kaspersky

Kaspersky Security Center 14 Linux

Contenido

Configuración de la tarea
Configuración de programa
Consola de administración
Copia de seguridad de los datos del Servidor de administración
Derechos de administrador
Directiva
Dispositivos administrados
Dominio de difusión
Estación de trabajo del administrador
Estado de protección
Estado de protección de la red
Gravedad de un evento
Grupo de administración
Grupo de aplicaciones con licencia
Grupo de roles
HTTPS
Instalación local
Instalación manual
Instalación remota
JavaScript
Kaspersky Private Security Network (KSN Privada)
Kaspersky Security Center System Health Validator (SHV)
Operador de Kaspersky Security Center
Paquete de instalación
Perfil
Perfil de aprovisionamiento
Perfil de configuración
Periodo de vigencia de la licencia
Propietario del dispositivo
Protección antivirus para redes
Proveedor de servicios de protección antivirus
Puerta de enlace de conexión
Punto de distribución
Repositorio de eventos
Restauración
Restauración de los datos del Servidor de administración
Servidor de administración
Servidor de administración doméstico
Servidor de administración virtual
Servidor web de Kaspersky Security Center
Servidores de actualizaciones de Kaspersky
SSL
Tarea
Tarea de grupo
Tarea local
Tarea para dispositivos específicos
Tienda de aplicaciones
Usuarios internos

Ayuda de Kaspersky Security Center 14 Linux

	**Novedades** Descubra las novedades de la última versión de la aplicación.		**Aplicaciones de Kaspersky. Licencias y activación** Active las aplicaciones de Kaspersky en unos pocos pasos.
	**Requisitos de hardware y software** Compruebe qué sistemas operativos y versiones de aplicaciones son compatibles.		**Configurar la protección de la red** Administrar la seguridad de la organización.
	**Instalación** Instale el Servidor de administración y Kaspersky Security Center Web Console 14.		**Aplicaciones de Kaspersky. Actualización de bases de datos y módulos de software** Mantenga la fiabilidad del sistema de protección.
	**Descubrimiento de dispositivos conectados a la red** Descubra los dispositivos nuevos y existentes en la red de su organización.		**Supervisión e informes** Ver su infraestructura, estados de protección y estadísticas.
	**Aplicaciones de Kaspersky. Despliegue centralizado** Despliegue aplicaciones de Kaspersky.		**Ajuste de puntos de distribución y puertas de enlace de conexión** Configure sus puntos de distribución.

Novedades

Kaspersky Security Center 14 Linux

Kaspersky Security Center 14 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 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.

Acerca del Kaspersky Security Center Linux

Esta sección incluye información acerca del objetivo de Kaspersky Security Center Linux y de sus características y componentes principales.

Kaspersky Security Center Linux (también llamado Kaspersky Security Center) está diseñado para implementar y administrar la protección de dispositivos Linux® mediante un Servidor de administración basado en Linux para cumplir con los requisitos de los entornos Linux puros.

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 Kaspersky Security Center que tiene un Servidor de administración basado en Windows®, Kaspersky Security Center Linux tiene un conjunto de características diferentes.

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.

- Realice 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.

- 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.

Kit de distribución

Puede comprar la aplicación a través de las tiendas en línea de Kaspersky (por ejemplo, en https://latam.kaspersky.com) o a través de empresas asociadas.

Si compra Kaspersky Security Center Linux en una tienda en línea, copiará la aplicación desde el sitio web de la tienda. La información requerida para la activación de la aplicación se envía por correo electrónico después del pago.

Requisitos de hardware y software

Servidor de administración

Requisitos de hardware mínimos:

- CPU con una frecuencia de funcionamiento de 1 GHz o más. Para sistemas operativos de 64 bits, la frecuencia mínima admisible es de 1.4 GHz.
- RAM: 4 GB.
- Espacio disponible en disco: 10 GB

Se admiten los siguientes sistemas operativos:

- Debian GNU/Linux 11.x (Bullseye) (32 bits o 64 bits)
- Debian GNU/Linux 10.x (Buster) (32 bits o 64 bits)
- Debian GNU/Linux 9.x (Stretch) (32 bits o 64 bits)
- Ubuntu Server 20.04 LTS (Focal Fossa) (64 bits)
- Ubuntu Server 18.04 LTS (Bionic Beaver) (64 bits)
- CentOS 7.x (64 bits)
- Red Hat Enterprise Linux Server 8.x (64 bits)
- Red Hat Enterprise Linux Server 7.x (64 bits)
- SUSE Linux Enterprise Server 12, todos los Service Pack (64 bits)
- SUSE Linux Enterprise Server 15, todos los Service Pack (64 bits)
- Astra Linux Special Edition 1.7 (incluido el modo de entorno de software cerrado y el modo obligatorio) 64 bits
- Astra Linux Special Edition 1.6 (incluido el modo de entorno de software cerrado y el modo obligatorio) (64 bits)
- Astra Linux Common Edition 2.12 (64 bits)
- Alt Server 10 (64 bits)
- Alt Server 9.2 (64 bits)
- Alt 8 SP Server (LKNV.11100-01) (64 bits)
- Alt 8 SP Server (LKNV.11100-02) (64 bits)

- Alt 8 SP Server (LKNV.11100-03) (64 bits)
- Oracle Linux 7 (64 bits)
- Oracle Linux 8 (64 bits)
- RED OS 7.3 Server (64 bits)
- RED OS 7.3 Certified Edition (64 bits)

Se admiten las siguientes plataformas de virtualización:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware Workstation 16 Pro
- Microsoft Hyper-V Server 2012 (64 bits)
- Microsoft Hyper-V Server 2012 R2 (64 bits)
- Microsoft Hyper-V Server 2016 (64 bits)
- Microsoft Hyper-V Server 2019 (64 bits)
- Microsoft Hyper-V Server 2022 (64 bits)
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 17
- KVM. Se admiten los siguientes sistemas operativos:
  - Alt 8 SP Server (LKNV.11100-01) (64 bits)
  - Alt Server 10 (64 bits)
  - Astra Linux Special Edition 1.7 (incluido el modo de entorno de software cerrado y el modo obligatorio) 64 bits
  - Debian GNU/Linux 11.x (Bullseye) (32 bits o 64 bits)
  - Ubuntu Server 20.04 LTS (Focal Fossa) (64 bits)
  - RED OS 7.3 Server (64 bits)
  - RED OS 7.3 Certified Edition (64 bits)

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

- MySQL 5.7 Community (32 bits o 64 bits)

- MySQL 8.0 (32 bits o 64 bits)
- MariaDB 10.5.x (32 bits o 64 bits)
- MariaDB 10.4.x (32 bits o 64 bits)
- MariaDB 10.3.22 y versiones posteriores (32 bits o 64 bits)
- MariaDB Server 10.3 (32 bits o 64 bits) con motor de almacenamiento InnoDB
- MariaDB 10.1.30 y versiones posteriores (32 bits o 64 bits)

Kaspersky Security Center 14 Web Console

Servidor de Kaspersky Security Center 14 Web Console

Requisitos de hardware mínimos:

- CPU: 4 núcleos, frecuencia de funcionamiento de 2.5 GHz
- RAM: 8 GB.
- Espacio disponible en disco: 40 GB

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

- Debian GNU/Linux 11.x (Bullseye)
- Debian GNU/Linux 10.x (Buster)
- Debian GNU/Linux 9.x (Stretch)
- Ubuntu Server 20.04 LTS (Focal Fossa)
- Ubuntu Server 18.04 LTS (Bionic Beaver)
- CentOS 7.x
- Red Hat Enterprise Linux Server 8.x
- Red Hat Enterprise Linux Server 7.x
- SUSE Linux Enterprise Server 12 (todos los Service Pack)
- SUSE Linux Enterprise Server 15 (todos los Service Pack)
- SUSE Linux Enterprise Desktop 15 (Service Pack 3) (ARM de 64 bits)
- Astra Linux Special Edition 1.7 (incluido el modo de entorno de software cerrado y el modo obligatorio)
- Astra Linux Special Edition 1.6 (incluido el modo de entorno de software cerrado y el modo obligatorio)
- Astra Linux Common Edition 2.12

- Alt Server 10
- Alt Server 9.2
- Alt 8 SP Server (LKNV.11100-01)
- Alt 8 SP Server (LKNV.11100-02)
- Alt 8 SP Server (LKNV.11100-03)
- Oracle Linux 8
- Oracle Linux 7
- RED OS 7.3 Server
- RED OS 7.3 Certified Edition

De entre las plataformas de virtualización, se admite KVM en los siguientes sistemas operativos:

- Alt 8 SP Server (LKNV.11100-01) (64 bits)
- Alt Server 10 (64 bits)
- Astra Linux Special Edition 1.7 (incluido el modo de entorno de software cerrado y el modo obligatorio) 64 bits
- Debian GNU/Linux 11.x (Bullseye) (32 bits o 64 bits)
- Ubuntu Server 20.04 LTS (Focal Fossa) (64 bits)
- RED OS 7.3 Server (64 bits)
- RED OS 7.3 Certified Edition (64 bits)

Dispositivos cliente

Para usar Kaspersky Security Center 14 Web Console en un dispositivo cliente, solo se necesita un navegador.

Los requisitos de hardware y software para el dispositivo serán los que imponga el navegador con el que se acceda a Kaspersky Security Center 14 Web Console.

Navegadores:

- Mozilla Firefox Extended Support Release 91.8.0 y versiones posteriores (la versión 91.8.0 se publicó el 5 de abril de 2022)
- Mozilla Firefox 99.0 y versiones posteriores (la versión 99.0 se publicó el 5 de abril de 2022)
- Google Chrome 100.0.4896.88 y versiones posteriores (compilación oficial)
- Microsoft Edge 100 y versiones posteriores
- Safari 15 en macOS

Agente de red

Requisitos de hardware mínimos:

- CPU con una frecuencia de funcionamiento de 1 GHz o más. Para sistemas operativos de 64 bits, la frecuencia mínima admisible es de 1.4 GHz.
- RAM: 512 MB.
- Espacio disponible 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.

Se admiten los siguientes sistemas operativos:

- Debian GNU/Linux 11.x (Bullseye) (32 bits o 64 bits)
- Debian GNU/Linux 10.x (Buster) (32 bits o 64 bits)
- Debian GNU/Linux 9.x (Stretch) (32 bits o 64 bits)
- Ubuntu Server 20.04 LTS (Focal Fossa) (32 bits o 64 bits)
- Ubuntu Server 20.04.04 LTS (Focal Fossa) (ARM de 64 bits)
- Ubuntu Server 18.04 LTS (Bionic Beaver) (32 bits o 64 bits)
- Ubuntu Desktop 20.04 LTS (Focal Fossa) (32 bits o 64 bits)
- Ubuntu Desktop 18.04 LTS (Bionic Beaver) (32 bits o 64 bits)
- CentOS 8.x (64 bits)
- CentOS 7.x (64 bits)
- CentOS 7.x (ARM de 64 bits)
- Red Hat Enterprise Linux Server 8.x (64 bits)
- Red Hat Enterprise Linux Server 7.x (64 bits)
- Red Hat Enterprise Linux Server 6.x (32 bits o 64 bits)
- SUSE Linux Enterprise Server 12, todos los Service Pack (64 bits)
- SUSE Linux Enterprise Server 15, todos los Service Pack (64 bits)
- SUSE Linux Enterprise Desktop 15, todos los Service Pack (64 bits)
- SUSE Linux Enterprise Desktop 15 (Service Pack 3) (ARM de 64 bits)
- openSUSE 15 (64 bits)
- EulerOS 2.0 SP8 (ARM)

- Pardus OS 19.1 (64 bits)
- Astra Linux Special Edition 1.7 (incluido el modo de entorno de software cerrado y el modo obligatorio) 64 bits
- Astra Linux Special Edition 1.6 (incluido el modo de entorno de software cerrado y el modo obligatorio) (64 bits)
- Astra Linux Common Edition 2.12 (64 bits)
- Astra Linux Special Edition 4.7 (ARM)
- Alt Server 10 (64 bits)
- Alt Server 9.2 (64 bits)
- Alt Workstation 10 (32 bits o 64 bits)
- Alt Workstation 9.2 (32 bits o 64 bits)
- Alt 8 SP Server (LKNV.11100-01) (64 bits)
- Alt 8 SP Server (LKNV.11100-02) (64 bits)
- Alt 8 SP Server (LKNV.11100-03) (64 bits)
- Alt 8 SP Workstation (LKNV.11100-01) (32 bits 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)
- Mageia 4 (32 bits)
- Oracle Linux 7 (64 bits)
- Oracle Linux 8 (64 bits)
- Linux Mint 19.x (32 bits)
- Linux Mint 20.x (64 bits)
- AlterOS 7.5 y versiones posteriores (64 bits)
- GosLinux IC6 (64 bits)
- RED OS 7.3 (64 bits)
- RED OS 7.3 Server (64 bits)
- RED OS 7.3 Certified Edition (64 bits)
- ROSA Enterprise Linux Server 7.3 (64 bits)
- ROSA Enterprise Linux Desktop 7.3 (64 bits)
- ROSA COBALT Workstation 7.3 (64 bits)

- ROSA COBALT Server 7.3 (64 bits)
- Lotos (versión del núcleo Linux: 4.19.50; entorno de escritorio: MATE) (64 bits)

Se admiten las siguientes plataformas de virtualización:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware Workstation 16 Pro
- Microsoft Hyper-V Server 2012 (64 bits)
- Microsoft Hyper-V Server 2012 R2 (64 bits)
- Microsoft Hyper-V Server 2016 (64 bits)
- Microsoft Hyper-V Server 2019 (64 bits)
- Microsoft Hyper-V Server 2022 (64 bits)
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- KVM. Se admiten los siguientes sistemas operativos:
  - Alt 8 SP Server (LKNV.11100-01) (64 bits)
  - Alt Server 10 (64 bits)
  - Astra Linux Special Edition 1.7 (incluido el modo de entorno de software cerrado y el modo obligatorio) 64 bits
  - Debian GNU/Linux 11.x (Bullseye) (32 bits o 64 bits)
  - Ubuntu Server 20.04 LTS (Focal Fossa) (64 bits)
  - RED OS 7.3 (64 bits)
  - RED OS 7.3 Server (64 bits)
  - RED OS 7.3 Certified Edition (64 bits)

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

Acerca de Kaspersky Security Center 14 Web Console

Kaspersky Security Center 14 Web Console es una aplicación web diseñada para administrar el estado del sistema de seguridad de la red protegida por las aplicaciones de Kaspersky.

El uso de la aplicación le permite hacer lo siguiente:

- Administrar el estado del sistema de seguridad de su organización.
- Instalar aplicaciones de Kaspersky en dispositivos de su red y administrar las aplicaciones instaladas.
- Administrar directivas creadas para sus dispositivos conectados en red.
- Administrar de cuentas de usuario.
- Gestione tareas para aplicaciones instaladas en sus dispositivos de red.
- Ver los informes sobre el estado del sistema de seguridad.
- Administrar la entrega de informes a los administradores del sistema y otros expertos en TI.

Kaspersky Security Center 14 Web Console proporciona una interfaz web que garantiza la interacción entre su dispositivo y el Servidor de administración a través de un navegador. El Servidor de administración es una aplicación diseñada para administrar las aplicaciones Kaspersky instaladas en los dispositivos de red. El Servidor de administración se conecta a los dispositivos de su red a través de canales protegidos por el protocolo SSL. Cuando se conecta a Kaspersky Security Center 14 Web Console con su navegador, el navegador establece una conexión con Servidor de Kaspersky Security Center 14 Web Console.

Kaspersky Security Center 14 Web Console funciona de la siguiente manera:

1. Utilice un navegador para conectarse a Kaspersky Security Center 14 Web Console, donde se muestran la interfaz del portal web.
2. Utilice los controles del portal web para elegir un comando que desee ejecutar. Kaspersky Security Center 14 Web Console realiza las siguientes operaciones:
    - Si selecciona un comando utilizado para recibir información (por ejemplo, para ver una lista de dispositivos), Kaspersky Security Center 14 Web Console genera una solicitud de información para el Servidor de administración, recibe los datos necesarios y los envía al navegador en un formato de fácil visualización.
    - Si seleccionó un comando utilizado para la administración (por ejemplo, instalación remota de una aplicación), Kaspersky Security Center 14 Web Console recibe el comando desde el navegador y lo envía al Servidor de administración. A continuación, la aplicación recibe el resultado del Servidor de administración y lo envía al navegador en un formato de fácil visualización.

Kaspersky Security Center 14 Web Console es una aplicación multilingüe. Puede cambiar el idioma de la interfaz en cualquier momento, sin necesidad de cerrar y volver a abrir la aplicación. Al instalar Kaspersky Security Center 14 Web Console junto con Kaspersky Security Center, Kaspersky Security Center 14 Web Console tiene el mismo idioma de interfaz que el archivo de instalación. Cuando solo instala Kaspersky Security Center 14 Web Console, la aplicación tiene el mismo idioma de la interfaz que su sistema operativo. Si Kaspersky Security Center 14 Web Console no admite el idioma del archivo de instalación o del sistema operativo, el idioma inglés se configura de forma predeterminada.

Lista de aplicaciones de Kaspersky admitidas

Kaspersky Security Center Linux admite la implementación y administración centralizadas de Kaspersky Endpoint Security para Linux. Esta aplicación permite proteger tanto estaciones de trabajo como servidores de archivos. Consulte la Página web del ciclo de vida del soporte del producto para las versiones de las aplicaciones.

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 basada en Windows, instala el Servidor de administración en un dispositivo Windows y la solución basada en Linux tiene la versión del Servidor de administración que está diseñada para instalarse en un dispositivo Linux.

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	
	Solución basada en Windows	**Solución basada en Linux**
Ubicación del Servidor de administración	En las instalaciones	En las instalaciones
Ubicación del sistema de administración de bases de datos (DBMS)	En las instalaciones	En las instalaciones
Sistema operativo para instalar el Servidor de administración en	Windows	Linux
Tipo de consola de administración	En las instalaciones y basado en la web	Basado en la web
Sistema operativo para instalar la consola de administración basada en web en	Windows o Linux	Windows o Linux
Jerarquía de servidores de administración	✓	✓
Jerarquía de grupos de administración	✓	✓
Sondeo de red	✓	✓ (solo por rangos de IP)
Número de dispositivos administrados	100000	20000
Protección de dispositivos administrados: Windows, Linux y macOS	✓	– (protección de dispositivos Linux solamente)
Protección de dispositivos móviles.	✓	–
Protección de máquinas virtuales	✓	–
Protección de infraestructura de nube pública	✓	–
Gestión de seguridad centrada en dispositivos	✓	✓
Gestión de seguridad centrada en el usuario	✓	✓
Directivas para aplicaciones	✓	✓
Tareas para aplicaciones de Kaspersky	✓	✓
Kaspersky Security Network	✓	–

Proxy de KSN	✓	–
Kaspersky Private Security Network	✓	–
Implementación centralizada de claves de licencia para aplicaciones de Kaspersky	✓	✓
Compatibilidad con servidores de administración virtuales	✓	✓
Instalación de actualizaciones de software de terceros y reparación de vulnerabilidades de software de terceros	✓	– (usando solo una tarea de instalación remota)
Notificaciones sobre eventos ocurridos en dispositivos administrados	✓	✓
Creación y gestión de cuentas de usuario	✓	✓
Supervisión del estado de las directivas y tareas	✓	✓
Despliegue del clúster de conmutación por error de Kaspersky	✓	✓

Conceptos básicos

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

Servidor de administración

Los componentes de Kaspersky Security Center 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 "Servidor de administración de Kaspersky Security Center"
- Configurado para iniciarse automáticamente junto con el sistema operativo
- Con la cuenta **LocalSystem** o la cuenta de usuario seleccionada durante la instalación del Servidor de administración

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 14, 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 14 Web Console instalado en un dispositivo Linux, la aplicación muestra los nombres de los Servidores de administración que especificó como confiables en el archivo de respuesta.

Puede conectarse al Servidor de administración a través de Kaspersky Security Center Web Console 14.

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.

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

En una jerarquía, el Servidor de administración de Linux en Kaspersky Security Center solo puede funcionar como un Servidor secundario manejado por un Servidor de administración principal de Kaspersky Security Center basado en Windows o Kaspersky Security Center Cloud Console.

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.

- De qué manera los proveedores de servicios usan Kaspersky Security Center. Los proveedores de servicios únicamente necesitan instalar Kaspersky Security Center y Kaspersky Security Center 14 Web Console. Para administrar un gran número de dispositivos cliente de varias organizaciones, un proveedor de servicios puede agregar Servidores de administración virtuales a una 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 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 reinicia el Servidor de administración principal y todos los Servidores de administración virtuales.

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://<nombre del Servidor web>:<puerto HTTPS>/public/<objeto>`

donde:

- `<nombre del Servidor web>` es el nombre del Servidor web de Kaspersky Security Center.
- `<puerto HTTPS>` es un puerto HTTPS del Servidor web 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 el 8061.
- `<objeto>` es una subcarpeta o archivo al cual 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.

Agente de red

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

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

- Con el nombre "Agente de red de Kaspersky Security Center 14 Linux"
- Configurado para iniciarse automáticamente junto con el sistema operativo
- se ejecuta utilizando la cuenta LocalSystem.

Un dispositivo que tiene el Agente de red instalado se denomina *dispositivo administrado* o *dispositivo*. Puede obtener el Agente de red de una de las siguientes fuentes:

- Paquete de instalación almacenado en el Servidor de administración (para usar esta fuente, el Servidor de administración debe estar instalado)
- Paquete de instalación publicado en los servidores web de Kaspersky

No es necesario instalar el Agente de red en el dispositivo donde se instala el Servidor de administración, ya que la versión de servidor de del Agente de red se instala automáticamente junto con el Servidor de administración.

Los nombres de los procesos que el Agente de red inicia son los siguientes:

- klnagent64.service (para un sistema operativo de 64 bits)

- klnagent32.service (para un sistema operativo de 32 bits)

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* (de ahora en adelante *grupo*) es un conjunto lógico de dispositivos administrados que se han combinado en función de un rasgo específico para que se los pueda administrar como una única unidad de Kaspersky Security Center.

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 equipo que utiliza esa persona del grupo de administración Contadores al grupo de administración Desarrolladores. Al efectivizarse el traspaso, el equipo recibirá automáticamente la configuración que los desarrolladores requieren para sus aplicaciones.

Dispositivo administrado

Un *dispositivo administrado* es una computadora que ejecuta Linux y que tiene el Agente de red instalado. 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. Nuestro Servidor de administración admite un máximo de 20 000 dispositivos.

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

Los dispositivos en los que se instaló Kaspersky Security Center Web Console 14 se denominan *estaciones 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

Un componente especial, el *complemento web de administración*, se utiliza para la administración remota del software Kaspersky a través de Kaspersky Security Center 14 Web Console. 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 14 Web Console y una aplicación específica de Kaspersky. El complemento de administración permite configurar tareas y directivas para esa aplicación.

Puede descargar complementos web de administración desde la página web de atención al cliente 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
- Funciones de Kaspersky Security Center 14 Web Console para mostrar los datos de los sistemas y los eventos de la aplicación y las estadísticas transmitidas desde 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. La directiva tiene 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 evitar la creación de varias instancias de una sola directiva, Kaspersky Security Center 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

Kaspersky Security Center administra las aplicaciones de seguridad de Kaspersky instaladas en los dispositivos mediante la creación y ejecución de *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
- Creación de un paquete de instalación basado en la imagen del SO de un dispositivo de referencia

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, a través de la interfaz de aplicaciones 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 las tareas se guardan en el registro de eventos y en el registro de eventos de Kaspersky Security Center, tanto de forma centralizada 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.

- 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 (vea la siguiente imagen) 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.

Directiva y parámetros locales 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 la información relativa a los dispositivos en red. 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 pasarela a los dispositivos de un grupo de administración para que se conecten con el Servidor 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.

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 que tiene 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 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 incidente con el nivel de importancia *Advertencia*. El incidente se publicará en las propiedades del dispositivo, en la sección **Incidentes**.

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.

Licencias

En esta sección encontrará información sobre los conceptos generales relacionados con la licencia de Kaspersky Security Center 14.

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 a través de los siguientes métodos:

- 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 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.

  Tenga en cuenta que, cuando instala el Agente de red para Linux, el Contrato de licencia de usuario final para el Agente de red se muestra en inglés. Puede consultar el Contrato de licencia de usuario final para el Agente de red en otros idiomas en la carpeta /opt/kaspersky/klnagent64/share/license antes de aceptar los términos del Contrato de licencia de usuario final durante la instalación.

- 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.

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 la aplicación por un tiempo limitado en el marco del Contrato de licencia de usuario final.

Una licencia le da derecho a los siguientes tipos de servicios:

- El uso de la aplicación de conformidad con los términos del Contrato de licencia de usuario final
- Recibir soporte técnico

El alcance de los servicios y el período de validez dependen del tipo de licencia que se utiliza para activar la aplicación.

Se ofrecen los siguientes tipos de licencia:

- *De prueba*. Se trata de 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 se deshabilitan. Para continuar usando la aplicación, se debe adquirir una licencia comercial.

  La aplicación puede activarse con una licencia de prueba solo una vez.

- *Comercial*. Se trata de una licencia paga, otorgada al comprar la aplicación.

  Cuando la licencia comercial caduca, la aplicación se continúa ejecutando, pero con funcionalidad limitada (por ejemplo, se pierde la capacidad de actualizar las bases de datos de Kaspersky Security Center). Para continuar usando todas las funciones de Kaspersky Security Center, debe renovar su licencia comercial.

Se recomienda renovar la licencia antes de que caduque para garantizar la máxima protección posible contra las amenazas a la seguridad.

Acerca del certificado de licencia

Un *certificado de licencia* es un documento que se entrega adjunto a un archivo de clave o código de activación.

El certificado de licencia contiene la siguiente información sobre la licencia otorgada:

- Clave de licencia o número de pedido
- Información sobre el usuario al que se le ha otorgado 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 en que comienza la validez 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 una clave que actualmente utiliza la aplicación. 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://www.kaspersky.com/products-and-services-privacy-policy.

La Política de privacidad también está disponible sin conexión:

- Puedes leer la Política de privacidad antes de instalar Kaspersky Security Center.
- El texto de la Política de privacidad se incluye en el archivo license.txt, en la carpeta de instalación de Kaspersky Security Center.
- 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 se entrega como parte de las aplicaciones de Kaspersky para la protección de redes corporativas. También se puede descargar desde el sitio web de Kaspersky.

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.
- Control del estado de la seguridad antivirus de una organización.

- Instalación remota de aplicaciones.
- Visualización de la lista de imágenes de sistema operativo disponibles para la instalación remota.
- La configuración centralizada de aplicaciones instaladas en dispositivos cliente.
- Enumeración y modificación de los grupos de aplicaciones con licencia existentes.
- Estadísticas e informes sobre el funcionamiento de la aplicación, así como notificaciones sobre eventos críticos.
- Visualización y edición manual de la lista de componentes de hardware que detectó el sondeo de la red.
- Operaciones centralizadas con archivos que se movieron a la cuarentena o copia de seguridad y archivos cuyo procesamiento se pospuso.
- Administración de roles de usuario.

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.

Puede restaurar un archivo de clave si se ha eliminado accidentalmente. Es posible que necesite un archivo de clave para registrar una cuenta de Kaspersky CompanyAccount, por ejemplo.

Para recuperar el archivo de clave, realice cualquiera de las siguientes acciones:

- Póngase en contacto con el vendedor de la licencia.
- Reciba un archivo de clave a través del sitio web de Kaspersky mediante su código de activación disponible.

Sobre la provisión de datos

Datos transferidos al Titular del derecho

Proporcionado en el Contrato de licencia de usuario final de Kaspersky Security Center 14 Linux.

Datos procesados localmente

Kaspersky Security Center 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
- 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

Para realizar sus funciones principales, Kaspersky Security Center Linux puede recibir, almacenar y procesar la siguiente información:

- Información sobre los dispositivos conectados a la red de la organización, recibida mediante el análisis de intervalos IP. El Servidor de administración recaba datos de forma independiente o recibe información del Agente de red.
- 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 14 Web Console:
    - Especificaciones técnicas del dispositivo administrado y de sus componentes necesarias para identificar el dispositivo: nombre y descripción del dispositivo; dominio DNS y nombre DNS; dirección IPv4; dirección IPv6; ubicación de red; dirección MAC; tipo de sistema operativo; indicación de si el dispositivo es una máquina virtual y tipo de hipervisor; indicación de si el dispositivo es una máquina virtual dinámica que forma parte de una VDI.
    - Otras especificaciones de dispositivos administrados y sus componentes necesarios para la auditoría de dispositivos administrados: 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, si el dispositivo es una máquina virtual, el tipo de máquina virtual.
    - 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.
- 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 ingresada por el usuario en Kaspersky Security Center 14 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.

- 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 14 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 14 Web Console.

- Datos tratados por la función Administración de vulnerabilidades y parches. El Agente de red transfiere desde el dispositivo al Servidor de administración información sobre el hardware detectado en los dispositivos administrados (registro de Hardware).

- Categorías de aplicaciones creadas por el usuario. El usuario ingresa datos en la interfaz de Kaspersky Security Center 14 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.

- 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.

- 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.

- Detalles de los códigos de activación ingresados. El usuario ingresa datos en la Consola de administración o en la interfaz de Kaspersky Security Center 14 Web Console.

- Cuentas de usuario: nombre, descripción, nombre completo, dirección de correo electrónico, número de teléfono principal y contraseña. El usuario ingresa datos en la interfaz de Kaspersky Security Center 14 Web Console.

- Historial de revisiones de los objetos de administración. El usuario ingresa datos en la interfaz de Kaspersky Security Center 14 Web Console.

- Registro de objetos de administración eliminados. El usuario ingresa datos en la interfaz de Kaspersky Security Center 14 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 14 Web Console.

- Datos necesarios para mostrar comunicaciones de Kaspersky en Kaspersky Security Center 14 Web Console. El usuario ingresa datos en la interfaz de Kaspersky Security Center 14 Web Console.

- Datos que se necesitan para el funcionamiento de los complementos de las aplicaciones administradas en Kaspersky Security Center 14 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 14 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 14 Web Console.

- Registro de eventos de Kaspersky para los componentes de Kaspersky Security Center Linux y las aplicaciones de Kaspersky administradas. El registro de eventos de Kaspersky se almacena en cada dispositivo y nunca se transfiere al Servidor de administración.

- Certificado utilizado para establecer una conexión segura entre los dispositivos administrados y los componentes de Kaspersky Security Center Linux. El usuario ingresa datos en la interfaz de Kaspersky Security Center 14 Web Console.

- Datos del Servidor de administración que el usuario ingresa en la interfaz de Kaspersky Security Center 14 Web Console.

- Cualquier dato que el usuario ingresa en la interfaz de Kaspersky Security Center 14 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 14 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 y el Agente de red a los que se le asignó un punto de distribución recopilan información sobre los dispositivos de la red.

Los datos detallados se almacenan en la base de datos del Servidor de administración. Los nombres de usuario y las contraseñas se almacenan de 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).

Kaspersky protege toda la información que recibe según las exigencias de la ley y según las reglas de Kaspersky pertinentes. Los datos se transmiten a través de un canal seguro.

Al seguir los vínculos de la Consola de administración o de Kaspersky Security Center 14 Web Console, el usuario da su consentimiento para que los siguientes datos se transfieran en forma automática:

- Código de Kaspersky Security Center Linux
- Versión de Kaspersky Security Center Linux
- Ubicación de Kaspersky Security Center Linux
- Id. de 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 recibidos en forma anónima y solo con fines estadísticos generales. La información recibida se utiliza para generar estadísticas de resumen, que no contienen ningún tipo de dato personal o confidencial. Según se acumulan nuevos datos, se borran los datos más antiguos (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 necesita renovar su suscripción, puede hacerlo en el sitio web de su proveedor de servicios.

Eventos sobre límites de licencia superados

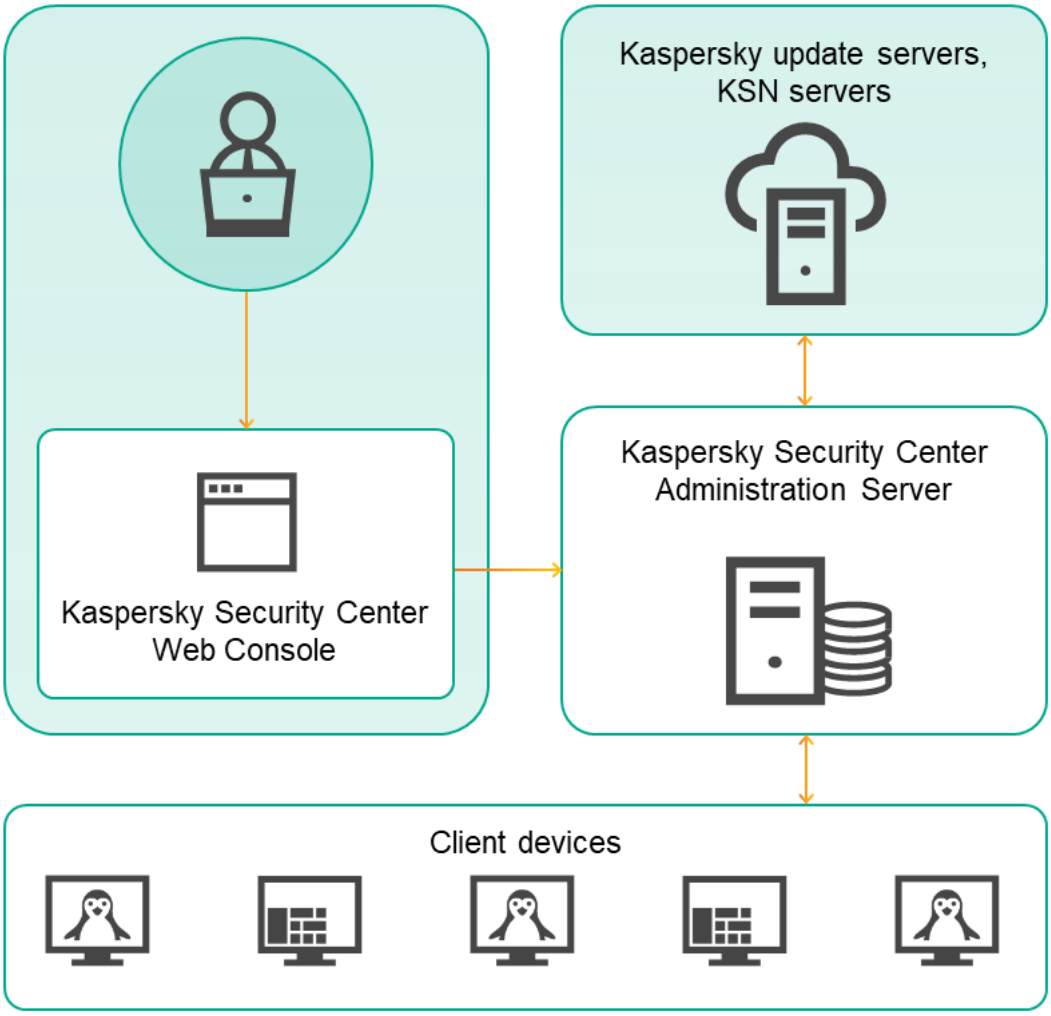
Kaspersky Security Center Linux le permite obtener información sobre eventos cuando las aplicaciones de Kaspersky instaladas en dispositivos cliente superan ciertos límites de licencia.

El nivel de importancia de estos eventos se define sobre la base de estas 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**.

Arquitectura

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



Arquitectura de Kaspersky Security Center 14 Linux

Kaspersky Security Center 14 Linux está compuesto 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 rápidamente a las amenazas, mejora el rendimiento de algunos componentes de protección y reduce la probabilidad de encontrarse con falsos positivos.
- **Dispositivos del cliente.** Dispositivos de la empresa cliente protegidos por Kaspersky Security Center 14 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 y Kaspersky Security Center 14 Web Console

La siguiente figura muestra el diagrama de despliegue del Servidor de administración de Kaspersky Security Center y Kaspersky Security Center 14 Web Console.

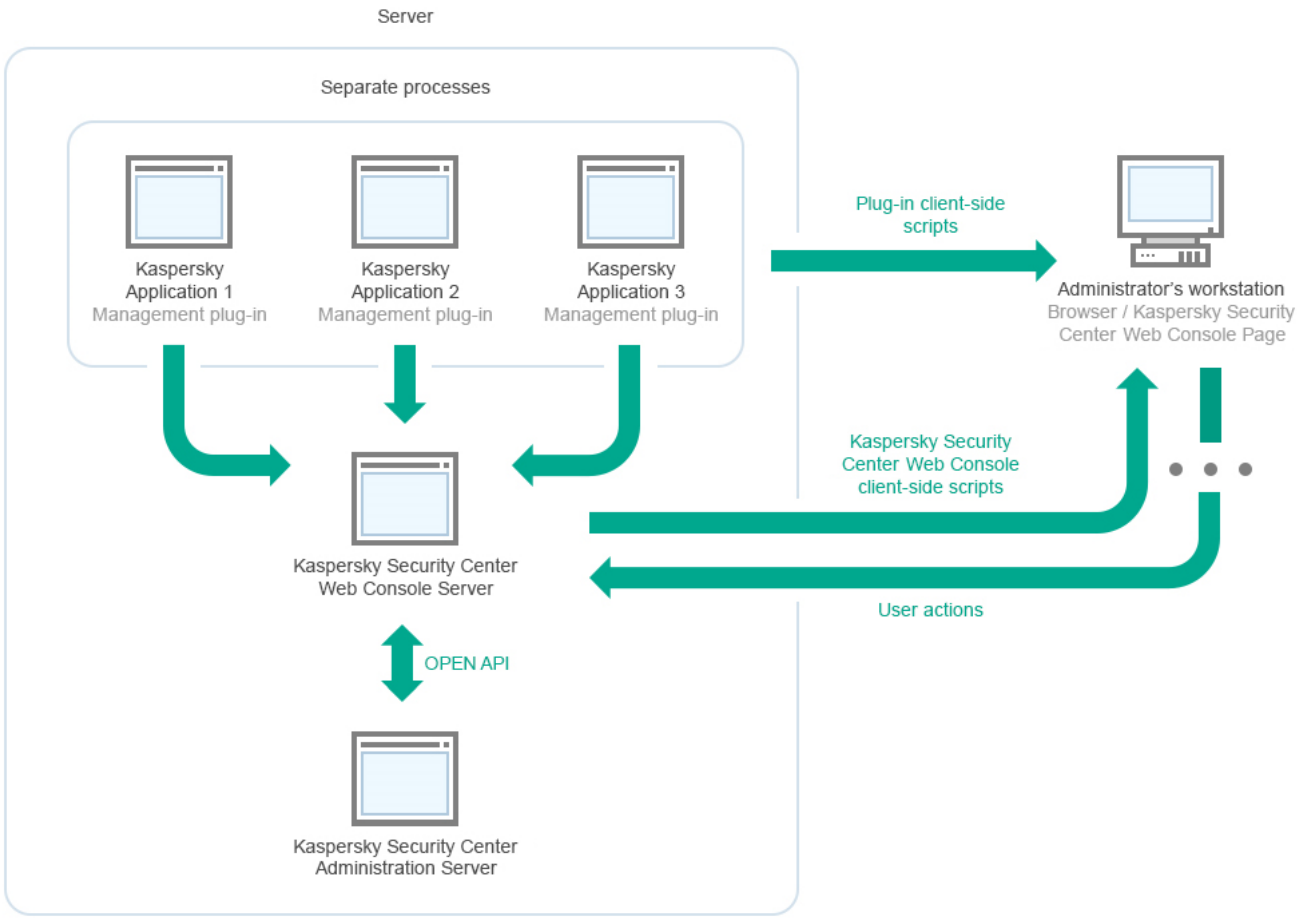


Diagrama de despliegue del Servidor de administración de Kaspersky Security Center y Kaspersky Security Center 14 Web Console

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 14 Web Console.

Como administrador, acceda a Kaspersky Security Center 14 Web Console usando un navegador en su estación de trabajo.

