para la conexión con el Servidor de administración en las propiedades de la directiva del Agente de red para cada una de las oficinas, excepto la oficina local donde el Servidor de administración doméstico se encuentra localizado. Debe especificar las direcciones de los Servidores de administración en perfiles de conexión y habilitar o deshabilitar la opción **Usar para recibir actualizaciones solamente**:

- Habilite la opción si necesita que el Agente de red se sincronice con el Servidor de administración doméstico mientras usa el Servidor local para descargar actualizaciones únicamente.
- Deshabilite la opción si es necesario para que el Agente de red sea administrado completamente por el Servidor de administración local.

Después de esto, debe configurar las condiciones de conmutación para los perfiles recién creados: al menos una condición para cada una de las oficinas, excepto la oficina local. El propósito de cada condición consiste en la detección de elementos que son específicos para el entorno de la red de una oficina. Si una condición es verdadera, el perfil correspondiente se activa. Si ninguna de las condiciones es verdadera, el Agente de red cambia al Servidor de administración doméstico.

Acerca de cambiar el Agente de red a otros Servidores de administración

Kaspersky Security Center Linux ofrece la opción de cambiar el Agente de red de un dispositivo cliente a otros Servidores de administración si se modificaron las siguientes opciones de configuración de red:

- **Condición para la dirección del servidor DHCP**: La dirección IP del servidor del Protocolo de configuración dinámica de host (DHCP) de la red ha cambiado.

  El ajuste **Condición para la dirección del servidor DHCP** no está disponible actualmente.

- **Condición para dirección predeterminada de la puerta de enlace de conexión**: la dirección de la puerta de enlace principal de la red ha cambiado.
- **Condición para dominio DNS**: cambió el sufijo DNS de la subred.
- **Condición para la dirección del servidor DNS**: cambió la dirección IP del servidor DNS de la red.
- **Condición para la dirección del servidor WINS**: cambió la dirección IP del servidor WINS de la red. Este parámetro solo está disponible para dispositivos con Windows.
- **Condición para la resolución de nombres**: el nombre DNS o NetBIOS del dispositivo cliente cambió.
- **Condición para subred**: la máscara y la dirección de subred cambiaron.

- **Condición para la accesibilidad del dominio de Windows**: el estado del dominio de Windows al cual está conectado el dispositivo cliente cambió. Este parámetro solo está disponible para dispositivos con Windows.

- **Condición para la accesibilidad de la dirección de conexión SSL**: el dispositivo cliente puede o no puede (según la opción que seleccione) establecer una conexión SSL con un Servidor específico (nombre: puerto). Para la conexión, use un servidor dedicado con software capaz de soportar una carga elevada y solicitudes frecuentes procedentes del Agente de administración. No especifique el puerto del Servidor de administración. Para cada servidor, además puede especificar un certificado SSL. En este caso, el Agente de red verifica el certificado del servidor además de verificar la capacidad de una conexión SSL. Si el certificado no coincide, la conexión genera un error.

La configuración inicial de la conexión del Agente de red al Servidor de administración se define durante la instalación del Agente de red. Posteriormente, si se han creado reglas para cambiar el Agente de red a otros Servidores de administración, el Agente de red responde a los cambios en la configuración de red del siguiente modo:

- Si la configuración de la red cumple con una de las reglas creadas, el Agente de red se conecta con el Servidor de administración especificado en esta regla. Las aplicaciones instaladas en dispositivos cliente cambian a directivas fuera de la oficina siempre que este comportamiento esté habilitado por una regla.

- Si no se aplica ninguna de las reglas, el Agente de red revertirá a la configuración predeterminada de la conexión con el Servidor de administración especificado durante la instalación. Las aplicaciones instaladas en dispositivos cliente vuelven a las directivas activas.

- Si el Servidor de administración no es accesible, el Agente de red utilizará las directivas fuera de la oficina.

Para que el Agente de red pase a utilizar una directiva fuera de la oficina, es necesario que la opción **Habilitar el modo de fuera de la oficina cuando el Servidor de administración no esté disponible** esté habilitada en la directiva del Agente de red.

La configuración de la conexión del Agente de red al Servidor de administración se guarda en un perfil de conexión. En el perfil de conexión puede crear reglas para cambiar dispositivos cliente a directivas fuera de la oficina además de configurar el perfil para que pueda utilizarse solo para descargar actualizaciones.

Creación de un perfil de conexión para usuarios fuera de la oficina

Para crear un perfil para la conexión del Agente de red con el Servidor de administración para usuarios fuera de la oficina, haga lo siguiente:

1. Si desea crear un perfil de conexión para un grupo de dispositivos administrados, abra la directiva del Agente de red correspondiente al grupo en cuestión. Para ello, realice las siguientes acciones:

   a. En el menú principal, vaya a **Administración de activos** → **Directivas**.

   b. Seleccione el grupo de administración relacionado con la creación del perfil de conexión:

      - Para el grupo raíz, puede continuar con el siguiente paso.

      - Para un subgrupo, haga clic en el botón **Mostrar jerarquía** en la parte superior de la página y, luego, en la ventana que se abre, haga clic en el nombre del subgrupo requerido.

Verá la ruta al grupo seleccionado en la parte superior de la página. Si es necesario, puede hacer clic en un vínculo con el nombre del grupo de administración para ir al grupo. De forma predeterminada, el último vínculo de la ruta se encuentra inactivo. Además, puede cerrar la ventana de jerarquía si hace clic en el botón **Ocultar jerarquía**.

c. Agregue la directiva del Agente de red para el grupo de dispositivos administrados. Si esa directiva ya existe, haga clic en el nombre de la misma para abrir sus propiedades.

2. Si desea crear un perfil de conexión para un dispositivo administrado específico, haga lo siguiente:

a. En el menú principal, vaya a **Administración de activos** → **Dispositivos administrados**.

b. Haga clic en el nombre del dispositivo administrado.

c. En la ventana que se abre, que contendrá las propiedades del dispositivo administrado, vaya a la pestaña **Aplicaciones**.

d. Haga clic en el nombre de la directiva del Agente de red a la que solo aplique el dispositivo administrado seleccionado.

3. En la ventana de propiedades que se abre, vaya a **Configuración de la aplicación** → **Conectividad** → **Perfiles de conexión.**

4. En la sección **Perfiles de conexión al Servidor de administración** haga clic en el botón **Agregar**.

De forma predeterminada, la lista de perfiles de conexión contiene los perfiles <Modo sin conexión> y <Servidor de administración doméstico>. Los perfiles no pueden ser modificados o eliminados.

El perfil <Modo sin conexión> no especifica ningún Servidor para la conexión. Por lo tanto, el Agente de red, cuando se cambia a ese perfil, no intenta conectarse a ningún Servidor de administración mientras las aplicaciones instaladas en los dispositivos cliente se ejecutan bajo directivas fuera de la oficina. El perfil <Modo sin conexión> puede ser utilizado si los dispositivos están desconectados de la red.

El perfil <Servidor de administración doméstico> se utiliza para establecer conexión con el Servidor de administración seleccionado durante la instalación del Agente de red. El perfil <Servidor de administración doméstico> se aplica cuando un dispositivo se conecta de nuevo al Servidor de administración doméstico después de haberse ejecutado en una red externa durante algún tiempo.

5. En la ventana **Perfil de configuración** que se abre, configure el perfil de conexión:

- **Nombre del perfil**

  En el campo de entrada, puede ver o modificar el nombre del perfil de conexión.

- **Dirección del Servidor de administración**

  La dirección del Servidor de administración a la que debe conectarse el dispositivo cliente al activarse el perfil.

- **Número de puerto**

  Número de puerto que se utilizará para la conexión.

- **Puerto SSL**

  Número de puerto para la conexión si se utiliza el protocolo SSL.

- **Usar conexión SSL**

  Si se habilita esta opción, la conexión se establece a través un puerto seguro mediante el protocolo SSL.

Esta opción está activada de forma predeterminada. Recomendamos no deshabilitar esta opción; de lo contrario, la conexión quedará desprotegida.

- Seleccione la opción **Usar servidor proxy** si desea usar un servidor proxy al conectarse a Internet. Si selecciona esta opción, se habilitarán campos para que configure los ajustes pertinentes. Deberá introducir los siguientes valores de conexión del servidor proxy:

  - **Dirección**

    Dirección del servidor proxy usado para conectar Kaspersky Security Center Linux a Internet.

  - **Número de puerto**

    Número del puerto a través del cual se establecerá la conexión proxy de Kaspersky Security Center Linux.

  - **Autenticación del servidor proxy**

    Si se selecciona esta casilla, en los campos de entrada se podrán especificar las credenciales para la autenticación del servidor proxy.

  - **Nombre de usuario**

    Cuenta de usuario con la que se establece la conexión al servidor proxy (este campo está disponible si se selecciona la casilla **Autenticación del servidor proxy**).

  - **Contraseña**

    Contraseña que especifica el usuario con cuya cuenta se establece la conexión al servidor proxy (este campo está disponible si se selecciona la casilla **Autenticación del servidor proxy**).

    Para ver la contraseña indicada, mantenga presionado el botón **Mostrar** durante la cantidad de tiempo que sea necesario.

- **Dirección de la puerta de enlace de conexión**

  La dirección de la puerta de enlace a través de la cual los dispositivos cliente se conectan al Servidor de administración.

- **Habilitar el modo de fuera de la oficina cuando el Servidor de administración no esté disponible**

  Marque esta casilla para permitir que las aplicaciones instaladas en un dispositivo cliente usen perfiles de directiva para dispositivos en modo fuera de la oficina, así como directivas para fuera de la oficina, en cualquier intento de conexión si el Servidor de administración no está disponible. Si no hay una directiva fuera de la oficina definida para la aplicación, se utilizará la directiva activa.

  Si se deshabilita esta opción, las aplicaciones utilizarán directivas activas.

  Esta casilla está desactivada por defecto.

- **Usar para recibir actualizaciones solamente**

  Si se habilita esta opción, el perfil se utilizará solamente para que las aplicaciones instaladas en el dispositivo cliente descarguen actualizaciones. Para otras operaciones, la conexión al Servidor de administración será establecida con los parámetros de conexión iniciales definidos durante la instalación del Agente de red.

  Esta opción está activada de forma predeterminada.

- **Sincronizar configuración de conexión con la configuración del Servidor de administración especificada en este perfil**

  Si se habilita esta opción, el Agente de red se conectará al Servidor de administración usando la configuración especificada en las propiedades del perfil.

  Si se deshabilita esta opción, el Agente de red se conectará al Servidor de administración usando la configuración original especificada durante la instalación.

  Esta opción estará disponible si la opción **Usar para recibir actualizaciones solamente** se encuentra deshabilitada.

  Esta opción está deshabilitada de forma predeterminada.

Se creará un perfil para la conexión del Agente de red con el Servidor de administración para usuarios fuera de la oficina. Cuando el Agente de red se conecte al Servidor de administración con el nuevo perfil, las aplicaciones instaladas en el dispositivo cliente quedarán sujetas a directivas para dispositivos en modo fuera de la oficina o directivas para fuera de la oficina.