Cuando realice acciones específicas en Kaspersky Security Center 14 Web Console, el Servidor de Kaspersky Security Center 14 Web Console comunica con Servidor de administración de Kaspersky Security Center a través de OpenAPI. El Servidor de Kaspersky Security Center 14 Web Console solicita la información requerida de Servidor de administración de Kaspersky Security Center y muestra los resultados de sus operaciones en Kaspersky Security Center 14 Web Console.

Puertos usados por Kaspersky Security Center Linux

Las siguientes tablas muestran los puertos predeterminados que deben estar abiertos en el Servidor de administración y en 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.
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 recibir conexiones 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 recibir conexiones de los Servidores de administración al crear una 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.
13299	klserver	TCP (TLS)	Recepción de conexiones de Kaspersky Security Center 14 Web Console destinadas al Servidor de administración; recepción de conexiones para el Servidor de administración realizadas mediante OpenAPI	Kaspersky Security Center 14 Web Console, 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.
13111 (solo si el dispositivo está ejecutando el servicio Proxy de KSN)	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 dispositivo está ejecutando el servicio Proxy de KSN)	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.
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**).
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 14 Web Console. Puede cambiar el número de puerto predeterminado mediante la utilidad klscflag.

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 MariaDB). Consulte la documentación del DBMS para obtener la información necesaria.

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

Puerto usado por el servidor de Kaspersky Security Center Linux 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)	Recibiendo conexiones del navegador web al Kaspersky Security Center 14 Web Console	Kaspersky Security Center 14 Web Console. Puede cambiar el número de puerto predeterminado cuando instala Kaspersky Security Center 14 Web Console. Si instala Kaspersky Security Center 14 Web Console en el sistema operativo Linux ALT, deberá indicar un número de puerto distinto del 8080: el puerto 8080 es utilizado por el sistema operativo.

La siguiente tabla muestra el puerto que debe estar abierto en los dispositivos administrados en los que se instaló 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 mando enviadas por el Servidor de administración 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.

La siguiente tabla muestra los puertos que deben estar abiertos en un dispositivo administrado que tiene instalado el Agente de red y que se designó como punto de distribución. Los puertos enumerados deben estar abiertos en 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 los agentes de red	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 dispositivo está ejecutando el servicio Proxy de KSN)	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 dispositivo está ejecutando el servicio Proxy de KSN)	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.

Puertos usados por Kaspersky Security Center 14 Web Console

El dispositivo en el que instale el Servidor de Kaspersky Security Center 14 Web Console (también denominado Kaspersky Security Center 14 Web Console) debe tener abiertos los puertos que se indican en la siguiente tabla.

Puertos usados por Kaspersky Security Center 14 Web Console

Número de puerto	Nombre del servicio	Protocolo	Objetivo del puerto	Al
2001	KSCWebConsolePlugin	HTTPS	Puerto de API que utilizan los procesos del complemento de administración para recibir solicitudes provenientes de KSCWebConsoleManagementService	Ejecu proce node.e compl de admin
1329, 2003	KSCWebConsoleManagementService	HTTPS	Puertos API que se utilizan para recibir solicitudes del servicio KSCWebConsole que se ejecuta en el mismo dispositivo	Actua de los compo de Kas Secur Cente Conso
2005	KSCWebConsole	HTTPS	Puerto de la API. Se utiliza para recibir las solicitudes del servicio KSCWebConsoleManagementService, que se ejecuta en el mismo dispositivo.	Ejecu proce node.e Kaspe Secur Cente Conso
8200	—	HTTP	Puerto de la API. Se utiliza para generar certificados con HashiCorp Vault (para más información, visite el sitio web de HashiCorp Vault).	Instala Kaspe Secur Cente Web C y actu de los compo de Kas Secur Cente Web C
4150, 4151, 4152	KSCWebConsoleMessageQueue	HTTPS	Puertos API del agente de mensajes que se utilizan para la comunicación entre los procesos de Kaspersky Security Center 14 Web Console y los complementos de administración	Intera entre Kaspe Secur Cente Conso compl de admin

Instalación

Esta sección describe la instalación de Kaspersky Security Center y Kaspersky Security Center 14 Web Console.

Escenario de instalación principal

Este escenario describe cómo instalar el Servidor de administración de Kaspersky Security Center 14 y Kaspersky Security Center Web Console 14, realizar la configuración inicial del Servidor de administración utilizando 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 14 Linux, puede obtener una prueba gratuita de 30 días en el sitio web de Kaspersky.

Etapas

El escenario de instalación principal se desarrolla en etapas:

1. **Elija la estructura de protección adecuada para su organización**

   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).

   Decida si usará una jerarquía de servidores de administración en su organización. Para tomar esta decisión, evalúe si podría (y debería) cubrir todos sus dispositivos cliente con un solo Servidor de administración o si, por el contrario, debería definir una jerarquía de servidores de administración. En algunos casos, resulta necesario definir una jerarquía de servidores de administración que refleje la estructura organizativa de la organización cuya red se busca proteger.

2. **Realice los preparativos para usar 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. **Instalación de un sistema de gestión de bases de datos (DBMS)**

   Instale el DBMS que utilizará Kaspersky Security Center o utilice uno existente.

4. **Configure los puertos**

   Asegúrese de que se encuentren abiertos todos los puertos necesarios para permitir la interacción de los componentes en la estructura de seguridad seleccionada.

   Si tiene que brindar acceso a Internet al Servidor de administración, configure los puertos y defina los ajustes de conexión pertinentes para la configuración de su red.

5. **Instalación de Kaspersky Security Center**

Seleccione un dispositivo Linux que desee utilizar como Servidor de administración, asegúrese de que el dispositivo cumpla con los requisitos de software y hardware y, entonces, instale Kaspersky Security Center en el dispositivo. La versión de servidor del Agente de red se instala en el dispositivo junto con el Servidor de administración.

6. **Instalar Kaspersky Security Center Web Console 14 y los complementos de administración**

   Seleccione un dispositivo Linux que desee utilizar como estación de trabajo del administrador, asegúrese de que el dispositivo cumpla con los requisitos de software y hardware y, luego, instale Kaspersky Security Center Web Console 14 en el dispositivo. Kaspersky Security Center 14 Web Console se puede instalar en el mismo dispositivo en el que está instalado el servidor de administración, o en uno diferente.

   Descargue el complemento web de administración de Kaspersky Endpoint Security para Linux y luego instálelo en el mismo dispositivo donde está instalado Kaspersky Security Center 14 Web Console.

7. **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 contra virus y otras amenazas, y para administrar el dispositivo como cualquier otro dispositivo administrado, le recomendamos instalar Kaspersky Endpoint Security para 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.

8. **Realizar la configuración inicial**

   Cuando la instalación del Servidor de administración se completa, en la primera conexión con el Servidor de administración, el Asistente de inicio rápido se ejecuta automáticamente. Realice la configuración inicial del Servidor de administración según los requisitos existentes. 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.

9. **Detección de dispositivos de red**

   Descubra 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.

10. **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. Podrá asignar tareas de grupo a los grupos de administración, definir el alcance de las 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.

11. **Designar los puntos de distribución**

    Se asignan puntos de distribución a los grupos de administración automáticamente, pero usted puede asignarlos manualmente, si es necesario. 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.

12. **Instalación del Agente de red y aplicaciones de seguridad en dispositivos en red**

Despliegar 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 del 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).

13. **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.

14. **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.

15. **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.

Instalación de un sistema de gestión de bases de datos

Instale el sistema de administración de bases de datos (DBMS) que utilizará Kaspersky Security Center. Puede elegir entre uno de los DBMS admitidos.

Para obtener información sobre cómo instalar el DBMS seleccionado, consulte su documentación.

Si usa MariaDB, necesita configurar los ajustes recomendados para un trabajo óptimo del DBMS con Kaspersky Security Center.

Configurar el servidor MariaDB x64 para que funcione con Kaspersky Security Center 14 Linux

Si utiliza el servidor MariaDB para Kaspersky Security Center, habilite la compatibilidad del almacenamiento InnoDB y MEMORY y las codificaciones UTF-8 y UCS-2.

Configuraciones recomendadas del archivo my.cnf

Para configurar el archivo my.cnf:

1. Abra el archivo my.cnf en un editor de texto.
2. Escriba las siguientes líneas en el 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=<valor>
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
```

El valor de `innodb_buffer_pool_size` no debe ser inferior al 80 % del tamaño previsto de la base de datos KAV.

Se recomiendo usar el valor del parámetro `innodb_flush_log_at_trx_commit=0`, debido a que los valores "1" o "2" afectan de modo negativo la velocidad operativa de MariaDB.

De forma predeterminada, los complementos del optimizador `join_cache_incremental`, `join_cache_hashed`, y `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 el valor `on`, quiere decir que están habilitados los complementos optimizadores.

   Si estas líneas faltan o tienen el valor `off`, haga 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'
   ```

Están habilitados los complementos `join_cache_incremental`, `join_cache_hash` y `join_cache_bka`.

Instalación de Kaspersky Security Center

Este procedimiento describe cómo instalar Kaspersky Security Center.

Antes de la instalación:

- Instalación de un sistema de gestión de bases de datos.

- Asegúrese de que el dispositivo en el que desea instalar Kaspersky Security Center esté ejecutando una de las distribuciones de Linux compatibles.

Use el archivo de instalación que corresponda para la distribución de Linux instalada en su dispositivo (ksc-web-console-[número_de_versión].deb o ksc-web-console-[número_de_versión].x86_64.rpm). El archivo de instalación debe descargarse del sitio web de Kaspersky.

Instalar Kaspersky Security Center:

1. En la línea de comandos, ejecute los comandos provistos en esta instrucción bajo una cuenta con privilegios de raíz.

2. Cree un grupo 'kladmins' y una cuenta sin privilegios 'ksc'. La cuenta debe 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
   ```

3. Ejecute la instalación de Kaspersky Security Center. Según su distribución de Linux, ejecute uno de los siguientes comandos:

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

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

4. Ejecute la configuración de Kaspersky Security Center:
   ```
   # /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. Ingresar `y` si entiende y acepta los términos del EULA. Ingresar `n` si no acepta los términos del EULA. Para utilizar Kaspersky Security Center, debe aceptar los términos del EULA.

   b. Ingresar `y` si comprende y acepta los términos de la Política de privacidad, y acepta que sus datos se manejen y transmitan (incluso a terceros países) como se describe en la Política de privacidad. Ingresar `n` si no acepta los términos de la Política de privacidad. Para utilizar Kaspersky Security Center, debe aceptar los términos de la Política de privacidad.

6. Cuando se le solicite, ingrese la siguiente configuración:

   a. Ingrese el nombre DNS del Servidor de administración o la dirección IP estática.

   b. Introduzca el número de puerto del Servidor de administración. De manera predeterminada, se utiliza el puerto 14000.

   c. Introduzca el número de puerto SSL del Servidor de administración. De manera predeterminada, se utiliza el puerto 13000.

   d. Evalúe el número aproximado de dispositivos que pretende administrar:

      - Si tiene de 1 a 100 dispositivos en red, ingrese 1.

      - Si tiene de 101 a 1000 dispositivos en red, ingrese 2.

- Si tiene más de 1000 dispositivos en red, ingrese 3.

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 forma 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 forma predeterminada, se utiliza la cuenta 'ksc'.

h. Introduzca la dirección IP del dispositivo en el que está instalada la base de datos.

i. Introduzca el número de puerto de la base de datos. Este puerto se utiliza para comunicarse con el Servidor de administración. De manera predeterminada, se utiliza el puerto 3306.

j. Escriba el nombre de la base de datos.

k. Ingrese el inicio de sesión de la cuenta raíz de la base de datos que utiliza para acceder a la base de datos.

l. Introduzca la contraseña de la cuenta raíz de la base de datos que utiliza para acceder a la base de datos.

Espere a que los servicios se agreguen e inicien automáticamente:

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

m. Cree una cuenta que actuará como administrador del Servidor de administración. Introduzca 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 16 caracteres.
- La contraseña debe contener caracteres de al menos tres de los grupos enumerados a continuación:
  - Letras mayúsculas (A-Z)
  - Letras minúsculas (a-z)
  - Números (0-9)
  - Carácter especial (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

Se agrega el usuario y se instala Kaspersky Security Center.

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`

Instalación de Kaspersky Security Center 14 Web Console

En esta sección se describe cómo instalar el Servidor de Kaspersky Security Center 14 Web Console (también denominada Kaspersky Security Center 14 Web Console) en dispositivos con sistema operativo Linux. Antes de la instalación, debe instalar un sistema de administración de bases de datos y el Servidor de administración de Kaspersky Security Center.

Utilice uno de los siguientes archivos 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_compitlación].x86_64.rpm
- Para Alt 8 SP: ksc-web-console-[número_de_compilación]-alt8p.x86_64.rpm

El archivo de instalación debe descargarse del sitio web de Kaspersky.

Para instalar Kaspersky Security Center 14 Web Console:

1. Asegúrese de que el dispositivo en el que desea instalar Kaspersky Security Center 14 Web Console esté ejecutando una de las distribuciones de Linux compatibles.
2. Lea el Contrato de licencia de usuario final (EULA) en el paquete de instalación (archivo /var/opt/kaspersky/ksc-web-console/license-<XX>.txt, donde <XX> es un código de idioma). 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 14 Web Console al Servidor de administración. Nombre este archivo ksc-web-console-setup.json y colóquelo en el siguiente directorio: /etc/ksc-web-console-setup.json.

   Ejemplo de un archivo de respuesta que contiene el conjunto mínimo de parámetros, y la dirección y el puerto predeterminados:

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

   Cuando instale Kaspersky Security Center 14 Web Console en el sistema operativo Linux ALT, debe especificar un número de puerto distinto del 8080, debido a que el sistema operativo utiliza el puerto 8080.

Kaspersky Security Center 14 Web Console no se puede actualizar utilizando el mismo archivo de instalación .rpm. Si desea cambiar la configuración de un archivo de respuestas y usar este archivo para reinstalar la aplicación, primero debe eliminar la aplicación y luego volver a instalarla con el nuevo archivo de respuestas.

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 14 Web Console con un archivo .deb, ejecute el siguiente comando:
     ```
     $ sudo dpkg -i ksc-web-console-[número_de_compilación].x86_64.deb
     ```
   - Para instalar Kaspersky Security Center 14 Web Console desde un archivo .rpm, ejecute el siguiente comando:
     ```
     $ sudo rpm -ivh --nodeps ksc-web-console-[build_number].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 rpm -Uvh --nodeps --force ksc-web-console-
       [número_de_compilación].x86_64.rpm
       ```
     - Para dispositivos que ejecutan un sistema operativo basado en Debian:
       ```
       $ sudo dpkg -i 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 14 Web Console se instala en el siguiente directorio: /var/opt/kaspersky/ksc-web-console.

5. Reinicie todos los servicios de Kaspersky Security Center 14 Web Console mediante el siguiente comando:
   ```
   $ sudo systemctl restart KSC*
   ```

Cuando finalice la instalación, puede usar su navegador para abrir e iniciar sesión en Kaspersky Security Center 14 Web Console.

Parámetros de instalación de Kaspersky Security Center 14 Web Console

Para instalar el Servidor de Kaspersky Security Center 14 Web Console en dispositivos que ejecutan Linux, debe crear un archivo de respuesta en un archivo .json, que contenga los parámetros para conectar Kaspersky Security Center 14 Web Console al Servidor de administración.

Ejemplo de un archivo de respuesta que contiene el conjunto mínimo de parámetros, y la dirección y el puerto predeterminados:

```
{
  "address": "127.0.0.1",
  "port": 8080,
  "defaultLangId": 1049,
  "enableLog": false,
```

```
  "trusted": "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
Server",
  "acceptEula": true,
  "certPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer",
  "webConsoleAccount": "Grupo1:Usuario1",
  "managementServiceAccount": "Grupo1:Usuario2",
  "serviceWebConsoleAccount": "Grupo:Usuario3",
  "pluginAccount": "Grupo1:Usuario4",
  "messageQueueAccount": "Grupo1:Usuario5"
}
```

Cuando instale Kaspersky Security Center 14 Web Console en el sistema operativo Linux ALT, 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 14 Web Console en dispositivos que ejecutan Linux

Parámetro	Descripción	Valores dispon
`dirección`	Dirección del Servidor de Kaspersky Security Center 14 Web Console (obligatorio).	Valor de cadena.
`puerto`	Número de puerto que utiliza el Servidor de Kaspersky Security Center 14 Web Console para conectarse al Servidor de administración (obligatorio).	Valor numérico.
`defaultLangId`	Idioma de la interfaz de usuario (de forma predeterminada, `1033`).	Código numérico del idioma: • Alemán: `1031` • Inglés: `1033` • Español: `3082` • Español (México): `2058` • Francés: `1036` • Japonés: `1041` • Kazajo: `1087` • Polaco: `1045` • Portugués (Brasil): `1046` • Ruso: `1049` • Turco: `1055` • Chino simplificado: `4` • Chino tradicional: `31748`

		Si no se especifica ningún valor, se usa el
`enableLog`	Habilitar o no habilitar el registro de actividad de Kaspersky Security Center 14 Web Console.	Valor booleano: • `verdadero`: el registro está habilitadc predeterminada). • `falso`: el registro está desactivado.

`de confianza`	Lista de Servidores de administración de confianza con derecho a conectarse a Kaspersky Security Center 14 Web Console. Cada Servidor de administración se debe definir con los siguientes parámetros:
	• Dirección del Servidor de administración
	• El puerto de OpenAPI que utiliza Kaspersky Security Center 14 Web Console para conectar al Servidor de administración (de forma predeterminada, 13299)
	• Ruta al certificado del Servidor de administración
	• El nombre del Servidor de administración que se mostrará en la ventana del inicio de sesión
	Los parámetros se separan con barras verticales. Si se especifican varios Servidores de administración, sepárelos con dos barras verticales.
		Valor de cadena en el siguiente formato:
		`" server address|port|certificate`
		Ejemplo:
		`“X.X.X.X|13299|/cert/server-1.ce 1||Y.Y.Y.Y|13299|/cert/server-2.`

`acceptEula`	Aceptar o no aceptar los términos y condiciones del Contrato de licencia de usuario final (EULA). El archivo que contiene los términos del EULA se descarga junto con el archivo de instalación.	Valor booleano: • `verdadero`: He leído, entendido y ace términos del Contrato de licencia de u • `falso`: No acepto los términos del Cc predeterminada).
`certDomain`	Si desea generar un nuevo certificado, use este parámetro para especificar el nombre de dominio para el que se generará un nuevo certificado.	Valor de cadena.
`certPath`	Si desea usar un certificado existente, use este parámetro para especificar la ruta al archivo de clave.	Valor de cadena. Especifique la ruta `"/var/opt/kaspersky/klnagent_srv` para utilizar el certificado existente. Para especifique la ruta donde se almacena es

`keyPath`	Si desea usar un certificado existente, use este parámetro para especificar la ruta al archivo de certificado.	Valor de cadena.
`webConsoleAccount`	Nombre de la cuenta con la cual se está ejecutando el servicio KSCWebConsole.	Valor de cadena en el siguiente formato: Por ejemplo: `"Grupo1:Usuario1"`. Si no se especifica ningún valor, el instala Center 14 Web Console crea una nueva c predeterminado `gestión_usuario_%ui`
`managementServiceAccount`	Nombre de la cuenta privilegiada bajo la cual se ejecuta el servicio KSCWebConsoleManagement.	Valor de cadena en el siguiente formato: Por ejemplo: `"Grupo1:Usuario1"`. Si no se especifica ningún valor, el instala Center 14 Web Console crea una nueva c predeterminado `usuario_nodejs_%uic`
`serviceWebConsoleAccount`	Nombre de la cuenta privilegiada bajo la cual se ejecuta el servicio KSCSvcWebConsole.	Valor de cadena en el siguiente formato: Por ejemplo: `"Grupo1:Usuario1"`. Si no se especifica ningún valor, el instala Center 14 Web Console crea una nueva c predeterminado `usuario_svc_nodejs_`
`pluginAccount`	Nombre de la cuenta con la cual se está ejecutando el servicio KSCWebConsolePlugin.	Valor de cadena en el siguiente formato: Por ejemplo: `"Grupo1:Usuario1"`. Si no se especifica ningún valor, el instala Center 14 Web Console crea una nueva c predeterminado `usuario_web_plugin_`
`messageQueueAccount`	Nombre de la cuenta con la cual se está ejecutando el servicio KSCWebConsoleMessageQueue.	Valor de cadena en el siguiente formato: Por ejemplo: `"Grupo1:Usuario1"`. Si no se especifica ningún valor, el instala Center 14 Web Console crea una nueva c predeterminado `usuario_mensaje_col`

Si especifica los parámetros de `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `serviceWebConsoleAccount` o `messageQueueAccount`, asegúrese de que las cuentas de usuario personalizadas pertenezcan al mismo grupo de seguridad. Si no se especifican estos parámetros, el instalador de Kaspersky Security Center 14 Web Console crea un grupo de seguridad predeterminado y luego crea cuentas de usuario con nombres predeterminados en este grupo.

Cuentas para trabajar con el DBMS

La siguiente tabla proporciona información sobre las propiedades de las cuentas elegidas para trabajar con MariaDB DBMS.

Un *DBMS local* es un DBMS instalado en el mismo dispositivo que el Servidor de administración. Un *DBMS remoto* es un DBMS instalado en un dispositivo diferente.

Conceda todos los derechos necesarios para la cuenta del Servidor de administración antes de iniciar el servicio del Servidor de administración.

DBMS: MariaDB

Ubicación del DBMS	Local o remota	Local o remota
Quién crea la base de datos "KAV"	El instalador (automáticamente)	El administrador (manualmente)
Cuenta con la cual se está ejecutando el instalador	Local o de dominio, con derechos de administrador local.	Local o de dominio, con derechos de administrador local.
Cuenta del servicio del Servidor de administración	Local o de dominio	Local o de dominio
Derechos de la cuenta interna de DBMS utilizada por el instalador y el servicio del Servidor de administración para acceder a DBMS	Se requiere acceso de root.	`GRANT ALL` para la base de datos KAV, y `SELECT`, `SHOW VIEW`, `PROCESS` para las tablas del sistema.

Despliegue del clúster de conmutación por error de Kaspersky

Esta sección contiene información general sobre el clúster de conmutación por error de Kaspersky e instrucciones sobre la preparación y despliegue del clúster de conmutación por error de Kaspersky en su red.

Escenario: despliegue de un clúster de conmutación por error de Kaspersky

Un clúster de conmutación por error de Kaspersky proporciona una alta disponibilidad de Kaspersky Security Center y minimiza el tiempo de inactividad del Servidor de administración en caso de una falla. El clúster de conmutación por error se basa en dos instancias idénticas de Kaspersky Security Center instaladas en dos equipos. 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.

Requisitos previos

Cuenta con hardware que cumple con los requisitos para el clúster de conmutación por error.

El despliegue de las aplicaciones de Kaspersky se divide en etapas:

1. **Crear una cuenta para los servicios de Kaspersky Security Center**

   Cree una cuenta de usuario de dominio nueva o seleccione una existente bajo la cual se ejecutarán los servicios de Kaspersky Security Center. Agregue la cuenta seleccionada en el grupo de administradores locales en cada uno de los nodos y en el servidor de archivos.

2. **Preparación del servidor de archivos**

   Prepare el servidor de archivos para que funcione como un componente del clúster de conmutación por error de Kaspersky. Asegúrese de que el servidor de archivos cumpla con los requisitos de hardware y software, cree dos carpetas compartidas para los datos de Kaspersky Security Center y configure los permisos para acceder a las carpetas compartidas.

   Instrucciones: Preparación de un servidor de archivos para el clúster de conmutación por error de Kaspersky

3. **Preparación de nodos activos y pasivos**

   Prepare dos equipos con hardware y software idénticos para que funcionen como nodos activos y pasivos.

   Instrucciones: Preparación de nodos para el clúster de conmutación por error de Kaspersky

4. **Instalación del sistema de administración de bases de datos (DBMS)**

   Usted cuenta con dos opciones:

   - Si desea utilizar MariaDB Galera Cluster, no necesita una computadora dedicada para DBMS. Instale MariaDB Galera Cluster en cada uno de los nodos.
   - Si desea utilizar cualquier otro SGBD compatible, instale el DBMS seleccionado en una computadora dedicada.

5. **Instalación de Kaspersky Security Center**

   Instale Kaspersky Security Center en el modo de clúster de conmutación por error en ambos nodos. Primero debe instalar Kaspersky Security Center en el nodo activo y luego instalarlo en el pasivo.

6. **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 detener uno de los servicios de Kaspersky Security Center en el nodo activo: kladminserver, klnagent, ksnproxy, klactprx o klwebsrv. Una vez que se detiene el servicio, la administración de la protección se debe cambiar automáticamente al nodo pasivo.

Resultados

El clúster de conmutación por error de Kaspersky se implementó. Familiarícese con los eventos que conducen al cambio entre los nodos activo y pasivo.

Acerca del clúster de conmutación por error de Kaspersky

Un clúster de conmutación por error de Kaspersky proporciona una alta disponibilidad de Kaspersky Security Center y minimiza el tiempo de inactividad del Servidor de administración en caso de una falla. El clúster de conmutación por error se basa en dos instancias idénticas de Kaspersky Security Center instaladas en dos equipos. 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.

> En un clúster de conmutación por error de Kaspersky, todos los servicios de Kaspersky Security Center se administran automáticamente. No intente reiniciar los servicios manualmente.

Requisitos de hardware y software

Para implementar un clúster de conmutación por error de Kaspersky, debe tener el siguiente hardware:

- Dos equipos con idéntico hardware y software. Estos equipos actuarán como nodos activos y pasivos.
- Un servidor de archivos que ejecuta Linux, con el sistema de archivos EXT4. Debe proporcionar un equipo dedicado que actuará como servidor de archivos.

Asegúrese de haber proporcionado un ancho de banda de red elevado entre el servidor de archivos y los nodos activo y pasivo.

- Un equipo con sistema de administración de base de datos (DBMS). Si usa MariaDB Galera Cluster como un DBMS, no se requiere una computadora dedicada para este propósito.

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 falla o se cancela deliberadamente por el usuario. Los servicios de Kaspersky Security Center son los siguientes: kladminserver, klnagent, klactprx y klwebsrv.
- La conexión de red entre el nodo activo y el almacenamiento en el servidor de archivos se interrumpe o termina.

Preparación de un servidor de archivos para un clúster de conmutación por error de Kaspersky

Un servidor de archivos funciona como un componente necesario de un clúster de conmutación por error de Kaspersky.

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
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. Deberá especificar las rutas a las carpetas compartidas mientras configura la instalación de Kaspersky Security Center.

   Ejecute el siguiente comando:

   ```
   sudo yum install nfs-utils
   ```

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

Habilite el inicio automático mediante el siguiente comando:

```
sudo systemctl enable rpcbind
```

4. Reinicie el servidor de archivos.

El servidor de archivos está preparado. Para implementar el clúster de conmutación por error de Kaspersky, siga las instrucciones adicionales en este escenario.

Preparación de nodos para un clúster de conmutación por error de Kaspersky

Prepare dos equipos para que funcionen como nodos activos y pasivos para un clúster de conmutación por error de Kaspersky.

Para preparar los nodos para un clúster de conmutación por error de Kaspersky:

1. Asegúrese de tener dos equipos que cumplan con los requisitos de hardware y software. Estos equipos actuarán como nodos activos y pasivos del clúster de conmutación por error.

2. Para que los nodos funcionen como clientes NFS, instale el paquete nfs-utils en cada nodo.

   Ejecute el siguiente comando:

   ```
   sudo yum install nfs-utils
   ```

3. Cree puntos de montaje mediante los siguientes comandos:

   ```
   sudo mkdir -p /mnt/KlFocStateShare
   sudo mkdir -p /mnt/KlFocDataShare_klfoc
   ```

4. Compruebe que las carpetas compartidas se puedan montar correctamente. [paso opcional]

   Ejecute el siguiente comando:

   ```
   sudo mount -t nfs -o vers=4,nolock,local_lock=none,auto,user,rw {server}:{path to
   the KlFocStateShare folder} /mnt/KlFocStateShare
   sudo mount -t nfs -o vers=4,nolock,local_lock=none,noauto,user,rw {server}:{path to
   the KlFocDataShare_klfoc folder} /mnt/KlFocDataShare_klfoc
   ```

   Aquí, `{server}:{ruta a la carpeta KlFocStateShare}` y `{server}:{ruta a la carpeta KlFocDataShare_klfoc}` son las rutas de red a las carpetas compartidas en el servidor de archivos.

   Una vez que las carpetas compartidas se hayan montado correctamente, desmóntelas ejecutando los siguientes comandos:

   ```
   sudo umount /mnt/KlFocStateShare
   ```

```
sudo umount /mnt/KlFocDataShare_klfoc
```

5. Haga coincidir los puntos de montaje y las carpetas compartidas:
```
sudo vi /etc/fstab
{server}:{path to the KlFocStateShare folder} /mnt/KlFocStateShare nfs
vers=4,nolock,local_lock=none,auto,user,rw 0 0
{server}:{path to the KlFocDataShare_klfoc folder} /mnt/KlFocDataShare_klfoc nfs
vers=4,nolock,local_lock=none,noauto,user,rw 0 0
```
Aquí, `{server}:{ruta a la carpeta KlFocStateShare}` y `{server}:{ruta a la carpeta KlFocDataShare_klfoc}` son las rutas de red a las carpetas compartidas en el servidor de archivos.

6. Reinicie ambos nodos.

7. Monte las carpetas compartidas ejecutando los siguientes comandos:
```
mount /mnt/KlFocStateShare
mount /mnt/KlFocDataShare_klfoc
```

8. Asegúrese de que los permisos para acceder a las carpetas compartidas pertenezcan a ksc:kladmins.

   Ejecute el siguiente comando:
```
sudo ls -la /mnt/
```

9. Realice una de las siguientes acciones:

- En cada uno de los nodos, cree un adaptador de red virtual. Por ejemplo, ejecute los siguientes comandos:

  a. Descubra los nombres de las interfaces mediante el siguiente comando:
```
ifconfig
```

  b. Ejecute el siguiente script (en adelante, los nombres de las interfaces se proporcionan como ejemplos):
```
#!/bin/bash
PHYSICAL_IFACE=ens160
VIRTUAL_IFACE=macvlan1
ip link del $VIRTUAL_IFACE > /dev/null 2>&1
ip link add link $PHYSICAL_IFACE $VIRTUAL_IFACE type macvlan
if [ "$?" -ne "0" ]; then
    echo ERROR adding new virtual adapter $VIRTUAL_IFACE!
    exit $?
fi
ip link set $VIRTUAL_IFACE down
if [ "$?" -ne "0" ]; then
    echo ERROR disabling virtual adapter $VIRTUAL_IFACE!
    exit $?
fi
```

  c. Ejecute el siguiente comando:
```
ip addr add {Dirección IP del adaptador de red virtual} dev {nombre del
adaptador de red virtual}
```

  La dirección IP debe estar vacante cuando cree el adaptador de red virtual. Los adaptadores de red virtual en ambos nodos deben tener la misma dirección IP.

  d. Compruebe que el adaptador de red virtual se haya creado correctamente.

  Ejecute el siguiente comando:
```
ip link set macvlan1 up
ifconfig
```

e. Deshabilite el adaptador de red virtual ejecutando el siguiente comando:

```
ip link set macvlan1 down
```

- Utilice un equilibrador de carga de terceros. Por ejemplo, puede utilizar un servidor nginx. En este caso, haga lo siguiente:

  a. Proporcione un equipo dedicado basado en Linux con nginx instalado.

  b. Configure el equilibrio de carga. Configure el nodo activo como servidor principal y el nodo pasivo como servidor de respaldo.

  c. En el servidor nginx, abra todos los puertos del Servidor de administración: TCP 13000, UDP 13000, TCP 13291, TCP 13299 y TCP 17000.

Los nodos están preparados. Para implementar el clúster de conmutación por error de Kaspersky, siga las instrucciones adicionales del escenario.

Instalación de Kaspersky Security Center en los nodos del clúster de conmutación por error de Kaspersky

Este procedimiento describe cómo instalar Kaspersky Security Center en los nodos del clúster de conmutación por error de Kaspersky. Kaspersky Security Center se instala por separado en ambos nodos del clúster de conmutación por error de Kaspersky. 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.

Use el archivo de instalación que corresponda para la distribución de Linux instalada en su dispositivo (ksc-web-console-[número_de_versión].deb o ksc-web-console-[número_de_versión].x86_64.rpm). El archivo de instalación debe descargarse del sitio web de Kaspersky.

Solo un usuario del grupo de dominio KLAdmins puede instalar Kaspersky Security Center en cada nodo.

Instalación en el nodo principal (activo)

Para instalar Kaspersky Security Center en el nodo principal:

1. Asegúrese de que el dispositivo en el que desea instalar Kaspersky Security Center esté ejecutando una de las distribuciones de Linux compatibles.

2. En la línea de comandos, ejecute los comandos provistos en esta instrucción bajo una cuenta con privilegios de raíz.

3. Ejecute la instalación de Kaspersky Security Center. Según su distribución de Linux, ejecute uno de los siguientes comandos:

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

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

4. Ejecute la configuración de Kaspersky Security Center:

   ```
   sudo /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. Ingresar `y` si entiende y acepta los términos del EULA. Ingresar `n` si no acepta los términos del EULA. Para utilizar Kaspersky Security Center, debe aceptar los términos del EULA.

    b. Ingresar `y` si comprende y acepta los términos de la Política de privacidad, y acepta que sus datos se manejen y transmitan (incluso a terceros países) como se describe en la Política de privacidad. Ingresar `n` si no acepta los términos de la Política de privacidad. Para utilizar Kaspersky Security Center, 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, ingrese la siguiente configuración:

    a. Ingrese la ruta local al punto de montaje del recurso compartido de estado.

    b. Ingrese la ruta local al punto de montaje del recurso compartido de datos.

    c. Elija un modo de conectividad de clúster de conmutación por error: a través de un adaptador de red virtual o un equilibrador de carga externo.

    d. Si usa un adaptador de red virtual, ingrese el nombre.

    e. Cuando se le solicite ingresar el nombre de DNS del Servidor de administración o la dirección IP estática, ingrese la dirección IP del adaptador de red virtual o la dirección IP del balanceador de carga externo.

    f. Introduzca el número de puerto del Servidor de administración. De manera predeterminada, se utiliza el puerto 14000.

    g. Introduzca el número de puerto SSL del Servidor de administración. De manera predeterminada, se utiliza el puerto 13000.

    h. Evalúe el número aproximado de dispositivos que pretende administrar:

        - Si tiene de 1 a 100 dispositivos en red, ingrese 1.
        - Si tiene de 101 a 1000 dispositivos en red, ingrese 2.
        - Si tiene más de 1000 dispositivos en red, ingrese 3.

    i. Ingrese el nombre del grupo de seguridad para los servicios. De forma predeterminada, se utiliza el grupo 'kladmins'.

    j. 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 forma predeterminada, se utiliza la cuenta 'ksc'.

    k. Introduzca el nombre de la cuenta para iniciar otros servicios. La cuenta debe ser miembro del grupo de seguridad ingresado. De forma predeterminada, se utiliza la cuenta 'ksc'.

    l. Introduzca la dirección IP del dispositivo en el que está 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 manera predeterminada, se utiliza el puerto 3306.

    n. Escriba el nombre de la base de datos.

o. Ingrese el inicio de sesión de la cuenta raíz de la base de datos que utiliza para acceder a la base de datos.

p. Introduzca la contraseña de la cuenta raíz de la base de datos que utiliza para acceder a la base de datos.

Espere a que los servicios se agreguen e inicien automáticamente:

- klnagent_srv
- kladminserver_srv
- klactprx_srv
- klwebsrv_srv

q. Cree una cuenta que actuará como administrador del Servidor de administración. Introduzca el nombre de usuario y la contraseña. La contraseña de usuario no puede tener menos de 8 ni más de 16 caracteres.

Se agrega el usuario y se instala Kaspersky Security Center en el nodo principal.

Instalación en el nodo secundario (pasivo)

Para instalar Kaspersky Security Center en el nodo secundario:

1. Asegúrese de que el dispositivo en el que desea instalar Kaspersky Security Center esté ejecutando una de las distribuciones de Linux compatibles.

2. En la línea de comandos, ejecute los comandos provistos en esta instrucción bajo una cuenta con privilegios de raíz.

3. Ejecute la instalación de Kaspersky Security Center. Según su distribución de Linux, ejecute uno de los siguientes comandos:

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

4. Ejecute la configuración de Kaspersky Security Center:

   ```
   sudo /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. Ingresar `y` si entiende y acepta los términos del EULA. Ingresar `n` si no acepta los términos del EULA. Para utilizar Kaspersky Security Center, debe aceptar los términos del EULA.

   b. Ingresar `y` si comprende y acepta los términos de la Política de privacidad, y acepta que sus datos se manejen y transmitan (incluso a terceros países) como se describe en la Política de privacidad. Ingresar `n` si no acepta los términos de la Política de privacidad. Para utilizar Kaspersky Security Center, debe aceptar los términos de la Política de privacidad.

6. Seleccione **Nodo de clúster secundario** como un modo de instalación del Servidor de administración.

7. Cuando se le solicite, ingrese la ruta local al punto de montaje del recurso compartido estatal.

Kaspersky Security Center está instalado en el nodo secundario.

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`

Ahora, puede probar el clúster de conmutación por error de Kaspersky para asegurarse de que lo configuró correctamente y de que el clúster funciona bien.

Iniciar y detener nodos del clúster manualmente

Es posible que deba detener todo el clúster de conmutación por error de Kaspersky o desconectar temporalmente 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:

1. En el nodo activo, vaya a /opt/kaspersky/ksc64/sbin.
2. Abra la línea de comando y luego ejecute uno de los siguientes comandos:
   - Para detener el clúster, ejecute: `klfoc -stopcluster --stp klfoc`
   - Para iniciar el clúster, ejecute: `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 comando y luego desconecte el nodo del clúster mediante 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 comando y luego conecte el nodo al clúster mediante el comando `attach_node.cmd`.

9. En el nodo activo, inicie el clúster de conmutación por error mediante el comando `klfoc -startcluster --stp klfoc`.

El nodo se mantiene y se adjunta al clúster de conmutación por error.

Certificados para trabajar con Kaspersky Security Center

Esta sección contiene información sobre los certificados de Kaspersky Security Center y explica cómo emitir y reemplazar certificados para la Consola Web de Kaspersky Security Center 14 y cómo renovar un certificado para el Servidor de administración si el Servidor interactúa con Kaspersky Security Center 14 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 del Servidor web
- Certificado de Kaspersky Security Center 14 Web Console

Los certificados que se utilizan por defecto son autofirmados, es decir, son certificados emitidos por el propio Kaspersky Security Center. Si así lo exigen los requisitos de su red o los estándares de seguridad de su organización, puede reemplazarlos por certificados personalizados. 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 entre las dos clases de certificados es que los personalizados no se renuevan automáticamente al caducar. Para reemplazar certificados autofirmados por personalizados, deberá usar, según el tipo de certificado, la utilidad klsetsrvcert o la Consola de administración de Kaspersky Security Center 14 Web Console. 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)

Certificados del Servidor de administración

Se requiere un certificado del Servidor de administración para los siguientes propósitos:

- Autenticación del Servidor de administración al conectarse a Kaspersky Security Center Web Console 14
- Interacción segura entre el Servidor de administración y el Agente de red en los dispositivos administrados
- Autenticación cuando los Servidores de administración primarios 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 la carpeta /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 14 Web Console. El certificado del Servidor de administración se denomina certificado común ("C").

El certificado del Servidor de administración es válido por 397 días. Kaspersky Security Center genera un certificado de reserva común ("CR") en forma automática 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.

Si el certificado del Servidor de administración tiene un período de validez superior a 397 días, el navegador web mostrará un error.

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 se conectaron anteriormente al Servidor de administración a través de SSL perderán la conexión y arrojarán el "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.

Cabe destacar que el certificado del Servidor de administración se puede guardar en una copia de seguridad que no incluya ningún otro ajuste del Servidor. Esta facilidad permite mudar el Servidor de administración de un dispositivo a otro sin perder información.