Acceso remoto a dispositivos administrados

Esta sección proporciona información sobre el acceso remoto a dispositivos administrados.

Uso de la opción "No desconectarse del Servidor de administración" para proporcionar conectividad continua entre un dispositivo administrado y el Servidor de administración

Si no usa servidores push, Kaspersky Security Center Linux no proporciona conectividad continua entre los dispositivos administrados y el Servidor de administración. Los Agentes de red en los dispositivos administrados periódicamente establecen conexiones y se sincronizan con el Servidor de administración. El intervalo entre esas sesiones de sincronización se define en una directiva del Agente de red. Si se requiere una sincronización temprana, el Servidor de administración (o un punto de distribución, si está en uso) envía un paquete de red firmado a través de una red IPv4 o IPv6 al puerto UDP del Agente de red. El puerto por defecto es el 15000. Si ninguna conexión a través de UDP es posible entre el Servidor de administración y un dispositivo administrado, la sincronización se ejecutará en la siguiente conexión regular del Agente de red al Servidor de administración dentro del intervalo de sincronización.

Algunas operaciones no se pueden realizar sin una conexión temprana entre el Agente de red y el Servidor de administración, como ejecutar y detener tareas locales, o recibir estadísticas para una aplicación administrada. Para resolver este problema, si no utiliza servidores push, puede usar la opción **No desconectar del Servidor de administración** para garantizar conectividad continua entre el dispositivo administrado y el Servidor de administración.

Para proporcionar conexión continua entre un dispositivo administrado y el Servidor de administración:

1. En el menú principal, vaya a **Administración de activos → Dispositivos administrados**.

   Se muestra la lista de dispositivos administrados.

2. En la lista de dispositivos administrados, haga clic en el vínculo con el nombre del dispositivo de su interés.

3. En la ventana de propiedades del dispositivo, en la sección **General**, active la opción **No desconectar del Servidor de administración**.

Hay una conexión continua establecida entre el dispositivo administrado y el Servidor de administración.

El número total máximo de dispositivos con la opción **No desconectar del Servidor de administración** seleccionada es 300.

Acerca de la comprobación de la hora de conexión entre un dispositivo y el Servidor de administración

Cuando se apaga un dispositivo, el Agente de red notifica el Servidor de administración de este evento. En Kaspersky Security Center Web Console, ese dispositivo se muestra como apagado. Sin embargo, el Agente de red no puede notificar el Servidor de administración de todos los eventos de este tipo. Por lo tanto, el Servidor de Administración analiza periódicamente el atributo **Conectado al Servidor de administración** (el valor de este atributo se muestra en Kaspersky Security Center Web Console, en las propiedades del dispositivo, en la sección **General**) para cada dispositivo y lo compara con el intervalo de sincronización de la configuración actual del Agente de red. Si un dispositivo no ha respondido durante más de tres intervalos de sincronización sucesivos, ese dispositivo se marca como apagado.

Acerca de la sincronización forzada

Aunque Kaspersky Security Center Linux sincroniza automáticamente el estado, la configuración, las tareas y las directivas de dispositivos administrados, en algunos casos el administrador tiene que saber si la sincronización ya se realizó para un dispositivo especificado en un momento en particular.

La ventana de propiedades de un dispositivo administrado contiene el botón **Forzar sincronización**. Cuando Kaspersky Security Center Linux ejecuta el comando de sincronización, el Servidor de administración intenta conectarse con el dispositivo. Si la conexión se establece, se realiza una sincronización forzada en ese momento. Si la comunicación no puede establecerse, la sincronización forzada se pospone hasta la siguiente conexión programada entre el Agente de red y el Servidor de administración.

Guía de dimensionamiento

Esta sección proporciona información sobre el dimensionamiento de Kaspersky Security Center Linux.

Acerca de esta Guía

La Guía de dimensionamiento de Kaspersky Security Center Linux (también denominada "Kaspersky Security Center") está orientada a los profesionales que instalan y administran Kaspersky Security Center, así como también a aquellos que brindan Servicio de soporte técnico a las organizaciones que usan Kaspersky Security Center.

Todas las recomendaciones y evaluaciones se dan para las redes en las que Kaspersky Security Center administra la protección de dispositivos que tengan instalado el software de Kaspersky.

Para obtener y mantener un rendimiento óptimo en diferentes condiciones operativas, debe tener en cuenta la cantidad de dispositivos en red, la topología de red y el conjunto de funciones de Kaspersky Security Center que necesita.

Esta Guía proporciona la siguiente información:

- Limitaciones de Kaspersky Security Center
- Evaluaciones para los nodos clave de Kaspersky Security Center (Servidores de administración y puntos de distribución):
    - Requisitos de hardware para Servidores de administración y puntos de distribución
    - Evaluación del número y la jerarquía de los Servidores de administración
    - Cálculo del número y la configuración de los puntos de distribución
- Configuración del registro de eventos en la base de datos según el número de dispositivos en red
- Prácticas recomendadas habituales para la optimización del Prácticas recomendadas comunes para optimizar el rendimiento
- Configuración de tareas específicas destinadas a un rendimiento óptimo de Kaspersky Security Center
- Tasa de tráfico (carga de red) entre el Servidor de administración de Kaspersky Security Center y cada dispositivo protegido

Se recomienda consultar esta guía en los siguientes casos:

- Al planear recursos antes de la instalación de Kaspersky Security Center
- Al planear cambios significativos en la escala de la red en la que se implementa Kaspersky Security Center
- Al dejar de utilizar Kaspersky Security Center dentro de un segmento de red limitado (un entorno de prueba) y cambiar al despliegue en gran escala de Kaspersky Security Center en la red corporativa
- Al realizar cambios en el conjunto de funciones de Kaspersky Security Center utilizadas

Limitaciones de Kaspersky Security Center Linux

La tabla siguiente muestra las limitaciones de la versión actual de Kaspersky Security Center Linux.

Limitaciones de Kaspersky Security Center Linux

Tipo de limitación	Valor
Número máximo de dispositivos administrados por Servidor de administración	50000
Número máximo de dispositivos con la opción **No desconectar del Servidor de administración** seleccionada	300
Número máximo de grupos de administración	10000
Número máximo de eventos para almacenar	45 000 000
Número máximo de directivas	2000
Número máximo de tareas	2000
Número máximo de perfiles en una directiva	100
Número máximo de Servidores de administración secundarios en un solo Servidor de administración principal	500
Número máximo de Servidores de administración virtual	500
Número máximo de dispositivos que puede atender un punto de distribución	10000
Número máximo de dispositivos que pueden usar una única puerta de enlace de conexión	10 000, incluidos los dispositivos móviles
Número máximo de dispositivos móviles por Servidor de administración	100 000 menos el número de dispositivos administrados inmóviles

Evaluaciones para Servidores de administración

Esta sección proporciona los requisitos de software y hardware para los dispositivos utilizados como Servidores de administración. También se proporcionan recomendaciones para calcular el número y la jerarquía de los Servidores de administración según la configuración de la red de la organización.

Recomendamos que, después de instalar el Servidor de administración y el DBMS en los dispositivos, instale Kaspersky Endpoint Security for Linux en esos dispositivos. Para conocer los requisitos de hardware de Kaspersky Endpoint Security, consulte la Ayuda de Kaspersky Endpoint Security for Linux.

La carga creada por Kaspersky Endpoint Security for Linux cuando se integra con Managed Detection and Response y Kaspersky Endpoint Detection and Response Expert (local) no se tiene en cuenta en los cálculos para la instalación simultánea de Kaspersky Security Center Linux y KES_LIN>.

Evaluación de recursos del hardware para el Servidor de administración

Esta sección contiene evaluaciones que proporcionan una guía para planificar recursos de hardware para el Servidor de administración.

Requisitos de hardware para DBMS y el Servidor de administración

Las siguientes tablas proporcionan información sobre los requisitos de hardware mínimos (obtenidos durante pruebas) para DBMS y el Servidor de administración. Para ver una lista completa de los sistemas operativos y de los DBMS admitidos, consulte la lista de requisitos de hardware y software.

Debe habilitar el archivo de intercambio en el dispositivo con el Servidor de administración instalado. El tamaño mínimo del archivo de intercambio debe ser 1.5 veces mayor que el volumen de RAM.

Después de instalar el Servidor de administración y el DBMS en un dispositivo, recomendamos instalar Kaspersky Endpoint Security for Linux.
Para la instalación simultánea, debe tener un mínimo de 300 IOPS, así como agregar 1,5 GB de RAM y un 15 % de CPU a los requisitos del Servidor de administración.
Para conocer los requisitos de hardware de Kaspersky Endpoint Security, consulte la Ayuda de Kaspersky Endpoint Security for Linux.

Para obtener información sobre la configuración de seguridad necesaria para trabajar con Kaspersky Security Center Linux, consulte la Ayuda de Kaspersky Endpoint Security for Linux.

La red incluye 50,000 dispositivos

Configuración del dispositivo con el Servidor de administración instalado

Hardware	Valor
CPU	8 núcleos (se recomiendan 12 núcleos), 2500 MHz
RAM	16 GB
Espacio en disco	300 GB, 150 IOPS o más

Configuración del dispositivo con PostgreSQL DBMS instalado

Hardware	Valor
CPU	16 núcleos, 2500 MHz
RAM	32 GB
Espacio en disco	300 GB, 150 IOPS o más

Configuración de nodos para un clúster de conmutación por error

Hardware	Valor
CPU	8 núcleos (se recomiendan 12 núcleos), 2500 MHz
RAM	16 GB
Espacio en disco	300 GB, 150 IOPS o más
Controlador de interfaz de red	1 Gbps

Configuración del dispositivo que tiene instalados el Servidor de administración y el DBMS.

Hardware	Valor
CPU	24 núcleos (se recomiendan 28 núcleos), 2500 MHz
RAM	48 GB
Espacio en disco	600 GB, 300 IOPS o más

La red incluye 30,000 dispositivos

Configuración del dispositivo con el Servidor de administración instalado

Hardware	Valor
CPU	6 núcleos (se recomiendan 8 núcleos), 2500 MHz
RAM	12 GB
Espacio en disco	200 GB, 150 IOPS o más

Configuración del dispositivo con PostgreSQL DBMS instalado

Hardware	Valor
CPU	12 núcleos, 2500 MHz
RAM	22 GB
Espacio en disco	250 GB, 150 IOPS o más

Configuración de nodos para un clúster de conmutación por error

Hardware	Valor
CPU	6 núcleos (se recomiendan 8 núcleos), 2500 MHz
RAM	12 GB
Espacio en disco	200 GB, 150 IOPS o más
Controlador de interfaz de red	1 Gbps

Configuración del dispositivo que tiene instalados el Servidor de administración y el DBMS.