Certificado del Servidor web

El Servidor web —uno de los componentes del Servidor de administración de Kaspersky Security Center— utiliza un tipo de certificado especial. Este certificado es necesario para publicar paquetes de instalación del Agente de red que descargue posteriormente en los dispositivos administrados. El Servidor web puede usar distintos certificados para tal fin.

El Servidor web utiliza uno de los siguientes certificados, en orden de prioridad:

1. Certificado del Servidor web personalizado, elegido manualmente mediane Kaspersky Security Center 14 Web Console
2. certificado común del Servidor de administración ("C")

Certificado de Kaspersky Security Center 14 Web Console

El Servidor de Kaspersky Security Center 14 Web Console (en adelante, Web Console) tiene su propio certificado. Cuando abre un sitio web, el navegador verifica si su 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. La advertencia se muestra porque Web Console utiliza un certificado autofirmado, generado automáticamente por Kaspersky Security Center. 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.

Requisitos para los certificados personalizados que se utilizan en Kaspersky Security Center

En la siguiente tabla se enumeran los requisitos que deben reunir los certificados personalizados para los distintos componentes de Kaspersky Security Center.

Requisitos que deben reunir los certificados de Kaspersky Security Center

Tipo de certificado	Requisitos	Comentarios
Certificado común, certificado de reserva común ("C", "CR")	Longitud mínima de la clave: 2048. Restricciones básicas: • CA: cierto • 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 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 campo `subjectAltName` debe tener un valor válido, es decir, debe haberse definido un nombre alternativo del sujeto (SAN) para el certificado.	N/C.

	El certificado se ajusta tanto a los requisitos que los navegadores web exigen para los certificados de los servidores como a los requisitos básicos que ordena actualmente el CA/Browser Forum.	
Certificado de Kaspersky Security Center 14 Web Console	El contenedor PEM que se utilice para especificar el certificado debe incluir toda la cadena de claves públicas. El campo `subjectAltName` debe tener un valor válido, es decir, debe haberse definido un nombre alternativo del sujeto (SAN) para el certificado. El certificado se ajusta tanto a los requisitos que los navegadores web exigen para los certificados de los servidores como a los requisitos básicos que ordena actualmente el CA/Browser Forum.	Kaspersky Security Center 14 Web Console no es compatible con los certificados cifrados.

Reemisión del certificado de Kaspersky Security Center Web Console 14

La mayoría de los navegadores imponen un límite al plazo de validez de un certificado. Para estar dentro de este límite, el plazo de validez del certificado de Kaspersky Security Center 14 Web Console está limitado a 397 días. Puede reemplazar un certificado existente recibido de una autoridad de certificación (CA) emitiendo un nuevo certificado autofirmado manualmente. Como alternativa, puede volver a emitir su certificado de Kaspersky Security Center 14 Web Console caducado.

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. La advertencia se muestra porque 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:

- Especifique un certificado personalizado cuando lo vuelva a emitir (opción recomendada). Cree un certificado que sea de confianza en su infraestructura y que cumpla con los requisitos para certificados personalizados.
- Añada el certificado de Web Console a la lista de certificados de navegador de confianza después de volverlo a emitir. Recomendamos que utilice esta opción solo si no puede crear un certificado personalizado.

Para volver a emitir el certificado caducado de Kaspersky Security Center 14 Web Console:

Vuelva a instalar Kaspersky Security Center 14 Web Console realizando una de las siguientes acciones:

- Si desea utilizar el mismo archivo de instalación de Kaspersky Security Center 14 Web Console, elimine Kaspersky Security Center 14 Web Console y luego instale la misma versión de Kaspersky Security Center 14 Web Console.
- Si desea utilizar un archivo de instalación de una versión actualizada, ejecutar el comando de actualización.

El certificado de Kaspersky Security Center 14 Web Console se vuelve a emitir por otro período de validez de 397 días.

Reemplazo del certificado de Kaspersky Security Center 14 Web Console

De forma predeterminada, el certificado de navegador del Servidor de Kaspersky Security Center 14 Web Console (también denominado Kaspersky Security Center 14 Web Console) se genera automáticamente al instalar la aplicación. Este certificado puede reemplazarse por uno personalizado.

Para reemplazar el certificado de Kaspersky Security Center 14 Web Console por uno personalizado:

1. Crear un nuevo archivo de respuesta requerido para la instalación de Kaspersky Security Center 14 Web Console.
2. En este archivo, especifique las rutas al archivo de certificado personalizado y al archivo de clave mediante los parámetros `certPath` y `keyPath`.
3. Vuelva a instalar Kaspersky Security Center 14 Web Console especificando el nuevo archivo de respuesta. Realice una de las siguientes acciones:
   - Si desea utilizar el mismo archivo de instalación de Kaspersky Security Center 14 Web Console, elimine Kaspersky Security Center 14 Web Console y luego instale la misma versión de Kaspersky Security Center 14 Web Console.
   - Si desea utilizar un archivo de instalación de una versión actualizada, ejecutar el comando de actualización.

Kaspersky Security Center 14 Web Console ahora utilizará el nuevo certificado.

Conversión de un certificado PFX al formato PEM

Para utilizar un certificado PFX en Kaspersky Security Center 14 Web Console, primero debe convertirlo al formato PEM mediante cualquier utilidad multiplataforma conveniente 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_de_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 14 Web Console no admite certificados protegidos con frases 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 están listos para usar, por lo que puede especificarlos en el instalador de Kaspersky Security Center 14 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 útil reemplazar el certificado inmediatamente después de la instalación del Servidor de administración y antes de que el Asistente de inicio rápido se complete.

Si el certificado del Servidor de administración tiene un período de validez superior a 397 días, el navegador web mostrará un error.

Requisitos previos

El nuevo certificado se debe crear en el formato PKCS#12 (por ejemplo, mediante la PKI de la organización) y se debe emitir a través de una autoridad de certificación (CA) de confianza. Además, el nuevo certificado debe incluir toda la cadena de confianza y una clave privada, que se debe almacenar en el archivo con la extensión pfx o p12. Para el nuevo certificado, se deben cumplir los requisitos que se enumeran en la siguiente tabla.

Tipo de certificado: certificado común, certificado de reserva común ("C", "CR")

Requisitos:

- 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 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.

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.

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 reemplazar el certificado del Servidor de administración:

Desde la línea de comandos, ejecute la siguiente utilidad:

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

No necesita descargar la utilidad klsetsrvcert. Esta utilidad se incluye en el kit de distribución de Kaspersky Security Center. No es compatible con versiones anteriores de Kaspersky Security Center.

La descripción de los parámetros de la utilidad klsetsrvcert se presenta en la siguiente tabla.

Valores de los parámetros de la utilidad klsetsrvcert

Parámetro	Valor
`-t <tipo>`	Tipo del certificado para reemplazar. Posibles valores del parámetro `<type>`: • `C`: reemplazar el certificado común para los puertos 13000 y 13291. • `CR`: reemplazar el certificado de reserva común para los puertos 13000 y 13291.
`-f <time>`	Horario para cambiar el certificado, utilizando el formato "DD-MM-AAAA hh:mm" (para los puertos 13000 y 13291). Utilice este parámetro si desea reemplazar el certificado común o 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 <archivo de entrada>`	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 <chkopt>`	Parámetros de validación del certificado (separados por punto y coma). Para usar 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.
`-g <nombre dns>`	Un nuevo certificado se creará para el nombre de DNS especificado.
`-r <calistfile>`	Lista de autoridades de certificación raíz de confianza, formato PEM.
`-l <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 <inputfile> -p <password> -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.

Conexión de los Agentes de red al Servidor de administración mediante la utilidad klmover

Después de reemplazar el certificado del Servidor de administración mediante la línea de comando utilidad klsetsrvcert, debe establecer la conexión SSL entre los Agentes de red y el Servidor de administración, ya que la conexión está interrumpida.

Para especificar el nuevo certificado del Servidor de administración y restaurar la conexión:

Desde la línea de comandos, ejecute la siguiente utilidad:

```
klmover [-address <dirección del servidor>] [-pn <número de puerto>] [-ps <número de puerto SSL>] [-nossl] [-cert <ruta al archivo del certificado>]
```

Esta utilidad se copia automáticamente en la carpeta de instalación del Agente de red, cuando el Agente de red está instalado en un dispositivo cliente.

La descripción de los parámetros de la utilidad klmover se presenta en la siguiente tabla.

Valores de los parámetros de la utilidad de klmover

Parámetro	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 el 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 el 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.

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.

Acerca de las actualizaciones de Kaspersky Security Center Linux

Puede instalar la versión 14 del Servidor de administración en un dispositivo que tenga una versión anterior del Servidor de administración instalada (a partir de la versión 13). Al actualizar a la versión 14, se conservan todos los datos y configuraciones de la versión anterior del Servidor de administración.

Durante la actualización, es fundamental que el DBMS no sea utilizado simultáneamente por el Servidor de administración y por otras aplicaciones.

Puede actualizar una versión del Servidor de administración a través de uno de los siguientes métodos:

- Al usar el archivo de instalación de Kaspersky Security Center
- 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

Si su red incluye varios Servidores de administración, debe actualizar cada Servidor manualmente. Kaspersky Security Center Linux no admite la actualización centralizada.

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 complemento del Agente de red se actualizan automáticamente.

Actualización de Kaspersky Security Center Linux mediante el archivo de instalación

Para actualizar el Servidor de administración de una versión anterior (a partir de la versión 13) a la versión 14, puede instalar una nueva versión sobre una anterior mediante el archivo de instalación de Kaspersky Security Center.

Para actualizar una versión anterior del Servidor de administración a la versión 14, mediante el archivo de instalación:

1. Descargue el archivo de instalación de Kaspersky Security Center con un paquete completo para la versión 14 desde el sitio web de Kaspersky:
   - Para dispositivos que ejecutan un sistema operativo basado en RPM: ksc64-<número de versión>-11247.x86_64.rpm
   - Para dispositivos que ejecutan un sistema operativo basado en Debian: ksc64_<número de versión>-11247_amd64.deb
2. Actualice el paquete de instalación mediante un administrador de paquetes que utilice en su Servidor de administración. Por ejemplo, puede usar los siguientes comandos en la línea de comandos de la terminal en una cuenta con privilegios de raíz:
   - Para dispositivos que ejecutan un sistema operativo basado en RPM:
     ```
     $ sudo rpm -Uvh --nodeps --force ksc64-<número de versión>-11247.x86_64.rpm
     ```
   - Para dispositivos que ejecutan un sistema operativo basado en Debian:
     ```
     $ sudo dpkg -i ksc64_<número de versión>-11247_amd64.deb
     ```

Una vez que el comando se ha ejecutado 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.

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:

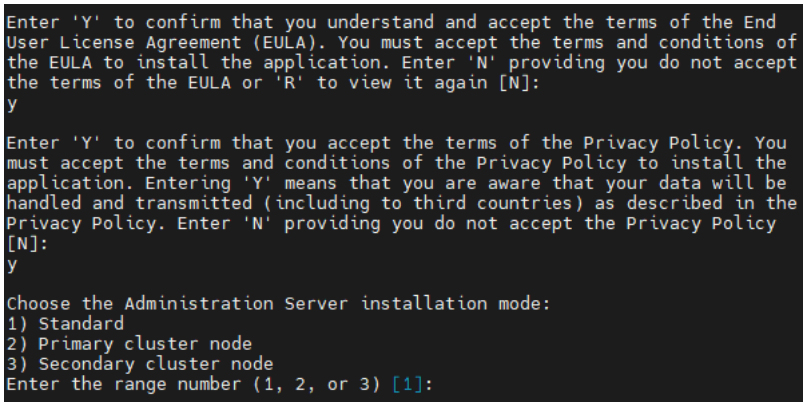
   a. Ingrese 'Y' para confirmar que ha leído, comprendido y aceptado completamente los términos y condiciones del EULA.

   b. Ingrese 'Y' nuevamente para confirmar que ha leído, entendido y aceptado completamente la Política de privacidad que describe el manejo de datos.

   La instalación de la aplicación en su dispositivo continuará después de que seleccione 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.



Aceptar los términos del EULA y la Política de privacidad, y seleccionar el modo de instalación estándar del Servidor de administración en el terminal de la 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. 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.

Actualización de Kaspersky Security Center Linux mediante copia de seguridad

Para actualizar el Servidor de administración de una versión anterior (a partir de la versión 13) a la versión 14, puede crear una copia de seguridad de los datos del Servidor de administración y restaurar estos datos después de instalar una nueva versión Kaspersky Security Center. 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 una versión anterior del Servidor de administración a la versión 14, mediante la copia de seguridad:

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.
3. Instalar Kaspersky Security Center versión 14 en el antiguo Servidor de administración.
4. Restaurar los datos del Servidor de administración de la copia de seguridad creada antes de la actualización.
5. 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.

Iniciar sesión en Kaspersky Security Center 14 Web Console y cerrar sesión

Puede iniciar sesión en la Kaspersky Security Center 14 Web Console después de instalar el Servidor de administración y el Servidor de Web Console. Debe conocer la dirección web del Servidor de administración y el número de puerto especificado durante la instalación (de forma predeterminada, el puerto es 8080). En su navegador, JavaScript debe estar habilitado.

Para iniciar sesión en Kaspersky Security Center 14 Web Console:

1. En su navegador, vaya a <dirección web del Servidor de administración>:<Número de puerto>.

   Se muestra la página de inicio de sesión.

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 Servidor de administración, solo se mostrarán los campos Inicio de sesión y Contraseña.

3. Realice una de las siguientes acciones:

   - Para iniciar sesión en el Servidor de Administración físico, ingrese el nombre de usuario y la contraseña de Administrador local.
   - Si se crean uno o más Servidores de administración virtuales en el Servidor y desea iniciar sesión en un Servidor virtual:

     a. Haga clic en **Configuración avanzada**.

     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.

Después de iniciar sesión, se muestra el panel de control, que contiene el idioma y el tema que usó la última vez. Puede navegar por Kaspersky Security Center 14 Web Console y usarlo para trabajar con Kaspersky Security Center Linux.

Para cerrar sesión en Kaspersky Security Center 14 Web Console:

1. Haga clic en su nombre de usuario en la esquina superior derecha de la pantalla.

2. En el menú desplegable, seleccione **Salir**.

Kaspersky Security Center 14 Web Console se cierra y se muestra la página de inicio de sesión.

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. Esta configuración se realiza mediante el Asistente de inicio rápido. Cuando el Asistente se está ejecutando, puede 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.
- Configura la entrega mediante correo electrónico de notificaciones de eventos que ocurren durante la operación del Servidor de administración y las aplicaciones administradas (para garantizar la entrega de una notificación exitosa, el servicio de Messenger debe ejecutarse en el Servidor de administración y en todos los dispositivos de destino).
- Crear una directiva de protección para estaciones de trabajo y servidores, así como tareas de análisis antivirus, 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 crea directivas de únicamente para las aplicaciones cuya carpeta **DISPOSITIVOS ADMINISTRADOS** no contiene directivas. El Asistente de inicio rápido no crea tareas si alguna tarea con el mismo nombre ya se creó para el nivel superior de la jerarquía de dispositivos administrados.

La aplicación le solicita automáticamente que ejecute el Asistente de inicio rápido después de instalar el Servidor de administración y conectarse 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 la ventana principal de la aplicación, haga clic en el ícono de **Configuración** ( ) ubicado junto al nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, elija la sección **General**.
3. Haga clic en **Iniciar el Asistente de inicio rápido**.

El Asistente le solicita a realizar la configuración inicial del Servidor de administración. Siga las instrucciones del Asistente. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

Paso 1. Especificar la configuración de la conexión a Internet

Especifique la configuración del Acceso a Internet para Kaspersky Security Center Linux.

Seleccione la casilla **Usar servidor proxy** si desea usar un servidor proxy al conectarse a Internet. Si esta casilla se selecciona, los campos están disponibles para escribir la configuración. Deberá introducir los siguientes valores de conexión del servidor proxy:

- **Dirección**

- **Número de puerto**
- **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** (este campo está disponible si se selecciona la casilla de verificación **Autenticación del servidor proxy**)

  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** (este campo está disponible si se selecciona la casilla de verificación **Autenticación del servidor proxy**)

  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.

Paso 2. 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 formada por 20 caracteres alfanuméricos. Se ingresa un código de activación para agregar una clave que activa Kaspersky Security Center. Recibe el código de activación en la dirección de correo electrónico que especificó después de comprar Kaspersky Security Center.

  Para activar la aplicación con un código de activación, necesita acceso a Internet para establecer la conexión con los servidores de activación de Kaspersky.

  Si seleccionó esta opción de activación, puede activar la opción **Distribuir clave de licencia automáticamente a los dispositivos administrados**.

  Si esta opción está activada, 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 DE KASPERSKY** 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.

  Para activar la aplicación con un archivo de clave, no es necesario conectarse a los servidores de activación de Kaspersky.

  Si seleccionó esta opción de activación, puede activar la opción **Distribuir clave de licencia automáticamente a los dispositivos administrados**.

  Si esta opción está activada, 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 DE KASPERSKY** del menú principal.

- Posponiendo la activación de aplicaciones

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 3. Creación de una configuración básica para la protección de la red

Puede ver la lista de directivas y tareas creadas.

Espere la creación de directivas y tareas de completarse antes de ir al paso siguiente del Asistente.

Paso 4. 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.

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 ingresar 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. El número de puerto predeterminado es el 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 de manera predeterminada, y la configuración de autenticación ESMTP no está disponible.

Puede probar la configuración de la notificación por correo electrónico nueva haciendo clic en el botón **Enviar mensaje de prueba**.

Paso 5. Cierre del Asistente de inicio rápido

Para finalizar el Asistente, haga clic en el botón **Finalizar**.

Una vez que haya completado el Asistente de inicio rápido, puede ejecutar el Asistente de despliegue de la protección para instalar automáticamente programas de seguridad o el Agente de red en los dispositivos de su 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 ubica en **DESCUBRIMIENTO Y DESPLIEGUE → DESPLIEGUE Y ASIGNACIÓN → 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.

Iniciar el Asistente de despliegue de la protección

El Asistente de despliegue de la protección también se puede ejecutar manualmente en cualquier momento.

Para iniciar manualmente el Asistente de despliegue de la protección,

En la ventana principal de la aplicación, haga clic en **DESCUBRIMIENTO Y DESPLIEGUE → DESPLIEGUE Y ASIGNACIÓN → ASISTENTE DE DESPLIEGUE DE LA PROTECCIÓN**.

Se abre el Asistente de despliegue de la protección. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

Paso 1. 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.

Paso 2. 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 se activó la distribución automática 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 detalles de la clave de licencia.

Paso 3. 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 de Kaspersky Security Center.

Seleccione la última versión del Agente de red.

Paso 4. 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 resultarle útil para, por ejemplo, ejecutar una tarea en dispositivos que tengan una versión específica de un sistema operativo.

Paso 5. 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 mediante las herramientas de Linux.

  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 habilita esta opción, los paquetes de instalación se transferirán a los dispositivos cliente mediante las herramientas del sistema operativo a través de los puntos 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.

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 habilitada de manera predeterminada.

Paso 6. Eliminar las 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 7. 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.

Paso 8. 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 instaló en los dispositivos cliente.

- **Se necesita una cuenta (no se utiliza el Agente de red)**

  Si selecciona esta opción, podrá especificar los datos de la cuenta con la que se ejecutará el instalador de la aplicación. Puede indicar estos datos si los dispositivos a los que asignó la tarea no tienen instalado el Agente de red.

  Puede especificar varias cuentas de usuario si, por ejemplo, ninguna tiene todos los permisos requeridos en todos los dispositivos a los que se asignó la tarea. En ese caso, la tarea se ejecutará con todas las cuentas agregadas, en orden consecutivo, comenzando por la primera de la lista.

  Si no agrega ninguna cuenta, la tarea se ejecutará con la cuenta con la que se haya iniciado el servicio del Servidor de administración.

Paso 9. Comenzar 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.

Configuración del Servidor de administración

Esta sección describe el proceso de configuración y las propiedades del Servidor de administración de Kaspersky Security Center Linux.

Configuración de la conexión de Kaspersky Security Center 14 Web Console al Servidor de administración

Para configurar los puertos de conexión del Servidor de administración:

1. En la parte superior de la pantalla, haga clic en el ícono de la **Configuración** ( ) al lado del nombre del Servidor de administración requerido.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, elija la sección **Puertos de conexión**.

La aplicación muestra la configuración de conexión principal del servidor seleccionado.

Para definir la lista de direcciones IP admitidas que podrán iniciar sesión en Kaspersky Security Center

De forma predeterminada, para iniciar sesión en Kaspersky Security Center, se puede utilizar cualquier dispositivo que permita abrir la Consola Web de Kaspersky Security Center 14 (en adelante, Consola Web). Si lo desea, puede hacer que el Servidor de administración únicamente acepte conexiones de dispositivos que tengan una dirección IP permitida. Con ello, si un intruso averigua los datos de una cuenta de Kaspersky Security Center, no podrá iniciar sesión en Kaspersky Security Center porque la dirección IP de su dispositivo no estará en la lista de direcciones permitidas.

El control de dirección IP se realiza cuando el usuario inicia sesión en Kaspersky Security Center o ejecuta una aplicación que interactúa con el Servidor de administración a través de la interfaz OpenAPI de Kaspersky Security Center. En este momento, el dispositivo de un usuario 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 Web Console

  Si utiliza Web Console para iniciar sesión en Kaspersky Security Center, puede usar las herramientas de su sistema operativo para configurar un firewall en el dispositivo que tenga instalado el servidor de Web Console. El firewall puede evitar que un intruso inicie sesión en Kaspersky Security Center desde un dispositivo que no sea el que tenga instalado el servidor de 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:

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 su directorio actual a la carpeta de instalación de Kaspersky Security Center (normalmente, /opt/kaspersky/ksc64/sbin).

3. Ingrese el siguiente comando (recuerde utilizar derechos de administrador):
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<direcciones IP>" -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 "<direcciones IP>" -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 (recuerde utilizar derechos de administrador):
   `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.

Visualización del registro de conexiones al 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 la ventana principal de la aplicación, haga clic en el ícono de **Configuración** ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, elija la sección **Puertos de conexión**.

3. Habilitar la opción **Registrar eventos de conexiones del Servidor de administración**.

Todos los eventos adicionales de la conexión con el Servidor de administración, los resultados de autenticación y los errores de SSL se guardarán en el archivo %ProgramData%\KasperskyLab\adminkit\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.

Si el número de eventos de la base de datos alcanza el valor máximo que especificó el administrador, la aplicación elimina los eventos más antiguos y los reemplaza por los nuevos. Cuando el Servidor de administración elimina los eventos antiguos, no puede guardar los nuevos eventos en la base de datos. Durante este período de tiempo, la información sobre los eventos que fueron rechazados se escribe en el Registro de eventos de Kaspersky. Los nuevos eventos se ponen en cola y se guardan en la base de datos una vez finalizada la operación de borrado.

Para limitar la cantidad de eventos que se pueden almacenar en el repositorio de eventos en el Servidor de administración:

1. En la parte superior de la pantalla, haga clic en el ícono de **Configuración** ( ) ubicado junto al nombre del Servidor de administración pertinente.

Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, elija la sección **Repositorio de eventos**. Especifique el número máximo de eventos almacenados en la base de datos.

3. Haga clic en el botón **Guardar**.

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.

Tenga en cuenta que 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.

Puede crear una copia de seguridad de los datos del Servidor de administración mediante uno de los siguientes métodos:

- Al crear y ejecutar una tarea de copia de seguridad de datos a través de Kaspersky Security Center Web Console 14.
- Al ejecutar la utilidad klbackup en el dispositivo que hace instalar 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:

- Base de datos del Servidor de administración (directivas, tareas, parámetros de la aplicación, 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.

La recuperación de los datos del Servidor de administración solo se puede realizar mediante la utilidad klbackup.

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 son creadas a través del Asistente de inicio rápido. Si se eliminó una tarea de copia de seguridad creada por el Asistente de inicio rápido, puede crear 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. Vaya a **DISPOSITIVOS** → **TAREAS**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para agregar tareas.
3. En la primera página del Asistente, en la lista **Aplicación**, seleccione **Kaspersky Security Center 14**. A continuación, en la lista **Tipo de tarea**, seleccione **Copia de seguridad de los datos del Servidor de administración**.
4. Cuando el Asistente se lo solicite, introduzca la siguiente información:
   - Carpeta para almacenamiento de copias de seguridad
   - Contraseña para la copia de seguridad (opcional)
   - Número máximo de copias de seguridad para guardar
5. Si habilita la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de la tarea**, podrá modificar la configuración predeterminada de la tarea. Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Podrá modificar la configuración predeterminada en cualquier otro momento.
6. Haga clic en el botón **Finalizar**.

Se crea la tarea y se la agrega a la lista de tareas.

Utilidad de copia de seguridad y recuperación de datos (klbackup)

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 utilidad klbackup se puede ejecutar en cualquiera de los siguientes modos:

- Interactivo
- No interactivo

Copia de seguridad y recuperación de datos en modo interactivo

Para crear una copia de seguridad de los datos del Servidor de administración en modo interactivo:

1. Ejecute la utilidad klbackup ubicada en la carpeta de instalación de Kaspersky Security Center (generalmente, /opt/kaspersky/ksc64/sbin/klbackup).

   Se inicia el Asistente de copia de seguridad y restauración.

2. En la primera ventana del Asistente, seleccione **Realizar copia de seguridad de los datos del Servidor de administración**.

   Si marcó la opción **Limitar la copia de seguridad o restauración al certificado del Servidor de administración**, solo se guardará una copia de seguridad del certificado del Servidor de administración.

   Haga clic en **Siguiente**.

3. En la siguiente ventana del Asistente, especifique una contraseña y una carpeta de destino para la copia de seguridad y, a continuación, haga clic en el botón **Siguiente** para iniciar la copia de seguridad.

Para recuperar datos del Servidor de administración en modo interactivo:

1. Ejecute la utilidad klbackup ubicada en la carpeta de instalación de Kaspersky Security Center (generalmente, /opt/kaspersky/ksc64/sbin/klbackup). Para iniciar este programa, use la cuenta que haya usado al instalar el Servidor de administración.

   Se inicia el Asistente de copia de seguridad y restauración.

2. En la primera ventana del Asistente, seleccione **Restaurar datos del Servidor de administración**.

   Si selecciona la opción **Limitar la copia de seguridad o restauración al certificado del Servidor de administración**, solo se recuperará el certificado del Servidor de administración.

   Haga clic en **Siguiente**.

3. En la ventana **Opciones de restauración** del Asistente:

   - Especifique la carpeta que contiene una copia de seguridad de los datos del Servidor de administración. Asegúrese de que el nombre del archivo sea backup.zip.

   - Especifique la contraseña que se ingresó durante la creación de la copia de seguridad de los datos.

     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.