Hardware	Valor
CPU	16 núcleos (se recomiendan 20 núcleos), 2500 MHz
RAM	34 GB
Espacio en disco	450 GB, 300 IOPS o más

La red incluye 10,000 dispositivos

Configuración del dispositivo con el Servidor de administración instalado

Hardware	Valor
CPU	4 núcleos (se recomiendan 6 núcleos), 2500 MHz
RAM	8 GB
Espacio en disco	100 GB, 150 IOPS o más

Configuración del dispositivo con PostgreSQL DBMS instalado

Hardware	Valor
CPU	6 núcleos, 2500 MHz
RAM	10 GB
Espacio en disco	200 GB, 150 IOPS o más

Configuración de nodos para un clúster de conmutación por error

Hardware	Valor
CPU	4 núcleos (se recomiendan 6 núcleos), 2500 MHz
RAM	8 GB
Espacio en disco	100 GB, 150 IOPS o más
Controlador de interfaz de red	1 Gbps

Configuración del dispositivo que tiene instalados el Servidor de administración y el DBMS.

Hardware	Valor
CPU	8 núcleos (se recomiendan 14 núcleos), 2500 MHz
RAM	18 GB
Espacio en disco	300 GB, 300 IOPS o más

La red incluye 1000 dispositivos

Configuración del dispositivo con el Servidor de administración instalado

Hardware	Valor
CPU	2 núcleos, 2500 MHz
RAM	6 GB
Espacio en disco	10 GB, 150 IOPS o más

Configuración del dispositivo con PostgreSQL DBMS instalado

Hardware	Valor
CPU	2 núcleos, 2500 MHz
RAM	4 GB
Espacio en disco	20 GB, 150 IOPS o más

Configuración de nodos para un clúster de conmutación por error

Hardware	Valor
CPU	2 núcleos, 2500 MHz
RAM	6 GB
Espacio en disco	10 GB, 150 IOPS o más
Controlador de interfaz de red	1 Gbps

Configuración del dispositivo que tiene instalados el Servidor de administración y el DBMS.

Hardware	Valor
CPU	4 núcleos, 2500 MHz
RAM	10 GB
Espacio en disco	30 GB, 300 IOPS o más

Las pruebas se ejecutaron con la configuración siguiente:

- La asignación automática de puntos de distribución está habilitada en el Servidor de administración, o los puntos de distribución se asignan manualmente de acuerdo con la tabla recomendada.
- PostgreSQL DBMS no incluye extensiones distintas de plpgsql.

En el dispositivo que tiene DBMS instalado, la base de datos consume aproximadamente 100 GB de espacio en disco y el registro de transacciones consume aproximadamente 200 GB de espacio en disco.

Evaluación de espacio de la base de datos

La fórmula siguiente permite calcular de manera aproximada la cantidad de espacio que debe reservarse en la base de datos:

(600 * C + 2.3 * E + 2.5 * A + 1.2 * N * F), KB

donde:

- C es el número de dispositivos

  > Si los dispositivos administrados incluyen máquinas virtuales dinámicas, C es la suma del número de dispositivos administrados no dinámicos y el número de máquinas virtuales dinámicas con el Agente de red creadas entre dos ejecuciones consecutivas de la tarea **Mantenimiento del Servidor de administración**.

- E es el número de eventos que se almacenan
- A es el número total de objetos de Active Directory:
  - Cuentas del dispositivo
  - Cuentas de usuario
  - Cuentas de grupos de seguridad
  - Unidades de organización de Active Directory

  Si el análisis de Active Directory se encuentra deshabilitado, A se considera igual a cero.
- N es la cantidad promedio de archivos ejecutables que se incluyen en el inventario de un dispositivo de endpoint.
- F es el número de dispositivos de endpoint, donde se incluye en el inventario de los archivos ejecutables.

Si planea habilitar (en la configuración de la directiva de Kaspersky Endpoint Security) la notificación del Servidor de administración en las aplicaciones que ejecuta, necesitará gigabytes adicionales (0.03 * C) para almacenar en la base de datos la información sobre las aplicaciones que ejecuta.

Durante el funcionamiento, siempre aparece un cierto *espacio no asignado* en la base de datos. Por lo tanto, el tamaño real del archivo de base de datos suele ser aproximadamente el doble de la cantidad de espacio ocupado en la base de datos.

No se recomienda limitar explícitamente el tamaño del registro de transacciones. Se recomienda dejar el valor predeterminado del parámetro MAXSIZE.

Evaluación de espacio en el disco

El espacio en disco del Servidor de administración que se necesitará para la carpeta /var/opt/kaspersky/klnagent_srv/ se puede calcular con la siguiente fórmula:

(724 * C + 0.15 * E + 0.17 * A), KB

donde:

- C es el número de dispositivos

  > Si los dispositivos administrados incluyen máquinas virtuales dinámicas, C es la suma del número de dispositivos administrados no dinámicos y el número de máquinas virtuales dinámicas con el Agente de red creadas entre dos ejecuciones consecutivas de la tarea **Mantenimiento del Servidor de administración**.

- E es el número de eventos que se almacenan
- A es el número total de objetos de Active Directory:
  - Cuentas del dispositivo
  - Cuentas de usuario
  - Cuentas de grupos de seguridad
  - Unidades de organización de Active Directory

Si el análisis de Active Directory se encuentra deshabilitado, A se considera igual a cero.

Evaluación del número y configuración de Servidores de administración

Para reducir la carga en el Servidor de administración principal, puede asignar un Servidor de administración separado a cada grupo de administración. El número de Servidores de administración secundarios no puede exceder 500 para un mismo Servidor de administración principal.

Recomendamos que cree la configuración de Servidores de administración en correspondencia con la configuración de la red de su organización.

Recomendaciones para conectar máquinas virtuales dinámicas a Kaspersky Security Center

Las máquinas virtuales dinámicas (también conocidas como VM dinámicas) consumen más recursos que las máquinas virtuales estáticas.

Para obtener más información sobre las máquinas virtuales dinámicas, consulte Compatibilidad para máquinas virtuales dinámicas.

Cuando se conecta una nueva VM dinámica, Kaspersky Security Center Linux crea un registro para esa VM dinámica en Kaspersky Security Center Web Console y mueve la VM dinámica al grupo de administración. Tras ello, la VM dinámica se agrega a la base de datos del Servidor de administración. El Servidor de administración se sincroniza totalmente con el Agente de red instalado en esta VM dinámica.

En la red de una organización, el Agente de red crea las siguientes listas de red para cada VM dinámica:

- Hardware
- Software instalado
- Vulnerabilidades detectadas
- Eventos y listas de archivos ejecutables del componente Control de aplicaciones

El Agente de red transfiere estas listas de red al Servidor de administración. El tamaño de las listas de red depende de los componentes instalados en la VM dinámica y puede afectar el rendimiento de Kaspersky Security Center Linux y del sistema de administración de bases de datos (DBMS). Tenga en cuenta que la carga puede crecer en forma no lineal.

Una vez que el usuario termina de utilizar y apaga la VM dinámica, la máquina se elimina de la infraestructura virtual y las entradas sobre la VM se eliminan de la base de datos del Servidor de administración.

Todas estas acciones consumen una gran cantidad de recursos de Kaspersky Security Center Linux y de la base de datos del Servidor de administración y pueden, por ende, tener un impacto en el rendimiento de Kaspersky Security Center Linux y del DBMS. No recomendamos conectar más de 20 000 VM dinámicas a Kaspersky Security Center Linux.

Puede conectar más de 20 000 VM dinámicas a Kaspersky Security Center Linux si estas realizan operaciones estándar (por ejemplo, actualizaciones de bases de datos) y consumen, como máximo, un 80 % de la memoria disponible y entre un 75 % y un 80 % de los núcleos disponibles.

> El consumo de recursos puede aumentar o disminuir cuando se realizan cambios en la configuración de una directiva, en el software o en el sistema operativo de una VM dinámica. Lo ideal es que se consuma entre un 80 % y un 95 % de los recursos.

Cálculos para puntos de distribución y puertas de enlace de conexión

Esta sección proporciona los requisitos de hardware para dispositivos utilizados como puntos de distribución junto con recomendaciones para calcular el número de puntos de distribución y puertas de enlace de conexión, según la configuración de la red corporativa.

Requisitos para un punto de distribución

En este artículo, se describen los requisitos de hardware y software para puntos de distribución basados en Windows y Linux.

Si hay tareas de instalación remota pendientes en el Servidor de administración, el dispositivo que actúa como punto de distribución también debe tener espacio libre suficiente para albergar el tamaño total de los paquetes de instalación que se instalarán.

Si hay una o más instancias de la tarea de instalación de actualizaciones (parches) y reparación de vulnerabilidades pendientes en el Servidor de administración, el dispositivo designado como punto de distribución también debe contar con una cantidad de espacio libre equivalente al doble del tamaño total de todos los parches que se instalarán.

Si utiliza el esquema donde los puntos de distribución reciben las actualizaciones de las bases de datos y los módulos de software de la aplicación directamente de los servidores de actualizaciones de Kaspersky, los puntos de distribución deben estar conectados a Internet.

> No se recomienda asignar el Servidor de Administración como punto de distribución, ya que esto aumentará la carga sobre el Servidor de Administración.

Requisitos de hardware para puntos de distribución basados en Windows

Requisitos mínimos de hardware para puntos de distribución basados en Windows

Número de dispositivos cliente	CPU	RAM	RAM, con administración de parches habilitada	Espacio en disco
10000	4 núcleos, 2500 MHz	8 GB	8 GB	120 GB
5000	4 núcleos, 2500 MHz	6 GB	8 GB	120 GB
1000	2 núcleos, 2500 MHz	4 GB	8 GB	120 GB

Requisitos de hardware para puntos de distribución basados en Linux

Requisitos mínimos de hardware para puntos de distribución basados en Linux

Número de dispositivos cliente	CPU	RAM	Espacio en disco
10000	4 núcleos, 2500 MHz	10 GB	120 GB
5000	4 núcleos, 2500 MHz	8 GB	120 GB
1000	2 núcleos, 2500 MHz	6 GB	120 GB

Cálculo de la cantidad de puntos de distribución y su configuración

Cuantos más dispositivos cliente contiene una red, más puntos de distribución se requieren. Le recomendamos que no deshabilite la asignación automática de puntos de distribución. Cuando se habilita la asignación automática de puntos de distribución, el Servidor de administración asigna puntos de distribución si el número de dispositivos cliente es bastante grande y define su configuración.

La utilización de puntos de distribución exclusivamente asignados

Si planea usar ciertos dispositivos específicos como puntos de distribución (es decir, servidores asignados exclusivamente), puede optar por no usar la asignación automática de puntos de distribución. En este caso, compruebe que los dispositivos a los que planea hacer puntos de distribución tengan el volumen suficiente de espacio libre en disco, que no se apaguen con frecuencia y que tengan el modo de suspensión desactivado.

Número de puntos de distribución dedicados en una red con un solo segmento de red, según el número de dispositivos de la red

Número de dispositivos cliente por segmento de red	Número de puntos de distribución
Menos de 300	0 (no corresponde utilizar puntos de distribución)
Más de 300	Aceptable: (N / 10 000 + 1), recomendado: (N / 5000 + 2), donde N es el número de dispositivos conectados a la red

Número de puntos de distribución dedicados en una red con varios segmentos de red, según el número de dispositivos de la red

Número de dispositivos cliente en cada segmento de red	Número de puntos de distribución
Menos de 10	0 (no corresponde utilizar puntos de distribución)
10–100	1
Más de 100	Aceptable: (N / 10 000 + 1), recomendado: (N / 5000 + 2), donde N es el número de dispositivos conectados a la red

Uso de dispositivos cliente estándar (estaciones de trabajo) como puntos de distribución

Si planea usar dispositivos cliente estándar (es decir, estaciones de trabajo) como puntos de distribución, le recomendamos que siga los lineamientos de las siguientes tablas. Al designar los puntos de distribución según estas recomendaciones, evitará las sobrecargas en los canales de comunicación y en el Servidor de administración.

Número de estaciones de trabajo designadas como puntos de distribución en una red que contiene un único segmento de red, en función del número de dispositivos en red

Número de dispositivos cliente por segmento de red	Número de puntos de distribución
Menos de 300	0 (no corresponde utilizar puntos de distribución)
Más de 300	(N / 300 + 1), donde N es el número de dispositivos en red; debe haber al menos 3 puntos de distribución

Número de estaciones de trabajo designadas como puntos de distribución en una red que contiene múltiples segmentos de red, en función del número de dispositivos en red

Número de dispositivos cliente en cada segmento de red	Número de puntos de distribución
Menos de 10	0 (no corresponde utilizar puntos de distribución)
10–30	1
31–300	2
Más de 300	(N / 300 + 1), donde N es el número de dispositivos en red; debe haber al menos 3 puntos de distribución

Cuando un punto de distribución se encuentra apagado o no está disponible por algún motivo, los dispositivos administrados en su alcance pueden obtener actualizaciones del Servidor de administración.

Evaluación del número de pasarelas de conexión

Si planea usar una puerta de enlace de conexión, le recomendamos que designe un dispositivo especial para esta función.

Una puerta de enlace de conexión puede cubrir un máximo de 10 000 dispositivos administrados.

Registro de información sobre eventos para tareas y directivas

Esta sección proporciona evaluaciones asociadas con el almacenamiento de eventos en la base de datos del Servidor de administración y ofrece recomendaciones sobre cómo minimizar el número de eventos, reduciendo así la carga en el Servidor de administración.

De forma predeterminada, en las propiedades de cada tarea y directiva se especifica que todos los eventos asociados con la ejecución de la tarea y la aplicación de la directiva se almacenen en el registro.

Sin embargo, si una tarea se ejecuta con bastante frecuencia (por ejemplo, más de una vez por semana) y en un número bastante grande de dispositivos (por ejemplo, más de 10 000), el número de eventos puede ser demasiado grande y los eventos puede inundar la base de datos. En este caso, se recomienda seleccionar una de dos opciones en la configuración de la tarea:

- **Guardar eventos relacionados con el progreso de la tarea**. En este caso, la base de datos solo recibe información sobre el inicio, el progreso y la finalización de la tarea (satisfactoria, con una advertencia o error) de cada dispositivo en el que se ejecuta.

- **Guardar solo los resultados de la ejecución de la tarea**. En este caso, la base de datos recibe solo información sobre la finalización de la tarea (satisfactoria, con una advertencia o error) de cada dispositivo en el que se ejecuta la tarea.

Si se ha definido una directiva para un número bastante grande de dispositivos (por ejemplo, más de 10 000), el número de eventos también puede ser grande y los eventos pueden inundar la base de datos. En este caso, se recomienda elegir solo los eventos más críticos en la configuración de la directiva y habilitar su registro. Se recomienda desactivar el registro de todos los demás eventos.

Al hacerlo, reducirá la cantidad de eventos en la base de datos, aumentará la velocidad de ejecución de los escenarios asociados con el análisis de la tabla de eventos en la base de datos y disminuirá el riesgo de que una gran cantidad de eventos sobrescriban eventos críticos.

También puede reducir el plazo de almacenamiento para eventos asociados con una tarea o directiva. El período predeterminado es de 7 días para eventos relacionados con tareas y de 30 días para eventos relacionados con directivas. Cuando cambie el plazo de almacenamiento del evento, tenga en cuenta los procedimientos de trabajo establecidos en su organización y la cantidad de tiempo que el administrador del sistema puede dedicar al análisis de cada evento.

Se recomienda modificar la configuración de almacenamiento del evento en cualquiera de los siguientes casos:

- Los eventos referidos a cambios en el estado intermedio de tareas de grupo y los eventos referidos a la aplicación de directivas son un gran porcentaje de todos los eventos en la base de datos de Kaspersky Security Center Linux.
- El registro del sistema operativo comienza a mostrar entradas sobre la eliminación automática de eventos cuando se excede el límite establecido sobre la cantidad total de eventos almacenados en la base de datos.

Elija las opciones de registro de eventos en el supuesto de que la cantidad óptima de eventos procedentes de un solo dispositivo por día no debe exceder 20. Puede aumentar este límite ligeramente, si es necesario, pero solo si el número de dispositivos en su red es relativamente pequeña (menos de 10 000).

Prácticas recomendadas para un Servidor de administración que administra una gran cantidad de dispositivos

Prácticas recomendadas para el uso del DBMS

Configure la tarea **Mantenimiento del Servidor de administración** para que se ejecute de forma regular, especialmente si utiliza PostgreSQL como DBMS.

Excluya la carpeta del DBMS del análisis de IOC.

Prácticas recomendadas para directivas y perfiles

Reduzca la cantidad de directivas activas para cada componente (como Kaspersky Endpoint Security para Windows). Puede reemplazar las directivas con perfiles de directivas.

Prácticas recomendadas para un Servidor de administración que administra una gran cantidad de dispositivos

Reduzca la cantidad de tareas que se ejecuten simultáneamente, en especial las de instalación remota y administración de parches.

Reduzca el número y optimice la programación de las tareas que operan con selecciones de dispositivos.

En la sección **Configuración de eventos** de los ajustes de las directivas, minimice la cantidad de tipos de eventos que se guardan.

Prácticas recomendadas para el almacenamiento de eventos

Reduzca la frecuencia de los eventos de un mismo tipo del componente Control de aplicaciones. Consulte el siguiente artículo para obtener más detalles: Acerca del bloqueo de eventos frecuentes.

Reduzca el plazo por el que se almacenan los eventos de los componentes (como Kaspersky Endpoint Security para Windows) y los eventos informativos sobre las vulnerabilidades reparadas.

Habilite la opción **Guardar eventos relacionados con el progreso de la tarea** en las propiedades de las tareas generales, como las tareas de actualización. Consulte el siguiente artículo para obtener más detalles: Registro de información sobre eventos para tareas y directivas.

Optimice la configuración de la tarea de inventario. Consulte el siguiente artículo para obtener más detalles: Tarea de inventario.

Consideraciones específicas y configuración óptima de ciertas tareas

Ciertas tareas están sujetas a consideraciones específicas relacionadas con el número de dispositivos en red. Esta sección ofrece recomendaciones sobre la configuración óptima de configuraciones para tales tareas.

El descubrimiento de dispositivos, la tarea de copia de seguridad de datos, la tarea de mantenimiento de la base de datos y las tareas de grupo para actualizar Kaspersky Endpoint Security son parte de la funcionalidad básica de Kaspersky Security Center Linux.

La tarea de inventario es parte de la función de Administración de vulnerabilidades y parches y no está disponible si no está activada.

Frecuencia de descubrimiento de dispositivos

No es aconsejable aumentar la frecuencia predeterminada del descubrimiento de dispositivos porque esto puede crear una carga excesiva en los controladores de dominio. En cambio, se recomienda programar el sondeo a la frecuencia mínima posible permitida por las necesidades de su organización. Las recomendaciones para calcular la programación óptima se proporcionan en la tabla a continuación.

Programación para el descubrimiento de dispositivos

Número de dispositivos en red	Frecuencia recomendada para el descubrimiento de dispositivos
Menos de 10000	Frecuencia predeterminada o menos
10 000 o mayor	Una vez por día o menos

Tarea de copia de seguridad de datos del Servidor de administración y tarea de mantenimiento de la base de datos

El Servidor de administración deja de funcionar cuando se ejecutan las siguientes tareas:

- Copia de seguridad de los datos del Servidor de administración
- Mantenimiento del Servidor de administración

Cuando se ejecutan estas tareas, la base de datos no puede recibir ningún dato.

Es posible que tenga que reprogramar estas tareas para que no se ejecuten al mismo tiempo que otras tareas del Servidor de administración.

Tareas de grupo para actualizar Kaspersky Endpoint Security

Si el Servidor de administración actúa como origen de la actualización, la opción de programación recomendada para las tareas de actualización de grupo de Kaspersky Endpoint Security 10 y versiones posteriores es **Al descargar nuevas actualizaciones al repositorio** cuando la casilla **Utilizar retardo aleatorio automático para el inicio de tareas** esté seleccionada.

Si se crea una tarea local para descargar actualizaciones de servidores de Kaspersky al repositorio en cada punto de distribución, la programación periódica es óptima y recomendada para la tarea de actualización del grupo de Kaspersky Endpoint Security. El valor del período de aleatorización debe ser de una hora en este caso.

Tarea de inventario

Puede reducir la carga a la que se somete la base de datos cuando se obtiene información sobre los archivos ejecutables. Para tal fin, recomendamos que ejecute una tarea de inventario para Kaspersky Endpoint Security en dispositivos de referencia, que tengan instalada una selección de aplicaciones estándar.

El número de archivos ejecutables recibidos por el Servidor de administración desde un único dispositivo no puede ser mayor que 150 000. Cuando Kaspersky Security Center Linux alcanza este límite, no puede recibir ningún archivo nuevo.

Normalmente, el número de archivos en un dispositivo cliente común no supera los 60 000. El número de archivos ejecutables en un servidor de archivos puede ser mayor e incluso superar el umbral de 150 000.

Detalles de margen de la carga de la red entre Servidor de administración y dispositivos protegidos

Esta sección proporciona los resultados de las mediciones de prueba del tráfico de red con una descripción de las condiciones bajo las cuales se realizaron las mediciones. Puede consultar esta información cuando planifique la infraestructura de red y la capacidad de rendimiento de los canales de red dentro de su organización (o entre el Servidor de administración y otra organización con dispositivos para proteger). Al conocer la capacidad de rendimiento de la red, también puede estimar aproximadamente cuánto tiempo demorarán las diferentes operaciones de transmisión de datos.

Tasa de tráfico en diferentes escenarios

La siguiente tabla muestra los resultados de las pruebas de medición realizadas en el tráfico entre el Servidor de administración y un dispositivo administrado en diferentes escenarios.

De forma predeterminada, los dispositivos se sincronizan con el Servidor de administración cada 15 minutos o en un intervalo más largo. Sin embargo, si modifica la configuración de una directiva o tarea en el Servidor de administración la sincronización temprana se produce en los dispositivos a los que se aplica esa directiva/tarea, por lo que las nuevas configuraciones se transmiten a los dispositivos.