4. Haga clic en el botón **Siguiente** para restaurar los datos.

Copia de seguridad y recuperación de datos en modo no interactivo

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 BACKUP_PATH [-logfile LOGFILE] [-use_ts]|[-restore] [-password PASSWORD]
[-online]
```

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 BACKUP_PATH`: Guardar información en la carpeta BACKUP_PATH o usar datos de la carpeta BACKUP_PATH para la recuperación (parámetro obligatorio).

- `-logfile LOGFILE`: 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 BACKUP_PATH.

- `-use_ts`: para guardar datos, copiar información en la carpeta BACKUP_PATH, en la subcarpeta con un nombre que contenga la hora y fecha de la operación y del sistema actual en formato `klbackup YYYY-MM-DD # HH-MM-SS`. Si no se especifica una clave, la información se guarda en la raíz de la carpeta BACKUP_PATH.

  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 `C:\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 partir de la información almacenada en la carpeta BACKUP_PATH. Si no se dispone de una clave, se crea una copia de seguridad de los datos en la carpeta BACKUP_PATH.

- `-password PASSWORD`: guardar o recuperar el certificado del Servidor de administración; para cifrarlo o descifrarlo, utilice la contraseña especificada en el parámetro PASSWORD.

  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.

- `-online`: Para generar la copia de seguridad, crear una instantánea del volumen. Con ello se minimiza el tiempo de inactividad del Servidor de administración. Esta opción no tiene ningún efecto cuando la utilidad se emplea en modo de recuperación.

Mover el Servidor de administración y un servidor de base de datos 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.
- 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, puede ejecutar la tarea de copia de seguridad de datos a través de Kaspersky Security Center Web Console 14 o ejecute la utilidad klbackup.

2. 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, Kaspersky Security Center Web Console 14 y el Agente de red. Además, compruebe que haya puertos utilizados en el Servidor de administración disponibles.

3. En el nuevo dispositivo, instale el sistema de gestión de base de datos (DBMS) que utilizará el Servidor de administración.

   Cuando seleccione un DBMS, tenga en cuenta la cantidad de dispositivos cubiertos por el Servidor de administración.

4. Instale el Servidor de administración en el dispositivo seleccionado.

   Tenga en cuenta que, si mueve el servidor de la base de datos al dispositivo nuevo, debe especificar la dirección local como la dirección IP del dispositivo en el que está instalada la base de datos (el elemento "h" en las instrucciones de Instalación de Kaspersky Security Center). Si necesita mantener el servidor de la base de datos en el dispositivo anterior, ingrese la dirección IP del dispositivo anterior en el elemento "h" de las instrucciones de Instalación de Kaspersky Security Center.

5. Una vez completada la instalación, recupere los datos del Servidor de administración en el nuevo dispositivo mediante la utilidad klbackup.

   > Si utiliza SQL Server como DBMS en los dispositivos anteriores y nuevos, tenga en cuenta que la versión de SQL Server instalada en el dispositivo nuevo debe ser igual o posterior a la versión de SQL Server instalada en el dispositivo anterior. De lo contrario, no podrá recuperar los datos del Servidor de administración en el dispositivo nuevo.

6. Abra Kaspersky Security Center Web Console 14 y conéctese al Servidor de administración.

7. Verifique que todos los dispositivos del cliente estén conectados al Servidor de administración.

8. Desinstale el Servidor de administración y el servidor de la base de datos del dispositivo anterior.

Crear un Servidor de administración virtual

Puede crear servidores de administración virtuales y agregarlos a grupos de administración.

Para crear y agregar un Servidor de administración virtual:

1. En la ventana principal de la aplicación, haga clic en el ícono de **Configuración** ( ) ubicado junto al nombre del Servidor de administración pertinente.

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 del 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.

7. Haga clic en **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 14 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 formas:

- Modifique la instalación existente de Kaspersky Security Center 14 Web Console para agregar el servidor secundario a la lista de servidores de administración fiables. Luego podrá conectarse al Servidor de administración virtual en Kaspersky Security Center 14 Web Console.

  1. En el dispositivo donde está instalada Kaspersky Security Center 14 Web Console, ejecute el archivo ejecutable ksc-web-console-<número de versión>.<número de compilación>.exe en una cuenta con privilegios administrativos.
  2. Se iniciará el asistente de configuración.
  3. En la primera página del asistente, seleccione la opción **Actualizar**.
  4. En la página **Tipo de modificación**, seleccione la opción **Editar la configuración de conexión**.
  5. En la página **Servidores de administración de confianza**, agregue el Servidor de administración secundario necesario.
  6. En la última página del asistente, haga clic en **Modificar** para aplicar la nueva configuración.
  7. Cuando la aplicación se haya reconfigurado, haga clic en el botón **Finalizar**.

- Use Kaspersky Security Center 14 Web Console para conectarse directamente al Servidor de administración secundario donde se creó el servidor virtual. Luego podrá cambiar al Servidor de administración virtual en Kaspersky Security Center 14 Web Console.

- Utilice la consola de administración basada en MMC para conectarse directamente al servidor virtual.

Jerarquía de Servidores de administración

Un MSP puede ejecutar varios Servidores de administración. Puede ser poco conveniente administrar varios Servidores de administración independientes, por lo que se puede aplicar una jerarquía.

En una jerarquía, el Servidor de administración de Linux en Kaspersky Security Center solo puede funcionar como un Servidor secundario manejado por un Servidor de administración principal de Kaspersky Security Center basado en Windows o Kaspersky Security Center Cloud Console.

La configuración "principal/secundario" de dos Servidores de administración proporciona las opciones siguientes:

- Un Servidor de administración secundario hereda directivas y tareas del Servidor de administración principal. De esta forma se previene la duplicación de parámetros.
- 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.

Creación de una jerarquía de servidores de administración: agregar un Servidor de administración secundario

En una jerarquía, el Servidor de administración de Linux en Kaspersky Security Center solo puede funcionar como un Servidor secundario manejado por un Servidor de administración principal de Kaspersky Security Center basado en Windows o Kaspersky Security Center Cloud Console.

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 que se pueda conectar mediante Kaspersky Security Center 14 Web Console:

1. Asegúrese de que el puerto 13000 del futuro Servidor de administración principal esté disponible para la recepción de conexiones desde los Servidores de administración secundarios.
2. En el futuro Servidor de administración principal, haga clic en el ícono de **Configuración** ( ).
3. En la página de propiedades que se abre, haga clic en la pestaña **Servidores de administración**.
4. Seleccione la casilla de verificación junto al nombre del grupo de administración al que desea agregar el Servidor de administración.
5. En la línea del menú, haga clic en **Conectar Servidor de administración secundario**.

   Se inicia el Asistente de conexión del Servidor de administración secundario.

6. En la primera página del asistente, complete los siguientes campos:

- **Nombre para mostrar del Servidor de administración 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 de administración secundario (opcional)**

  Escriba la dirección IP o el nombre de dominio del Servidor de administración secundario.

- **Puerto SSL del Servidor de administración**

  Especifique el número del puerto de SSL en el Servidor de administración principal. El número de puerto predeterminado es el 13000.

- **Puerto de la API del Servidor de administración**

  Especifique el número del puerto en el Servidor de administración principal para recibir conexiones de OpenAPI. El número de puerto predeterminado es el 13299.

- **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.

- **Usar servidor proxy**

  Seleccione esta opción 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**
  - **Nombre de usuario**
  - **Contraseña**

7. Siga las instrucciones adicionales del asistente.

Al concluir el asistente, se creará 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 aparecerá en el Servidor de administración principal, en el grupo de administración en el que se lo haya agregado.

Agregado del Servidor de administración secundario (realizado en el futuro Servidor de administración secundario)

Si no pudo conectarse al futuro Servidor de administración secundario (por ejemplo, debido a que se desconectó temporalmente o no estaba disponible para la conexión), aún puede agregar un Servidor de administración secundario.

Para agregar un Servidor de administración como secundario que no se pueda conectar mediante Kaspersky Security Center 14 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 ícono de **Configuración** ( ).

   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. En el campo **Dirección del Servidor de administración principal**, ingrese el nombre de red del Servidor de administración principal futuro.

   e. Seleccione el archivo guardado anteriormente con el certificado del futuro Servidor de administración principal haciendo clic en **Examinar**.

   f. De ser necesario, seleccione la casilla **Conectar el Servidor de administración principal a un Servidor de administración secundario en DMZ**.

   g. Si la conexión con el futuro Servidor de administración secundario se realiza a través de un servidor proxy, seleccione la opción **Usar servidor proxy** y especifique la configuración de la conexión.

   h. Haga clic en **Guardar**.

Así se constituye la jerarquía "principal/secundario". El Servidor de administración principal comienza recibiendo conexión del Servidor de administración secundario 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.

Ver la lista de servidores de administración secundarios

Para ver la lista de los Servidores de administración secundarios (incluido el virtual), haga lo siguiente:

En la ventana principal de la aplicación, haga clic en el nombre del Servidor de administración, que se encuentra junto al ícono de **Configuración** ( ).

Se muestra una lista desplegable con el nombre de los servidores de administración secundarios (incluidos los virtuales).

Haga clic en alguno de los nombres para interactuar con el Servidor de administración correspondiente.

Los grupos de administración también se muestran, pero aparecen en gris y no están disponibles para su administración en este menú.

Si está conectado a su Servidor de administración principal en Kaspersky Security Center 14 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 formas:

- Modifique la instalación existente de Kaspersky Security Center 14 Web Console para agregar el servidor secundario a la lista de servidores de administración fiables. Luego podrá conectarse al Servidor de administración virtual en Kaspersky Security Center 14 Web Console.

  1. En el dispositivo donde está instalada Kaspersky Security Center 14 Web Console, ejecute el archivo ejecutable ksc-web-console-<número de versión>.<número de compilación>.exe en una cuenta con privilegios administrativos.
  2. Se iniciará el asistente de configuración.
  3. En la primera página del asistente, seleccione la opción **Actualizar**.
  4. En la página **Tipo de modificación**, seleccione la opción **Editar la configuración de conexión**.
  5. En la página **Servidores de administración de confianza**, agregue el Servidor de administración secundario necesario.
  6. En la última página del asistente, haga clic en **Modificar** para aplicar la nueva configuración.
  7. Cuando la aplicación se haya reconfigurado, haga clic en el botón **Finalizar**.

- Use Kaspersky Security Center 14 Web Console para conectarse directamente al Servidor de administración secundario donde se creó el servidor virtual. Luego podrá cambiar al Servidor de administración virtual en Kaspersky Security Center 14 Web Console.

- Utilice la consola de administración basada en MMC para conectarse directamente al servidor virtual.

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. Vaya a **USUARIOS Y ROLES** → **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 los ajustes del usuario, seleccione la pestaña **Seguridad de autenticación**.

4. En la pestaña **Seguridad de autenticación**, seleccione la opción **Solicitar autenticación para comprobar el permiso de modificación de las cuentas de usuario** si desea solicitar las credenciales cada vez que se cambie o modifique la configuración de la cuenta. De lo contrario, seleccione la opción **Permitir a los usuarios modificar esta cuenta sin autenticación adicional**.

5. Haga clic en el botón **Guardar**.

Verificación en dos pasos

Esta sección describe cómo puede utilizar la verificación en dos pasos para reducir el riesgo de acceso no autorizado a Kaspersky Security Center 14 Web Console.

Escenario: configurar la verificación en dos pasos para todos los usuarios

Este escenario describe cómo habilitar la verificación en dos pasos para todos los usuarios y cómo excluir cuentas de usuario de la verificación en dos pasos. Si no habilitó la verificación en dos pasos para su cuenta antes de habilitarla para otros usuarios, la aplicación abre primero la ventana para habilitar la verificación en dos pasos para su cuenta. Este escenario también describe cómo habilitar la verificación en dos pasos para su cuenta.

> Si habilitó la verificación en dos pasos para su cuenta, puede pasar a la etapa de habilitación de la verificación en dos pasos para todos los usuarios.

Requisitos previos

Antes de comenzar:

- Asegúrese de que su cuenta de usuario tenga el derecho de Modificar ACL de objeto del área funcional **Características generales: Permisos de usuario** para modificar la configuración de seguridad de las cuentas de otros usuarios.

- Asegúrese de que los demás usuarios del Servidor de administración instalen una aplicación de autenticación en sus dispositivos.

Etapas

La habilitación de la verificación en dos pasos para todos los usuarios se realiza en etapas:

1. **Instalación de una aplicación de autenticación en un dispositivo**

   Puede instalar Google Authenticator, Microsoft Authenticator o cualquier otra aplicación de autenticación que admita el algoritmo de contraseña de un solo uso basada en el tiempo.

2. **Sincronizar la hora de la aplicación de autenticación con la hora del dispositivo en el que está instalado el Servidor de administración**

   Asegúrese de que la hora establecida en la aplicación de autenticación esté sincronizada con la hora del Servidor de administración.

3. **Habilitar la verificación en dos pasos para su cuenta y recibir la clave secreta de su cuenta**

   Después de habilitar la verificación en dos pasos para su cuenta, puede habilitar la verificación en dos pasos para todos los usuarios.

4. **Habilitación de la verificación en dos pasos para todos los usuarios**

   Los usuarios con la verificación en dos pasos habilitada deben usarla para iniciar sesión en el Servidor de administración.

5. **Editar el nombre del emisor de un código de seguridad**

   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.

6. **Excluir las cuentas de usuario para las que no es necesario habilitar la verificación en dos pasos**

   Si es necesario, puede excluir a los usuarios de la verificación en dos pasos. Los usuarios con cuentas excluidas no tienen que utilizar la verificación en dos pasos para iniciar sesión en el Servidor de administración.

Resultados

Una vez completado este escenario:

- La verificación en dos pasos está habilitada para su cuenta.
- La verificación en dos pasos está habilitada para todas las cuentas de usuario del Servidor de administración, excepto para las cuentas de usuario que fueron excluidas.

Sobre la verificación en dos pasos para una cuenta

Kaspersky Security Center Linux proporciona una verificación en dos pasos para los usuarios de Kaspersky Security Center 14 Web Console. Cuando la verificación en dos pasos está habilitada para su cuenta, cada vez que inicia sesión en Kaspersky Security Center 14 Web Console, ingresa su nombre de usuario, contraseña y un código de seguridad adicional de un solo uso. Para recibir un código de seguridad de un solo uso, debe tener una aplicación de autenticación en su equipo o dispositivo móvil.

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. El nombre del emisor se utiliza como identificador del Servidor de administración en la aplicación de autenticación. Si cambia el nombre del emisor del código de seguridad, debe emitir una nueva clave secreta y pasarla a la aplicación de autenticación. Los códigos de seguridad son de un solo uso y válidos por hasta 90 segundos (el tiempo exacto puede variar).

Cualquier usuario para el que esté habilitada la verificación en dos pasos puede volver a emitir su clave secreta. Cuando un usuario se autentifica con la clave secreta reemitida y la utiliza para iniciar sesión, el Servidor de administración guarda la nueva clave secreta de la cuenta de usuario. Si el usuario ingresa la nueva clave secreta de manera incorrecta, el Servidor de administración no guarda la nueva clave secreta y deja la clave secreta actual válida para la autenticación posterior.

Cualquier software de autenticación que admita el algoritmo de contraseña de un solo uso basado en el tiempo (TOTP) se puede utilizar como una aplicación de autenticación, por ejemplo, Google Authenticator. Para generar el código de seguridad, debe sincronizar la hora establecida en la aplicación de autenticación con la hora establecida para el Servidor de administración.

Una 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. Pasa la clave secreta generada o el código QR a la aplicación de autenticación.
3. La aplicación de autenticación genera un código de seguridad de un solo uso que se pasa a la ventana de autenticación del Servidor de administración.

Recomendamos que instale una aplicación de autenticación en varios dispositivos. Guarde la clave secreta (o el código QR) y guárdela en un lugar seguro. Esto le ayudará a restaurar el acceso a Kaspersky Security Center 14 Web Console en caso de que pierda el acceso a su dispositivo móvil.

Para asegurar el uso de Kaspersky Security Center, puede habilitar la verificación en dos pasos para su cuenta y habilitar la verificación en dos pasos para todos los usuarios.

Puede excluir cuentas de la verificación en dos pasos. Puede ser necesario para las cuentas de servicio que no pueden recibir un código de seguridad para la autenticación.

La verificación en dos pasos funciona de acuerdo con las siguientes reglas:

- Solo una cuenta de usuario que tenga el derecho Modificar ACL de objeto en el área funcional **Características generales: Permisos de usuario** puede habilitar la verificación en dos pasos para todos los usuarios.
- Solo un usuario que haya habilitado la verificación en dos pasos para su propia cuenta puede habilitar la opción de verificación en dos pasos para todos los usuarios.
- Solo un usuario que haya habilitado la verificación en dos pasos para su propia cuenta puede excluir otras cuentas de usuario de la lista de verificación en dos pasos habilitada para todos los usuarios.
- Un usuario puede habilitar la verificación en dos pasos solo para su cuenta.
- Una cuenta de usuario que tiene el derecho Modificar ACL de objeto en el área funcional **Características generales: Permisos de usuario** y ha iniciado sesión en Kaspersky Security Center 14 Web Console mediante la verificación en dos pasos puede deshabilitar la verificación en dos pasos: para cualquier otro usuario solo si la verificación en dos pasos para todos los usuarios está deshabilitada, para un usuario excluido de la lista de la verificación en dos pasos que está habilitada para todos los usuarios.
- Cualquier usuario que haya iniciado sesión en Kaspersky Security Center 14 Web Console mediante la verificación en dos pasos puede volver a emitir su clave secreta.
- Puede habilitar la opción de verificación en dos pasos para todos los usuarios del Servidor de administración con el que está trabajando actualmente. Si habilita esta opción en el Servidor de administración, también la habilita para las cuentas de usuario de sus Servidores de administración virtuales y deshabilita la verificación en dos pasos para las cuentas de usuario de los Servidores de administración secundarios.

Si la verificación en dos pasos está habilitada para una cuenta de usuario en el Servidor de administración de Kaspersky Security Center versión 13 o superior, el usuario no podrá iniciar sesión en Kaspersky Security Center Web Console versiones 12, 12.1 o 12.2.

Habilitación de la verificación en dos pasos para su cuenta

Puede habilitar la verificación en dos pasos solo para su cuenta.

Antes de habilitar la verificación en dos pasos para su cuenta, verifique que haya una aplicación de autenticación instalada en su dispositivo móvil. Asegúrese de que la hora establecida en la aplicación de autenticación esté sincronizada con la hora establecida del dispositivo en el que está instalado el Servidor de administración.

Para habilitar la verificación en dos pasos para una cuenta de usuario, siga estos pasos:

1. Vaya a **USUARIOS Y ROLES** → **USUARIOS**.
2. Haga clic en el nombre de su cuenta.
3. En la ventana que se abre con los ajustes del usuario, seleccione la pestaña **Protección de cuentas**.
4. En la pestaña **Protección de cuentas**:
   - Seleccione la opción **Solicitar nombre de usuario, contraseña y código de seguridad (verificación en dos pasos)** si desea habilitar la verificación en dos pasos para una cuenta de usuario:
     - En la ventana de verificación en dos pasos que se abre, ingrese la clave secreta en la aplicación de autenticación o escanee el código QR y reciba el código de seguridad de un solo uso.

       Puede especificar la clave secreta en la aplicación de autenticación manualmente o escanear el código QR con su dispositivo móvil.
     - En la ventana de verificación en dos pasos, especifique el código de seguridad generado por la aplicación de autenticación y, a continuación, haga clic en el botón **Confirmar y aplicar**.
5. Haga clic en el botón **Guardar**.

La verificación en dos pasos está habilitada para su cuenta.

Habilitación de la verificación en dos pasos para todos los usuarios

Puede habilitar la verificación en dos pasos para todos los usuarios del Servidor de administración si su cuenta tiene el derecho Modificar ACL de objeto en el área funcional **Características generales: Permisos de usuario** y si es autenticado mediante el uso de la verificación en dos pasos. Si no habilitó la verificación en dos pasos para su cuenta antes de habilitarla para todos los usuarios, la aplicación abre la ventana para habilitar la verificación en dos pasos para su cuenta.

Para habilitar la verificación en dos pasos para todos los usuarios, siga estos pasos:

1. En la ventana principal de la aplicación, haga clic en el ícono de **Configuración** ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Seguridad de autenticación** de la ventana de propiedades, cambie el botón de activación de la opción **verificación en dos pasos para todos los usuarios** a la posición de habilitado.

La verificación en dos pasos está habilitada para todos los usuarios. A partir de ahora, los usuarios del Servidor de administración, incluidos los usuarios que se agregaron después de habilitar la verificación en dos pasos para todos los usuarios, tienen que configurar la verificación en dos pasos para sus cuentas, excepto los usuarios que están excluidos de la verificación en dos pasos.

Deshabilitar la verificación en dos pasos para una cuenta de usuario

Puede deshabilitar la verificación en dos pasos para su cuenta, así como para una cuenta de cualquier otro usuario.

> Puede deshabilitar la verificación en dos pasos de la cuenta de otro usuario solo si su cuenta tiene el derecho Modificar ACL de objeto en el área funcional **Características generales: Permisos de usuario**.

Para deshabilitar la verificación en dos pasos para una cuenta de usuario, siga estos pasos:

1. Vaya a **USUARIOS Y ROLES** → **USUARIOS**.

2. Haga doble clic en la cuenta de usuario interna para la que desea deshabilitar la verificación en dos pasos. Puede ser su propia cuenta o la de cualquier otro usuario.

3. En la ventana que se abre con los ajustes del usuario, seleccione la pestaña **Protección de cuentas**.

4. En la pestaña **Protección de cuentas**, seleccione la opción **Solo solicitar nombre de usuario y contraseña** si desea deshabilitar la verificación en dos pasos para una cuenta de usuario.

5. Haga clic en el botón **Guardar**.

La verificación en dos pasos está deshabilitada para la cuenta de usuario.

Deshabilitar la verificación en dos pasos para todos los usuarios

Puede deshabilitar la verificación en dos pasos para todos los usuarios si la verificación en dos pasos está habilitada para su cuenta y su cuenta tiene el derecho Modificar ACL de objeto en el área funcional **Características generales: Permisos de usuario**. Si la verificación en dos pasos está deshabilitada para su cuenta, debe habilitar la verificación en dos pasos para su cuenta antes de deshabilitarla para todos los usuarios.

Para deshabilitar la verificación en dos pasos para todos los usuarios, siga estos pasos:

1. En la ventana principal de la aplicación, haga clic en el ícono de **Configuración** ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Seguridad de autenticación** de la ventana de propiedades, cambie el botón de activación de la opción **verificación en dos pasos para todos los usuarios** a la posición de deshabilitado.

3. Ingrese las credenciales de su cuenta en la ventana de autenticación.

La verificación en dos pasos está inhabilitada para todos los usuarios.

Excluir cuentas de la verificación en dos pasos

Puede excluir las cuentas de usuario de la verificación en dos pasos si tiene el derecho Modificar ACL de objeto en el área funcional **Características generales: Permisos de usuario**.

Si una cuenta de usuario se excluye de la lista de verificación en dos pasos para todos los usuarios, este usuario no tiene que utilizar la verificación en dos pasos.

> Puede ser necesario excluir cuentas de la verificación en dos pasos para las cuentas de servicio que no pueden pasar el código de seguridad durante la autenticación.

Si quiere excluir algunas cuentas de usuario de la verificación en dos pasos:

1. En la ventana principal de la aplicación, haga clic en el ícono de **Configuración** ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Seguridad de autenticación** de la ventana de propiedades, en la tabla de exclusiones de la verificación en dos pasos haga clic en el botón **Agregar**.

3. En la ventana que se abre:

   a. Seleccione las cuentas de usuario que desea excluir.

   b. Haga clic en el botón **Aceptar**.

Las cuentas de usuario seleccionadas se excluyen de la verificación en dos pasos.

Generar una nueva clave secreta

Puede generar una nueva clave secreta para una verificación en dos pasos para su cuenta solo si está autorizado a utilizar la verificación en dos pasos.

Para generar una nueva clave secreta para una cuenta de usuario, siga los siguientes pasos:

1. Vaya a **USUARIOS Y ROLES** → **USUARIOS**.

2. Haga clic en el nombre de la cuenta de usuario para la que desea generar una nueva clave secreta para la verificación en dos pasos.

3. En la ventana que se abre con los ajustes del usuario, seleccione la pestaña **Protección de cuentas**.

4. En la pestaña **Protección de cuentas**, haga clic en el vínculo **Generar una clave secreta nueva**.

5. En la ventana de verificación en dos pasos que se abre, especifique una nueva clave de seguridad generada por la aplicación de autenticación.

6. Haga clic en el botón **Confirmar y aplicar**.

Se genera una nueva clave secreta para el usuario.

Si pierde su dispositivo móvil, puede instalar una aplicación de autenticación en otro dispositivo móvil y generar una nueva clave secreta para restaurar el acceso a Kaspersky Security Center 14 Web Console.

Editar el nombre del emisor de un código de seguridad

Puede tener varios identificadores (se denominan 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.

Después de cambiar el nombre del emisor del código de seguridad, hay que volver a emitir una nueva clave secreta y pasarla a la aplicación de autenticación.

Para especificar un nuevo nombre de emisor del código de seguridad, siga estos pasos:

1. En la ventana principal de la aplicación, haga clic en el ícono de **Configuración** ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la ventana que se abre con los ajustes del usuario, seleccione la pestaña **Protección de cuentas**.

3. En la pestaña **Protección de cuentas**, haga clic en el vínculo **Editar**.

   Se abre la sección **Editar el emisor del código de seguridad**.

4. Se especifica un nuevo nombre de emisor del código de seguridad.

5. Haga clic en el botón **Aceptar**.

Se especifica un nuevo nombre de emisor del código de seguridad para el Servidor de administración.

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 forma predeterminada, el número máximo de intentos permitidos para introducir una contraseña 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.

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.

Para cambiar las credenciales de DBMS en un entorno de Linux mediante klsrvswch.exe:

1. Inicie una línea de comando de Linux.
2. Especifique la utilidad klsrvconfig en la ventana de línea de comando abierta:

   ```
   sudo /opt/kaspersky/ksc64/sbin/klsrvconfig -set_dbms_cred
   ```
3. Especifique un nuevo nombre de cuenta. Debe especificar las credenciales de una cuenta que exista en el DBMS.
4. Introduzca una nueva contraseña.
5. Especifique la nueva contraseña para su confirmación.

Se cambiaron las credenciales de DBMS.

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 la parte superior de la pantalla, haga clic en el ícono de **Configuración** () ubicado junto al nombre del Servidor de administración principal.
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.

Configuración de la interfaz

Puede configurar la interfaz de Kaspersky Security Center 14 Web Console para mostrar y ocultar secciones y elementos de la interfaz, según las funciones que se utilicen.

Para configurar la interfaz de Kaspersky Security Center 14 Web Console y adaptarla a las características que utilice:

1. En la ventana principal de la aplicación, haga clic en el menú de la cuenta.
2. En el menú desplegable, seleccione **Opciones de interfaz**.
3. En la ventana **Opciones de interfaz** que se abre, habilite o deshabilite las opciones obligatorias.
4. Haga clic en **Guardar**.

Luego, la consola muestra secciones en el menú principal de acuerdo con las opciones habilitadas. Por ejemplo, si habilita **Mostrar alertas EDR**, la sección **SUPERVISIÓN E INFORMES → ALERTAS** aparece en el menú principal.

Descubrimiento de dispositivos conectados a la red

Esta sección describe la búsqueda y la detección de dispositivos conectados a una red.

Kaspersky Security Center le permite encontrar dispositivos según 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 Kaspersky Security Center y sus Servidores de administración secundarios.
- Dispositivos no asignados administrados por el Servidor de administración de Kaspersky Security Center 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**

   Cuando complete el Asistente de inicio rápido, realice la detección de dispositivos manualmente.

2. **Configurando futuros sondeos**

   Asegúrese de que el sondeo de intervalos 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.

3. **Configurar reglas para que los dispositivos descubiertos se agreguen a grupos de administración (opcional)**

   Si aparecen nuevos dispositivos de la red, que se detectan durante las encuestas regulares y 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 arreglan según las reglas configuradas. (O, si no se configura ninguna regla, los dispositivos se quedan en el grupo **Dispositivos no asignados**).

Sondeo de intervalos IP

Kaspersky Security Center intenta realizar una resolución de nombres inversa para cada dirección de Ipv4 desde el rango especificado a un nombre de DNS mediante las solicitudes de DNS estándar. Cuando la operación es exitosa, el servidor envía al nombre recibido una `solicitud de eco ICMP` (el mismo tipo de solicitud que se utiliza en el comando ping). Si el dispositivo responde, la información se agrega a la base de datos de Kaspersky Security Center. La resolución de nombres inversa es necesaria para excluir dispositivos de red que pueden tener dirección IP, pero que no son computadoras (por ejemplo, impresoras y 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, Kaspersky Security Center obtiene rangos de IP para el sondeo desde 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 incluye automáticamente la red 192.168.0.0/24 en la lista de direcciones del sondeo. Kaspersky Security Center sondea todas las direcciones desde 192.168.0.1 hasta 192.168.0.254.

Si solo está habilitado el sondeo de rango de IP, Kaspersky Security Center detecta dispositivos solo con direcciones IPv4. Si su red incluye dispositivos IPv6, active Sondeo de Zeroconf de dispositivos.

Cómo ver y modificar la configuración del sondeo de intervalos IP

Para ver y modificar las propiedades del sondeo de intervalos IP:

1. Vaya a **DESCUBRIMIENTO Y DESPLIEGUE → DESCUBRIMIENTO → INTERVALOS IP**.
2. Haga clic en el botón **Propiedades**.

   Se abre la ventana de 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.

- **Cada mes en los días especificados de semanas seleccionadas**

  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 manera predeterminada.

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, Kaspersky Security Center obtiene rangos de IP para el sondeo desde 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 incluye automáticamente la red 192.168.0.0/24 en la lista de direcciones del sondeo. Kaspersky Security Center sondea todas las direcciones desde 192.168.0.1 hasta 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 de Zeroconf, Kaspersky Security Center sondea toda la red.

Para agregar un nuevo intervalo IP:

1. Vaya a **DESCUBRIMIENTO Y DESPLIEGUE → DESCUBRIMIENTO → 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 rango 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. De manera predeterminada, los resultados de un sondeo tienen una vida útil 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.
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**. Cuando se complete el sondeo, haga clic en el botón **Dispositivos** para ver la lista de dispositivos descubiertos. 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. 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 rango 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 puede sondear las redes que tienen dispositivos con direcciones IPv6. En este caso, no se especifican los rangos de IP y Kaspersky Security Center sondea toda la red mediante el uso de una red de configuración cero (denominada *Zeroconf*). Para comenzar a usar Zeroconf, debe instalar la utilidad avahi-browse en el dispositivo Linux que sondea las redes: Servidor de administración o un punto de distribución.

Para habilitar el sondeo de Zeroconf:

1. 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**.

Luego, Kaspersky Security Center empieza a sondear su red. En este caso, se ignoran los rangos de IP especificados.

Etiquetas de dispositivo

En esta sección, se brinda una descripción de las etiquetas para dispositivos y se ofrecen instrucciones para crearlas y modificarlas, así como para etiquetar dispositivos de forma manual o automática.

Acerca de las etiquetas de dispositivo

Kaspersky Security Center le permite *etiquetar* dispositivos. Las etiquetas son rótulos que se asignan a los dispositivos y que permiten agruparlos, describirlos o encontrarlos. Pueden utilizarse para crear selecciones, hallar dispositivos específicos y distribuir dispositivos en grupos de administración.

Puede etiquetar dispositivos manual o automáticamente. Utilice el etiquetado manual para rotular dispositivos puntuales. Kaspersky Security Center realiza el etiquetado automático de acuerdo con las reglas de etiquetado especificadas.

Los dispositivos se etiquetan automáticamente cuando reúnen las condiciones de las reglas configuradas. 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.

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 **DISPOSITIVOS → ETIQUETAS → ETIQUETAS DEL DISPOSITIVO**.
2. Haga clic en **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 **DISPOSITIVOS → ETIQUETAS → ETIQUETAS DEL DISPOSITIVO**.
2. Haga clic en el nombre de la etiqueta que desee modificar.
   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

Para eliminar una etiqueta de dispositivo:

1. En el menú principal, vaya a **DISPOSITIVOS → ETIQUETAS → ETIQUETAS DEL DISPOSITIVO**.
2. En la lista, seleccione el botón de opción adyacente a la etiqueta que desee eliminar.
3. 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.

> La etiqueta eliminada no desaparecerá automáticamente de las reglas de etiquetado automático. Después de eliminar la etiqueta, se la asignará a un nuevo dispositivo solo cuando el dispositivo reúna las condiciones de una regla que asigne esa etiqueta.

Ver los dispositivos que tienen asignada una etiqueta

Para ver cuáles dispositivos tienen asignada una etiqueta:

1. En el menú principal, vaya a **DISPOSITIVOS → ETIQUETAS → ETIQUETAS DEL DISPOSITIVO**.
2. Haga clic en el vínculo **Ver dispositivos** junto a una etiqueta para ver a qué dispositivos se la ha asignado.

   Si no ve el vínculo **Ver dispositivos** al lado de una etiqueta, significa que no se la ha asignado a ningún dispositivo.

La lista de dispositivos que aparece muestra solo los dispositivos que tienen asignada la etiqueta.

Para regresar a la lista de etiquetas de dispositivo, haga clic en el botón **Atrás** de su navegador.

Ver las etiquetas asignadas a un dispositivo

Para ver las etiquetas asignadas a un dispositivo:

1. En el menú principal, vaya a **DISPOSITIVOS → 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.

Puede asignar otra etiqueta al dispositivo o quitarle una etiqueta que tenga asignada. También puede ver una lista con todas las etiquetas de dispositivo creadas en el Servidor de administración.

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 **Sin inconvenientes** 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. Vea las etiquetas asignadas al dispositivo al que desee quitarle una etiqueta.
2. Active la casilla de verificación adyacente a la etiqueta que desee quitar del dispositivo.
3. Haga clic en el botón **Desasignar etiqueta**.
4. En la ventana que se abre, haga clic en **Sí**.

El dispositivo pierde la etiqueta.

> La etiqueta desasignada no se elimina. Si lo desea, puede eliminarla manualmente.

Ver las reglas de etiquetado automático de dispositivos

Para ver las reglas que se utilizan para etiquetar dispositivos automáticamente,

Realice cualquiera de las siguientes acciones:

- En el menú principal, vaya a **DISPOSITIVOS → ETIQUETAS → REGLAS DE ETIQUETADO AUTOMÁTICO**.
- En el menú principal, vaya a **DISPOSITIVOS → ETIQUETAS** y, luego, haga clic en el enlace **Configurar reglas de etiquetado automático**.
- Vea las etiquetas asignadas a un dispositivo y después haga clic en el botón **Configuración**.

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 cualquiera 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 cualquiera 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, active 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 las condiciones de activación de la regla. 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.
   - **Aplicaciones**: presencia del Agente de red en el dispositivo, tipo y versión de sistema operativo, arquitectura del sistema operativo.
   - **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. Active la casilla de verificación ubicada junto a la regla que desee eliminar.
3. Haga clic en **Eliminar**.
4. En la ventana que se abre, haga clic de nuevo en **Eliminar**.

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.

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.

Acerca de las etiquetas de aplicación

Kaspersky Security Center Linux permite etiquetar aplicaciones de terceros (aplicaciones creadas por vendedores de software que no son de Kaspersky). 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 **OPERACIONES → 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 **OPERACIONES → APLICACIONES DE TERCEROS → ETIQUETAS DE APLICACIÓN**.
2. Active la casilla de verificación 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 **OPERACIONES → 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 de verificación 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 **OPERACIONES → 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 de verificación 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 **OPERACIONES → APLICACIONES DE TERCEROS → ETIQUETAS DE APLICACIÓN**.

2. En la lista, seleccione la etiqueta de aplicación que desee eliminar.

3. 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.

Despliegue del software de Kaspersky

En esta sección se describe cómo puede usar Kaspersky Security Center 14 Web Console para desplegar las aplicaciones de Kaspersky en los dispositivos cliente de su organización.

Escenario: Despliegue inicial de las aplicaciones de Kaspersky

En este escenario se explica cómo desplegar aplicaciones de Kaspersky por medio de Kaspersky Security Center 14 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.

El despliegue de las aplicaciones de Kaspersky se divide en etapas:

1. **Descargar el complemento web de administración para la aplicación**

   Descargue el complemento web de administración para Kaspersky Endpoint Security para Linux desde el sitio web de Kaspersky y, luego, agregue el complemento a Kaspersky Security Center 14 Web Console.

2. **Descargar y crear paquetes de instalación para aplicaciones de Kaspersky**

   Descargar el paquete de distribución del Agente de red desde el sitio web de Kaspersky y, luego, crear un paquete de instalación del Agente de red.

   Puede usar el paquete de distribución descargado para instalar el Agente de red localmente. Para ello, siga las instrucciones proporcionadas en la documentación de Kaspersky Endpoint Security para Linux.

3. **Descargar y crear un paquete de instalación para Kaspersky Endpoint Security para Linux**

   Descargue el paquete de distribución de Kaspersky Endpoint Security para Linux desde el sitio web de Kaspersky y, luego, crear un paquete de instalación de Kaspersky Endpoint Security para Linux.

4. **Creación de paquetes de instalación independientes (opcional)**

   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 utiliza paquetes independientes para instalar las aplicaciones de Kaspersky, se pueden ignorar las etapas 5 y 6 a continuación.

5. **Creación, configuración y ejecución de la tarea de instalación remota**