Tasa de tráfico entre el Servidor de administración y el dispositivo administrado

Procedimiento	Tráfico del Servidor de administración hacia cada dispositivo administrado	Tráfico de cada dispositivo administrado al Servidor de administración
Instalación de Kaspersky Endpoint Security for Linux con bases de datos actualizadas	390 MB	3.3 MB
Instalación del Agente de red	75 MB	397 KB
Instalación simultánea del Agente de red y Kaspersky Endpoint Security for Linux	459 MB	3.6 MB
Actualización inicial de las bases de datos antivirus sin actualizar las bases de datos incluidas en el paquete (si la participación en Kaspersky Security Network está deshabilitada)	113 MB	1.8 MB
Actualización diaria de las bases de datos antivirus (si está habilitada la participación en Kaspersky Security Network)	22 MB	373 MB
Sincronización inicial antes de la actualización de las bases de datos en un dispositivo (transferencia de directivas y tareas)	382 KB	446 KB
Sincronización inicial después de actualización de bases de datos en un dispositivo	20 KB	157 KB
Sincronización sin cambios en el Servidor de administración (según el cronograma)	18 KB	23 KB
Sincronización cuando se cambia una configuración única en una directiva de grupo (tan pronto como se modifique la configuración)	19 KB	20 KB
Sincronización cuando se cambia una configuración única en una tarea de grupo (tan pronto como se modifique la configuración)	14 KB	11 KB
Sincronización forzada	110 KB	109 KB
Evento **del Virus detectado** (1 virus)	44 KB	50 KB
Evento **del Virus detectado** (10 virus)	58 KB	77 KB

Procedimiento	Tráfico del Servidor de administración hacia cada dispositivo administrado	Tráfico de cada dispositivo administrado al Servidor de administración
Tráfico único después de habilitar la lista de registro de aplicaciones	hasta 10 KB	hasta 12 KB
Tráfico diario cuando se habilita la lista de registro de aplicaciones	hasta 840 KB	hasta 1 MB

Uso promedio de tráfico por 24 horas

El uso promedio de tráfico en 24 horas entre el Servidor de administración y un dispositivo administrado es el siguiente:

- El tráfico del Servidor de administración al dispositivo administrado es de 840 KB.
- El tráfico del dispositivo administrado al Servidor de administración es de 1 MB.

El tráfico se ha medido en las siguientes condiciones:

- Dispositivo administrado con Agente de red y Kaspersky Endpoint Security para Linux instalados.
- Ningún punto de distribución asignado al dispositivo.
- La característica Administración de vulnerabilidades y parches no estaba habilitada.
- Frecuencia de sincronización con el Servidor de administración: 15 minutos.

Problemas conocidos y limitaciones

Kaspersky Security Center Linux tiene las siguientes limitaciones, que no son críticas para el funcionamiento de la aplicación:

- 8698100: La tarea **Copia de seguridad de los datos del Servidor de administración** finaliza con el error "Compruebe si SQL Server tiene acceso a la carpeta de destino" cuando se utiliza la autenticación bidireccional entre la utilidad klpg_dump y PostgreSQL.

- 10253149: En las propiedades de la directiva de Kaspersky Endpoint Security para Windows (**Configuración de eventos** → **Advertencias**), al acceder a las propiedades del tipo de evento **Tarea interrumpida**, no se muestra el texto de la sección desplegable sobre el atributo de evento masivo.

- 10723777: Al actualizar las bases de datos mediante **Descargar actualizaciones en el repositorio del Servidor de administración**, Kaspersky Security Center Linux intenta utilizar bases de datos con una localización distinta de la suya si esta no es inglés (en).

- 10427694: En Ubuntu 24.04, debido a problemas con el procesamiento de llamadas al sistema asíncronas, el Servidor de administración genera volcados por error.

- 10007954: Después de crear e iniciar la tarea **Buscar vulnerabilidades y actualizaciones requeridas**, al acceder a los resultados de la tarea en el Servidor secundario, se produce el error "Se interrumpió la conexión con el Servidor de administración".

- 10671377: Al usar PostgreSQL o Postgres Pro 18.1–18.5, las tareas en ejecución pueden terminar con el error "'[53000]' ERROR: no hay búfer local vacío disponible". Se recomienda actualizar PostgreSQL a la versión 18.6 o seguir estos pasos:

  1. Detener el servicio del Servidor de administración.
  2. Detener el servicio del DBMS.
  3. Agregar la siguiente línea al final del archivo postgresql.conf: `[[effective_io_concurrency=0]]`.
  4. Iniciar el servicio del DBMS.
  5. Verificar que el valor de la opción `effective_io_concurrency` sea `0` mediante la siguiente consulta:
     `SELECT setting FROM pg_settings WHERE name = 'effective_io_concurrency';`
  6. Iniciar el servicio del Servidor de administración.

- 10564198: Al actualizar Kaspersky Security Center Linux a la versión 16.3 en los nodos de un clúster de conmutación por error de Kaspersky Security Center Linux, la ejecución del script postinstall.pl para configurar el Servidor de administración puede provocar errores de instalación.

- 8994760: Si tiene derechos de acceso en Servidores de administración virtuales, pero no tiene derechos de acceso en el Servidor de administración principal e intenta iniciar sesión en Kaspersky Security Center Linux, se produce un error y se muestra incorrectamente el mensaje de error **Su solicitud no puede procesarse en este momento. Espere e inténtelo de nuevo**. El texto del error debe ser el siguiente: **Verifique sus derechos de acceso. Debe tener derechos de acceso en el servidor principal o en uno de los servidores virtuales únicamente. Comuníquese con el administrador principal y vuelva a intentarlo**

- 10302954: Al especificar las condiciones para una regla de traslado de dispositivos, si en la pestaña **Red** activa la opción **El dispositivo se encuentra en un subgrupo del grupo Dominios**, la lista desplegable de subgrupos aparece vacía.

- 10253149: Para las directivas de aplicaciones, si en la pestaña **Configuración de eventos** selecciona un evento masivo, no se muestra el bloque expandible **Mostrar más** con una advertencia sobre el efecto de dichos eventos en el rendimiento del Servidor de administración o del DBMS.

- 9302142: La opción **Usar el Agente de red como una puerta de enlace de conexión en la DMZ** no es compatible con Microsoft Windows en Arm.

- 9065814: Puede ocurrir un error al intentar la autenticación de dominio desde un dispositivo basado en Windows en un dominio de Samba 4.

- 9335676: Después de cambiar el nodo principal en un clúster de DBMS de alta disponibilidad, es posible que el acceso a Kaspersky Security Center Web Console no esté disponible o se demore significativamente. Si Kaspersky Security Center Web Console permanece inaccesible durante más de 10 minutos, reinicie el servicio de IAM con el siguiente comando:

  ```
  systemctl restart kliam_srv.service
  ```

- 9157005, 9157085: Al ejecutar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* en un dispositivo administrado de Windows con la opción **Comenzar la instalación cuando se esté por reiniciar o apagar el dispositivo** habilitada, la tarea puede fallar con un error. Este problema puede ocurrir cuando se programa la instalación de una gran cantidad de actualizaciones. Para resolver el problema, ejecute la tarea sin habilitar la opción **Comenzar la instalación cuando se esté por reiniciar o apagar el dispositivo**.

- 9272534: Si la tabla de usuarios contiene más de 50 000 usuarios, solo se muestran los primeros 50 000 y no se muestran los demás.

- 9291235: Después de restaurar una copia de seguridad en la versión 16.1 del Servidor de administración, Kaspersky Security Center Web Console muestra la página de inicio de sesión. Después de una autenticación exitosa, se solicita un código de seguridad de un solo uso para la autenticación de dos factores. Cuando se ingresa un código de seguridad de un solo uso válido, se muestra un mensaje de error que indica que el código de seguridad de un solo uso es incorrecto. En este caso, espere unos minutos y luego actualice manualmente la página para volver a intentar iniciar sesión en Kaspersky Security Center Web Console. Una vez que el proceso de restauración de la copia de seguridad se haya completado por completo, la autenticación se realizará correctamente en el próximo intento.

- 7939561: Al intentar modificar una cuenta de usuario protegida, hacer clic en el botón **Cancelar** en la ventana de entrada de credenciales de **Protección de cuentas** produce un error.

- 8562938: El simple hecho de abrir el puerto para dispositivos móviles en las propiedades de la directiva del Servidor de administración no habilita la función Administración de dispositivos móviles y no activa la generación de un certificado móvil. Para habilitar la función Administración de dispositivos móviles, el puerto para dispositivos móviles debe estar abierto en las propiedades del Servidor de administración.

- 8732282: Para un usuario que tiene habilitada la opción **El usuario no puede cambiar la contraseña** en las propiedades de la cuenta de Active Directory, no se ejecutará la acción de respuesta **Restablecer contraseña** en Active Directory. El administrador del controlador de dominio tiene que deshabilitar la opción **El usuario no puede cambiar la contraseña** para este usuario o restablecer la contraseña manualmente. Este problema ocurre si tiene la licencia de Kaspersky Next XDR Optimum, la integración con Active Directory está habilitada y el usuario está incluido en un grupo de seguridad de Active Directory.

- 8688182: Si el usuario tiene habilitada la opción **La contraseña nunca caduca** en las propiedades de la cuenta de Active Directory, luego de ejecutar la acción de respuesta **Restablecer contraseña** se deshabilita la opción **La contraseña nunca caduca** y el usuario debe cambiar su contraseña de dominio en el próximo inicio de sesión. Este problema ocurre si tiene la licencia de Kaspersky Next XDR Optimum, la integración con Active Directory está habilitada y el usuario está incluido en un grupo de seguridad de Active Directory.

- 8703857: La conexión al servidor proxy para Kaspersky Security Center Web Console y los complementos web de administración solo se establece si el servidor proxy admite la autenticación básica.

- 7911778: Cuando ejecuta la tarea **Desinstalar aplicación de forma remota** para desinstalar el Agente de red de un dispositivo que está ejecutando un sistema operativo con la arquitectura Arm y cuya hora no está sincronizada con el Servidor de administración, el estado de la tarea no cambia de **En ejecución** a **Completada**, incluso después de que el Agente de red se desinstaló correctamente del dispositivo. Para resolver este problema, sincronice la hora del dispositivo con el Agente de red instalado y la hora del dispositivo con el Servidor de administración antes de ejecutar **Desinstalar aplicación de forma remota**.

- 6896585: Un dispositivo administrado no puede conectarse a KSN a través del servicio del proxy de KSN si Kaspersky Security Center Linux está instalado en un dispositivo que tiene letras del alfabeto cirílico en su nombre.

- 7523299: El Agente de red no se reinicia después de finalizar el proceso en un dispositivo administrado que ejecuta CentOS 6.6.

- 7835858: Si crea una tarea con la configuración de programación **Cada N días** y **Por días de la semana** en Kaspersky Security Center Web Console 15.2 o posterior y luego abre la tarea en versiones anteriores de la Consola de administración o Kaspersky Security Center Web Console (por ejemplo, cuando la tarea también se aplica en los servidores de administración secundarios, que pueden operar tanto en Linux como en Windows), es posible que la configuración de programación se muestre incorrectamente o que se produzca un error.