   Este paso es parte del Asistente de inicio rápido. Si decide no ejecutar el Asistente de despliegue de la protección, debe crear esta tarea manualmente y configurarla 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.

6. **Creación y configuración de tareas.**

   La tarea *Instalar actualización* de Kaspersky Endpoint Security para Linux debe estar configurada.

Este paso forma parte del Asistente de inicio rápido: la tarea se crea y configura automáticamente con la configuración predeterminada. Si no ejecutó el Asistente, debe crear esta tarea manualmente y configurarlas manualmente. Si utiliza el Asistente de inicio rápido, asegúrese de que la programación de la tarea cumpla con sus requisitos. (De forma predeterminada, el inicio programado para la tarea se establece en **Manualmente**, pero es posible que desee elegir otra opción).

7. **Creando directivas**

   Crear la directiva para Kaspersky Endpoint Security para Linux manualmente o a través del Asistente de inicio rápido. Puede utilizar la configuración predeterminada de la directiva; también puede modificar la configuración predeterminada de la directiva de acuerdo con sus necesidades en cualquier momento.

8. **Verificación de los resultados**

   Asegúrese de que la distribución se completó 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.

Añadir complementos de administración para aplicaciones de Kaspersky

Para desplegar una aplicación Kaspersky, como Kaspersky Endpoint Security para Linux, debe descargar el complemento de administración de la aplicación.

Para descargar e instalar un complemento de administración para una aplicación de Kaspersky:

1. Descargue el complemento web de administración para Kaspersky Endpoint Security para Linux del sitio web de Kaspersky.
2. Abrir Kaspersky Security Center 14 Web Console.
3. En la lista desplegable **Configuración de la consola**, seleccione **Complementos web**.

   Se muestra una lista de complementos de administración disponibles.
4. Haga clic en el botón **Agregar desde archivo**.

   Se muestra la ventana **Agregar desde archivo**.
5. Haga clic en el botón **Cargar archivo ZIP**.
6. Especifique el archivo ZIP descargado del complemento web.
7. Haga clic en el botón **Cargar firma**.
8. Especifique el archivo TXT descargado de la firma del complemento web.

9. Haga clic en el botón **Agregar**.

   Kaspersky Security Center verifica los archivos cargados y luego agrega e instala el complemento web.

10. Cuando la instalación se haya completado, haga clic en **Aceptar**.

El complemento web de administración se instala con la configuración predeterminada y se muestra en la lista de complementos web de administración.

Creación de 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.

Al crear un paquete de instalación personalizada, puede especificar parámetros de línea de comandos, por ejemplo, para instalar la aplicación en modo silencioso.

Para crear un paquete de instalación personalizado:

1. Realice una de las siguientes acciones:

   - Vaya a **DESCUBRIMIENTO Y DESPLIEGUE → DESPLIEGUE Y ASIGNACIÓN → PAQUETES DE INSTALACIÓN**.
   - Vaya a **OPERACIONES → REPOSITORIOS → 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. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

3. En la primera página del Asistente, seleccione **Crear un paquete de instalación a partir de un archivo**.

4. En la siguiente página del Asistente, 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.

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. En la siguiente página del Asistente, 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.

   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.

   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 adecuado.

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 de un paquete de instalación:
  - **Nombre**. Nombre del paquete de instalación personalizado.
  - **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.
  - **Sistema operativo**. 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.

Un paquete de instalación independiente es un archivo ejecutable (installer.exe) que puede almacenar en el Servidor web o en una carpeta compartida, enviar por correo electrónico o transferir al dispositivo cliente mediante algún otro método. 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. Realice una de las siguientes acciones:

   - Vaya a **DESCUBRIMIENTO Y DESPLIEGUE → DESPLIEGUE Y ASIGNACIÓN → PAQUETES DE INSTALACIÓN**.
   - Vaya a **OPERACIONES → REPOSITORIOS → PAQUETES DE INSTALACIÓN**.

   Se muestra una lista de paquetes de instalación disponibles en el Servidor de administración.

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.

3. Seleccione la opción **Usar un paquete independiente**.

   Se inicia el Asistente de creación de un paquete de instalación independiente. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

4. En la primera página del Asistente, 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.

   Esta opción está habilitada de manera 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 la página **Mover a lista de dispositivos administrados** del Asistente, la opción **No mover los dispositivos** se selecciona de forma predeterminada. Si no desea que el dispositivo cliente se mueva a un grupo de administración después de la instalación del Agente de red, deje seleccionada esta opción.

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**.

6. En la página siguiente del Asistente, cuando finalice el proceso de creación del paquete de instalación independiente, haga clic en el botón **FINALIZAR**.

   El Asistente de creación de un paquete de instalación independiente se cierra.

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.

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, se muestran las siguientes propiedades:

- **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.

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 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. Esas tareas se crean y se asignan a dispositivos a través de un Asistente dedicado. Para asignar una tarea a dispositivos con mayor rapidez y facilidad, puede especificar los dispositivos en la ventana Asistente de cualquier modo que le resulte cómodo:

- **Seleccionar dispositivos de la red detectados por el Servidor de administración**. En este caso, la tarea se asigna a dispositivos específicos. Estos pueden ser tanto dispositivos asignados a grupos de administración como dispositivos no asignados.
- **Especificar las direcciones de los dispositivos manualmente o importarlas de una lista**. Puede especificar nombres de DNS, direcciones IP y subredes IP de los dispositivos a los cuales debe 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.
- **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.

Para una instalación remota correcta en el dispositivo en el cual no se instaló ningún Agente de red, se deben abrir los siguientes puertos: a) TCP 139 y 445; b) UDP 137 y 138. De manera predeterminada, estos puertos se abren en todos los dispositivos incluidos en el dominio. La utilidad de preparación para instalaciones remotas los abre automáticamente.

Instalar una aplicación en los dispositivos seleccionados

Esta sección contiene información sobre cómo instalar una aplicación de forma remota en un grupo de administración, dispositivos con direcciones IP específicas o una selección de dispositivos administrados.

Para instalar una aplicación en dispositivos específicos:

1. Establezca una conexión con el Servidor de administración que controla los dispositivos relevantes.
2. En el menú principal, vaya a **DISPOSITIVOS** → **TAREAS**.
3. Haga clic en **Agregar**.

   Se inicia el Asistente para agregar tareas.
4. En la sección **Tipo de tarea**, seleccione **Instalar aplicación de forma remota**.
5. 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.

   - **Especificar las direcciones de los dispositivos manualmente o importarlas de una lista**

     Puede especificar nombres de DNS, direcciones IP y subredes IP de los dispositivos a los cuales debe asignar la tarea.

     Puede 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 en los dispositivos que utilizan los contadores o si quiere analizar los dispositivos de una subred 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 resultarle útil para, por ejemplo, ejecutar una tarea en dispositivos que tengan una versión específica de un sistema operativo.
6. Siga las instrucciones del Asistente.

   El Asistente para agregar tareas crea una tarea de instalación remota para la aplicación seleccionada en dispositivos específicos. Si seleccionó la opción **Asignar tarea a un grupo de administración**, la tarea es grupal.
7. 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 dispositivos especificados.

Instalar una aplicación mediante las directivas de grupo de Active Directory

Si quiere instalar una aplicación de Kaspersky en sus dispositivos administrados a través de Kaspersky Security Center, puede hacerlo mediante directivas de grupo de Active Directory.

Para instalar una aplicación utilizando directivas de grupo de Active Directory, el paquete de instalación de la misma debe incluir el Agente de red.

Para instalar una aplicación mediante las directivas de grupo de Active Directory:

1. Ejecute el Asistente de implementación de protección. Siga las instrucciones del Asistente.
2. En la página Configuración de la tarea de instalación remota del Asistente, seleccione la opción **Asignar la instalación del paquete en las directivas de grupo de Active Directory**.
3. En la sección Seleccione las cuentas con las que se accederá a los dispositivos, elija la opción **Se necesita una cuenta (no se utiliza el Agente de red)**.
4. Agregue la cuenta con privilegios de administrador en el dispositivo donde está instalado Kaspersky Security Center o la cuenta incluida en el grupo de dominios Propietarios del creador de directivas de grupo.
5. Asigne los permisos necesarios a la cuenta seleccionada:
   a. Vaya a **Panel de control** → **Herramientas administrativas** y abra **Administración de directivas de grupo**.
   b. Haga clic en el nodo del dominio pertinente.
   c. Haga clic en la sección **Delegación**.
   d. En la lista desplegable **Permiso**, seleccione **Vincular objetos de directiva de grupo**.
   e. Haga clic en **Agregar**.
   f. En la ventana **Seleccionar usuario, equipo o grupo** que se abre, seleccione la cuenta pertinente.
   g. Haga clic en **Aceptar** para cerrar la ventana **Seleccionar usuario, equipo o grupo**.
   h. En la lista **Grupos y usuarios**, seleccione la cuenta que acaba de agregar y, luego, haga clic en **Avanzado** → **Avanzado**.
   i. En la lista **Entradas de permiso**, haga doble clic en la cuenta que acaba de agregar.
   j. Otorgue los siguientes permisos:
      - **Crear objetos de grupo**
      - **Eliminar objetos de grupo**
      - **Crear objetos de contenedor de directivas de grupo**
      - **Eliminar objetos de contenedor de directivas de grupo**
   k. Haga clic en **Aceptar** para guardar los cambios.
6. Siga las instrucciones del Asistente para configurar las demás opciones.
7. Ejecute de forma manual la tarea de instalación remota creada o espere a que se inicie según la programación.

Se inicia la siguiente secuencia de instalación remota:

1. Cuando la tarea está en ejecución, en cada dominio que incluya cualquier dispositivo cliente del grupo especificado se crean los siguientes objetos:

   - Un objeto de directiva de grupo (GPO) bajo el nombre **Kaspersky_AK{GUID}**.

   - Un grupo de seguridad que corresponde al GPO. Este grupo de seguridad incluye dispositivos cliente cubiertos por la tarea. El contenido del grupo de seguridad define el alcance del GPO.

2. Las aplicaciones de Kaspersky seleccionadas se instalan en los dispositivos cliente directamente desde la carpeta Share (la carpeta compartida en red de Kaspersky Security Center). En la carpeta de instalación de Kaspersky Security Center, se creará una carpeta auxiliar anidada, que contendrá el archivo .msi de la aplicación que se instalará.

3. Los dispositivos que sume al alcance de la tarea se agregarán al grupo de seguridad cuando la tarea se ejecute nuevamente. Si la opción **Ejecutar tareas no realizadas** está seleccionada en la programación de tareas, los dispositivos se agregarán al grupo de seguridad inmediatamente.

4. Los dispositivos que elimine del alcance de la tarea se quitarán del grupo de seguridad cuando la tarea se ejecute nuevamente.

5. Cuando una tarea se elimina de Active Directory, también se eliminan el GPO, el enlace al GPO y el grupo de seguridad correspondiente.

Si desea aplicar otro esquema de instalación mediante Active Directory, puede configurar los parámetros requeridos manualmente. Por ejemplo, esto puede ser necesario en los siguientes casos:

- Cuando el administrador de la protección antivirus no tiene derechos para hacer cambios en Active Directory de ciertos dominios.

- Cuando el paquete de instalación original debe almacenarse en un recurso de red distinto.

- Cuando resulta necesario vincular un GPO con determinadas unidades de Active Directory.

Existen siguientes opciones para usar un esquema de instalación alternativa a través Active Directory:

- Si la instalación se realizará directamente desde la carpeta compartida de Kaspersky Security Center, en las propiedades del GPO debe especificar el archivo .msi situado en la subcarpeta exec de la carpeta del paquete de instalación para la aplicación requerida.

- Si el paquete de instalación tiene que ubicarse en otro recurso de red, debe copiar en él todo el contenido de la carpeta exec porque, además del archivo con la extensión .msi, la carpeta contiene los archivos de configuración generados cuando se creó el paquete. Para instalar la clave de licencia junto con la aplicación, copie también el archivo de clave a esta carpeta.

Instalar aplicaciones en los Servidores de administración secundarios

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 agregar tareas creará la tarea de instalación remota de la aplicación seleccionada en los Servidores de administración secundarios específicos.

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.

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 **DISPOSITIVOS → 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 introducir la contraseña, seleccione esta opción y especifique la contraseña de la cuenta root. Kaspersky Security Center 14 Linux transmite la contraseña de forma cifrada al dispositivo de destino, descifra la contraseña y, a continuación, inicia el procedimiento de instalación en nombre de la cuenta raíz con la contraseña especificada.

     Kaspersky Security Center 14 Linux no utiliza 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 14 Linux utiliza el directorio especificado como directorio temporal para acceder 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.

Reemplazo de aplicaciones de seguridad de terceros

La Instalación de aplicaciones de seguridad de Kaspersky a través de Kaspersky Security Center Linux puede requerir la eliminación del software de terceros incompatible con la aplicación instalada. Kaspersky Security Center proporciona varias formas de eliminar las aplicaciones de terceros.

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. Cuando esta opción se activa, Kaspersky Security Center elimina la aplicación incompatible antes de instalar una aplicación de seguridad en un dispositivo administrado.

Instrucciones: Eliminación de aplicaciones incompatibles antes de la instalación

Eliminar aplicaciones incompatibles a través de una tarea dedicada

Para eliminar aplicaciones incompatibles, 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** con el 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.

Instrucciones: Creación de una directiva

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 la ventana principal de la aplicación, vaya a **DISPOSITIVOS → TAREAS**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para agregar tareas. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.
3. Para la aplicación Kaspersky Security Center, seleccione el tipo de tarea **Desinstalar aplicación de forma remota**.
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. 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 Kaspersky Security Center. Seleccione las casillas 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.

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 aplicación, Kaspersky Security Center usará este 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 comprueba si la aplicación seleccionada tiene o no un comando de desinstalación definido por el proveedor de la aplicación. Si se encuentra el comando, Kaspersky Security Center 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.

7. 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 cuando la tarea está asignada a dispositivos en los que se instaló 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 instalado ningún Agente de red 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 no puede desinstalar una aplicación en un dispositivo administrado dentro del número de ejecuciones del instalador especificadas por el parámetro, Kaspersky Security Center deja de entregar la utilidad de desinstalación a este 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 verifica si la configuración de la utilidad de desinstalación corresponde al sistema operativo del dispositivo cliente. Si la configuración no es corresponde, Kaspersky Security Center no transmite los archivos y no intenta desinstalar la aplicación. Por ejemplo, para desinstalar una aplicación de los dispositivos de un grupo de administración que incluye dispositivos que ejecutan varios sistemas operativos, puede asignar la tarea de desinstalación al grupo de administración y luego habilitar esta opción para omitir los dispositivos que ejecutan un sistema operativo que no sea el requerido.

8. 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 utilizando, 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 necesitan 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 guardó 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 manera predeterminada.

9. 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 instaló en los dispositivos cliente.

   - **Se necesita una cuenta (no se utiliza el Agente de red)**

     Si selecciona esta opción, podrá especificar los datos de la cuenta con la que se ejecutará el instalador de la aplicación. Puede indicar estos datos si los dispositivos a los que asignó la tarea no tienen instalado el Agente de red.

     Puede especificar varias cuentas de usuario si, por ejemplo, ninguna tiene todos los permisos requeridos en todos los dispositivos a los que se asignó la tarea. En ese caso, la tarea se ejecutará con todas las cuentas agregadas, en orden consecutivo, comenzando por la primera de la lista.

     Si no agrega ninguna cuenta, la tarea se ejecutará con la cuenta con la que se haya iniciado el servicio del Servidor de administración.

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. Podrá modificar la configuración predeterminada en cualquier otro momento.

11. Haga clic en el botón **Finalizar**.

    Se crea la tarea y se la agrega a la lista de tareas.

12. Haga clic en el nombre de la nueva tarea para abrir la ventana de propiedades de la tarea.

13. En la ventana de propiedades de la tarea, configure los ajustes generales de la tarea.

14. Haga clic en el botón **Guardar**.

15. Ejecute la tarea manualmente o espere a que se inicie a consecuencia de la programación configurada para la tarea.

Al finalizar la tarea de desinstalación remota, la aplicación seleccionada se eliminará de los dispositivos seleccionados.

Preparación de un dispositivo que ejecuta SUSE Linux Enterprise Server 15 para la instalación del Agente de red

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 verificar 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.

Después de preparar el dispositivo SUSE Linux Enterprise Server 15, implementar e instalar el Agente de red.

Aplicaciones de Kaspersky: licencias y activación

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. Ha habilitado la opción **Clave de licencia distribuida automáticamente** para las tres. Los dispositivos de su organización tienen instalada una aplicación de seguridad de Kaspersky (por ejemplo, Kaspersky Endpoint Security para 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 desplegar en el dispositivo: una clave de licencia llamada *Clave_1* y una clave de licencia llamada *Clave_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

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, puede seleccionar la clave que debe desplegarse a los dispositivos y seleccionar los dispositivos con comodidad, por ejemplo, seleccionando 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 → LICENCIAS DE KASPERSKY**.
2. Haga clic en el botón **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.
   - **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 14 Web Console permite distribuir la clave de licencia en los dispositivos cliente mediante la tarea de *Distribución de claves de licencia*.

Para distribuir una clave de licencia a sus dispositivos cliente:

1. En el menú principal, vaya a **DISPOSITIVOS → TAREAS**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para agregar tareas.
3. Seleccione la aplicación para la que desee agregar una clave de licencia.
4. En la lista **Tipo de tarea**, seleccione **Agregar clave de licencia**.
5. Siga las instrucciones del Asistente.
6. 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. Podrá modificar la configuración predeterminada en cualquier otro momento.
7. Haga clic en el botón **Crear**.

   Se crea la tarea y se la agrega a la lista de tareas.
8. Para ejecutar la tarea, selecciónela en la lista de tareas y haga clic en el botón **Iniciar**.

Cuando se ejecute 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. En el menú principal, vaya a **OPERACIONES → LICENCIAS → LICENCIAS DE KASPERSKY**.
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**.
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. Este límite está definido en las propiedades de la clave de licencia. Cuando se llega al límite de dispositivos, el proceso de distribución se detiene automáticamente y la clave de licencia no se transfiere a más dispositivos.

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.

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:

En el menú principal, vaya a **OPERACIONES → LICENCIAS → LICENCIAS DE KASPERSKY**.

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. En el menú principal, vaya a **OPERACIONES → LICENCIAS → LICENCIAS DE KASPERSKY**.
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.

Para ver qué claves de licencia se despliegan en un dispositivo cliente específico:

1. En el menú principal, vaya a **DISPOSITIVOS → 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.

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. Vaya a **OPERACIONES → LICENCIAS → LICENCIAS DE KASPERSKY**.
2. Seleccione el archivo de clave o el código de activación que desee eliminar del repositorio.
3. Haga clic en el botón **Eliminar**.
4. Haga clic en el botón **Aceptar** para confirmar la operación.

El archivo de clave o el código de activación que haya seleccionado se eliminará del repositorio.

Puede volver a agregar una clave de licencia eliminada o agregar una clave de licencia 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**, elija 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.
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 DE KASPERSKY**.
   - En el menú principal, vaya a **SUPERVISIÓN E INFORMES → PANEL** y, luego, haga clic en el vínculo **Ver licencias por caducar** junto a una notificación.

   Se abre la ventana **LICENCIAS DE KASPERSKY**, 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: la versión, la ubicación utilizada, el ID de la licencia del software (es decir, el ID de la licencia que está renovando) y si compró la licencia 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.

En Kaspersky Security Center 14 Web Console, las notificaciones se muestran cuando una licencia está a punto de caducar, de acuerdo con el siguiente programa:

- 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 selecciona una solución, Kaspersky Security Center 14 Linux lo redirige a la página web relacionada en el sitio web de Kaspersky para obtener 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, por sus siglas en inglés). 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.

Configurar la protección de la red

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.

Escenario: 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 adicionales para su red.

Requisitos previos

Antes de comenzar, compruebe que hizo lo siguiente:

- Instaló el Servidor de administración de Kaspersky Security Center
- Instaló Kaspersky Security Center 14 Web Console
- Completó el escenario de instalación principal de Kaspersky Security Center
- Completado el Asistente de inicio rápido o creado 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

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: configuración de la tarea de grupo para actualizar Kaspersky Endpoint Security.

   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**

   Cuando ocurre un evento en una aplicación administrada, el dispositivo cliente en el que tuvo lugar el suceso transfiere información al respecto a 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 en conjunto) 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 monitorear los incidentes 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. Si hace esto, las directivas y los perfiles se aplicarán 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 y Kaspersky Security Center 14 Web Console. Considere también utilizar una administración de seguridad centrada en el usuario, ya sea en reemplazo o como complemento de este enfoque centrado en el usuario. 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 configura la protección de su red en el Asistente de inicio rápido, Kaspersky Security Center crea la directiva predeterminada para Kaspersky Endpoint Security para Linux. 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.

   A través de las condiciones de activación, podrá aplicar perfiles diferentes a, por ejemplo, los dispositivos que tengan configuraciones de hardware específicas o a los que estén marcados con etiquetas específicas. Puede usar las etiquetas para filtrar dispositivos que reúnen criterios específicos. Podría, por ejemplo, crear una etiqueta llamada *CentOS*, marcar con ella los dispositivos que utilicen el sistema operativo CentOS y especificarla como condición de activación para un perfil de directiva. Ello hará que las aplicaciones de Kaspersky instaladas en dispositivos con CentOS queden sujetas a un perfil de directiva específico.

   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 manera predeterminada, Kaspersky Security Center sincroniza automáticamente el Servidor de administración 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 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 especifica 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 y Kaspersky Security Center 14 Web Console y de 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.

   Cuando configura la protección de su red en el Asistente de inicio rápido, Kaspersky Security Center crea 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 sincroniza automáticamente el Servidor de administración 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 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 especifica 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.

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 tareas** está seleccionada.

Ajustes de la directiva del Agente de red

Para configurar la directiva del Agente de red:

1. En el menú principal, vaya a **DISPOSITIVOS → DIRECTIVAS Y PERFILES**.
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.

General

En la pestaña, 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:
  - **Directiva activa**

    Si se selecciona esta opción, se activa la directiva.

    Esta opción está seleccionada de manera predeterminada.

  - **Directiva 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 desde 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 habilitada de manera 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 grupos de administración anidados (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 manera 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 las siguientes secciones de la pestaña **Configuración de eventos**:

- **Error funcional**
- **Advertencia**
- **Información**

Cada sección contiene una lista con los distintos tipos de eventos y la cantidad de días por las 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 forma predeterminada, todos los tipos de eventos están sujetos a los ajustes de notificación generales configurados para el Servidor de administración entero. 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 incidente**. 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 incidente**, haga clic en este y especifique dónde almacenar los eventos ocurridos y cómo notificarlos.

Si el Agente de red detectó un incidente, puede administrar este incidente utilizando la configuración de un dispositivo administrado.

Configuración de la aplicación

Configuración

En la sección **Configuración**, puede configurar la directiva del Agente de red:

- **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.

  El valor predeterminado es de 2 megabytes (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 para 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 (o de la directiva fuera de la oficina) que se encontraba vigente cuando la directiva se entregó en el dispositivo administrado
  - 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 directiva activos

    Puede utilizar esta información para solucionar problemas o verificar que la directiva aplicada al dispositivo sea la esperada. Esta opción está deshabilitada de manera predeterminada.

Repositorios

En la sección **Repositorios**, puede seleccionar los tipos de objetos sobre los que el Agente de red enviará detalles al Servidor de administración. La directiva del Agente de red podría impedirle modificar algunos ajustes de esta sección.

- **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 habilitada de manera predeterminada.

- **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.

Red

La sección **Red** contiene tres subsecciones:

- **Conectividad**
- **Perfiles de conexión**
- **Programación de conexiones**

En la subsección **Conectividad**, 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.

    Si define un intervalo de sincronización inferior a 15 minutos, la sincronización se realizará cada 15 minutos. Si el intervalo de sincronización está configurado en 15 minutos o más, la sincronización se realiza en el intervalo de sincronización especificado.

  - 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 marcada de manera 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 habilitada de manera predeterminada.

  - Usar la puerta de enlace de conexión del punto de distribución (si está disponible) con los ajustes de conexión predeterminados

    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 habilitada de manera predeterminada.

- Usar puerto UDP

Si necesita que los dispositivos administrados se conecten al servidor proxy de KSN a través de un puerto UDP, habilite la opción **Usar puerto UDP** y especifique un número de **puerto UDP**. Esta opción está habilitada de manera predeterminada. El puerto UDP predeterminado de conexión al servidor proxy de KSN es 15111.

- Número de puerto UDP

  En este campo, puede indicar el número del puerto UDP. El número de puerto predeterminado es el 15000.

  El sistema decimal se usa para los registros.

En la subsección **Perfiles de conexión** de la sección **Red**, puede especificar las configuraciones de ubicación de la red y activar el modo fuera de la oficina cuando el Servidor de administración no está disponible. Los ajustes de la sección **Perfiles de conexión** solo están disponibles en dispositivos con Windows.

- 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

  Los perfiles de conexión solo son compatibles con dispositivos que ejecutan Windows. No recomendamos usar esta opción.

  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

  En el grupo de configuración **Perfiles de conexión** no se pueden agregar nuevos elementos a la lista **Perfiles de conexión al Servidor de administración**, así que el botón **Agregar** está inactivo. Tampoco se pueden modificar los perfiles de conexión preestablecidos.

- Habilitar el modo 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 manera 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 manera 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:

- **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 manera predeterminada.

- **Intervalos IP**

  Si se habilita esta opción, el Servidor de administración sondeará automáticamente los rangos IP de acuerdo con la programación que configuró al hacer clic en el enlace **Configurar programación de sondeos**.

  Si se deshabilita esta opción, el Servidor de administración no sondeará los rangos 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 manera 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**

- **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 manera predeterminada.

- **Autenticación del servidor proxy**

  Si marca esta casilla, podrá utilizar los campos de entrada para especificar credenciales de autenticación para el servidor proxy.

  Esta casilla está desmarcada de manera predeterminada.

- **Nombre de usuario**
- **Contraseña**

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.

Historial de revisiones

En esta pestaña, puede ver la lista de revisiones de la directiva y revertir los cambios realizados en la directiva, si es necesario.

Cambiar la prioridad de las reglas de movimiento de dispositivos

Toda regla de movimiento de dispositivos tiene una prioridad.

Para aumentar o disminuir la prioridad de una regla de movimiento:

Mueva la regla hacia arriba o hacia abajo en la lista, respectivamente, utilizando el mouse.

Tareas

Esta sección describe tareas utilizadas por Kaspersky Security Center.

Acerca de las tareas

Kaspersky Security Center administra las aplicaciones de seguridad de Kaspersky instaladas en los dispositivos mediante la creación y ejecución de *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 se pueden crear utilizando Kaspersky Security Center 14 Web Console solo si el complemento de administración para esa aplicación está instalado en el Servidor de Kaspersky Security Center 14 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 14 Web Console o por el usuario de un dispositivo remoto (por ejemplo, a través de la interfaz de aplicaciones 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*: tareas que se realizan en un conjunto de dispositivos, independientemente de si están incluidos en algún 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.

- 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 **DISPOSITIVOS → TAREAS**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para agregar tareas. 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. Podrá modificar la configuración predeterminada en cualquier otro momento.

4. Haga clic en el botón **Finalizar**.

Se crea la tarea y se la agrega a la lista de tareas.

Iniciar una tarea manualmente

La aplicación inicia las tareas siguiendo la programación configurada en las propiedades de cada tarea. Si necesita iniciar una tarea en un momento arbitrario, puede hacerlo manualmente.

Para iniciar una tarea manualmente:

1. En el menú principal, vaya a **DISPOSITIVOS → TAREAS**.
2. En la lista de tareas, active la casilla de verificación ubicada junto a la tarea que desee iniciar.
3. Haga clic en el botón **Iniciar**.

Se inicia la tarea. Puede verificar el estado de la tarea en la columna **Estado** o haciendo clic en el botón **Resultado**.

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:

Vaya a **DISPOSITIVOS → 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 relacionada con el Servidor de administración y *Actualizar* se refiere al Agente de red.

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 las tareas.

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 utilizando, 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 necesitan 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. Por ejemplo, si el usuario está editando un documento en un procesador de textos y no guardó 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 manera predeterminada.

- Programación de la tarea:
  - **Inicio programado**

    Seleccione y configure la programación según la cual se ejecutará la tarea.

    - **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 forma predeterminada, la tarea se ejecutará cada seis 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.

  Por defecto, la tarea se ejecutará cada lunes a la hora actual 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.

- **Diario (no compatible con horario de verano)**

  La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta programación no tiene en cuenta los cambios de horario estacionales. La hora de inicio de la tarea se mantendrá sin cambios incluso si el reloj se atrasa o se adelanta una hora debido al horario de verano.

  No recomendamos usar esta programación. Es necesaria para mantener la compatibilidad con versiones anteriores de Kaspersky Security Center Linux.

  De forma predeterminada, la tarea se iniciará todos los días a la hora actual del sistema.

- **Semanal**

  La tarea se ejecutará cada semana en el día y a la hora que indique.

- **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 p. m.

- **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 habilitada de manera predeterminada.

- **Cada mes en los días especificados de semanas seleccionadas**

  La tarea se ejecutará periódicamente, en los días del mes y a la hora que indique.

  Por defecto, no hay ningún día seleccionado; la hora de inicio predeterminada es las 18:00:00 p. m.

- **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. Puede seleccionar cómo se deberá completar esa tarea anterior (correctamente o con errores) para que se dé inicio a la tarea subsiguiente.

- **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 se ejecutarán las tareas programadas en los dispositivos cliente; las tareas con las opciones de programación **Manual**, **Una vez** e **Inmediatamente** solo se ejecutarán en aquellos dispositivos cliente que estén 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 habilitada de manera predeterminada.

- **Utilizar retardo aleatorio automático para el inicio de tareas**

  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.

- **Utilizar un retardo aleatorio para el inicio de tareas dentro de un intervalo de (min)**

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 manera 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 nombres de DNS, direcciones IP y subredes IP de los dispositivos a los cuales debe asignar la tarea.

    Puede 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 en los dispositivos que utilizan los contadores o si quiere analizar los dispositivos de una subred 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 resultarle útil para, por ejemplo, ejecutar una tarea en 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.

- 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 manera 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.

Ajustes que se configuran tras crear una tarea

Los siguientes ajustes pueden definirse solamente cuando la tarea ya se creó.

- 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 habilitada de manera 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 manera predeterminada.

- Ajustes de programación avanzados:

  - **Activar el dispositivo con la función Wake-on-LAN antes de que se inicie la tarea (min)**

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 el dispositivo cuando se complete la tarea**. Encontrará esta opción en la misma ventana.

Esta opción está deshabilitada de manera predeterminada.

- Apagar el dispositivo 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 manera predeterminada.

- Detener la tarea si se ha estado ejecutando durante más tiempo que (min)

  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 manera 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 habilitada de manera 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 manera 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 manera 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 habilitada de manera 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 revisión.**

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 le permite reemplazar automáticamente la contraseña anterior por la nueva en todas las tareas en las que se especifica la cuenta. También puede cambiar la contraseña manualmente en las propiedades de cada tarea.

Para iniciar el Asistente para cambiar contraseñas de tareas:

1. En la pestaña **DISPOSITIVOS**, seleccione **TAREAS**.
2. Haga clic en **Administrar credenciales de cuentas para tareas de inicio**.

Siga las instrucciones del Asistente.

Paso 1. Especificar credenciales

Especifique las nuevas credenciales que actualmente son válidas en su sistema. Cuando cambia al siguiente paso del Asistente, Kaspersky Security Center verifica si el nombre de cuenta especificado coincide con el nombre de cuenta 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 14 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 reemplaza la contraseña solo para aquellas tareas en las que se encuentran 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 vaya al siguiente paso del Asistente.

Paso 3. Ver los resultados

En el último paso del Asistente, vea 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 le permite ver los resultados de la ejecución para tareas de grupos, tareas para dispositivos específicos y tareas del Servidor de administración. No se pueden ver resultados de la ejecución para tareas locales.

Para ver los resultados de la tarea:

1. En la ventana de propiedades de la tarea, seleccione la sección **General**.
2. Haga clic en el enlace **Resultados** para abrir la ventana **Resultados de la tarea**.

Administración de dispositivos cliente

En esta sección, se describe cómo administrar los dispositivos incluidos en los grupos de administración.

Configuración de un dispositivo administrado

Para ver la configuración de un dispositivo administrado:

1. Seleccione **DISPOSITIVOS** → **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.

General

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.

- **Grupo**

  Grupo de administración en el que está incluido el dispositivo cliente.

- **Última actualización**

Fecha en que las bases de datos o las aplicaciones se actualizaron por última vez en el dispositivo.

- Visible por última vez

  Fecha y hora en que el dispositivo se vio en la red por última vez.

- 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.

- No desconectar del Servidor de administración

  Cuando esta opción está habilitada, se mantiene una conexión permanente entre el dispositivo administrado y el Servidor de administración. Podría habilitar esta función si no utiliza servidores push, que ofrecen 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 instaló el Servidor de administración y no se puede deshabilitar en ese caso.

Red

La sección de **Redes** 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

  Nombre del dominio DNS del dispositivo cliente.