- 7208621: Cuando importa la tarea *Descargar actualizaciones a los repositorios de puntos de distribución* o *Verificación de actualizaciones*, se habilita la opción **Seleccionar dispositivos a los que se asignará la tarea**. Estas tareas no se pueden asignar a una selección de dispositivos o a dispositivos específicos. Si asigna la tarea *Descargar actualizaciones a los repositorios de puntos de distribución* o *Verificación de actualizaciones* a dispositivos específicos, la tarea se importará incorrectamente.

- 6511063: Si se detectó una aplicación en la sección **Registro de aplicaciones** en un dispositivo Linux, las propiedades de la aplicación no contienen información sobre los archivos ejecutables relacionados.

- 5915107: En informes en formato carta, los saltos de página pueden hacer un corte horizontal en las líneas de texto.

- 5556109: Un dispositivo administrado que tiene más de un adaptador de red envía al Servidor de administración información sobre la dirección MAC del adaptador de red que no se utilizó para conectarse al Servidor de administración.

- 9093038: Si el Servidor de administración de Kaspersky Security Center Linux no se inicia después de la instalación y el registro del sistema operativo contiene el error 213/SECUREBITS relacionado con kladminserver_srv.service, ejecute los siguientes comandos como superusuario:

```
mkdir -p /etc/systemd/system/kladminserver_srv.service.d
echo "[Service]" > /etc/systemd/system/kladminserver_srv.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/kladminserver_srv.service.d/override.conf
mkdir -p /etc/systemd/system/klwebsrv_srv.service.d
echo "[Service]" > /etc/systemd/system/klwebsrv_srv.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/klwebsrv_srv.service.d/override.conf
```

  Si Kaspersky Security Center Web Console no se inicia después de la instalación y el registro del sistema operativo contiene el error 213/SECUREBITS relacionado con KSCWebConsole.service, ejecute los siguientes comandos como superusuario:

```
mkdir -p /etc/systemd/system/KSCSvcWebConsole.service.d
echo "[Service]" > /etc/systemd/system/KSCSvcWebConsole.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCSvcWebConsole.service.d/override.conf
mkdir -p /etc/systemd/system/KSCWebConsoleManagement.service.d
echo "[Service]" > /etc/systemd/system/KSCWebConsoleManagement.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsoleManagement.service.d/override.conf
mkdir -p /etc/systemd/system/KSCWebConsoleNATS.service.d
echo "[Service]" > /etc/systemd/system/KSCWebConsoleNATS.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsoleNATS.service.d/override.conf
mkdir -p /etc/systemd/system/KSCWebConsolePlugin.service.d
echo "[Service]" > /etc/systemd/system/KSCWebConsolePlugin.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsolePlugin.service.d/override.conf
mkdir -p /etc/systemd/system/KSCWebConsole.service.d
echo "[Service]" > /etc/systemd/system/KSCWebConsole.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsole.service.d/override.conf
```

  Si el servicio kliam_srv no se inicia después de la instalación y el registro del sistema operativo contiene el error 213/SECUREBITS relacionado con el servicio, ejecute los siguientes comandos como superusuario:

```
mkdir -p /etc/systemd/system/kliam_srv.service.d
echo "[Service]" > /etc/systemd/system/kliam_srv.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/kliam_srv.service.d/override.conf
```

- 9165434: La autenticación de NTLM no funciona para cuentas de usuario dentro del grupo Usuarios protegidos.

Contacto con el Servicio de soporte técnico

En esta sección se explica cómo obtener soporte técnico y se describen los términos que rigen este servicio.

Cómo obtener soporte técnico

Si no encontró una solución a su problema en la documentación ni en otras fuentes de información sobre Kaspersky Security Center Linux, le recomendamos que se ponga en contacto con Soporte técnico. Los especialistas del Servicio de soporte técnico responderán a todas sus preguntas acerca de la instalación y el uso de Kaspersky Security Center.

Kaspersky brinda soporte para Kaspersky Security Center durante su ciclo de vida (consulte la página del ciclo de vida de soporte de la aplicación). Antes de comunicarse con el servicio de soporte técnico, lea las reglas de soporte técnico.

Para comunicarse con el servicio de soporte técnico, puede elegir alguna de estas opciones:

- Puede visitar el sitio web del Soporte técnico
- Enviando una solicitud al Soporte técnico de Kaspersky desde el portal de Kaspersky CompanyAccount

Consultas mediante Kaspersky CompanyAccount al servicio de soporte técnico

Kaspersky CompanyAccount es un portal para empresas que usan aplicaciones de Kaspersky. El portal Kaspersky CompanyAccount está diseñado para que los usuarios puedan comunicarse con los especialistas de Kaspersky fácilmente a través de solicitudes en línea. Puede usar Kaspersky CompanyAccount para realizar un seguimiento del estado de sus solicitudes en línea a medida que los expertos de Kaspersky las procesan y mantener un historial de dichas solicitudes.

Puede registrar a todos los empleados de su organización bajo una única cuenta de Kaspersky CompanyAccount. Una cuenta única le permite administrar de forma centralizada las solicitudes electrónicas enviadas a Kaspersky por los empleados registrados y administrar los privilegios de esos empleados a través de Kaspersky CompanyAccount.

El portal Kaspersky CompanyAccount está disponible en los siguientes idiomas:

- Inglés
- Español
- Italiano
- Alemán

- Polaco
- Portugués
- Ruso
- Francés
- Japonés

Para obtener más información sobre Kaspersky CompanyAccount, visite el sitio web del servicio de soporte técnico.

Obtener archivos de volcado del Servidor de administración

Los archivos de volcado del Servidor de administración contienen toda la información sobre los procesos del Servidor de administración en un determinado momento. Los archivos de volcado del Servidor de administración se almacenan en el directorio /var/lib/systemd/coredump. Los archivos de volcado se almacenan mientras Kaspersky Security Center Linux está en uso y se eliminan de forma permanente cuando se desinstala la aplicación. Los archivos de volcado no se envían a Kaspersky automáticamente.

Si el Servidor de administración falla, puede comunicarse con el Servicio de soporte técnico de Kaspersky. Un especialista del Servicio de soporte técnico puede solicitarle que envíe los archivos de volcado del Servidor de administración para su posterior análisis en Kaspersky.

Los archivos de volcado pueden contener datos personales. Antes de enviar información a Kaspersky, recomendamos protegerla contra accesos no autorizados.

Fuentes de información acerca de la aplicación

La página de Kaspersky Security Center Linux en el sitio web de Kaspersky

En la página de Kaspersky Security Center Linux en el sitio web de Kaspersky, puede ver información general sobre la aplicación, sus funciones y características.

La página de Kaspersky Security Center Linux en la Base de conocimientos

La *Base de conocimientos* es una sección del sitio web de soporte técnico de Kaspersky.

En la página de Kaspersky Security Center Linux en la Base de conocimientos, puede leer artículos que proporcionan información útil, recomendaciones y respuestas a las preguntas más frecuentes sobre cómo comprar, instalar y utilizar la aplicación.

Los artículos de la Base de conocimientos pueden proporcionar respuestas a preguntas relacionadas tanto con Kaspersky Security Center Linux como con otras aplicaciones de Kaspersky. Los artículos de la Base de conocimientos también pueden contener noticias del Servicio de soporte técnico.

Discutir las aplicaciones de Kaspersky con la comunidad

Si su pregunta no requiere una respuesta inmediata, puede analizarla con los expertos de Kaspersky y con otros usuarios en nuestro foro.

En el Foro, puede consultar temas de debate, publicar comentarios y crear temas nuevos.

> Se requiere una conexión a Internet para acceder a los recursos web.

Si no encuentra solución a su problema, comuníquese con el servicio de soporte técnico.

Glosario

Actualización

Procedimiento de sustitución o adición de nuevos archivos (bases de datos o módulos de software) descargados de los servidores de actualización de Kaspersky.

Actualización disponible

Conjunto de actualizaciones para los módulos de una aplicación de Kaspersky. El término incluye las actualizaciones críticas acumuladas durante cierto período de tiempo y aquellas que modifican la arquitectura de la aplicación.

Administración centralizada de aplicaciones

Administración remota de aplicaciones a través de los servicios disponibles para tal fin en Kaspersky Security Center.

Administración directa de aplicaciones

Administración de aplicaciones mediante una interfaz local.

Administrador de Kaspersky Security Center Linux

La persona que administra el funcionamiento de las aplicaciones a través del sistema de administración remota y centralizada Kaspersky Security Center Linux.

Administrador del cliente

Miembro del personal de una organización cliente que es responsable de supervisar el estado de la seguridad antivirus.

Administrador del proveedor de servicios

Un miembro del personal del proveedor de servicios de protección antivirus. Este administrador se encarga de instalar y mantener el sistema de protección antivirus basado en los productos antivirus de Kaspersky y también brinda soporte técnico a los clientes.

Agente de actualización

Equipo en el que se ha instalado el Agente de red y que se utiliza para distribuir actualizaciones, realizar sondeos de red, instalar aplicaciones en forma remota y recopilar información sobre los equipos asociados a un grupo de administración o a un dominio de difusión. Los puntos de distribución están diseñados para optimizar el tráfico de red y reducir la carga del Servidor de administración durante la distribución de actualizaciones. Los puntos de distribución pueden ser designados en forma manual por el administrador o de manera automática por el Servidor de administración.

Agente de autenticación

Interfaz que permite autenticarse para obtener acceso a un disco duro cifrado y cargar el sistema operativo si el disco duro de arranque se encuentra cifrado.

Agente de red

Componente de Kaspersky Security Center Linux que permite la interacción entre el Servidor de administración y las aplicaciones de Kaspersky instaladas en un nodo de red específico (una estación de trabajo o un servidor específicos). Este componente es el mismo para todas las aplicaciones para Windows de la empresa. Existen versiones independientes del Agente de red para las aplicaciones de Kaspersky para Novell®, Unix™ y Mac.

Aplicación incompatible

Una aplicación antivirus que no fue creada por Kaspersky o una aplicación de Kaspersky que no se puede administrar a través de Kaspersky Security Center Linux.

Archivo de clave

Archivo de formato xxxxxxxx.key que hace posible usar una aplicación de Kaspersky con una licencia comercial o de prueba. Solo puede usar la aplicación si tiene un archivo de clave.

Bases de datos antivirus

Bases de datos que contienen información sobre las amenazas a la seguridad informática de las que Kaspersky tiene conocimiento a la fecha de publicarse esas bases de datos. Las entradas de las bases de datos antivirus permiten detectar código malicioso en los objetos analizados. Las bases de datos antivirus son generadas por los especialistas de Kaspersky. Se actualizan cada una hora.

Brote de virus

Serie de intentos deliberados de infectar un dispositivo con un virus.

Carpeta Copia de seguridad

Carpeta especial para el almacenamiento de copias de datos del Servidor de administración creadas mediante la utilidad de copia de seguridad.

Certificado compartido

Certificado que se utiliza para identificar al usuario de un dispositivo móvil.

Certificado del Servidor de administración

El certificado se utiliza para autenticar el Servidor de administración cuando la Consola de administración se conecta a él y durante la comunicación con los dispositivos cliente. El certificado del Servidor de administración se crea durante la instalación del componente Servidor de administración y se almacena en la carpeta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert del Servidor de administración.

Clave activa

Una clave que está siendo utilizada por la aplicación.

Clave de reserva

Una clave que certifica el derecho a usar la aplicación, pero que no se está utilizando en un momento dado.

Cliente del Servidor de administración (dispositivo cliente)

Dispositivo, servidor o estación de trabajo en el que están instalados y se ejecutan el Agente de red y las aplicaciones administradas de Kaspersky.

Cloud Discovery

Cloud Discovery administra el acceso de los usuarios a los servicios en la nube. Algunos ejemplos de servicios en la nube son Microsoft Teams, Salesforce y Microsoft Office 365. Los servicios en la nube se agrupan en categorías, por ejemplo, *Uso compartido de archivos*, *Mensajería instantánea* y *Correo electrónico*.

Configuración de la aplicación

Ajustes de una aplicación que son comunes a todos los tipos de tareas y que rigen el funcionamiento general de esa aplicación (esto incluye, por ejemplo, los ajustes relativos al rendimiento, los informes y las copias de seguridad de la aplicación).

Configuración de la tarea

Ajustes de una aplicación que son específicos para cada tipo de tarea.

Consola de administración

Componente de Kaspersky Security Center Linux que proporciona la interfaz de usuario de los servicios administrativos del Servidor de administración y el Agente de red.

Copia de seguridad de los datos del Servidor de administración

Proceso de copiar los datos del Servidor de administración para crear una versión de respaldo que pueda restaurarse con la utilidad de copia de seguridad. La utilidad puede guardar lo siguiente:

- La base de conocimientos del Servidor de administración (directivas, tareas, configuración de las aplicaciones, eventos guardados en el Servidor de administración)
- Información de configuración relativa a la estructura de grupos de administración y dispositivos cliente
- Repositorio de archivos de instalación para la instalación remota de aplicaciones (el contenido de las carpetas Packages, Uninstall Updates)
- Certificado del Servidor de administración.

Derechos de administrador

Nivel de derechos y privilegios de usuario que se necesitan para administrar objetos de Exchange en una organización de Exchange.

Directiva

Una directiva determina la configuración de una aplicación y controla la capacidad de configurar esa aplicación en los equipos de un grupo de administración. Se debe crear una directiva individual para cada aplicación. Aunque es posible crear un número ilimitado de directivas para las aplicaciones instaladas en los dispositivos de cada grupo de administración, solamente puede haber una directiva aplicada a cada aplicación dentro de un grupo de administración.

Dispositivo MDM con iOS

Dispositivo móvil conectado al Servidor de MDM para iOS mediante el protocolo de MDM para iOS. Los dispositivos que ejecutan el sistema operativo iOS pueden conectarse y administrarse a través del protocolo de MDM para iOS.

Dispositivos administrados

Dispositivos corporativos que se encuentran conectados a la red y que se han incluido en un grupo de administración.

Dominio de difusión

Área lógica de una red en la que todos los nodos pueden intercambiar datos, utilizando para ello un canal de difusión en el nivel del modelo OSI (modelo de interconexión de sistemas abiertos).

Estación de trabajo del administrador

El dispositivo en el que está instalada la Consola de administración actúa como el componente que proporciona la interfaz de administración de Kaspersky Security Center Linux.

Desde la estación de trabajo del administrador, el administrador gestiona la parte del servidor de Kaspersky Security Center mediante la creación y el control de un sistema de protección centralizada para la red de la organización basado en aplicaciones de Kaspersky.

Estado de protección

Estado actual de la protección, que refleja el nivel de protección del dispositivo.

Estado de protección de la red

Estado de protección registrado en un momento determinado. Define la seguridad de los dispositivos corporativos conectados a la red. El estado de la protección de la red incluye factores como las aplicaciones de protección instaladas, el uso de claves y el número y los tipos de amenazas detectadas.

FileTransferBridge

Un componente interno de Kaspersky Security Center Linux que proporciona la distribución local de actualizaciones de las aplicaciones de Kaspersky. FileTransferBridge está integrado en el Agente de red (klnagent) y se ejecuta localmente en cada dispositivo administrado.

Cuando las aplicaciones de Kaspersky reciben actualizaciones de Kaspersky Security Center Linux, el Agente de red descarga los archivos de actualización del Servidor de administración o de un punto de distribución. Luego, FileTransferBridge transfiere los archivos localmente a las aplicaciones de Kaspersky instaladas, lo que garantiza la entrega confiable de las actualizaciones de las bases de datos y los parches de software.

FileTransferBridge utiliza los puertos TCP 30522 y 30523. Los puertos solo están a la escucha en la interfaz localhost (127.0.0.1) y no aceptan conexiones entrantes de redes externas.

Gravedad de un evento

Propiedad de un evento registrado durante la ejecución de una aplicación de Kaspersky. Hay cuatro niveles de gravedad:

- Evento crítico
- Error funcional
- Advertencia
- Información

Dos eventos de un mismo tipo pueden tener niveles de gravedad diferentes si ocurren en situaciones diferentes.

Grupo de administración

Un conjunto de dispositivos combinados de acuerdo con las funciones que realizan y con las aplicaciones de Kaspersky que tienen instaladas. Los dispositivos se agrupan y se tratan como una sola entidad para facilitar su administración. Cada grupo puede incluir otros grupos. Pueden crearse directivas de grupo y tareas de grupo para cada aplicación instalada en un grupo.

Grupo de roles

Un grupo de usuarios de dispositivos móviles Exchange ActiveSync a los que se les han otorgado los mismos derechos de administrador.

HTTPS

Protocolo seguro para transferir datos cifrados entre un navegador y un servidor web. HTTPS se usa para obtener acceso a información restringida, como datos corporativos o financieros.

Identity and Access Manager (IAM)

Un componente del Servidor de administración que le permite usar la autenticación de dominio (inicio de sesión único). La función de inicio de sesión único le permite a un usuario habilitar la autenticación segura en Kaspersky Security Center Web Console sin tener que volver a ingresar la contraseña en la red corporativa.

Instalación local

Instalación de una aplicación de protección en un dispositivo conectado a una red corporativa que implica iniciar manualmente la instalación desde un paquete de distribución de la aplicación de protección o ejecutar manualmente un paquete de instalación publicado que se haya descargado previamente en el dispositivo.

Instalación manual

Instalación de una aplicación de protección en un dispositivo de la red corporativa mediante un paquete de distribución. La instalación manual requiere la participación de un administrador o de otro especialista en TI. Por lo general, la instalación manual se realiza si la instalación remota ha finalizado con errores.

Instalación remota

Instalación de las aplicaciones de Kaspersky mediante los servicios proporcionados por Kaspersky Security Center Linux.

JavaScript

Lenguaje de programación que amplía la funcionalidad de las páginas web. Las páginas web que utilizan JavaScript pueden realizar ciertas funciones (por ejemplo, abrir ventanas adicionales o cambiar la vista de elementos de la interfaz) sin tener que actualizarse con datos nuevos solicitados al servidor web. Para ver páginas con JavaScript, habilite el uso de JavaScript en la configuración de su navegador.

Kaspersky Security Center System Health Validator (SHV)

Componente de Kaspersky Security Center Linux diseñado para verificar la operatividad del sistema operativo cuando Kaspersky Security Center Linux y Microsoft NAP funcionan simultáneamente.

Nagent ligero (LWNGT)

Protocolo para la interacción con Kaspersky Endpoint Security en dispositivos móviles. El LWNGT (también llamado protocolo móvil) funciona como Agente de red, pero sin instalar el Agente de red en dispositivos móviles.

Nivel de importancia del parche

Atributo del parche. Existen cinco niveles de importancia para los parches de Microsoft y los de terceros:

- Crítico
- Alto.
- Medio.
- Bajo.
- Desconocido.

El nivel de importancia de un parche de terceros o de Microsoft está determinado por el nivel de gravedad menos favorable entre las vulnerabilidades que el parche debe reparar.

Operador de Kaspersky Security Center

Usuario que supervisa el estado y el funcionamiento de un sistema de protección administrado mediante Kaspersky Security Center.

Paquete de instalación

Conjunto de archivos que se crea para instalar una aplicación de Kaspersky de manera remota, mediante el sistema de administración a distancia Kaspersky Security Center. El paquete de instalación contiene una serie de ajustes que se necesitan para instalar la aplicación y ejecutarla inmediatamente una vez que concluye la instalación. La aplicación se configura con los ajustes predeterminados. El paquete de instalación se crea usando archivos con las extensiones .kpd y .kud que vienen incluidos en el kit de distribución de la aplicación.

Perfil

Conjunto de ajustes para dispositivos móviles Exchange que define su comportamiento cuando están conectados a un servidor Microsoft Exchange.

Perfil de aprovisionamiento

Conjunto de ajustes para el funcionamiento de una aplicación en un dispositivo móvil iOS. Un perfil de aprovisionamiento contiene información sobre la licencia; está vinculado a una aplicación específica.

Perfil de configuración

Directiva que contiene un conjunto de ajustes y restricciones para un dispositivo móvil MDM con iOS.

Periodo de vigencia de la licencia

El periodo durante el cual se permite utilizar la funcionalidad de la aplicación y los servicios adicionales. Los servicios disponibles dependen del tipo de licencia.

Propietario del dispositivo

El usuario con el que el administrador puede comunicarse cuando surge la necesidad de realizar determinadas operaciones con un dispositivo.

Proveedor de servicios de protección antivirus

Organización que utiliza las soluciones de Kaspersky para brindarle servicios de protección antivirus a una organización cliente.

Puerta de enlace de conexión

Una *puerta de enlace de conexión* es un Agente de red que opera de un modo especial. Las puertas de enlace de conexión aceptan conexiones de otros agentes de red y las hacen llegar al Servidor de administración a través de la conexión que mantiene con el mismo. A diferencia de un Agente de red normal, una puerta de enlace de conexión no se encarga de establecer conexión con el Servidor de administración, sino que espera a que el Servidor de administración se conecte a ella.

Repositorio de eventos

Una parte de la base de datos del Servidor de administración que se utiliza para almacenar información sobre los eventos ocurridos en Kaspersky Security Center Linux.

Restauración

Proceso de tomar un objeto original de Cuarentena o Copia de seguridad y colocarlo en su carpeta de origen (la carpeta en la que el objeto se encontraba antes ser desinfectado, eliminado o puesto en cuarentena) o en una carpeta elegida por el usuario.

Restauración de los datos del Servidor de administración

Restauración de los datos del Servidor de administración a partir de la información guardada en "Copia de seguridad" mediante la utilidad de copia de seguridad. La utilidad puede restaurar lo siguiente:

- La base de conocimientos del Servidor de administración (directivas, tareas, configuración de las aplicaciones, eventos guardados en el Servidor de administración)
- Información de configuración relativa a la estructura de grupos de administración y dispositivos cliente
- Repositorio de archivos de instalación para la instalación remota de aplicaciones (el contenido de las carpetas Packages, Uninstall Updates)
- Certificado del Servidor de administración.

Seguridad antivirus de la red

Conjunto de medidas técnicas y organizacionales que disminuyen el riesgo de permitir el ingreso de virus y spam en la red de una organización y que brindan protección contra los ataques de red, el phishing y otras amenazas. La seguridad antivirus de la red aumenta cuando se utilizan aplicaciones y servicios de seguridad, y cuando se aplica y se cumple la directiva corporativa de seguridad de datos.

Servidor de administración

Componente de Kaspersky Security Center que almacena centralmente información sobre todas las aplicaciones de Kaspersky instaladas en la red corporativa y las controla.

Servidor de administración doméstico

El Servidor de administración especificado durante la instalación del Agente de red. El Servidor de administración doméstico puede usarse en la configuración de los perfiles de conexión del Agente de red.

Servidor de administración virtual

Componente de Kaspersky Security Center Linux diseñado para administrar el sistema de protección de red de una organización cliente.

El Servidor de administración virtual es una clase particular de Servidor de administración secundario. En comparación con un Servidor de administración físico, los servidores de administración virtuales tienen las siguientes restricciones:

- El Servidor de administración virtual puede crearse solamente en un Servidor de administración principal.
- El Servidor de administración virtual usa la base de datos del Servidor de administración principal. Los servidores de administración virtuales no son compatibles con la tarea de copia de seguridad y restauración de datos ni con la tarea de búsqueda y descarga de actualizaciones.
- El Servidor virtual no admite la creación de Servidores de administración secundarios (incluidos Servidores virtuales).

Servidor de MDM para iOS

Componente de Kaspersky Security Center instalado en un dispositivo cliente que permite la conexión de dispositivos móviles iOS al Servidor de administración y la administración de dispositivos móviles iOS por medio del servicio Apple Push Notifications (APNs).

Servidor web de Kaspersky Security Center Linux

Componente de Kaspersky Security Center Linux que se instala junto con el Servidor de administración. El Servidor web está diseñado para transmitir paquetes de instalación independientes, perfiles de MDM para iOS y archivos de una carpeta compartida a través de una red.

Servidores de actualizaciones de Kaspersky

Servidores HTTP(S) de Kaspersky desde los que las aplicaciones de Kaspersky descargan actualizaciones para sus bases de datos y módulos de software.

SSL

Protocolo de cifrado de datos que se usa tanto en redes locales como en Internet. El protocolo SSL se utiliza en aplicaciones web para crear una conexión segura entre el cliente y el servidor.

Subred de reconocimiento de ubicación de red (NLA)

Servicio de Windows que ayuda al sistema operativo a identificar la red a la que está conectado. NLA detecta cambios en la red y ajusta la configuración de seguridad del dispositivo.

Tarea

Las funciones que realiza la aplicación de Kaspersky se implementan en forma de tareas. Algunas de estas tareas son Protección de archivos en tiempo real, Análisis completo del equipo y Actualización de las bases de datos.

Tarea de grupo

Tarea que se define para un grupo de administración y se ejecuta en todos los dispositivos cliente de ese grupo.

Tarea local

Una tarea definida y ejecutada en un solo dispositivo cliente.

Tarea para dispositivos específicos

Tarea asignada a un conjunto de dispositivos cliente tomados de grupos de administración arbitrarios y realizada en dichos dispositivos.

Tienda de aplicaciones

Componente de Kaspersky Security Center Linux. La Tienda de aplicaciones se utiliza para instalar aplicaciones en los dispositivos Android que pertenecen a los usuarios. La Tienda permite publicar los archivos APK de las aplicaciones y vínculos para acceder a las aplicaciones disponibles en Google Play.

Usuarios internos

Las cuentas de usuarios internos se utilizan para trabajar con servidores de administración virtuales. El administrador puede usar una cuenta de usuario interno para iniciar Kaspersky Security Center Web Console y ver información sobre el estado de la seguridad antivirus de la red. En Kaspersky Security Center Linux, los usuarios internos tienen los derechos de los usuarios reales.

Las cuentas de los usuarios internos se crean y utilizan exclusivamente para trabajar dentro de Kaspersky Security Center Linux. No se transfiere ningún dato sobre estos usuarios internos al sistema operativo. Kaspersky Security Center Linux se encarga de autenticar a los usuarios internos.

Vulnerabilidad

Una falla en un sistema operativo o una aplicación que los atacantes pueden aprovechar para penetrar en el sistema operativo o la aplicación y comprometer su integridad. La presencia de una gran cantidad de vulnerabilidades en un sistema operativo lo hace poco confiable, debido a que el malware que penetra en el sistema operativo puede generar interrupciones en el propio sistema operativo y en las aplicaciones instaladas.

Zona desmilitarizada (DMZ)

Segmento de una red local en la que hay servidores que atienden solicitudes provenientes de la Web global. El acceso desde la zona desmilitarizada a la red local de la organización se protege con un firewall para garantizar la seguridad de la LAN.

Información sobre el código de terceros

La información sobre código de terceros se encuentra en el archivo legal_notices.txt, en el directorio de instalación de la aplicación.

Avisos de marcas registradas

Las marcas registradas y las marcas de servicio son propiedad de sus respectivos dueños.

Adobe, Acrobat, Flash, PostScript y Shockwave son marcas comerciales registradas o marcas comerciales de Adobe en los Estados Unidos o en otros países.

AMD y AMD64 son marcas comerciales o marcas registradas de Advanced Micro Devices, Inc.

Amazon, Amazon Web Services, AWS, Amazon EC2 y AWS Marketplace son marcas registradas de Amazon.com, Inc. o de sus empresas vinculadas.

Apache es una marca comercial registrada o una marca comercial de Apache Software Foundation en los Estados Unidos o en otros países.

Apple, AirPlay, AirDrop, AirPrint, App Store, Apple Configurator, AppleScript, FaceTime, FileVault, iBook, iBooks, iCloud, iPad, iPhone, iTunes, Leopard, macOS, Mac, Mac OS, OS X, Safari, Snow Leopard, Tiger, QuickTime y Touch ID son marcas comerciales de Apple Inc.

Arm es una marca registrada de Arm Limited (o de sus filiales) en los EE. UU. y/o en otros lugares.

La palabra, la marca y los logotipos de Bluetooth son propiedad de Bluetooth SIG, Inc.

Ubuntu y LTS son marcas comerciales registradas de Canonical Ltd. Cisco, Cisco Jabber, Cisco Systems e IOS son marcas comerciales registradas o marcas comerciales de Cisco Systems, Inc. y/o sus empresas vinculadas en los Estados Unidos y en algunos otros países.

Citrix, XenServer son marcas comerciales o marcas comerciales registradas de Cloud Software Group, Inc. y/o sus filiales en los Estados Unidos y/u otros países.

Corel es una marca comercial o una marca comercial registrada de Corel Corporation y/o de sus filiales en Canadá, los Estados Unidos y/u otros países.

Cloudflare, el logotipo de Cloudflare y Cloudflare Workers son marcas comerciales o marcas comerciales registradas de Cloudflare, Inc. en los Estados Unidos y otras jurisdicciones.

Dropbox es una marca registrada de Dropbox, Inc.

Radmin es una marca comercial registrada de Famatech.

Firebird es una marca registrada de Firebird Foundation.

Foxit es una marca registrada de Foxit Corporation.

La marca FreeBSD es una marca registrada de The FreeBSD Foundation.

Google, Android, Chrome, Chromium, Dalvik, Firebase, Google Chrome, Google Earth, Google Play, Google Maps, Google Public DNS, Hangouts y YouTube son marcas comerciales de Google LLC.

EulerOS, FusionCompute y FusionSphere son marcas comerciales de Huawei Technologies Co., Ltd.

Intel, Core, Xeon son marcas comerciales de Intel Corporation o sus subsidiarias.

IBM y QRadar son marcas comerciales de International Business Machines Corporation y están registradas en muchas jurisdicciones del mundo.

Node.js es una marca registrada de Joyent, Inc.

Linux es una marca registrada de Linus Torvalds en los Estados Unidos y en otros países.

Logitech es una marca comercial registrada o una marca comercial de Logitech en los Estados Unidos y/o en otros países.

Microsoft, Active Directory, ActiveSync, BitLocker, Excel, Forefront, Internet Explorer, InfoPath, Hyper-V, Microsoft Edge, MultiPoint, MS-DOS, PowerShell, PowerPoint, SharePoint, SQL Server, Office 365, OneNote, Outlook, Skype, Tahoma, Visio, Win32, Windows, Windows PowerShell, Windows Media, Windows Server, Windows Phone, Windows Vista y Windows Azure son marcas comerciales del grupo de empresas Microsoft.

Mozilla, Firefox y Thunderbird son marcas comerciales de la Fundación Mozilla en los Estados Unidos y en otros países.

Novell es una marca registrada de Novell Enterprises Inc. en los Estados Unidos y en otros países.

OpenSSL es una marca comercial de OpenSSL Software Foundation.

OpenVPN es una marca registrada de OpenVPN, Inc.

Oracle, Java, JavaScript y TouchDown son marcas registradas de Oracle o de sus empresas vinculadas.

Parallels, el logotipo de Parallels y Coherence son marcas comerciales o marcas comerciales registradas de Parallels International GmbH.

Chef es una marca comercial o una marca comercial registrada de Progress Software Corporation y/o una de sus subsidiarias o afiliadas en los EE. UU. y/o en otros países.

Puppet es una marca comercial o una marca comercial registrada de Puppet, Inc.

Python es una marca comercial o una marca comercial registrada de Python Software Foundation.

Red Hat, Fedora y Red Hat Enterprise Linux son marcas comerciales o marcas registradas de Red Hat, Inc. o sus filiales en Estados Unidos y otros países.

Ansible es una marca registrada de Red Hat Inc. en los Estados Unidos y en otros países.

CentOS es una marca comercial o una marca registrada de Red Hat, Inc. o sus filiales en Estados Unidos y otros países.

La marca comercial BlackBerry es propiedad de Research In Motion Limited y está registrada en los Estados Unidos. Su registro puede estar pendiente o haber sido concedido en otros países.

Rocky Linux es una marca registrada de The Rocky Enterprise Software Foundation.

Samsung es una marca comercial de SAMSUNG en los Estados Unidos o en otros países.

Debian es una marca registrada de Software in the Public Interest, Inc.

Splunk y SPL son marcas comerciales y marcas comerciales registradas de Splunk Inc. en los Estados Unidos y en otros países.

SUSE es una marca registrada de SUSE LLC en los Estados Unidos y en otros países.

La marca Symbian es propiedad de Symbian Foundation Ltd.

OpenAPI es una marca de The Linux Foundation.

UNIX es una marca registrada en los Estados Unidos y en otros países, licenciada exclusivamente a través de X/Open Company Limited.

Zabbix es una marca registrada de Zabbix SIA.