- Nombre NetBIOS

  Nombre del dispositivo cliente.

Sistema

La sección **Sistema** proporciona información sobre el sistema operativo instalado en el dispositivo cliente.

Protección

La sección **Protección** proporciona información sobre el estado actual de la protección antivirus en 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.

- Todos los problemas

  Tabla con una lista en la que se enumeran los problemas detectados por las aplicaciones administradas del dispositivo cliente. Cada problema está acompañado del estado que la aplicación sugiere asignar al dispositivo a raíz del problema.

- Protección en tiempo real

  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 a pedido

  Fecha y hora del último análisis antivirus realizado en el dispositivo cliente.

- Número total de amenazas detectadas

  Número total de amenazas detectadas en el dispositivo cliente desde la instalación de la aplicación antivirus (primer análisis del dispositivo) o desde la última vez que el contador de amenazas se puso en cero.

- Amenazas activas

  Número de archivos no procesados en el dispositivo cliente.

  Este campo no refleja el número de archivos no procesados en dispositivos móviles.

Estado del dispositivo definido por la aplicación

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

La sección **Aplicaciones** enumera todas las aplicaciones de Kaspersky que se encuentran instaladas en el dispositivo cliente. Haga 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

La sección **Directivas y perfiles de directivas activos** enumera las directivas y los perfiles de directivas que están activos en el dispositivo administrado.

Tareas

La sección **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 no se puede establecer una conexión, no se mostrará ningún estado.

Eventos

La sección **Eventos** muestra los eventos registrados en el Servidor de administración para el dispositivo cliente seleccionado.

Etiquetas

La sección **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.

Archivos ejecutables

La sección **Archivos ejecutables** 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

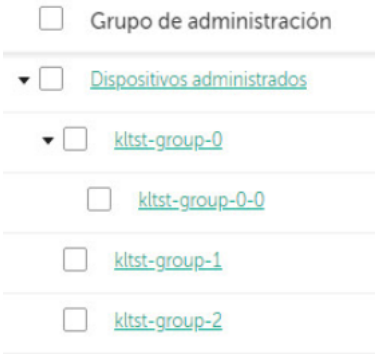
Haga clic en el botón **Propiedades** para ver y configurar el punto de distribución con el que interactúa el dispositivo.

Registro de hardware

En la sección **Registro de hardware**, puede ver información sobre el hardware instalado en el dispositivo cliente.

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. Vaya a **DISPOSITIVOS → 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 el botón **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. Vaya a **DISPOSITIVOS → JERARQUÍA DE GRUPOS**.
2. Haga clic en el botón **Importar**.

Se inicia el Asistente de nueva estructura de grupos de administración. Siga las instrucciones del Asistente.

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, en la sección **DISPOSITIVOS → 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.

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 la pestaña **DISPOSITIVOS → REGLAS DE MOVIMIENTO**.

2. Haga clic en **Agregar**.

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.

- 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.

  - Regla aplicada continuamente.

    La regla se aplicará siguiendo una programación definida automáticamente por el Servidor de administración (generalmente, una vez cada varias horas).

- 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.

- Habilitar regla

  Si esta opción está habilitada, la regla se activará 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.

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. 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. En el menú principal, vaya a la pestaña **DISPOSITIVOS → REGLAS DE MOVIMIENTO**.

   También puede seleccionar **DESCUBRIMIENTO Y DESPLIEGUE → DESPLIEGUE Y ASIGNACIÓN** y después seleccionar **REGLAS DE MOVIMIENTO**.

   Se muestra la lista de reglas de movimiento.

2. Active la casilla de verificación 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.

   - 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.

     - Regla aplicada continuamente.

       La regla se aplicará siguiendo una programación definida automáticamente por el Servidor de administración (generalmente, una vez cada varias horas).

- 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.

- Habilitar regla

  Si esta opción está habilitada, la regla se activará 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.

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 reglas 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;
- Aplicaciones administradas instaladas en dispositivos cliente, por ejemplo, Agente de red o Servidor de administración;
- Máquinas virtuales, que son los dispositivos cliente.

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 desactivada, la regla de movimiento de dispositivos se aplica a los dispositivos con todas las etiquetas seleccionadas.

Esta opción está deshabilitada de manera 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 manera 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 DNS del dispositivo

  Nombre de dominio DNS del dispositivo cliente que desea mover. Complete este campo si su red incluye un servidor DNS.

- 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 manera 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 manera 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 ha cambiado.
- **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 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 14** o **Servidor de administración de Kaspersky Security Center 14**.

  Si no selecciona ninguna aplicación administrada, la condición no se aplica.

- Versión del sistema operativo

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. La opción está desactivada de forma predeterminada.

- Arquitectura del sistema operativo

  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 el tamaño de bits del sistema operativo de los dispositivos cliente:

  1. En el menú principal, vaya a la sección **DISPOSITIVOS** → **DISPOSITIVOS ADMINISTRADOS**.
  2. Haga clic en el botón ( ) **Columns settings** a la derecha.
  3. Seleccione la opción **Arquitectura del sistema operativo**, y haga clic en el botón **Guardar**.

     Después, se muestra el tamaño de bits del sistema operativo para cada dispositivo administrado.

- Service Pack del sistema operativo

  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 cliente (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 móvil.
  - **Sin instalar**. La regla de movimiento de dispositivos solo se aplica a dispositivos móviles sin un certificado móvil.
  - **Ningún valor seleccionado**. La condición no se aplica.

- Compilación del sistema operativo

Este parámetro solo es válido para sistemas operativos Windows.

Puede indicar si el número de compilación del sistema operativo seleccionado deberá ser igual, anterior o posterior al valor introducido. También puede configurar la búsqueda de una regla de movimiento para todos los números de compilación, excepto el especificado.

- Número de versión del sistema operativo

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 una regla de movimiento de dispositivos para todos los números de versión 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.

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. Vaya a **DISPOSITIVOS → DISPOSITIVOS ADMINISTRADOS**.
2. Haga clic en el vínculo **Ruta actual:** `<ruta actual>` que se encuentra sobre la lista.
3. En la ventana que se abre, seleccione el grupo de administración al que desee agregar los dispositivos.
4. Haga clic en el botón **Agregar dispositivos**.

   Se inicia el Asistente para mover dispositivos.
5. 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.
     - 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: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %
6. 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.
7. 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 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.

Para mover uno o varios dispositivos a un grupo de administración seleccionado:

1. Abra el grupo de administración al que pertenezcan los dispositivos que desee mover. Para ello, realice una de las siguientes acciones:
   - Para abrir un grupo de administración, vaya a **DISPOSITIVOS** → **Grupos** → **<nombre del grupo>** → **DISPOSITIVOS ADMINISTRADOS**.
   - Para abrir el grupo **DISPOSITIVOS NO ASIGNADOS**, vaya a **DESCUBRIMIENTO Y DESPLIEGUE** → **DISPOSITIVOS NO ASIGNADOS**.
2. Active las casillas de verificación ubicadas junto a los dispositivos que desee mover a otro grupo.
3. Haga clic en el botón **Mover a un grupo**.
4. En la jerarquía de grupos de administración, active la casilla de verificación ubicada junto al grupo de administración al que desee mover los dispositivos seleccionados.
5. Haga clic en el botón **Mover**.

Los dispositivos seleccionados se moverán al grupo de administración seleccionado.

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 agregar tareas. Siga las instrucciones del Asistente. En la ventana **Nueva tarea** del Asistente para agregar tareas, seleccione la aplicación **Kaspersky Security Center 14** 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.

   - **Especificar las direcciones de los dispositivos manualmente o importarlas de una lista**

Puede especificar nombres de DNS, direcciones IP y subredes IP de los dispositivos a los cuales debe asignar la tarea.

Puede 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 en los dispositivos que utilizan los contadores o si quiere analizar los dispositivos de una subred 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 resultarle útil para, por ejemplo, ejecutar una tarea en 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.

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 **DISPOSITIVOS** → **JERARQUÍA DE GRUPOS**.
2. Haga clic en el nombre del grupo de administración de su interés.

   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 habilitada de manera 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 manera predeterminada.

5. En la sección **Actividad de los dispositivos**, active o desactive 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 habilitada de manera 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 habilitada de manera predeterminada.

6. Haga clic en **Guardar**.

Se guardarán y aplicarán los cambios.

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). 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 antivirus, detectó algunos virus en el dispositivo, y el número de virus encontrados supera el 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. • En pausa. • En ejecución.
El análisis antivirus no se ha realizado en mucho tiempo	El dispositivo es visible en la red y una aplicación de seguridad está instalada en el dispositivo, pero la tarea Análisis antivirus no se ejecutó durante 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.
Se debe reiniciar el dispositivo	El dispositivo es visible en la red, pero una aplicación requiere que el dispositivo se reinicie por más tiempo que el intervalo de tiempo especificado y por una de las razones seleccionadas.	Más de 0 minutos.
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.
Licencia caducada	El dispositivo es visible en la red, pero la licencia caducó.	• 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.
Se detectaron incidentes no procesados	Se han encontrado incidentes sin procesar en el dispositivo. Los incidentes pueden ser creados 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	El estado del dispositivo es definido por la aplicación administrada.	• Interruptor desactivado.

definido por la aplicación		• 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.	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 configuradas. 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.

Cuando Kaspersky Security Center Linux asigna un estado a un dispositivo, para algunas condiciones (consulte la columna Descripción de condición) se tiene en cuenta el indicador de visibilidad. 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*.

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. Abra la ventana Propiedades de una de las siguientes formas:

- En la carpeta **Directivas**, en el menú contextual de una directiva del Servidor de administración, seleccione **Propiedades**.
- Seleccione **Propiedades** en el menú contextual de un grupo de administración.

2. En la ventana de propiedades que se abre, en el panel **Secciones**, seleccione **Estado del dispositivo**.
3. En el panel derecho, en la sección **Fijar en Crítico si esto se cumple**, marque la casilla junto a una de las condiciones de la lista.

   Solo podrá modificar los ajustes que no estén bloqueados en la directiva primaria.

4. Configure el valor necesario para la condición seleccionada.

   Puede establecer valores para algunas condiciones pero no para todas.

5. Haga clic en **Aceptar**.

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. Abra la ventana Propiedades de una de las siguientes formas:
   - En la carpeta **Directivas**, en el menú contextual de una directiva del Servidor de administración, seleccione **Propiedades**.
   - Seleccione **Propiedades** en el menú contextual del grupo de administración.
2. En la ventana de propiedades que se abre, en el panel **Secciones**, seleccione **Estado del dispositivo**.
3. En el panel derecho, en la sección **Fijar en Advertencia si esto se cumple**, marque la casilla junto a una de las condiciones de la lista.

   Solo podrá modificar los ajustes que no estén bloqueados en la directiva primaria.

4. Configure el valor necesario para la condición seleccionada.

   Puede establecer valores para algunas condiciones pero no para todas.

5. Haga clic en **Aceptar**.

Cuando se cumplan las condiciones especificadas, se asignará el estado *Advertencia* al dispositivo administrado.

Directivas y perfiles de directivas

En Kaspersky Security Center 14 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. La directiva tiene 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:

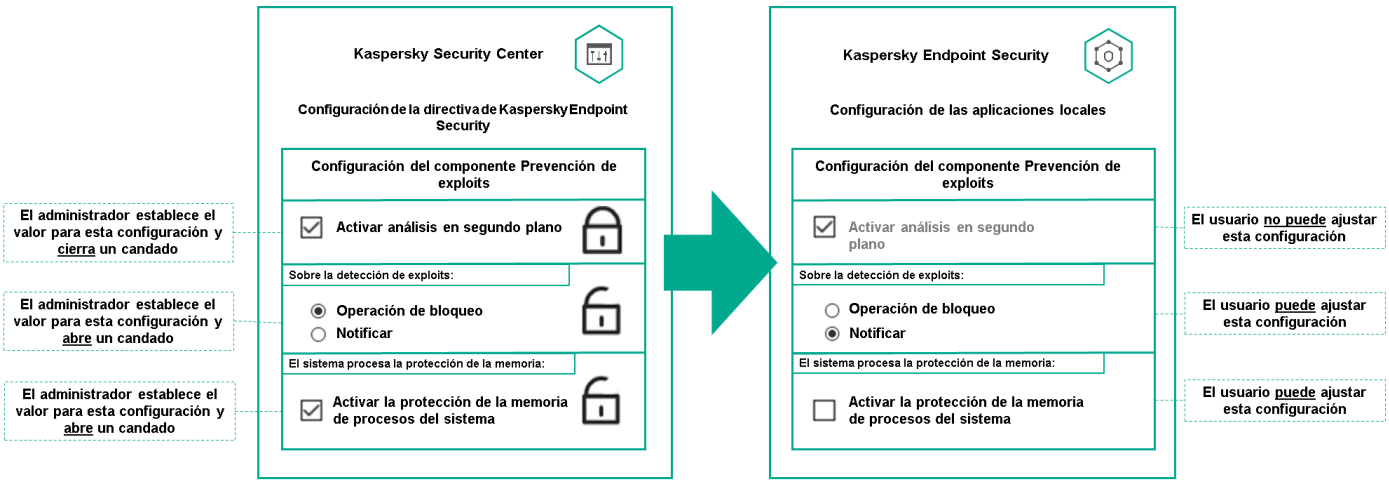
- Bloquear ajustes en la directiva de un subgrupo de administración
- Bloquear los ajustes de una aplicación de Kaspersky instalada en un dispositivo administrado

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.

Una directiva contiene los mismos ajustes que una aplicación de Kaspersky local. 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

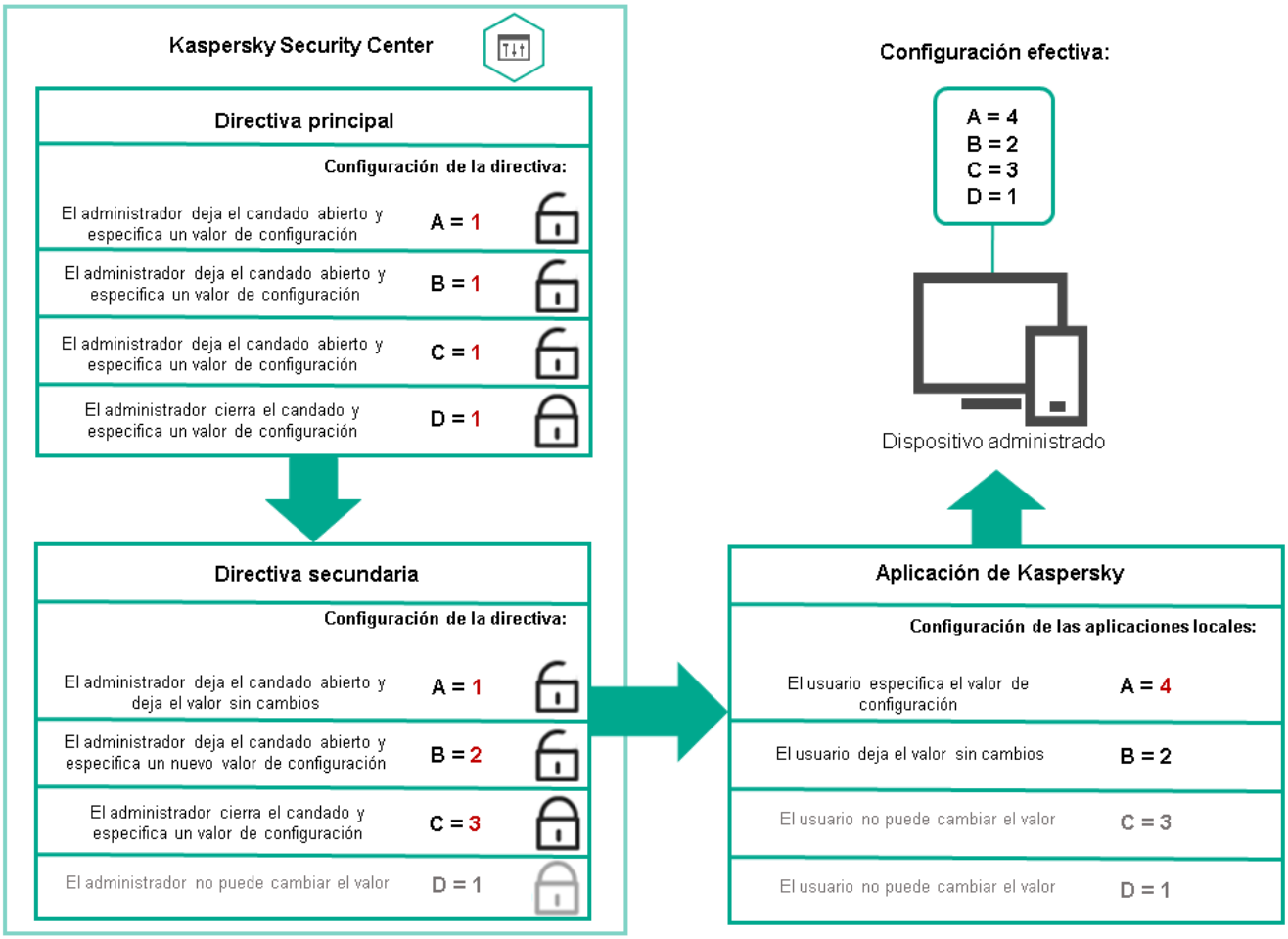
Si distintos dispositivos necesitan diferentes configuraciones, puede organizar los dispositivos en grupos de administración.

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.

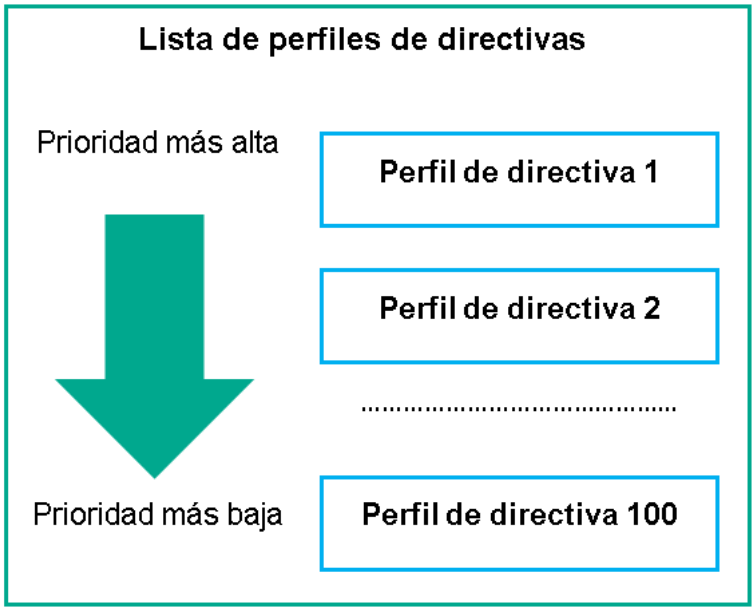
Las directivas de una misma aplicación se afectan las unas a las otras siguiendo el orden jerárquico de los grupos de administración. Los ajustes que se bloquean en una directiva de un grupo de administración primario (de nivel superior) sobrescriben los valores de configuración en la directiva de un subgrupo (vea la siguiente imagen).



Perfiles de directivas en una jerarquía de directivas

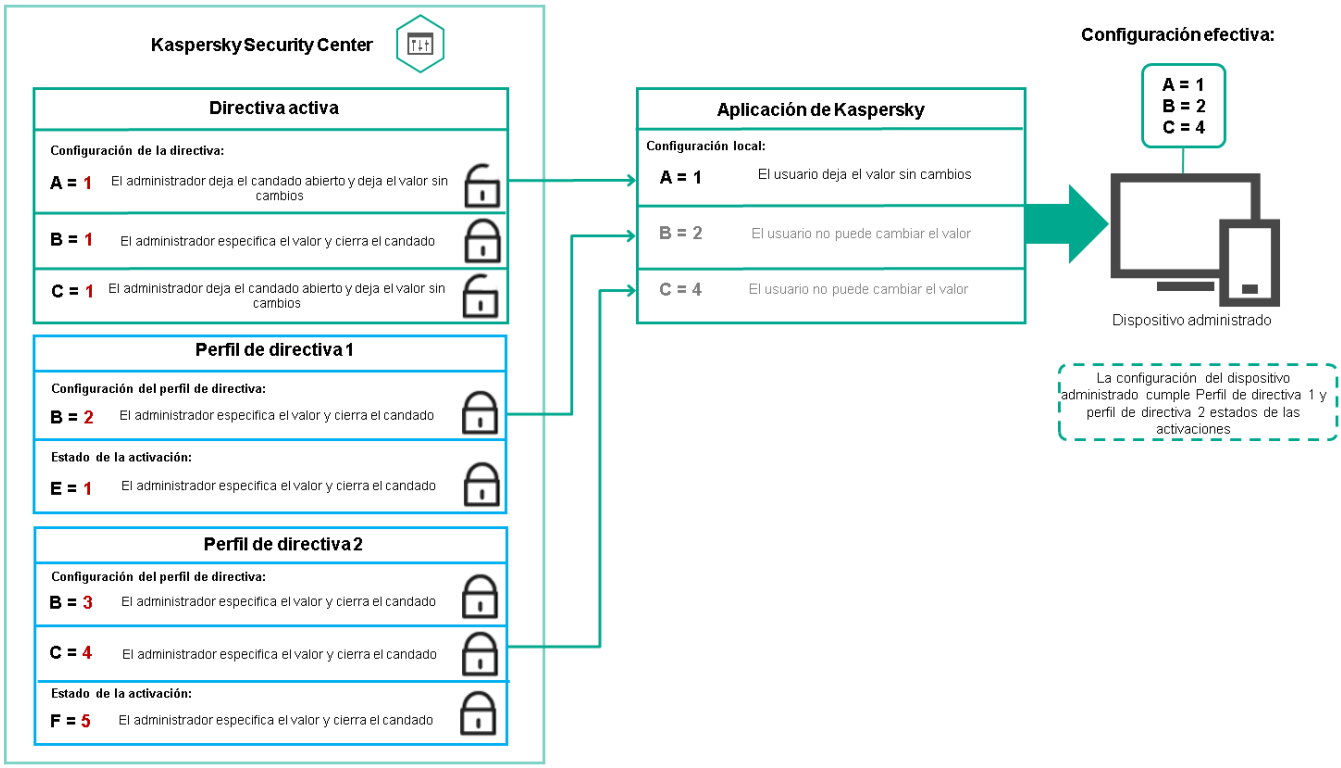
Los perfiles de directivas tienen las siguientes condiciones de asignación de prioridad:

- 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).

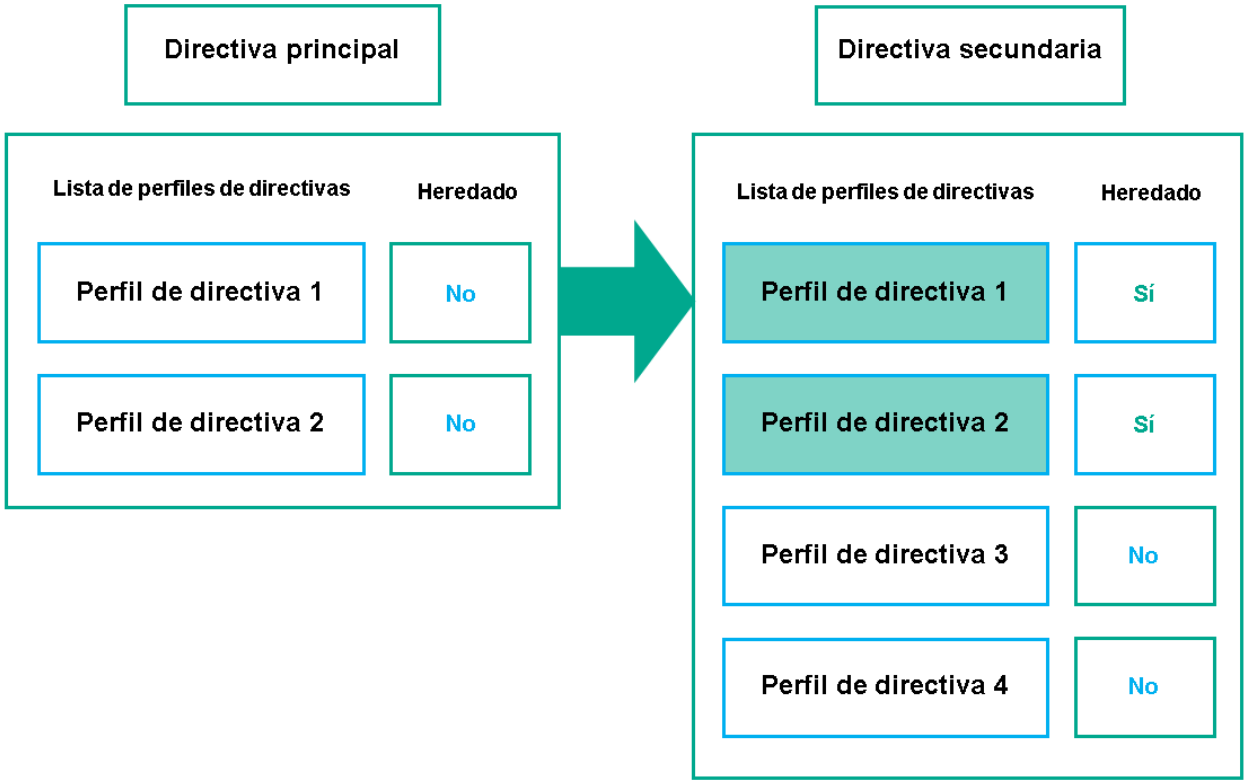


La configuración del dispositivo administrado cumple las condiciones de activación de varios perfiles de directiva

Perfiles de directivas en una jerarquía de herencia

Los perfiles de directivas definidos para directivas de distintos niveles jerárquicos se rigen por estas condiciones:

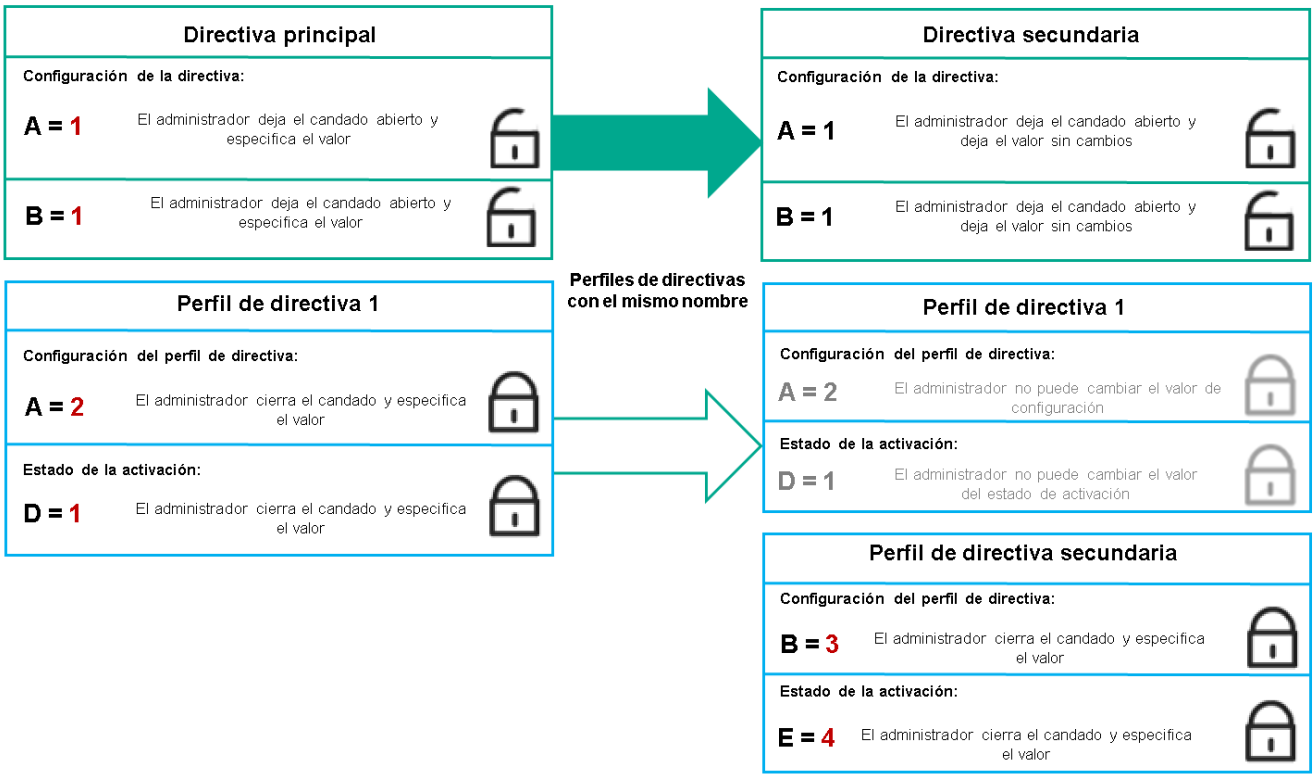
- Una directiva de nivel inferior hereda los perfiles de una directiva de nivel superior. Un perfil de directiva que se ha heredado de una directiva de nivel superior obtiene mayor prioridad que el nivel del perfil de directiva original.
- No se puede cambiar la prioridad de un perfil de directiva heredado (vea la siguiente imagen).



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 **DISPOSITIVOS → 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 directiva

Puede crear directivas nuevas y modificar o eliminar las directivas existentes.

Para crear una directiva:

1. Vaya a **DISPOSITIVOS → DIRECTIVAS Y PERFILES**.
2. Haga clic en **Agregar**.

   Se abre la ventana **Seleccionar aplicación**.
3. Seleccione la aplicación para la que desee crear la directiva.
4. Haga clic en **Siguiente**.

   Se abre la ventana de configuración de la nueva directiva, con la pestaña **General** seleccionada.
5. Si lo desea, cambie el nombre predeterminado, el estado predeterminado y las opciones de directiva predeterminadas.
6. 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.
7. 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

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.

8. Haga clic en **Guardar** para guardar la directiva.

La directiva aparecerá en la lista de directivas.

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 manera 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 herencia:
  - **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 habilitada de manera 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 grupos de administración anidados (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 manera 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 las 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**.

Historial de revisiones

La pestaña **Historial de revisiones** le permite ver la lista de revisiones de la directiva y revertir los cambios realizados en la directiva, si es necesario.

Modificar una directiva

Para modificar una directiva:

1. Vaya a **DISPOSITIVOS → DIRECTIVAS Y PERFILES**.
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

   Si necesita información detallada para configurar otra aplicación de seguridad, consulte la documentación de ese software.
4. Haga clic en **Guardar**.

Los cambios realizados en la directiva se guardarán en las propiedades de la directiva y aparecerán en la sección **Historial de revisiones**.

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.
2. Abra la pestaña **General**.
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.

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 **DISPOSITIVOS → DIRECTIVAS Y PERFILES**.
2. Marque la casilla ubicada junto a la directiva (o las directivas) que desee copiar.
3. Haga clic en el botón **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** en la parte inferior 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.

Para mover una directiva a otro grupo de administración:

1. En el menú principal, vaya a **DISPOSITIVOS → DIRECTIVAS Y PERFILES**.
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.

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. Vaya a **DISPOSITIVOS → 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:
   - Yaya a **DISPOSITIVOS** → **DISPOSITIVOS ADMINISTRADOS** → **Grupos** y, luego, seleccione el grupo de administración que contenga los dispositivos para sincronizar.
   - Genere una selección de dispositivos para ver la lista de dispositivos.
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 **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. Vaya a **DISPOSITIVOS** → **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 cuenta con un gráfico de distribución de directivas que permite conocer el estado de aplicación de una directiva por dispositivo.

Para ver el estado de distribución de una directiva en cada dispositivo:

1. Ir a **DISPOSITIVOS** → **DIRECTIVAS Y PERFILES**.

2. Marque la casilla ubicada junto a la directiva cuyo estado de distribución desee conocer.

3. En el menú que aparece, seleccione el vínculo **Distribución**.

   Se abre la ventana **<Nombre de la directiva>: resultados de la distribución**.

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. La lista puede mostrar un máximo de 100 000 dispositivos.

Para cambiar la cantidad de dispositivos que se muestran en la lista con los resultados de la distribución de una directiva:

1. Vaya a la sección **Opciones de interfaz** en la barra de herramientas.

2. En el campo **Límite de dispositivos que se incluirán en los resultados de distribución de las directivas**, indique un número de dispositivos (con un máximo de 100 000).

   De manera predeterminada, el límite es de 5000.

3. Haga clic en **Guardar**.

   El cambio se aplica y se guarda.

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 **DISPOSITIVOS → DIRECTIVAS Y PERFILES**.

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.

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, copiar, modificar o eliminar un perfil de directiva, y crear una regla de activación para un perfil de directiva.

Ver los perfiles de una directiva

Para ver los perfiles de una directiva:

1. En el menú principal, vaya a **DISPOSITIVOS → DIRECTIVAS Y PERFILES**.
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, la tabla estará vacía.

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.
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 una categoría de su interés. En el panel de resultados de la derecha, modifique 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.

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, incluyendo su nombre y su prioridad; el perfil de directiva original no sufrirá modificaciones.

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. Marque las casillas 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.

  - **Una regla de conexión al Servidor de administración está activa en este 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 manera 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 manera 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 manera 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 manera 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, marque 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 marca estas casillas, no se aplicará este criterio. Estas casillas están desmarcadas por defecto.

  - **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 manera 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.

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.

Usuarios y roles de usuario

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 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. Un rol puede asignarse a un conjunto de usuarios o a un conjunto de grupos de seguridad en cualquier nivel de la jerarquía de grupos de administración.

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 dispositivos y usuarios en una empresa puede ser significativa, pero el número de roles laborales que necesitará de ajustes de seguridad especiales siempre será notablemente 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:

- puede configurar 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 usted mismo.

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**, **Modificar** 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**.

Derechos de acceso a las funciones de la aplicación

Área funcional	Derecho	Acción del usuario: derecho necesario para realizar la acción	Tarea	Informe	
Características generales: **Administración de grupos de administración**	**Modificar**	• Agregar un dispositivo a un grupo de administración: **Modificar** • Eliminar un dispositivo de un grupo de administración: **Modificar** • Agregar un grupo de administración a otro grupo de administración: **Modificar** • Eliminar un grupo de administración de otro grupo de administración: **Modificar**	N/C	N/C	N
Características generales: **Acceder a objetos sin importar sus ACL**	**Leer**	Obtener acceso de lectura a todos los objetos: **Leer**	N/C	N/C	N
Características generales: **Funcionalidad básica**	• **Leer** • **Modificar** • **Ejecutar** • **Realizar operaciones en selecciones de dispositivos**	• Reglas de movimiento de dispositivos (crear, modificar o eliminar) para el Servidor virtual: **Modificar**, **Realizar operaciones en selecciones de dispositivos** • Obtener certificado personalizado del protocolo móvil (LWNGT): **Leer**	• "Descargar actualizaciones en el repositorio del Servidor de administración" • "Entregar informes" • "Distribuir paquete de instalación" • "Instalar aplicación en Servidores de	• "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"	N

		• Establecer certificado personalizado del protocolo móvil (LWNGT): **Escribir** • Obtener la lista de redes definidas por NLA: **Leer** • Agregar, modificar o eliminar la lista de redes definidas por NLA: **Modificar** • Ver la lista de control de acceso de los grupos: **Leer** • Ver el registro de eventos de Kaspersky: **Leer**	administración secundarios de forma remota"	• "Informe de errores" • "Informe de ataques de red" • "Informe conciso de las aplicaciones instaladas de defensa de perímetro" • "Informe conciso sobre los tipos de aplicaciones instaladas" • "Informe sobre usuarios de dispositivos infectados" • "Informe sobre incidentes" • "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 sobre aplicaciones prohibidas" • "Informe de Control web" • "Informe sobre permisos de usuario vigentes"

				• "Informe sobre derechos"	
Características generales: **Objetos eliminados**	• **Leer** • **Modificar**	• Ver objetos eliminados en la Papelera de reciclaje: **Leer** • Eliminar objetos de la Papelera de reciclaje: **Modificar**	N/C	N/C	N
Características generales: **Procesamiento de eventos**	• **Eliminar eventos** • **Editar configuración de notificación de eventos** • **Editar la configuración de registro de eventos** • **Modificar**	• 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**	N/C	N/C	C • •
Características generales: **Operaciones en el Servidor de administración**	• **Leer** • **Modificar** • **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: **Modificar** • Especificar los puertos del proxy de activación ejecutado en el Servidor de administración: **Modificar** • Especificar los puertos del proxy de activación para dispositivos móviles ejecutado en el Servidor de administración: **Modificar** • Especificar los puertos del Servidor	• "Copia de seguridad de los datos del Servidor de administración" • "Mantenimiento de bases de datos"	N/C	N

		web para la distribución de paquetes independientes: **Modificar** • Especificar los puertos del Servidor web para la distribución de perfiles de MDM: **Modificar** • Especificar los puertos SSL del Servidor de administración para la conexión a través de Web Console: **Modificar** • Especificar los puertos del Servidor de administración para la conexión de dispositivos móviles: **Modificar** • Especificar la cantidad máxima de eventos que se pueden almacenar en la base de datos del Servidor de administración **Modificar** • Especificar la cantidad máxima de eventos que puede enviar el Servidor de administración: **Modificar** • Especificar el período durante el cual puede enviar eventos el Servidor de administración: **Modificar**			
Características generales: **Despliegue del software de Kaspersky**	• **Administrar parches de Kaspersky** • **Leer**	Aprobar o rechazar la instalación del parche: **Administrar parches de Kaspersky**	N/C	• "Informe sobre el uso de claves de licencia por Servidor de administración virtual"	Pa in "K

	• **Modificar** • **Ejecutar** • **Realizar operaciones en selecciones de dispositivos**			• "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"	
Características generales: **Administración de claves**	• **Exportar archivo de clave** • **Modificar**	• Exportar un archivo de clave: **Exportar archivo de clave** • Modificar la configuración de la clave de licencia del Servidor de administración: **Modificar**	N/C	N/C	N
Características generales: **Administración de informes**	• **Leer** • **Modificar**	• Crear informes independientemente de sus ACL: **Escribir** • Ejecutar informes independientemente de sus ACL: **Leer**	N/C	N/C	N
Características generales: **Jerarquía de Servidores de administración**	**Configurar la jerarquía de Servidores de administración**	• Registrar, actualizar o eliminar Servidores de administración secundarios: **Configurar la jerarquía de Servidores de administración**	N/C	N/C	N
Características generales: **Permisos de usuario**	**Modificar ACL de objeto**	• Cambiar las propiedades de seguridad de cualquier objeto:	N/C	N/C	N

		Modificar ACL de objeto • Administrar roles de usuario: **Modificar ACL de objeto** • Administrar usuarios internos: **Modificar ACL de objeto** • Administrar grupos de seguridad: **Modificar ACL de objeto** • Administrar alias: **Modificar ACL de objeto**			
Características generales: **Servidores de administración virtuales**	• **Administrar Servidores de administración virtuales** • **Leer** • **Modificar** • **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**	N/C	N/C	N

Roles de usuario predefinidos

Los roles de usuario asignados a los usuarios de Kaspersky Security Center Linux les brindan los conjuntos de derechos que necesitan para acceder a las funciones de la aplicación.

Puede utilizar roles de usuario predefinidos, que ya vienen configurados con un conjunto de derechos, o puede crear roles nuevos y configurar los derechos necesarios a mano. 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 realizar cualquier operación con cualquier tipo de informe. También brinda acceso a todas las operaciones de visualización y permite, incluso, ver objetos eliminados (el rol otorga los permisos **Leer** y **Modificar** en el área **Objetos eliminados**). No permite realizar otras operaciones. Puede asignar este rol a la persona que realiza la auditoría de su organización.
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.

Características de las áreas funcionales. **Gestión de dispositivos móviles: General** y **Gestión del sistema** no están disponibles en Kaspersky Security Center Linux. Un usuario con los roles **Administrador de gestión de parches y vulnerabilidades/Operador** y **Administrador de gestión de dispositivos móviles/Operador** tienen acceso solo por los derechos del área funcional **Características generales**: **Básico**.

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, en **Características generales**: • **Funcionalidad básica** • **Procesamiento de eventos** • **Jerarquía de Servidores de administración** • **Servidores de administración virtuales**
Operador del Servidor de administración	Otorga los derechos **Leer** y **Ejecutar** en las siguientes áreas funcionales en **Características generales**: • **Funcionalidad básica** • **Servidores de administración virtuales**

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, en **Características generales**: • **Funcionalidad básica** • **Despliegue del software de Kaspersky** • **Administración de claves de licencia** 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** en las siguientes áreas funcionales en **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**
Administrador de Kaspersky Endpoint Security	Permite todas las operaciones en las siguientes áreas funcionales: • **Características generales: Funcionalidad básica** • Área de Kaspersky Endpoint Security (se incluyen todas las funciones)
Operador de Kaspersky Endpoint Security	Otorga los derechos **Leer** y **Ejecutar** en las siguientes áreas funcionales: • **Características generales: Funcionalidad básica** • Área de Kaspersky Endpoint Security (se incluyen todas las funciones)
Administrador principal	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 controlada**
Operador principal	Otorga los derechos **Leer** y **Ejecutar** (cuando corresponde) en las siguientes áreas funcionales: • **Características generales**: • **Funcionalidad básica**

	• **Objetos eliminados** • **Operaciones en el Servidor de administración** • **Despliegue del software de Kaspersky Lab** • **Servidores de administración virtuales** • Área de Kaspersky Endpoint Security (se incluyen todas las funciones)
Administrador de Administración de dispositivos móviles	Permite todas las operaciones en el área funcional **Características generales: Funcionalidad básica**.
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 controlada** Otorga los derechos **Leer**, **Modificar**, **Ejecutar**, **Guardar archivos de los dispositivos en la estación de trabajo del administrador** y **Realizar operaciones en selecciones de dispositivos** en el área funcional **Administración de sistemas: Conectividad**. 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**. Esta función no es compatible con Kaspersky Security Center 11 ni versiones posteriores.
Supervisor	Otorga el derecho **Leer** en las áreas funcionales **Características generales**: **Acceder a objetos sin importar sus ACL** y **Características generales**: **Administración de informes controlada**. 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.

Agregar una cuenta de un usuario interno

Para agregar una nueva cuenta de usuario interna a Kaspersky Security Center Linux:

1. En el menú principal, vaya a **USUARIOS Y ROLES** → **USUARIOS**.
2. Haga clic en **Agregar**.
3. En la ventana **Nueva entidad** que se abre, especifique la configuración de la nueva cuenta de usuario:
   - Mantenga la opción predeterminada, **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 16 caracteres
- La contraseña debe contener caracteres de al menos tres de los grupos enumerados a continuación:
  - Letras mayúsculas (A-Z)
  - Letras minúsculas (a-z)
  - Números (0-9)
  - Carácter especial (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- La contraseña no debe contener espacios en blanco, caracteres Unicode o la combinación de "." y "@", cuando "." está colocado delante de "@".

Para ver los caracteres que ha escrito, haga clic en el botón **Mostrar** y manténgalo presionado.

El número de intentos para escribir la contraseña es limitado. De manera predeterminada, el número máximo de intentos permitidos es 10. Puede cambiar el número permitido de intentos para ingresar una contraseña, como se describe en "Cambiar el número de intentos de ingreso de contraseña permitidos".

Si el usuario escribe una contraseña inválida el número de veces especificado, la cuenta de usuario se bloquea durante una hora. Puede desbloquear la cuenta de usuario solo cambiando la contraseña.

- **Nombre completo**
- **Descripción**
- **Dirección de correo electrónico**
- **Teléfono**

4. Haga clic en **Sin inconvenientes** para guardar los cambios.

La nueva cuenta de usuario aparece en la lista usuarios y grupos de usuarios.

Crear un grupo de usuarios

Para crear un grupo de usuarios:

1. En el menú principal, vaya a **USUARIOS Y ROLES** → **USUARIOS**.
2. Haga clic en **Agregar**.
3. En la ventana **Nueva entidad** que se abre, seleccione **Grupo**.
4. Configure los siguientes ajustes del nuevo grupo de usuarios:
   - **Nombre del grupo**

- **Descripción**

5. Haga clic en **Sin inconvenientes** para guardar los cambios.

El nuevo grupo de usuarios aparece en la lista de usuarios y grupos de usuarios.

Editar una cuenta de un usuario interno

Para modificar una cuenta de usuario interna en Kaspersky Security Center Linux:

1. En el menú principal, vaya a **USUARIOS Y ROLES** → **USUARIOS**.
2. Haga clic en el nombre de la cuenta de usuario que desea editar.
3. En la ventana de configuración de usuario que se abre, en la pestaña **General**, cambie la configuración de la cuenta de usuario:
   - **Descripción**
   - **Nombre completo**
   - **Dirección de correo electrónico**
   - **Teléfono principal**
   - **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 16 caracteres
     - La contraseña debe contener caracteres de al menos tres de los grupos enumerados a continuación:
       - Letras mayúsculas (A-Z)
       - Letras minúsculas (a-z)
       - Números (0-9)
       - Carácter especial (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - La contraseña no debe contener espacios en blanco, caracteres Unicode o la combinación de "." y "@", cuando "." está colocado delante de "@".

     Para ver la contraseña introducida, haga clic y mantenga presionado el botón **Mostrar**.

     El número de intentos para escribir la contraseña es limitado. De manera predeterminada, el número máximo de intentos permitidos es 10. Puede cambiar el número permitido de intentos; sin embargo, por razones de seguridad, no recomendamos que reduzca este número. Si el usuario escribe una contraseña inválida el número de veces especificado, la cuenta de usuario se bloquea durante una hora. Puede desbloquear la cuenta de usuario solo cambiando la contraseña.

- Si es necesario, cambie el botón de alternar a **Deshabilitado** para prohibir que el usuario se conecte a la aplicación. Puede desactivar una cuenta, por ejemplo, después de que un empleado abandone la empresa.

4. En la pestaña **Seguridad de autenticación**, 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. Haga clic en **Guardar** para guardar los cambios.

La cuenta de usuario actualizada aparece en la lista de usuarios y en los grupos de usuarios.

Editar un grupo de usuarios

Solo es posible editar grupos internos.

Para editar un grupo de usuarios:

1. En el menú principal, vaya a **USUARIOS Y ROLES** → **USUARIOS**.
2. Haga clic en el nombre del grupo de usuarios que desee editar.
3. Cuando se abra la ventana de configuración del grupo, cambie la configuración del grupo de usuarios:
   - **Nombre**
   - **Descripción**
4. Haga clic en **Guardar** para guardar los cambios.

El grupo de usuarios actualizado aparece en la lista de usuarios y grupos de usuarios.

Agregar cuentas de usuario a un grupo interno

Las únicas cuentas que se pueden agregar a un grupo interno son las de usuarios internos.

Para agregar cuentas de usuario a un grupo interno:

1. En el menú principal, vaya a **USUARIOS Y ROLES** → **USUARIOS**.
2. Active las casillas de verificación ubicadas junto a las cuentas de usuario que desee agregar al grupo.
3. Haga clic en el botón **Asignar grupo**.

4. En la ventana **Asignar grupo** que se abre, seleccione el grupo al que desee agregar las cuentas de usuario.
5. Haga clic en el botón **Asignar**.

   Las cuentas de usuario se agregan al 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 Security para dispositivos móviles.

Para designar a un usuario como propietario de un dispositivo:

1. En el menú principal, vaya a **USUARIOS Y ROLES → USUARIOS**.
2. Haga clic en el nombre de la cuenta de usuario que desee designar como propietario del dispositivo.
3. En la ventana que se abre con los ajustes del usuario, seleccione la pestaña **Dispositivos**.
4. Haga clic en **Agregar**.
5. En la lista de dispositivos, seleccione el dispositivo que desee asignar al usuario.
6. 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 **DISPOSITIVOS → DISPOSITIVOS ADMINISTRADOS**, haga clic en el nombre del dispositivo que desee asignar y luego haga clic en el vínculo **Administrar propietario del dispositivo**.

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**.
2. Seleccione la casilla de verificación junto al usuario o el grupo de seguridad que desea eliminar.
3. Haga clic en **Eliminar**.
4. En la ventana que se abre, haga clic en **Sin inconvenientes**.

   Se elimina el usuario o el grupo de seguridad.

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 **Sin inconvenientes** 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**.
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. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.
4. En la página **Seleccionar rol** del asistente, seleccione el rol de usuario que desee asignar.
5. En la página **Definir alcance** del asistente, seleccione el grupo de administración que desee agregar al alcance del rol de usuario.
6. Haga clic en el botón **Asignar rol** para cerrar el asistente.

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. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.
5. En la página **Definir alcance** del asistente, seleccione el grupo de administración que desee agregar al alcance del rol de usuario.
6. En la página **Seleccionar usuarios** del asistente, 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 el asistente.
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.

Eliminar un rol de usuario

Para eliminar un rol de usuario:

1. En el menú principal, vaya a **USUARIOS Y ROLES → Roles**.
2. Active la casilla de verificación ubicada junto al nombre del rol que desee eliminar.
3. Haga clic en **Eliminar**.
4. En la ventana que se abre, haga clic en **Sin inconvenientes**.

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 y perfiles**.
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. Active la casilla de verificación 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. Active la casilla de verificación 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.

Administración de revisiones de objetos

En esta sección encontrará información sobre la administración de revisiones de objetos. Kaspersky Security Center Linux permite que usted siga la modificación de objeto. Cuando un objeto se modifica de algún modo, se crea una *revisión*. Cada revisión lleva un número que la identifica.

Los objetos de aplicación que admiten la administración de la revisión incluyen:

- Servidores de administración
- Directivas
- Tareas
- Grupos de administración
- Cuentas de usuario
- Paquetes de instalación

Puede realizar las siguientes acciones con las revisiones de los objetos:

- Comparar una revisión seleccionada con la actual
- Comparar revisiones seleccionadas
- Comparar un objeto con una revisión seleccionada de otro objeto del mismo tipo
- Ver una revisión específica
- Deshacer los cambios realizados en un objeto y hacer que este revierta su estado al de una revisión específica
- Guardar revisiones como archivo .txt

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:

- Número de revisión del objeto
- Fecha y hora de modificación del objeto
- Nombre del usuario que modificó el objeto
- Acción realizada en el objeto
- 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 **Descripción**. En la ventana **Descripción de la revisión de objetos**, puede agregar una descripción de revisión.

Acerca de las revisiones de objetos

Puede realizar las siguientes acciones con las revisiones de los objetos:

- Comparar una revisión seleccionada con la actual
- Comparar revisiones seleccionadas
- Comparar un objeto con una revisión seleccionada de otro objeto del mismo tipo
- Ver una revisión específica
- Deshacer los cambios realizados en un objeto y hacer que este revierta su estado al de una revisión específica
- Guardar revisiones como archivo .txt

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:

- Número de revisión del objeto
- Fecha y hora de modificación del objeto
- Nombre del usuario que modificó el objeto
- Acción realizada en el objeto
- Descripción de la revisión vinculada al cambio en la configuración del objeto

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.

Eliminación de objetos

Esta sección proporciona información sobre la eliminación de objetos y la visualización de información sobre los objetos una vez que se eliminan.

Puede eliminar objetos como los siguientes:

- Directivas
- Tareas
- Paquetes de instalación
- Servidores de administración virtuales
- Usuarios
- Grupos de seguridad
- Grupos de administración

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**.

Usar la utilidad klscflag para abrir el puerto 13291

El Servidor de administración utiliza el puerto 13291 para recibir conexiones de las consolas de administración. En equipos que no son Windows, este puerto no está abierto de forma predeterminada. Si desea utilizar la Consola de administración basada en MMC o la utilidad klakaut, puede abrir el puerto a través de 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:

```
$ 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:

```
$ 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` indica que el puerto está abierto. De otra forma, se mostraría el valor `false`.

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

Escenario: 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

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, los módulos de software y las aplicaciones de Kaspersky de forma manual o utilizando directamente los servidores de actualizaciones 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 según lo descrito en el escenario para desplegar las aplicaciones de Kaspersky a través de Kaspersky Security Center 14 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**

   Existen distintos esquemas para instalar las actualizaciones para los componentes de Kaspersky Security Center y las aplicaciones de seguridad. Elija el esquema que mejor se ajuste a los requisitos de su red (o varios esquemas, si resultara necesario).

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.

   Esta 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. Una vez descargadas, las actualizaciones se pueden propagar a los dispositivos administrados.

   Si tiene puntos de distribución asignados en su red, las actualizaciones se copiarán automáticamente del repositorio del Servidor de administración a los repositorios de los puntos de distribución. Los dispositivos administrados incluidos en el alcance de cada punto de distribución descargarán las actualizaciones no del repositorio del Servidor de administración, sino del repositorio del punto de distribución que les corresponda.

   Instrucciones: Creación de la tarea para descargar actualizaciones en el repositorio del Servidor de administración

3. **Crear la tarea para descargar actualizaciones en los repositorios de los puntos de distribución (opcional)**

   De forma predeterminada, las actualizaciones se transfieren del Servidor de administración a los puntos de distribución. Si lo prefiere, puede hacer que Kaspersky Security Center 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: Creación de 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 **Desplegar actualizaciones** 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 el punto de distribución no descargan los archivos completos de las bases de datos y de los módulos de software de Kaspersky, sino archivos diferenciales (denominados 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. Debido a ello, el archivo diff ocupa menos espacio que el archivo completo. La reducción de tamaño se traduce en un menor volumen de 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 tareas *Actualizar* para las aplicaciones administradas, a fin de mantener al día las aplicaciones, los módulos de software y las bases de datos de Kaspersky (incluidas las bases de datos antivirus). Para garantizar actualizaciones a tiempo, recomendamos que, cuando defina la programación de estas tareas, elija la opción **Al descargar nuevas actualizaciones al repositorio**.

   Si algunos de sus dispositivos solo tienen conectividad IPv6 y quiere actualizar regularmente las aplicaciones de seguridad instaladas en ellos, asegúrese de que el Servidor de administración (versión 13.2 en adelante) y el Agente de red (versión 13.2 en adelante) estén instalados en los dispositivos administrados.

   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 acepte los términos, la actualización se podrá propagar a los dispositivos administrados.

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. Su siguiente tarea consistirá, entonces, en 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 verifica 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 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

  Kaspersky Security Center no puede actualizar las aplicaciones de Kaspersky automáticamente. Para actualizar las aplicaciones, descargue las últimas versiones de la aplicación desde el sitio web de Kaspersky e instálelas manualmente:

  - Servidor de administración de Kaspersky Security Center, Kaspersky Security Center Web Console 14
  - Agente de red, Kaspersky Endpoint Security para Linux, complemento web de administración

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:

- Opción 1. Utilizar una sola tarea: *Descargar actualizaciones en el repositorio del Servidor de administración*
- Opción 2. 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*

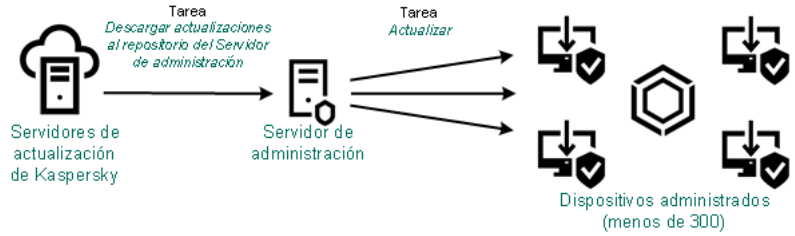
- Utilizar una carpeta local, una carpeta compartida o un servidor FTP (método manual)

- Descarga directa desde los servidores de actualizaciones de Kaspersky a Kaspersky Endpoint Security para Linux en los dispositivos administrados

- A través de una carpeta local o de red si el Servidor de administración no tiene conexión a Internet

Utilizar la tarea Descargar actualizaciones en el repositorio del Servidor de administración

En este esquema, Kaspersky Security Center 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).



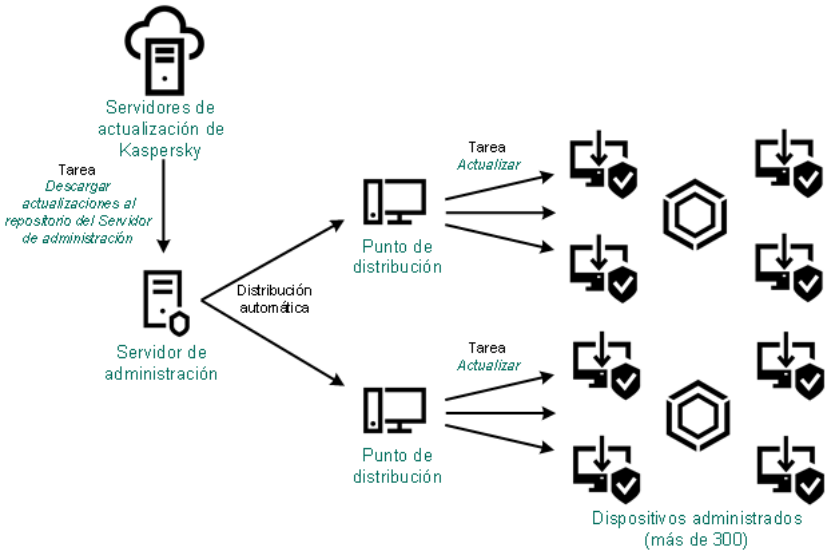
Actualización con la tarea Descargar actualizaciones en el repositorio del Servidor de administración sin utilizar puntos de distribución

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 nueve 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 puntos de distribución y la tarea Descargar actualizaciones en el repositorio del Servidor de administración

Cuando la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* está completa, las actualizaciones de las bases de datos de Kaspersky y los módulos de software para Kaspersky Endpoint Security para Linux se descargan en el repositorio del Servidor de administración. Estas actualizaciones se instalan a través de la tarea Actualizar de Kaspersky Endpoint Security para Linux.

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.

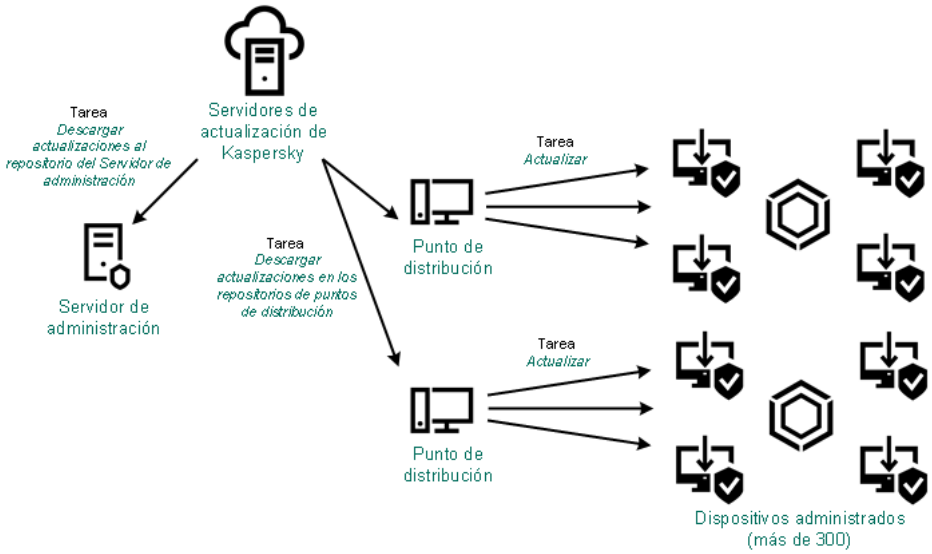
Cada aplicación de Kaspersky le solicita al Servidor de administración las actualizaciones que requiere. El Servidor de administración combina las solicitudes y descarga solo aquellas actualizaciones que han sido solicitadas por alguna aplicación. De este modo, se evita descargar la misma actualización 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 la aplicación
- 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.

Opción 2. 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 con la tarea Descargar actualizaciones en el repositorio del Servidor de administración y la tarea Descargar actualizaciones en los repositorios de los puntos de distribución

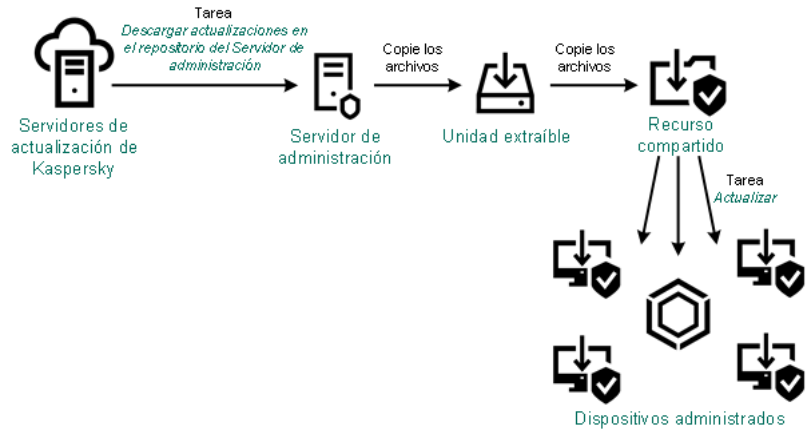
De forma predeterminada, el Servidor de administración y los puntos de distribución se comunican con los servidores de actualizaciones de Kaspersky y descargan las actualizaciones utilizando el protocolo HTTPS. Puede hacer que el Servidor de administración y/o los puntos de distribución utilicen el protocolo 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 y los módulos de software de Kaspersky para Kaspersky Security Center.

Utilizar una carpeta local, una carpeta compartida o un servidor FTP (método manual)

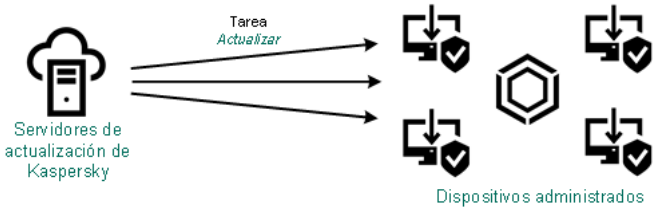
Si sus dispositivos cliente no tienen conexión con el Servidor de administración, puede usar una carpeta local o un recurso compartido como origen de actualizaciones para actualizar las bases de datos, los módulos de software y las aplicaciones de Kaspersky. De elegir esta alternativa, deberá copiar 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 la configuración de Kaspersky Endpoint Security para Linux (vea la siguiente imagen).



Actualización con una carpeta local, una carpeta compartida o un servidor FTP

Descarga directa desde los servidores de actualizaciones de Kaspersky a Kaspersky Endpoint Security para Linux en los dispositivos administrados

Puede configurar Kaspersky Endpoint Security para Linux 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 esta opción, la aplicación de seguridad no utiliza los repositorios que brinda Kaspersky Security Center. Para que las actualizaciones se descarguen directamente de los servidores de actualizaciones de Kaspersky, deberá definir esos servidores como origen de actualizaciones en la interfaz de la aplicación de seguridad. Para obtener más información sobre estos ajustes, consulte la documentación de Kaspersky Endpoint Security para Linux.

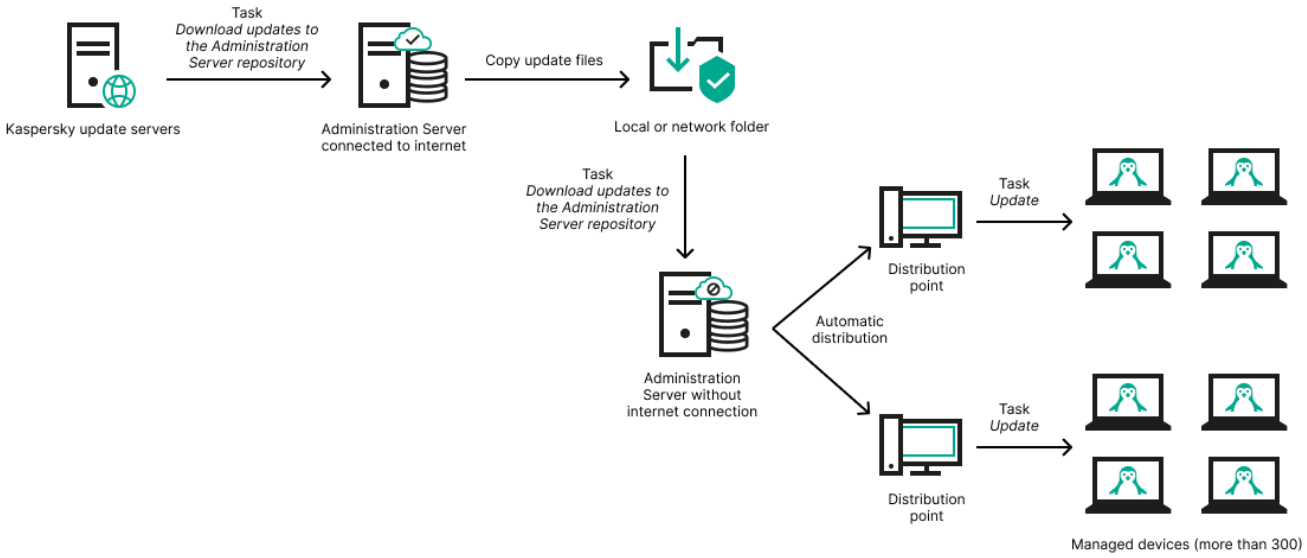
A través de una carpeta local o de red si el Servidor de administración no tiene conexión a Internet

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, active la opción **Descargar las actualizaciones usando el esquema antiguo**.



Actualizar a través de una carpeta local o 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*.

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.

El asistente de inicio rápido de Kaspersky Security Center crea automáticamente la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* del Servidor de administración. 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. Vaya a **DISPOSITIVOS → 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 ("*<>?\:|).

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. De lo contrario, puede configurar los ajustes de la tarea más tarde, en cualquier momento.

6. Haga clic en el botón **Finalizar**.

   La tarea se crea y se muestra en 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**

     Puede usar como origen de actualizaciones, los servidores de actualización de Kaspersky, una carpeta local o de red, o un Servidor de administración principal.

   - **Carpeta para almacenar actualizaciones**

     La ruta a la carpeta especificada para almacenar las actualizaciones guardadas. Puede copiar la ruta de la carpeta al Portapapeles. Esta ruta no se puede modificar en tareas de grupo.

   - **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.

     Esta opción está deshabilitada de manera predeterminada.

   - **Descargar archivos diff**

     Esta opción habilita la función de descarga de archivos diff.

     Esta opción está deshabilitada de manera 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 13.2 o una versión anterior

  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 de versión 13.2 o anterior, habilite la opción **Descargar actualizaciones utilizando el esquema anterior** en la tarea para el primer Servidor de administración.

Esta opción está deshabilitada de manera 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 manera predeterminada.

9. En la ventana de propiedades de la tarea, en la pestaña **Programación**, cree una programación para el inicio de la tarea. De ser necesario, configure los siguientes ajustes:

   - **Inicio programado**:

     Seleccione y configure la programación según la cual se ejecutará la tarea.

     - **Manual** (opción seleccionada por defecto)

       La tarea no se ejecutará automáticamente. Solo se la podrá iniciar en forma manual.

       Esta opción está habilitada de manera 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 forma predeterminada, la tarea se ejecutará cada seis 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.

  Por defecto, la tarea se ejecutará cada lunes a la hora actual del sistema.

- **Diario (no compatible con horario de verano)**

  La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta programación no tiene en cuenta los cambios de horario estacionales. La hora de inicio de la tarea se mantendrá sin cambios incluso si el reloj se atrasa o se adelanta una hora debido al horario de verano.

  No recomendamos usar esta programación. Es necesaria para mantener la compatibilidad con versiones anteriores de Kaspersky Security Center Linux.

  De forma predeterminada, la tarea se iniciará todos los días a la hora actual del sistema.

- **Semanal**

  La tarea se ejecutará cada semana en el día y a la hora que indique.

- **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 p. m.

- **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.

- **Cada mes en los días especificados de semanas seleccionadas**

  La tarea se ejecutará periódicamente, en los días del mes y a la hora que indique.

  Por defecto, no hay ningún día seleccionado; la hora de inicio predeterminada es las 18:00:00 p. m.

- **Al completarse otra tarea**

  La tarea actual se iniciará después de que se complete otra tarea. Puede seleccionar cómo se deberá completar esa tarea anterior (correctamente o con errores) para que se dé inicio a la tarea subsiguiente.

- 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 se ejecutarán las tareas programadas en los dispositivos cliente; las tareas con las opciones de programación **Manual**, **Una vez** e **Inmediatamente** solo se ejecutarán en aquellos dispositivos cliente que estén 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 habilitada de manera predeterminada.

  - **Utilizar retardo aleatorio automático para el inicio de tareas**

    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.

  - **Utilizar un retardo aleatorio para el inicio de tareas dentro de un intervalo de (min)**

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 manera predeterminada. El intervalo de tiempo predeterminado es de un minuto.

- **Detener la tarea si se ha estado ejecutando durante más tiempo que (min)**

  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 manera predeterminada. El tiempo de ejecución por defecto para las tareas es de 120 minutos.

10. Haga clic en el botón **Guardar**.

    La tarea queda creada y configurada.

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.

Ver actualizaciones descargadas

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. Puede ver las actualizaciones descargadas en la sección **ACTUALIZACIONES PARA BASES DE DATOS Y MÓDULOS DE SOFTWARE DE KASPERSKY**.

Para ver la lista de actualizaciones descargadas,

En el menú principal, vaya a **OPERACIONES → APLICACIONES DE KASPERSKY → ACTUALIZACIONES PARA BASES DE DATOS Y MÓDULOS DE SOFTWARE DE KASPERSKY**.

Aparece una lista con las actualizaciones disponibles.

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 *Verificación de actualizaciones* se completa con errores, las actualizaciones problemáticas 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 antivirus para una aplicación compatible con Kaspersky Security Center, como Kaspersky Endpoint Security para Linux. Cuando cree las tareas de actualización y análisis antivirus, seleccione el grupo de administración que contiene los dispositivos de prueba.

   La tarea *Verificación de actualizaciones* ejecutará las tareas de actualización y análisis antivirus 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 antivirus 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 **DISPOSITIVOS → 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**.
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 agregar tareas. Escriba un nombre para la tarea (si desea cambiar el nombre predeterminado).
   c. Seleccione el grupo de administración con dispositivos de prueba que creó en un paso anterior.
   d. Seleccione la tarea de actualización de una aplicación pertinente compatible con Kaspersky Security Center. Luego, seleccione la tarea de análisis antivirus.

      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.

        La opción está habilitada 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 habilitada de manera predeterminada.

   e. Indique qué cuenta se usará para ejecutar la tarea *Verificación de actualizaciones*. Puede usar su propia cuenta y dejar la opción **Cuenta predeterminada** habilitada. 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 su 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 específico:*

1. En el menú principal, vaya a **DISPOSITIVOS → TAREAS**.
2. Haga clic en el botón **Agregar**.

   Se inicia el Asistente para agregar tareas. 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 ("*<>?\:|).
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. Podrá modificar la configuración predeterminada en cualquier otro 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 manera 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. Si el acceso a la carpeta requiere autenticación, solo puede usarse el protocolo SMB. La carpeta local debe ser una carpeta del dispositivo en el que se encuentra instalado el Servidor de administración.

    > El servidor FTP/HTTP o la carpeta de red utilizada por un origen de actualizaciones debe contener una estructura de carpetas (con actualizaciones) que coincida con la estructura que se crea al usar los servidores de actualizaciones de Kaspersky.

  Si habilita la opción **No usar servidor proxy** para los orígenes de actualizaciones Servidores de actualizaciones de Kaspersky o Carpeta local o de red, los puntos de distribución no usarán un servidor proxy para descargar las actualizaciones aunque la opción **Usar servidor proxy** se encuentre habilitada en la configuración de la directiva del Agente de red de esos puntos de distribución.

- **Carpeta para almacenar actualizaciones**

  La ruta a la carpeta especificada para almacenar las actualizaciones guardadas. Puede copiar la ruta de la carpeta al Portapapeles. Esta ruta no se puede modificar en tareas de grupo.

- **Descargar archivos diff**

  Esta opción habilita la función de descarga de archivos diff.

  Esta opción está deshabilitada de manera 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 13.2 o una versión anterior

  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 de versión 13.2 o anterior, 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 manera predeterminada.

10. Programe la ejecución de la tarea. De ser necesario, configure los siguientes ajustes:

- **Inicio programado**:

  Seleccione y configure la programación según la cual se ejecutará la tarea.

  - **Manual** (opción seleccionada por defecto)

    La tarea no se ejecutará automáticamente. Solo se la podrá iniciar en forma manual.

    Esta opción está habilitada de manera 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 forma predeterminada, la tarea se ejecutará cada seis 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.

  Por defecto, la tarea se ejecutará cada lunes a la hora actual del sistema.

- **Diario (no compatible con horario de verano)**

  La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta programación no tiene en cuenta los cambios de horario estacionales. La hora de inicio de la tarea se mantendrá sin cambios incluso si el reloj se atrasa o se adelanta una hora debido al horario de verano.

  No recomendamos usar esta programación. Es necesaria para mantener la compatibilidad con versiones anteriores de Kaspersky Security Center Linux.

  De forma predeterminada, la tarea se iniciará todos los días a la hora actual del sistema.

- **Semanal**

  La tarea se ejecutará cada semana en el día y a la hora que indique.

- **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 p. m.

- **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.

- **Cada mes en los días especificados de semanas seleccionadas**

  La tarea se ejecutará periódicamente, en los días del mes y a la hora que indique.

  Por defecto, no hay ningún día seleccionado; la hora de inicio predeterminada es las 18:00:00 p. m.

- **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 antivirus 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. Puede seleccionar cómo se deberá completar esa tarea anterior (correctamente o con errores) para que se dé inicio a la tarea subsiguiente.

- **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 se ejecutarán las tareas programadas en los dispositivos cliente; las tareas con las opciones de programación **Manual**, **Una vez** e **Inmediatamente** solo se ejecutarán en aquellos dispositivos cliente que estén 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 habilitada de manera predeterminada.

- **Utilizar retardo aleatorio automático para el inicio de tareas**

  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.

- **Utilizar un retardo aleatorio para el inicio de tareas dentro de un intervalo de (min)**

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 manera 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

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. Como carpeta local, puede usar solo una carpeta en el Servidor de administración; como carpeta de red, solo puede utilizar un servidor FTP o HTTP.

Si agrega los servidores de actualización de Kaspersky y la carpeta local o de red, las actualizaciones se descargarán primero desde la carpeta. En caso de error durante la descarga, se utilizarán los servidores de actualización de Kaspersky.

En caso de que una carpeta compartida que contenga actualizaciones esté protegida con contraseña, habilite la opción **Definir cuenta para acceder a la carpeta compartida del origen de actualizaciones (si corresponde)** e ingrese las credenciales de cuenta requeridas para el acceso.

Para agregar las fuentes de actualizaciones:

1. Vaya a **DISPOSITIVOS → 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 línea **Orígenes de actualizaciones**, haga clic en el botón **Configurar**.
5. En la ventana que se abre, haga clic en el botón **Agregar**.
6. En la lista de fuentes de actualización, agregue las fuentes necesarias. Si selecciona la casilla de verificación **Carpeta local o de red**, especifique una ruta a la carpeta.
7. Haga clic en **Aceptar** y, a continuación, cierre la ventana de propiedades de la fuente de actualización.
8. En la ventana de actualización de fuente, haga clic en **Aceptar**.
9. 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.

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 activada 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.

Activación de la función de descarga de archivos diff: escenario

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 la ventana principal de la aplicación, haga clic en el ícono de **Configuración** ( ) ubicado junto al nombre del Servidor de administración pertinente.

   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 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 agregar tareas. Siga las instrucciones del Asistente.

- **Descargar archivos diff**

  Esta opción habilita la función de descarga de archivos diff.

  Esta opción está habilitada de manera 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 utilizando 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 forma predeterminada, las actualizaciones se localizan en: \\<nombre del servidor>\KLSHARE\Updates.

   O bien, puede configurar Kaspersky Security Center para copiar regularmente las actualizaciones a la carpeta que seleccione. 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 especifica una carpeta ubicada en una unidad flash o un disco duro externo como carpeta de destino para esta opción, este dispositivo de almacenamiento masivo siempre contendrá la última versión de las actualizaciones.
3. En los dispositivos sin conexión, configure Kaspersky Endpoint Security para Linux para que obtenga las actualizaciones de una carpeta local o de un recurso compartido (por ejemplo, una carpeta compartida o un servidor FTP).
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 se deban instalar las actualizaciones, inicie la tarea de actualización de Kaspersky Endpoint Security para Linux.

Cuando se complete la tarea de actualización, el dispositivo tendrá las bases de datos y los módulos de software de Kaspersky más recientes.

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.

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:

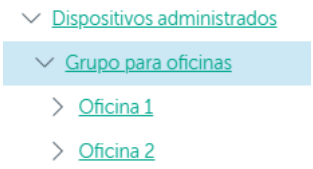
- Armar la estructura de grupos de administración tomando en cuenta la topología de la red. No es necesario que la estructura de grupos de administración refleje con absoluta precisión la topología de la red. Es suficiente con que haya coincidencia entre las partes independientes de la red y ciertos 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 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 designados exclusivamente en una red que contiene un único segmento de red, en función del número de dispositivos en red

Número de dispositivos cliente en el 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 designados exclusivamente en una red que contiene múltiples segmentos 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 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 en	Número de puntos de distribución

el segmento de red	
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 por 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.

Para asignar puntos de distribución automáticamente:

1. En la ventana principal de la aplicación, haga clic en el ícono de **Configuración** ( ) ubicado junto al nombre del Servidor de administración pertinente.

   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 activada, 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 su número y configuración.

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

Para designar manualmente un dispositivo como punto de distribución:

1. En la ventana principal de la aplicación, haga clic en el ícono de **Configuración** () ubicado junto al nombre del Servidor de administración pertinente.

   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 el botón **Aceptar**.

   El punto de distribución agregado aparecerá en la lista de puntos de distribución, en la sección **Puntos de distribución**.

8. En la lista de puntos de distribución, seleccione el punto de distribución que acaba de agregar 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.

     - Número de 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.

       De manera predeterminada, se utiliza el puerto 13000.

     - Usar multidifusión

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.

- **Número de puerto IP multidifusión**

  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.

- **Implementar actualizaciones**

  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 calcular cuántos puntos de distribución necesitará en su red para reducir los volúmenes de tráfico y de carga.

  Si deshabilita esta opción, el número de descargas de actualizaciones y la carga del Servidor de administración podrían aumentar. Esta opción está habilitada de manera predeterminada.

- **Implementar paquetes de instalación**

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 cuántos puntos de distribución necesitará en su red para reducir los volúmenes de tráfico y de 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 habilitada de manera predeterminada.

- 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 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 agregar tareas. Siga las instrucciones del Asistente.

  - **Descargar archivos diff**

    Esta opción habilita la función de descarga de archivos diff.

    Esta opción está habilitada de manera predeterminada.

- Configure el sondeo de rangos de IP por el punto de distribución.
  - **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 intervalos analizados.

Si habilita la opción **Habilitar el sondeo con la tecnología Zeroconf**, 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.

- En la sección **Avanzado**, especifique la carpeta en la que el punto de distribución guardará 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 el botón **Aceptar**.

    El dispositivo seleccionado se designa como punto de distribución.

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. Vaya a **DISPOSITIVOS → Grupos**.
2. En la estructura de grupos de administración, seleccione el grupo de administración para el que desee ver la lista de puntos de distribución.
3. Haga clic en la pestaña **PUNTOS DE DISTRIBUCIÓN**.
4. Utilice el botón **Asignar** para agregar nuevos puntos de distribución al grupo de administración y el botón **Desasignar** para quitar los puntos de distribución asignados.

   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, un punto de distribución puede funcionar como servidor push para los dispositivos administrados a través del protocolo móvil y para los dispositivos administrados por el 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 que utilice la opción **No desconectar del Servidor de administración** en los dispositivos administrados ni que envíe 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. Haga clic en el ícono de **Configuración** ( ) junto al nombre del Servidor de administración requerido.

   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 **Ejecutar servidor push**.

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 el botón **Aceptar**.

El servidor push está habilitado en el punto de distribución seleccionado.

Administración de aplicaciones de terceros en dispositivos cliente

En esta sección, se describen las características de Kaspersky Security Center Linux relacionadas con la administración de aplicaciones de terceros ejecutadas en dispositivos cliente.

Escenario: Administración de aplicaciones

Puede administrar el inicio de aplicaciones en dispositivos de usuario. Puede permitir o impedir que ciertas aplicaciones se ejecuten en estos equipos. A esta funcionalidad la ejecuta el componente Control de aplicaciones.

El componente Application Control está disponible para Kaspersky Endpoint Security 11.2 para Linux y versiones posteriores.

Requisitos previos

- Kaspersky Security Center Linux se implementó en su organización.
- Ha creado y activado una directiva para Kaspersky Endpoint Security para Linux.

Etapas

El escenario 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. Si sabe exactamente qué archivos ejecutables están instalados en los dispositivos administrados, puede omitir esta etapa.

   Instrucciones: Obtener y ver una lista de archivos ejecutables instalados en los dispositivos cliente

2. **Crear categorías de aplicaciones para el software utilizado en la organización**

   Analice las listas de aplicaciones y archivos ejecutables almacenados en los dispositivos administrados. Cree categorías de aplicaciones basadas en los resultados de este análisis. Recomendamos crear una categoría llamada “Aplicaciones de trabajo” que cubra las aplicaciones estándar que se utilicen en la organización. Luego, si tiene grupos de usuarios diferentes que trabajan con aplicaciones diferentes, puede crear una categoría de aplicaciones separada para cada grupo de usuarios.

   Instrucciones: Crear una categoría de aplicaciones con contenido agregado manualmente

3. **Configurar Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Linux**

   Configure el componente Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Linux con las categorías de aplicaciones que creó en la etapa anterior.

4. **Verificar la configuración de Control de aplicaciones**

   Asegúrese de haber hecho lo siguiente:

   - Crear las categorías de aplicaciones.

- Configurar Control de aplicaciones con las categorías de aplicaciones.

Resultados

Al concluir este escenario, la ejecución de aplicaciones en los dispositivos administrados estará bajo su control. Los usuarios pueden iniciar solo aquellas aplicaciones que están permitidas en su organización y no pueden iniciar las que están prohibidas.

Para obtener información detallada sobre Control de aplicaciones, consulte la Ayuda en línea de Kaspersky Endpoint Security para Linux.

Acerca de Control de aplicaciones

El componente Control de aplicaciones supervisa los intentos de los usuarios de iniciar aplicaciones y regula dicho inicio mediante el uso de reglas de Control de aplicaciones.

El componente Application Control está disponible para Kaspersky Endpoint Security 11.2 para Linux y versiones posteriores.

Cuando una aplicación no está alcanzada por una regla de Control de aplicaciones, la posibilidad de que se permita iniciarla depende del modo de funcionamiento del componente. Los modos disponibles son dos:

- *Lista de rechazados*. En este modo, se permite la ejecución de cualquier aplicación, excepto las que están alcanzadas por las reglas de bloqueo. Este modo está seleccionada de manera predeterminada.
- *Lista de admitidos*. En este modo, se impide la ejecución de todas las aplicaciones, excepto las que están alcanzadas por las reglas de autorización.

Las reglas de Control de aplicaciones se basan en categorías de aplicaciones. Estas categorías se crean sobre la base de criterios definidos por usted. En Kaspersky Security Center Linux, solo puede crear categorías con contenido agregado manualmente. Para sumar archivos ejecutables a una categoría de este tipo, deberá definir distintas condiciones: metadatos del archivo, código hash del archivo, certificado del archivo, categoría KL, ruta de acceso al archivo, etc.

Para obtener información detallada sobre Control de aplicaciones, consulte la Ayuda en línea de Kaspersky Endpoint Security para Linux.

Obtención y visualización de una lista de archivos ejecutables almacenados en los dispositivos cliente

Puede obtener una lista de los archivos ejecutables almacenados en los dispositivos administrados. Para hacer un inventario de los archivos ejecutables, debe crear una tarea de inventario.

La función de inventario de archivos ejecutables está disponible para Kaspersky Endpoint Security 11.2 para Linux y versiones posteriores.

Para crear una tarea que haga un inventario de los archivos ejecutables instalados en los dispositivos cliente:

1. Vaya a **DISPOSITIVOS** → **TAREAS**.

Se muestra la lista de tareas.

2. Haga clic en el botón **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Siga los pasos del Asistente.

3. En la página **Nueva tarea**, en la lista desplegable **Aplicación**, seleccione Kaspersky Endpoint Security para Linux.

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 el Asistente para agregar tareas haya finalizado, se crea y configura 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 en línea de Kaspersky Endpoint Security para Linux.

Una vez efectuada la tarea **Inventario**, se crea la lista de archivos ejecutables almacenados en los dispositivos administrados para que pueda verla.

Mientras se crea el inventario, se detectan los archivos ejecutables en los siguientes formatos: MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR, y HTML.

Para visualizar la lista de los archivos ejecutables almacenados en los dispositivos cliente, haga lo siguiente:

En la lista desplegable **OPERACIONES → APLICACIONES DE TERCEROS**, seleccione **ARCHIVOS EJECUTABLES**.

La página muestra la lista de los archivos ejecutables almacenados en los dispositivos cliente.

Crear 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 la lista desplegable **OPERACIONES → APLICACIONES DE TERCEROS**, seleccione **CATEGORÍAS DE APLICACIONES**.

   Se muestra una página con una lista de categorías de aplicaciones.

2. Haga clic en el botón **Agregar**.

   Se inicia el Asistente para crear nueva categoría. Siga los pasos del Asistente.

3. En la página **Seleccione un método para crear la categoría** del Asistente, 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 la página **Condiciones** del asistente, haga clic en el botón **Agregar** a fin de agregar un criterio de condición para incluir archivos en la categoría que se crea.

5. En la lista de la página **Criterios de la condición**, seleccione el tipo de regla que desee usar para crear la categoría:

   - Seleccionar el certificado del repositorio

     Seleccione esta opción para elegir certificados almacenados en el repositorio. Los archivos ejecutables que se hayan firmado conforme a esos certificados se agregarán a la categoría personalizada.

   - 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. Puede seleccionar una aplicación de este registro y especificar los siguientes metadatos del archivo:

       - 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.

     - 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 se almacena en la base de datos del Servidor de administración. Estos valores no ocupan una cantidad de espacio significativa en la base de datos.

SHA-256 es una función de hash criptográfica. En la actualidad, se la considera la más fiable en su clase, pues no se ha encontrado vulnerabilidad alguna en su algoritmo. Kaspersky Endpoint Security para Linux es compatible con computación SHA-256.

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 **SHA-256**.
- Marque la casilla **Hash MD5** solo si utiliza Kaspersky Endpoint Security para Linux. Kaspersky Endpoint Security para Linux no es compatible con la función hash MD5.

Metadatos

Seleccione esta opción si desea especificar los metadatos de los archivos (nombre, versión, proveedor, etc.). Los metadatos se enviarán al Servidor de administración. Los archivos ejecutables que contengan los metadatos especificados se agregarán a la categoría de aplicaciones.

Certificado

Seleccione esta opción para elegir certificados almacenados en el repositorio. Los archivos ejecutables que se hayan firmado conforme a esos certificados se agregarán a la categoría personalizada.

- 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 SHA-256) 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 es compatible con la 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.

El criterio seleccionado se agrega a la lista de condiciones.

Puede agregar tantos criterios como necesite para crear la categoría de aplicaciones.

6. En la página **Exclusiones** del Asistente, haga clic en el botón **Agregar** para agregar un criterio de condición exclusivo para excluir archivos de la categoría que se está creando.

7. En la lista de la página **Criterios de la condición**, seleccione un tipo de regla tal como lo hizo al elegir un tipo de regla para crear la categoría.

Cuando el Asistente finaliza, se crea la categoría de aplicaciones. La nueva categoría aparece 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 en línea de Kaspersky Endpoint Security para Linux.

Visualización de la lista de categorías de aplicaciones

Puede ver la lista de las categorías de aplicaciones configuradas y los parámetros de cada una.

Para ver la lista de categorías de aplicaciones:

En la pestaña **OPERACIONES**, en la lista desplegable **APLICACIONES DE TERCEROS**, seleccione **CATEGORÍAS DE APLICACIONES**.

Se muestra una página con una lista de categorías de aplicaciones.

Para ver las propiedades de una categoría de aplicaciones:

Haga clic en el nombre de la categoría de aplicaciones.

Se muestra la ventana de propiedades de la categoría de aplicaciones. 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 para Linux, podrá ver 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 configuró 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 configuró para aplicar sus reglas en modo de prueba.
- **Mensaje de bloqueo del inicio de una aplicación para el administrador** (evento de nivel *Advertencia*). Este evento aparece si Control de aplicaciones se configuró 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. Vaya a **SUPERVISIÓN E INFORMES → 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 **Siguiente** 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 manera 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 SHA-256 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 SHA-256. Si selecciona una función hash SHA-256, 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 SHA-256 de los archivos sin certificado) a las reglas de la categoría.

  Esta opción está seleccionada de manera 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 SHA-256 (los archivos sin hash se omitirán)**

  Cada archivo tiene su propia función hash SHA-256. Si selecciona una función hash SHA-256, 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 SHA-256 del archivo ejecutable.

- **Solo MD5 (modo discontinuado, solo para Kaspersky Endpoint Security 10 Service Pack 1)**

  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 en línea de Kaspersky Endpoint Security para Linux.

Supervisión e informes

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 o durante la operación, puede configurar las funciones de supervisión e informes para que se adapten mejor a sus necesidades.

Escenario: 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
   - Generación y revisión del Informe de errores

5. **Buscar dispositivos cliente que no se encuentren protegidos**

Instrucciones:

- Revisión del widget Nuevos dispositivos
- Generación y revisión del 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
   - Generación y revisión del 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, la Kaspersky Security Center 14 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 crear y ver selecciones de eventos definidos por el usuario según la configuración disponible en la interfaz de Kaspersky Security Center 14 Web Console para configurarlas.

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.

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.

El panel está disponible en Kaspersky Security Center 14 Web Console, en la sección **SUPERVISIÓN E INFORMES**, al hacer clic en **PANEL**.

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 14 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 textual con vínculos. Puede hacer clic en esos vínculos para acceder a información detallada.

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 E INFORMES** → **PANEL**.
2. Haga clic en el botón **Agregar o restaurar widget web**.
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.
4. Haga clic en el botón **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 E INFORMES** → **PANEL**.
2. Haga clic en el ícono de **Configuración** (⚙) ubicado junto al widget que desee ocultar.
3. Seleccione **Ocultar widget web**.
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 E INFORMES → 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 E INFORMES → 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 E INFORMES → 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 web** (conjunto de objetos de los que muestra la información el widget): por ejemplo, un grupo de administración o selección de dispositivos.
- **Elija una tarea**: tarea a la que corresponde la información mostrada por el widget.
- **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.
- **Fijar en Crítico si esto se cumple** y **Fijar en Advertencia si esto se cumple**: las reglas que determinan el color de un semáforo.

Acerca del modo solo panel

Puede configurar el modo solo 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. 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 ha creado una jerarquía de servidores de administración en su red, para configurar el modo solo panel, vaya al Servidor que tenga disponible la cuenta del usuario en la sección **USUARIOS Y ROLES → USUARIOS**. El servidor 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**.
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. A tal fin, la pestaña **Panel** le permitirá operar con los widgets tal como si estuviera en la sección **SUPERVISIÓN E INFORMES → PANEL**. Podrá hacer lo siguiente:
   - 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, 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 con su cuenta personalizada y utilizar el modo solo panel para monitorear las estadísticas sobre la protección de la red.

Informes

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.

Los informes están disponibles en Kaspersky Security Center 14 Web Console, en la sección **SUPERVISIÓN E INFORMES**, al hacer 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.

Crear una plantilla de informe

Para crear una plantilla de informe:

1. En el menú principal, vaya a **SUPERVISIÓN E INFORMES → INFORMES**.
2. Haga clic en **Agregar**.

   Se abre el Asistente de nueva plantilla de informe. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.
3. En la primera página del asistente, escriba el nombre del informe y seleccione el tipo de informe.
4. En la página **Alcance** del asistente, seleccione el conjunto de dispositivos cliente a los que corresponderán los datos de los informes basados en la nueva plantilla. El conjunto de dispositivos puede ser un grupo de administración, una selección de dispositivos, ciertos dispositivos puntuales o todos los dispositivos conectados a la red.
5. En la página **Período del informe** del Asistente, especifique el período que comprenderán los informes. Los valores disponibles son los siguientes:

   - 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.
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.

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 E INFORMES → 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.

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.

       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, cuando se genera un informe de este tipo, se corre el riesgo de que el dispositivo se quede sin memoria; de ocurrir este problema, no será posible siquiera ver el informe.

       Esta opción está habilitada de manera 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. Los valores disponibles son los siguientes:

       - 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 habilitada de manera 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 manera predeterminada.

- **Frecuencia de actualización de la caché (h)**

  Los servidores de administración secundarios transfieren datos a intervalos regulares 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 manera predeterminada.

- Pestaña **Campos**

  Seleccione los campos que se mostrarán en el informe y ordénelos con los botones **Subir** y **Bajar**. 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 la aplicación (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. Haga clic en el botón **Cerrar** (⨯) para cerrar 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 exportar un informe a un archivo XML o HTML.

Para exportar un informe a un archivo:

1. Vaya a **SUPERVISIÓN E INFORMES** → **INFORMES**.
2. Marque la casilla ubicada junto al informe que desee exportar a un archivo.
3. Haga clic en el botón **Reporte de exportación**.
4. En la ventana que se abre, cambiar el nombre del archivo del informe a través del campo **Nombre**. De forma predeterminada, el nombre del archivo coincide con el nombre de la plantilla de informe seleccionada.
5. Seleccione el tipo de archivo al que se exportará el informe: XML, HTML 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.
6. Haga clic en el botón **Reporte de exportación**.

   El informe se descargará en el formato seleccionado. El archivo se guardará en la carpeta predeterminada del dispositivo o se abrirá la ventana **Guardar como** estándar del navegador para que pueda guardarlo donde desee.

El informe se guarda en el archivo.

Generar y ver un informe

Para crear y ver un informe:

1. En el menú principal, vaya a **SUPERVISIÓN E INFORMES → 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.

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. Vaya a **SUPERVISIÓN E INFORMES → INFORMES**.
2. [Opcional] Marque 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 **Nueva tarea de entrega de informes**.
4. Se inicia el Asistente para crear nueva tarea. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.
5. En la primera página del asistente, escriba el nombre de la tarea. El nombre predeterminado es **Entregar informes (<N>)**, donde <N> es el número secuencial de la tarea.
6. En la página del Asistente que permite configurar la tarea, haga lo siguiente:
   a. Seleccione las plantillas de informe que entregará la tarea. Si seleccionó estas plantillas en el paso 2, omita este punto.
   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.

d. Si los informes se guardarán en una carpeta, si los informes guardados anteriormente en esta carpeta se sobrescribirán y si una cuenta específica se usará para acceder a la carpeta (para una carpeta compartida).

7. Si desea modificar otros ajustes de la tarea después de crearla, en la página **Finalizar la creación de la tarea** del Asistente, habilite la opción **Abrir los detalles de la tarea cuando se complete la creación**.

8. Haga clic en el botón **Crear** para crear la tarea y cerrar el Asistente.

   Se creará la tarea de entrega de informes. Si habilitó la opción **Abrir los detalles de la tarea cuando se complete la creación**, 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 E INFORMES → INFORMES**.

2. Marque las casillas ubicadas junto a las plantillas de informes que desee eliminar.

3. 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.

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.

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 crear y ver selecciones de eventos definidos por el usuario según la configuración disponible en la interfaz de Kaspersky Security Center 14 Web Console para configurarlas.

Selecciones de eventos están disponibles en Kaspersky Security Center 14 Web Console, en la sección **SUPERVISIÓN E INFORMES**, al hacer clic en **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**
  - **Errores funcionales**
  - **Advertencias**
  - **Mensajes de información**
- **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 E INFORMES → 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.
4. Haga clic en **Guardar** para guardar los cambios.

   Se abre la 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 E INFORMES → SELECCIONES DE EVENTOS**.
2. Marque la casilla ubicada junto a la selección de eventos que desee editar.
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 E INFORMES → SELECCIONES DE EVENTOS**.
2. Marque la casilla ubicada junto a la selección de eventos que desee iniciar.
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.
     c. 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.

Ver los detalles de un 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**.
3. En la ventana que se abre, puede hacer lo siguiente:
   - Ver la información del evento seleccionado
   - Ir a los eventos que se encuentran antes y después del elegido en el resultado de la selección de eventos
   - 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

Para exportar eventos a un archivo:

1. Genere una selección de eventos.

2. Marque la casilla ubicada junto al evento pertinente.

3. Haga clic en el botón **Exportar a archivo**.

El evento seleccionado se exporta a un archivo.

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 uno o varios eventos:

1. Genere una selección de eventos.

2. Marque las casillas ubicadas junto a los eventos pertinentes.

3. Haga clic en el botón **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 E INFORMES → SELECCIONES DE EVENTOS**.

2. Marque las casillas ubicadas junto a las selecciones de eventos que desee eliminar.

3. Haga clic en **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 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. 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. Seleccione **DISPOSITIVOS → DIRECTIVAS Y PERFILES**.

2. Realice una de las siguientes acciones:

   - Para configurar el plazo de almacenamiento de los eventos del Agente de red o de una aplicación de Kaspersky administrada, haga clic en el nombre de la directiva correspondiente.

     Se abrirá la página de propiedades de la directiva.

   - Para configurar los eventos del Servidor de administración, en la parte superior de la pantalla, haga clic en el ícono de la **Configuración** () al lado del nombre del Servidor de administración requerido.

     Si tiene una directiva para el Servidor de administración, puede hacer clic en el nombre de esta directiva.

     Se abre la página de propiedades del Servidor de administración (o la página de propiedades de la directiva 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**.

4. Seleccione la sección **Error funcional**, **Advertencia** o **Información**.

5. 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.

6. En el cuadro de edición debajo de este botón de alternancia, introduzca la cantidad de días para almacenar el evento.

7. 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 si la configuración del evento está bloqueada en la directiva del Servidor de administración de Kaspersky Security Center Linux, no podrá redefinir el valor del plazo de almacenamiento para un evento.

8. Haga clic en **Aceptar**.

   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.

Tipos de eventos

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 el Agente de red de Kaspersky Security Center Linux. Los tipos de eventos que pueden ocurrir en las aplicaciones de Kaspersky no se detallan en esta sección.

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

En la siguiente tabla, se enumeran los eventos del Servidor de administración de Kaspersky Security Center Linux que tienen el nivel de importancia **Crítico**.

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
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 ha superado alguna restricción 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 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	180 días

			activación válido o un archivo de clave en el Servidor de administración). Kaspersky Security Center Linux determina las reglas para generar eventos cuando se excede una restricción de licencia.	
El dispositivo ha cambiado a no administrado	4111	KLSRV_HOST_OUT_CONTROL	Este tipo de evento ocurre cuando un dispositivo administrado es visible en la red, pero no se ha conectado en un período específico al Servidor de administración. 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
El archivo de clave está en la lista de claves rechazadas	4124	KLSRV_LICENSE_BLACKLISTED	Este tipo de evento ocurre cuando Kaspersky agregó el código de activación o el archivo de clave utilizados a la lista de rechazados.	180 días

			Comuníquese con nuestro servicio de soporte técnico para más información.	
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. Kaspersky Security Center verifica una vez al día si alguna licencia está próxima a caducar. 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. Esta cantidad de días no se puede cambiar. 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	180 días

			término y por adelantado el pago correspondiente.	
El certificado ha caducado	4132	KLSRV_CERTIFICATE_EXPIRED	Este tipo de evento ocurre cuando caduca el certificado del Servidor de administración para Administración de dispositivos móviles. Deberá actualizar el certificado caducado. Si desea que los certificados se actualicen automáticamente, puede marcar la casilla **Volver a emitir certificados automáticamente si es posible** en los ajustes de emisión de certificados.	180 días

Eventos del Servidor de administración: nivel Error funcional

En la siguiente tabla, se enumeran los eventos del Servidor de administración de Kaspersky Security Center Linux que tienen el nivel de importancia **Error funcional**.

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 almacenami predetermi
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
Límite de instalaciones	4126	KLSRV_INVLICPROD_EXCEDED	El Servidor de administración genera	180 días

excedido en uno de los grupos de aplicaciones con licencia			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. Puede administrar claves de licencia de aplicaciones de terceros usando la funcionalidad 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.	
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	180 días

			que se emplea para obtener acceso a la(s) carpeta(s) tiene permiso de escritura. • Compruebe si cambió un nombre de usuario y / o una contraseña de la carpeta(s). • 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.	
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
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.	180 días

			• Compruebe la conexión de red.	
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 SQL Server 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. Por ejemplo, debido al mantenimiento preventivo, un servidor remoto con SQL Server instalado puede no estar disponible.	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: • Si su DBMS es SQL Server	180 días

			Express Edition: • En la documentación de SQL Server Express, revise el límite de tamaño de la base de datos de la versión que usa. Probablemente su base de datos del Servidor de administración haya excedido el límite de tamaño de la base de datos. • 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 cambiar la configuración de la directiva de Kaspersky Endpoint Security para Linux relacionada con el almacenamiento de eventos de Control de aplicaciones en la base de datos del Servidor de administración. • Si su DBMS no es SQL Server

			Express Edition: • No limite el número de eventos para almacenar en la base de datos del Servidor de administración. • Reduzca la lista de eventos para almacenar en la base de datos del Servidor de administración. Revise la información sobre la selección del DBMS.	

Eventos del Servidor de administración: nivel Advertencia

En la siguiente tabla, se enumeran los eventos del Servidor de administración de Kaspersky Security Center Linux que tienen el nivel de importancia **Advertencia**.

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 almacenar predeterm
Se ha superado el límite de la licencia	4098	KLSRV_EV_LICENSE_CHECK_100_110	Una vez al día, Kaspersky Security Center Linux comprueba si se ha superado alguna restricción 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 se ha utilizado entre un 100 % y un 110 % del total de unidades con licencia cubiertas por una sola licencia.	90 días

			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 excede una restricción de licencia.	
El dispositivo ha estado 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 se dio de baja el dispositivo. Puede responder al evento de los siguientes modos: • Elimine el dispositivo manualmente de la lista de dispositivos administrados.	90 días

			Especificar el intervalo de tiempo después del cual se crea el evento **El dispositivo ha estado inactivo en la red por mucho tiempo** con Kaspersky Security Center 14 Web Console. • Especificar el intervalo de tiempo después del cual el dispositivo se elimina automáticamente del grupo mediante Kaspersky Security Center 14 Web Console.	
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

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
El límite de instalaciones está por excederse en uno de los grupos de aplicaciones con licencia	4127	KLSRV_INVLICPROD_FILLED	Este tipo de evento ocurre cuando el número de instalaciones para las aplicaciones de terceros incluidas en un grupo de aplicaciones con licencia alcanza el 90 % del valor máximo permitido 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.	90 días

			Puede administrar claves de licencia de aplicaciones de terceros usando la funcionalidad de grupos de aplicaciones con licencia.	
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 configuró la integración con una infraestructura de claves públicas, 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

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
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 APN e instalarlo en un servidor de MDM para iOS.	No se alma
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 APN caduque, deberá 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 alma
No se pudo enviar el	4138	KLSRV_GCM_DEVICE_ERROR	Este tipo de evento ocurre cuando Mobile	90 días

mensaje de FCM al dispositivo móvil			Device Management se configuró para que la conexión a los dispositivos Android administrados se establezca utilizando Google Firebase Cloud Messaging (FCM) y el servidor de FCM no puede atender algunas de las solicitudes enviadas por el 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").	
Error de HTTP al enviar un mensaje del FCM al servidor de FCM	4139	KLSRV_GCM_HTTP_ERROR	Este tipo de evento ocurre cuando Mobile Device Management está configurado para utilizar Google Firebase Cloud Messaging (FCM) para la conexión de dispositivos móviles Android administrados y el servidor de FCM responde a una solicitud del Servidor de administración con un código HTTP distinto de 200 (OK).	90 días

			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 del evento y responda en consecuencia.	
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.	90 días

			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.	
Queda poco espacio libre en el disco duro	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
Queda poco 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. Si su DBMS es SQL Server Express Edition: • En la documentación del DBMS, consulte el límite de tamaño para una base de datos en su versión de SQL Server Express. Es probable que la base de datos del Servidor de	90 días

			administración esté a punto de alcanzar el tamaño máximo posible. • 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 cambiar la configuración de la directiva de Kaspersky Endpoint Security para Linux relacionada con el almacenamiento de eventos de Control de aplicaciones en la base de datos del Servidor de administración. Si su DBMS no es SQL Server Express Edition: • 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.	

Se ha interrumpido 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 de eventos de Kaspersky en el dispositivo en el que esté instalado el Servidor de administración secundario y responda en consecuencia.	90 días
Se ha interrumpido 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 de eventos de Kaspersky en el dispositivo en el que esté instalado el Servidor de administración principal y responda en consecuencia.	90 días
Se registraron nuevas actualizaciones para los módulos del software 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
Se superó el límite del número de eventos en la base de datos,	4145	KLSRV_EVP_DB_TRUNCATING	Este tipo de evento ocurre cuando el sistema comienza a eliminar eventos antiguos de la base	No se alma

se inició la eliminación de eventos			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.	
Se superó el límite del número de eventos en la base de datos, se eliminó 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 alma

Eventos del Servidor de administración: nivel Información

En la siguiente tabla, se enumeran los eventos del Servidor de administración de Kaspersky Security Center Linux que tienen el nivel de importancia **Información**.

Eventos del Servidor de administración: nivel Información

Nombre que se muestra para el tipo de evento	Id. del tipo de evento	Tipo de evento	Plazo de almacenamiento predeterminado
Se ha consumido más del 90 % de la clave de licencia	4097	KLSRV_EV_LICENSE_CHECK_90	30 días
Se detectó un nuevo dispositivo	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 días
Dispositivo agregado al grupo automáticamente	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 días
Dispositivo eliminado del grupo: estuvo inactivo en la red por mucho tiempo	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 días
El límite de instalaciones está por alcanzarse (se consumió más del 95 %) en uno de los grupos de aplicaciones con licencia	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 días
Se han encontrado archivos para enviar a Kaspersky para su análisis	4131	KLSRV_APS_FILE_APPEARED	30 días
El id. de instancia de FCM ha cambiado en este dispositivo móvil	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 días
Las actualizaciones se copiaron correctamente en la carpeta especificada	4122	KLSRV_UPD_REPL_OK	30 días
Se estableció la conexión con el Servidor de administración secundario	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 días
Se estableció la conexión con el Servidor de administración principal	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 días
Las bases de datos se han actualizado	4144	KLSRV_UPD_BASES_UPDATED	30 días
Auditoría: Se estableció la conexión con el Servidor de administración	4147	KLAUD_EV_SERVERCONNECT	30 días
Auditoría: El objeto se modificó	4148	KLAUD_EV_OBJECTMODIFY	30 días
Auditoría: El estado del objeto se modificó	4150	KLAUD_EV_TASK_STATE_CHANGED	30 días
Auditoría: La configuración del grupo se modificó	4149	KLAUD_EV_ADMGROUP_CHANGED	30 días
Auditoría: Se cerró la conexión con el Servidor de	4151	KLAUD_EV_SERVERDISCONNECT	30 días

administración			
Auditoría: Las propiedades del objeto se han modificado	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 días
Auditoría: Las propiedades del usuario se han modificado	4153	KLAUD_EV_OBJECTACLMODIFIED	30 días

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 Advertencia

La siguiente tabla muestra los eventos del Agente de red de Kaspersky Security Center que tienen el nivel de gravedad **Advertencia**.

Eventos del Agente de red: nivel Advertencia

Nombre que se muestra para el tipo de evento	Id. del tipo de evento	Tipo de evento	Plazo de almacenamiento predeterminado
Ocurrió un incidente	549	GNRL_EV_APP_INCIDENT_OCCURED	30 días

Eventos del Agente de red: nivel Información

La siguiente tabla muestra los eventos del Agente de red de Kaspersky Security Center que tienen el nivel de gravedad **Información**.

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 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
Dispositivo eliminado	7709	KLNAG_EV_DEVICE_REMOVE	30 días
Se detectó un nuevo dispositivo	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 días
Dispositivo autorizado	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 días

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 para 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 la ventana principal de la aplicación, haga clic en el ícono de **Configuración** ( ) ubicado junto al nombre del Servidor de administración pertinente.

   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, a continuación, 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 la ventana principal de la aplicación, haga clic en el ícono de **Configuración** ( ) ubicado junto al nombre del Servidor de administración pertinente.

   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 de 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.

Si el número de eventos de la base de datos alcanza el valor máximo que especificó el administrador, la aplicación elimina los eventos más antiguos y los reemplaza por los nuevos. Cuando el Servidor de administración elimina los eventos antiguos, no puede guardar los nuevos eventos en la base de datos. Durante este período de tiempo, la información sobre los eventos que fueron rechazados se escribe en el Registro de eventos de Kaspersky. Los nuevos eventos se ponen en cola y se guardan en la base de datos una vez finalizada la operación de borrado.

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.

Uso de 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.

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 le alertan sobre eventos agrupados por niveles de importancia (*Crítico*, *Advertencia* e *Informativo*).

La notificación en pantalla puede tener uno de estos dos estados:

- *Revisado*. Significa que ha realizado la acción recomendada para la notificación o ha asignado este estado para la notificación manualmente.
- *No revisado*. Significa que no ha realizado la acción recomendada para la notificación o ha asignado este estado para la notificación manualmente.

De forma predeterminada, la lista de notificaciones incluye notificaciones en el estado *No revisado*.

Puede supervisar la red de su organización, ver las notificaciones en pantalla y responder 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 en pantalla

Puede ver las notificaciones en pantalla de tres formas:

- En la sección **SUPERVISIÓN E INFORMES** →**NOTIFICACIONES**. Aquí puede ver las notificaciones relacionadas con las categorías predefinidas.
- En una ventana separada que se puede abrir sin importar qué sección esté usando en ese momento. En este caso puede marcar las notificaciones como revisadas.
- En el widget **Notificaciones por nivel de gravedad seleccionado**, en la sección **SUPERVISIÓN E INFORMES**→ **PANEL**. En el widget, puede ver solo notificaciones de eventos que se encuentran en los niveles de importancia *Crítico* y *Advertencia*.

Puede realizar acciones, por ejemplo, puede responder a un evento.

Para ver las notificaciones desde las categorías predefinidas:

1. En el menú principal, vaya a **SUPERVISIÓN E INFORMES** → **NOTIFICACIONES**.

   La categoría **Todas las notificaciones** se selecciona en el panel izquierdo y en el panel derecho se muestran todas las notificaciones.

2. En el panel izquierdo, seleccione una de las categorías:

   - **Despliegue**
   - **Dispositivos**
   - **Protección**
   - **Actualizaciones** (esto incluye notificaciones sobre las aplicaciones de Kaspersky disponibles para descargar y notificaciones sobre las actualizaciones que se han descargado para las bases de datos antivirus).
   - **Prevención de exploits**
   - **Servidor de administración** (esto incluye eventos que conciernen únicamente al Servidor de administración).
   - **Vínculos útiles** (esto incluye enlaces a recursos de Kaspersky, por ejemplo, Servicio de soporte técnico de Kaspersky, foro de Kaspersky, página de renovación de licencia o Enciclopedia de TI de Kaspersky).

- **Noticias de Kaspersky** (esto incluye información sobre lanzamientos de aplicaciones de Kaspersky).

Se muestra una lista de notificaciones de la categoría seleccionada. La lista contiene lo siguientes:

- Ícono relacionado con el tema de la notificación: despliegue (), protección (), actualizaciones (), administración de dispositivos (), prevención de vulnerabilidades (), servidor de administración ().
- Nivel de importancia de la notificación. Se muestran notificaciones de los siguientes niveles de importancia: **Notificaciones críticas** (), **Notificaciones de advertencia** (), **Notificaciones de información**. Las notificaciones de la lista se agrupan por niveles de importancia.
- **Notificación**. Esto contiene una descripción de la notificación.
- **Acción**. Esto contiene un vínculo a una acción rápida que le recomendamos que realice. Por ejemplo, al hacer clic en este vínculo, puede ir al repositorio e instalar aplicaciones de seguridad en los dispositivos, o ver una lista de dispositivos o una lista de eventos. Después de realizar la acción recomendada para la notificación, a esta notificación se le asigna el estado *Revisado*.
- **Antigüedad del estado**. Esto contiene la cantidad de días u horas que han pasado desde el momento en que se registró la notificación en el Servidor de administración.

Para ver las notificaciones en pantalla en una ventana separada por nivel de importancia:

1. En la esquina superior derecha de Kaspersky Security Center 14 Web Console, haga clic en el icono del **Banderín** ().

   Si el ícono del **Banderín** tiene un punto rojo, hay notificaciones que no se han revisado.

   Se abrirá una ventana con la lista de notificaciones. De forma predeterminada, se selecciona la pestaña **Todas las notificaciones** y se agrupan las notificaciones por nivel de importancia: *Crítico*, *Advertencia* e *Información*.

2. Seleccione la pestaña **Sistema**.

   Se muestra la lista de notificaciones de niveles de importancia *Crítico* () y *Advertencia* (). La lista de notificaciones incluye lo siguiente:

   - Marcador de color. Las notificaciones críticas están marcadas en rojo. Las notificaciones de advertencia están marcadas en amarillo.
   - Ícono que indica el tema de la notificación: despliegue (), protección (), actualizaciones (), administración de dispositivos (), prevención de vulnerabilidades (), servidor de administración ().
   - Descripción de la notificación.
   - Ícono del **banderín**. El íconi de **banderín** está en gris si a las notificaciones se les ha asignado el estado *No revisado*. Cuando selecciona el ícono de **banderín** gris y asigna el estado *Revisado* a una notificación, el ícono cambia al color blanco.
   - Enlace a la acción recomendada. Cuando realiza la acción recomendada después de hacer clic en el vínculo, a la notificación se le asigna el estado *Revisado*.
   - Número de días que han pasado desde la fecha en que se registró la notificación en el Servidor de administración.

3. Seleccione la pestaña **Más**.

Se muestra la lista de notificaciones de nivel de importancia *Información*.

La organización de la lista es la misma que para la lista en la pestaña **Sistema** (consulte la descripción anterior). La única diferencia es la ausencia de un marcador de color.

Puede filtrar las notificaciones por el intervalo de fecha en que se registraron en el Servidor de administración. Use la casilla **Mostrar filtro** para administrar el filtro.

Ver notificaciones en pantalla en el widget:

1. En la sección **PANEL**, seleccione **Agregar o restaurar widget web**.

2. En la ventana que se abre, haga clic en la categoría **Otros**, seleccione el widget **Notificaciones por nivel de gravedad seleccionado** y haga clic en Agregar.

   El widget aparece ahora en la pestaña **PANEL**. De forma predeterminada, las notificaciones del nivel de importancia *Crítico* se muestran en el widget.

   Puede hacer clic en el botón **Configuración** en el widget y cambiar la configuración del widget para ver las notificaciones del nivel de importancia *Advertencia*. O puede agregar otro widget: **Notificaciones por nivel de gravedad seleccionado**, con un nivel de importancia *Advertencia*.

   La lista de notificaciones en el widget está limitada por su tamaño e incluye dos notificaciones. Estas dos notificaciones se refieren a los últimos eventos.

La lista de notificaciones en el widget incluye lo siguiente:

- Ícono relacionado con el tema de la notificación: despliegue (), protección (), actualizaciones (), administración de dispositivos (), prevención de vulnerabilidades (), servidor de administración ().

- Descripción de la notificación con un vínculo a la acción recomendada. Cuando realiza la acción recomendada después de hacer clic en el vínculo, a la notificación se le asigna el estado *Revisado*.

- Número de días o número de horas que han pasado desde la fecha en que se registró la notificación en el Servidor de administración.

- Enlace a otras notificaciones. Al hacer clic en este vínculo, se le transfiere a la vista de notificaciones en la sección **NOTIFICACIONES** de la sección **SUPERVISIÓN E INFORMES**.

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). 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.

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 antivirus, detectó algunos virus en el dispositivo, y el número de virus encontrados supera el 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. • En pausa. • En ejecución.
El análisis antivirus no se ha realizado en mucho tiempo	El dispositivo es visible en la red y una aplicación de seguridad está instalada en el dispositivo, pero la tarea Análisis antivirus no se ejecutó durante 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.
Se debe reiniciar el dispositivo	El dispositivo es visible en la red, pero una aplicación requiere que el dispositivo se reinicie por más tiempo que el intervalo de tiempo especificado y por una de las razones seleccionadas.	Más de 0 minutos.
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.
Licencia caducada	El dispositivo es visible en la red, pero la licencia caducó.	• 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.
Se detectaron incidentes no procesados	Se han encontrado incidentes sin procesar en el dispositivo. Los incidentes pueden ser creados 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.	• 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.	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 configuradas. 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.

Cuando Kaspersky Security Center Linux asigna un estado a un dispositivo, para algunas condiciones (consulte la columna Descripción de condición) se tiene en cuenta el indicador de visibilidad. 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*.

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 **DISPOSITIVOS → 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 **Crítico**.
5. En el panel derecho, en la sección **Fijar en Crítico si esto se cumple**, 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**.

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 **DISPOSITIVOS → 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 **Fijar en Advertencia si esto se cumple**, 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**.

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 la parte superior de la pantalla, haga clic en el ícono de **Configuración** () ubicado junto al nombre del Servidor de administración pertinente.

   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 el 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 recibido 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. Estos dos archivos no dependen el uno del otro y el orden en que se los carga no es importante. 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**, especifique el asunto del correo electrónico. 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.

> 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 enviarán 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 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 el 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 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 **Enviar mensaje de prueba** para verificar si configuró las notificaciones correctamente: la aplicación envía una notificación de prueba al destinatario que especificó.

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.

- **Archivo ejecutable para ejecutar**

  Si se selecciona este método de notificación, en el campo de entrada puede especificar la aplicación que se iniciará cuando ocurra un evento.

  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. Antes de especificar el archivo, prepare el archivo y especifique los marcadores que definan los detalles del evento que se enviará en el mensaje de notificación. La carpeta y el archivo que especifique deben estar ubicados en el Servidor de administración.

  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.

3. En la pestaña, defina la configuración de la notificación.
4. Haga clic en el botón **Aceptar** para 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 E INFORMES → 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.

Notificaciones de eventos que se muestran al ejecutar un archivo ejecutable

Kaspersky Security Center Linux puede notificar al administrador acerca de los eventos en dispositivos del cliente al abrir un archivo ejecutable. El archivo ejecutable debe contener otro archivo ejecutable con marcadores del evento que se transmitirá al administrador.

Marcadores para describir un evento

Marcador	Descripción del marcador
%SEVERITY%	Nivel de importancia del evento
%COMPUTER%	Nombre del dispositivo en el cual sucedió el evento
%DOMAIN%	De dominio
%EVENT%	Evento
%DESCR%	Descripción del evento
%RISE_TIME%	Hora de creación
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Nombre de la tarea
%KL_PRODUCT%	Agente de red de Kaspersky Security Center Linux
%KL_VERSION%	Número de versión del Agente de red
%HOST_IP%	Dirección IP
%HOST_CONN_IP%	Dirección IP de la conexión

Ejemplo:
Las notificaciones de eventos se envían a través de un archivo ejecutable (como script1.bat) dentro del que se inicia otro archivo ejecutable (como script2.bat) con el marcador %COMPUTER%. Cuando sucede un evento, el archivo script1.bat se ejecuta en el dispositivo del administrador, que a su vez ejecuta el archivo script2.bat con el marcador %COMPUTER%. El administrador luego recibe el nombre del dispositivo en el cual sucedió el evento.

Novedades de Kaspersky

En esta sección, encontrará información para utilizar, configurar y deshabilitar las novedades de Kaspersky.

Acerca de las novedades de Kaspersky

La sección de anuncios de Kaspersky (**SUPERVISIÓN E INFORMES → Anuncios de Kaspersky**) lo mantiene informado al brindarle información relacionada con su versión de Kaspersky Security Center y las aplicaciones administradas instaladas en los dispositivos administrados. Kaspersky Security Center actualiza periódicamente la información de esta sección al eliminar anuncios obsoletos y agregar información nueva.

Kaspersky Security Center muestra solo los anuncios de Kaspersky que se relacionan con el Servidor de administración conectado actualmente y las aplicaciones de Kaspersky instaladas en los dispositivos administrados de este Servidor de administración. Las novedades de cada tipo de Servidor de administración (primario, secundario o virtual) se muestran por separado.

El Servidor de administración debe tener una conexión a Internet para recibir los anuncios de Kaspersky.

Las novedades sobre seguridad están pensadas para que mantenga actualizadas y en perfectas condiciones de funcionamiento las aplicaciones de Kaspersky instaladas en su red. Estas novedades pueden dar aviso de actualizaciones críticas que se hayan publicado para las aplicaciones de Kaspersky, de soluciones disponibles para las vulnerabilidades detectadas o de formas de solucionar otros problemas en las aplicaciones de Kaspersky. De forma predeterminada, los anuncios de Kaspersky están habilitados. Si no desea recibir estas novedades, deshabilite la función correspondiente.

Para mostrarle la información que corresponde a la configuración de protección de su red, Kaspersky Security Center envía datos a los servidores en la nube de Kaspersky y recibe solo los anuncios que se relacionan con las aplicaciones de Kaspersky instaladas en su red. El conjunto de datos que se puede enviar a los servidores se describe en el Contrato de licencia de usuario final que acepta al instalar el Servidor de administración de Kaspersky Security Center.

La nueva información se divide en las siguientes categorías, según su importancia:

1. Información crítica
2. Noticias importantes
3. Advertencia
4. Información

Cuando aparece nueva información en la sección de anuncios de Kaspersky, Kaspersky Security Center 14 Web Console muestra una etiqueta de notificación que corresponde al nivel de importancia de los anuncios. Haga clic en la etiqueta para ver la información en la sección de novedades de Kaspersky.

Puede especificar la configuración de los anuncios de Kaspersky, incluidas las categorías de anuncios que desea ver y dónde mostrar la etiqueta de notificación. Si no desea recibir estas novedades, puede deshabilitar la función.

Especificar la configuración de los anuncios de Kaspersky

En la sección Anuncios de Kaspersky, puede especificar la configuración de los anuncios de Kaspersky, incluidas las categorías de anuncios que desea ver y dónde mostrar la etiqueta de notificación.

Para configurar los anuncios de Kaspersky:

1. En el menú principal, vaya a **SUPERVISIÓN E INFORMES → NOVEDADES DE KASPERSKY**.
2. Haga clic en el vínculo **Configuración**.

   Se abre la ventana de configuración de los anuncios de Kaspersky.
3. Configure los siguientes ajustes:

   - Seleccione el nivel de importancia de los anuncios que desea ver. No se mostrarán los anuncios de otras categorías.
   - Seleccione dónde desea ver la etiqueta de notificación. La etiqueta puede aparecer en todas las secciones de la consola o en la sección **SUPERVISIÓN E INFORMES** y sus subsecciones.
4. Haga clic en el botón **Aceptar**.

   Se especifica la configuración de los anuncios de Kaspersky.

Dejar de recibir las novedades de Kaspersky

La sección de anuncios de Kaspersky (**SUPERVISIÓN E INFORMES → Anuncios de Kaspersky**) lo mantiene informado al brindarle información relacionada con su versión de Kaspersky Security Center y las aplicaciones administradas instaladas en los dispositivos administrados. Si ya no desea recibir novedades de Kaspersky, puede deshabilitar esta función.

Para dejar de recibir las novedades de Kaspersky:

1. En la ventana principal de la aplicación, haga clic en el ícono de **Configuración** ( ) ubicado junto al nombre del Servidor de administración pertinente.

   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.

Exportación de eventos a sistemas SIEM

En esta sección, se brindan instrucciones para configurar la exportación de eventos a un sistema SIEM.

Escenario: Configurar la exportación de eventos a un sistema SIEM

Kaspersky Security Center Linux permite configurar la exportación de eventos a sistemas SIEM mediante uno de los siguientes métodos: exportación a cualquier sistema SIEM que utilice el formato Syslog o exportación de 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 del sistema SIEM para que reciba 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:

  - Mediante los protocolos TCP/IP, UDP o TLS sobre TCP
  - Exportar los eventos directamente de la base de datos de Kaspersky Security Center (la base de datos de Kaspersky Security Center proporciona un conjunto de vistas públicas, que se describen en el documento el 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.

Antes de comenzar

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 los eventos en Kaspersky Security Center Linux

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. Puede exportar esta información a un sistema SIEM externo. Al hacerlo, permitirá que los administradores del sistema SIEM respondan oportunamente a los sucesos del sistema de seguridad que se registren en los dispositivos o grupos de dispositivos administrados.

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** en la política 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 se registra cuando ocurre un problema, fallo o error graves en el funcionamiento de la aplicación o en la ejecución de 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 de *información* 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.

Acerca de la exportación de eventos

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, por sus siglas en inglés).

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.

Formato Syslog de exportación de eventos

Puede enviar eventos en formato Syslog a cualquier sistema SIEM. A través del formato Syslog, puede transmitir cualquier evento que ocurra en el Servidor de administración y en las aplicaciones de Kaspersky instaladas en dispositivos administrados. Al exportar eventos en formato Syslog, puede seleccionar exactamente qué tipos de eventos se transmitirán al sistema SIEM.

Recepción de eventos por parte del sistema SIEM

El sistema SIEM debe recibir y correctamente analizar eventos recibidos de Kaspersky Security Center Linux. Para que esto ocurra, el sistema SIEM debe estar correctamente configurado. 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, 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**

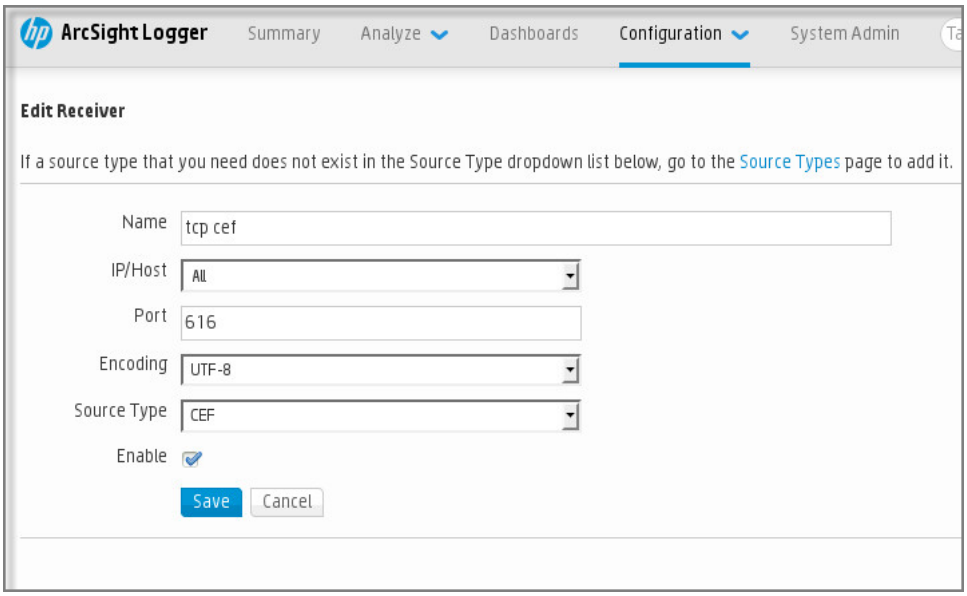
  Especifique el número de puerto utilizado para conectarse a Kaspersky Security Center Linux. Este puerto debe ser el mismo que el puerto que especifica en Kaspersky Security Center Linux durante la configuración con un sistema SIEM.

- **Formato de datos**

  Especifique el formato Syslog.

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. Estos mensajes deben analizarse; de lo contrario, el sistema SIEM no puede hacer uso de la información de los eventos. Los analizadores sintácticos de mensajes son parte del sistema SIEM; se usan para separar los contenido del mensaje en los campos relevantes, por ejemplo ID del evento, gravedad, descripción, parámetros, etcétera. 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.

Cada sistema SIEM tiene un conjunto de analizadores de mensajes estándar. Kaspersky también proporciona analizadores de mensajes para algunos sistemas SIEM, por ejemplo, para QRadar y ArcSight. Puede descargar estos analizadores de mensajes de los sitios web de los sistemas SIEM correspondientes. Al configurar el receptor, puede seleccionar utilizar uno de los analizadores de mensajes estándar o un analizador de mensajes de Kaspersky.

Marcar los eventos que se exportarán a un sistema SIEM en formato Syslog

En esta sección, se brindan instrucciones para seleccionar los eventos que se exportarán en formato Syslog a un sistema SIEM.

Acerca del marcado de 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.

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 **DISPOSITIVOS → DIRECTIVAS Y PERFILES**.
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. Seleccione las casillas adyacentes a 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 **DISPOSITIVOS → 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. Active las casillas de verificación ubicadas junto a los eventos que deban exportarse al 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. Realice una de las siguientes acciones:
   - Haga clic en el ícono de **Configuración** (🔧) junto al nombre del Servidor de administración pertinente.
   - En el menú principal, vaya a **DISPOSITIVOS** → **DIRECTIVAS Y PERFILES** y 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**.

   Como alternativa, para marcar un evento que desee exportar al sistema SIEM, puede utilizar la sección **Registro de los eventos** que se abre al hacer clic en el vínculo del evento en cuestión.

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 es usado 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.

Para configurar la exportación de eventos a un sistema SIEM en Kaspersky Security Center 14 Web Console:

1. En la lista desplegable **Configuración de la consola**, seleccione **Integración**.

   Se abre la ventana **Configuración de la consola**.

2. Seleccione la pestaña **Integración**.

3. En la pestaña **Integración**, vaya a la sección **SIEM**.

4. Haga clic en el vínculo **Configuración**.

   Se abre la sección **Exportar configuración**.

5. 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/IP, UDP y 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 un archivo con la lista de certificados de una entidad de certificación (también denominada "CA") de confianza y cargar ese archivo a Kaspersky Security Center Linux. Kaspersky Security Center Linux verificará si el certificado del servidor SIEM también ha sido firmado por una autoridad de certificación de confianza.

    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 agregar las huellas digitales SHA-1 de los certificados del sistema SIEM en Kaspersky Security Center. Para agregar una huella digital SHA-1, 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. Si utiliza esta opción, utilizará un certificado autofirmado emitido por Kaspersky Security Center. 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 generar uno en Kaspersky Security Center.

  - **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 archivos no dependen el uno del otro y no importa el orden en que se los carga. 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. 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.

6. Si lo desea, puede exportar eventos archivados desde la base de datos del Servidor de administración y establecer la fecha de inicio a partir de la cual desea iniciar la exportación de eventos archivados:
   a. Haga clic en el vínculo **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 el botón **Aceptar**.
7. Coloque el interruptor en la posición **Exportación automática de eventos a la base de datos del sistema SIEM HABILITADA**.
8. Haga clic en el botón **Guardar**.

La exportación de eventos al sistema SIEM queda configurada. En lo sucesivo, si la recepción de eventos está configurada en el sistema SIEM, el Servidor de administración exportará los eventos marcados al 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.

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 enviar la solicitud directamente a las vistas públicas y recuperar los datos del evento o crear su propia vista sobre la base 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 crear 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.

Creación de una consulta de SQL usando la utilidad klsql2

Esta sección describe cómo descargar y usar la utilidad klsql2, y cómo crear una consulta de SQL usando esta utilidad. Cuando crea una consulta de SQL por medio de la utilidad klsql2, no tiene que proporcionar el nombre de la base de datos ni los parámetros de acceso, porque la consulta se dirige a las vistas públicas de Kaspersky Security Center Linux directamente.

Para descargar y usar la utilidad klsql2:

1. Descargar la utilidad klsql2 desde sitio web de Kaspersky.
2. Copie y extraiga el archivo klsql2.zip descargado a cualquier carpeta en el dispositivo con el Servidor de administración de Kaspersky Security Center Linux instalado.

   El paquete klsql2.zip incluye los archivos siguientes:

   - klsql2.exe
   - src.sql
   - start.cmd
3. Abra el archivo src.sql en cualquier editor de texto.
4. En el archivo src.sql, escriba la consulta SQL que desea, y luego guarde el archivo.
5. En el dispositivo con el Servidor de administración de Kaspersky Security Center Linux instalado, en la línea de comandos, escriba el comando siguiente para ejecutar la consulta de SQL desde el archivo src.sql y guardar los resultados en el archivo result.xml:
   ```
   klsql2 -i src.sql -o result.xml
   ```
6. Abra el archivo result.xml creado recientemente para ver los resultados de la consulta.

Puede modificar el archivo src.sql y crear cualquier consulta 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, creada por medio de la utilidad klsql2.

El ejemplo siguiente ilustra la recuperación de eventos que ocurrieron en dispositivos durante los siete días anteriores, y muestra los eventos según la hora en la que se producen; los eventos más recientes se muestran primero.

Ejemplo:

```
SELECT
e.nId, /* identificador del evento */
e.tmRiseTime, /* hora en la que ocurrió el evento */
e.strEventType, /* nombre interno del tipo de evento */
e.wstrEventTypeDisplayName, /* nombre mostrado del evento */
e.wstrDescription, /* descripción mostrada del evento */
e.wstrGroupName, /* nombre del grupo, donde se encuentra el dispositivo */
```

```
h.wstrDisplayName, /* nombre que se muestra del dispositivo en el que se produjo el
evento */
CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp) & 255) AS varchar(4)) as strIp /* dirección IP del dispositivo en el
que se produjo el evento */
FROM v_akpub_ev_event e
INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

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 de SQL Server, MySQL o MariaDB, debe conocer el nombre de la base de datos a fin de conectarse desde su editor de scripts SQL.

Para ver el nombre de la base de datos de Kaspersky Security Center Linux:

1. Haga clic en el ícono de **Configuración** () junto al nombre del Servidor de administración requerido.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, elija 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.

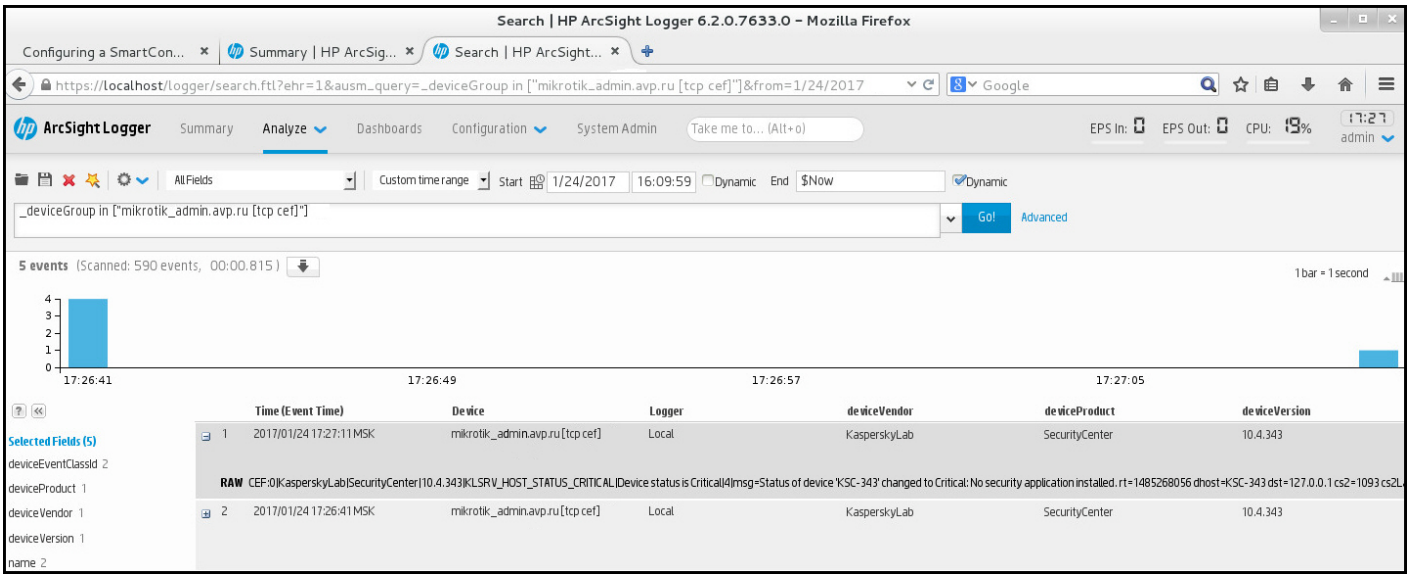
Ver los resultados de la exportación

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

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 proporciona una amplia gama de *selecciones predefinidas* (por ejemplo, **Dispositivos con estado Crítico**, **Protección deshabilitada**, **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.

Para ver una selección de dispositivos:

1. En el menú principal, vaya a **DISPOSITIVOS → 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 su interés.

Se mostrará el resultado de la selección de dispositivos.

Crear una selección de dispositivos

Para crear una selección de dispositivos:

1. En el menú principal, vaya a **DISPOSITIVOS → SELECCIONES DE DISPOSITIVOS**.

   Se muestra una página con una lista de selecciones de dispositivos.

2. Haga clic en el botón **Agregar**.

   Se abre la ventana **Configuración de la selección de dispositivos**.

3. Escriba el nombre de la nueva selección.

4. Especifique el tipo de dispositivos que desea incluir en la selección de dispositivos.

5. Haga clic en el botón **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 **Aceptar**.

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. Vaya a **DISPOSITIVOS → SELECCIONES DE DISPOSITIVOS**.

   Se muestra una página con una lista de selecciones de dispositivos.

2. Haga clic en la selección de dispositivos relevante definida por el usuario.

   Se abre la ventana **Configuración de la selección de dispositivos**.

3. En la pestaña **General**, especifique las condiciones que se deben cumplir para incluir los dispositivos en esta selección.

4. Haga clic en el botón **Guardar**.

El cambio se aplica y se guarda.

A continuación, encontrará una descripción de las condiciones que se utilizan para incluir dispositivos en una selección. Las condiciones se combinan usando el operador lógico "OR", con lo cual la selección incluirá aquellos dispositivos que cumplan con al menos una de las condiciones definidas.

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

Si habilita esta opción, la condición elegida se aplicará a la inversa. La selección incluirá aquellos dispositivos que no cumplan con la condición.

Esta opción está deshabilitada de manera predeterminada.

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 o dirección IP del dispositivo**
- Dominio de Windows

  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, una cadena 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>"**. La cadena entrecomillada 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 manera predeterminada.

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 manera predeterminada.

- La etiqueta debe incluirse

  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.

- La etiqueta debe excluirse

  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).

Actividad de red

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:

- El dispositivo es un 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 caigan dentro de los límites del intervalo especificado.

Si no activa esta casilla, no se aplicará este criterio.

Esta casilla no está marcada de manera predeterminada.

- 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 manera 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.

Aplicación

En la sección **Aplicación**, 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.

- 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 no está marcada de manera predeterminada.

- El dispositivo se administra a través de Kaspersky Security Center 14

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 aplicación incluirá aquellos dispositivos que no se administran mediante Kaspersky Security Center Linux.
- **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.

Sistema operativo

En la sección **Sistema operativo**, puede especificar los criterios que serán usados para incluir dispositivos en la selección según el tipo de sistema operativo.

- Versión del sistema operativo

  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.

- Arquitectura del sistema operativo

  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).

- Versión de Service Pack del sistema operativo

  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.

- Compilación del sistema operativo

Este parámetro solo es válido para sistemas operativos Windows.

Número de compilación del sistema operativo. Puede indicar si el número de compilación del sistema operativo seleccionado deberá ser igual, anterior o posterior al valor introducido. También puede hacer que la búsqueda incluya todos los números de compilación, excepto el especificado.

- Id. de versión del sistema operativo

  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.

Estado del dispositivo

En la sección **Estado del dispositivo**, puede configurar criterios para incluir dispositivos en una selección según la descripción del estado de dispositivos de una aplicación administrada:

- Estado del dispositivo

  Lista desplegable en la que puede seleccionar un estado de dispositivo: *Sin inconvenientes*, *Crítico* o *Advertencia*.

- 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: *Sin inconvenientes, Crítico* o *Advertencia*.

- Estado del dispositivo definido por la aplicación

  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.

Componentes de protección

En la sección **Componentes de protección**, 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 manera predeterminada.

- Último análisis

  Habilite esta opción para buscar dispositivos cliente basándose en la hora del último análisis antivirus. Utilice los campos de entrada para definir el período en el cual deberá haber ocurrido el último análisis antivirus.

  Esta opción está deshabilitada de manera predeterminada.

- Número total de 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 manera predeterminada.

Registro de aplicaciones

En la sección **Registro de aplicaciones**, puede configurar los criterios para buscar dispositivos según las aplicaciones que tienen instaladas:

- 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 manera predeterminada.

- Nombre de la aplicación de seguridad incompatible

  Lista desplegable en la que puede seleccionar aplicaciones de seguridad desarrolladas por 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 manera predeterminada.

Registro de hardware

En la sección **Registro de hardware**, puede configurar criterios para incluir dispositivos en la selección basándose en el hardware que tengan instalado:

- 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 incluirán en la selección.

  Puede ingresar el nombre del fabricante en la ventana de propiedades de sus dispositivos.

- **Número de serie**

  Las unidades de hardware que tengan el número de serie indicado 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**

  Las unidades de hardware pertenecientes al usuario especificado en este campo se incluirán en la selección.

- **Ubicación**

  Ubicación del dispositivo o de la unidad de hardware (por ejemplo, la sede central de la empresa o una sucursal). Las computadoras o los 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.

- **Frecuencia de la CPU, en MHz**

  Intervalo de frecuencias de un procesador. La selección incluirá aquellos dispositivos que tengan un procesador con un intervalo de frecuencias comprendido en los límites dispuestos en los campos (inclusive).

- **Núcleos de CPU virtuales**

  Intervalo del número de núcleos virtuales de un procesador. La selección incluirá aquellos dispositivos que tengan un procesador comprendido en los límites dispuestos en los campos (inclusive).

- **Volumen de disco duro, en GB**

Intervalo de valores referentes al tamaño del disco duro instalado en el dispositivo. La selección incluirá aquellos dispositivos que tengan un disco duro cuyo tamaño esté comprendido en los límites dispuestos en los campos (inclusive).

- Tamaño de RAM, en MB

  Intervalo de valores referentes a la cantidad de RAM instalada en el dispositivo. La selección incluirá aquellos dispositivos que tengan una cantidad de RAM comprendida en los límites dispuestos en los campos (inclusive).

Máquinas virtuales

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):

- Es una máquina virtual

  En la lista desplegable puede seleccionar las siguientes opciones:
  - **No es importante**.
  - **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:
  - **No es importante**.
  - **No**. Buscar dispositivos que no sean parte de una VDI.
  - **Sí**. Buscar dispositivos que sean parte de una VDI.

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 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 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.

Problemas que afectan al estado en las aplicaciones administradas

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. Si elige un problema incluido en las listas de varias aplicaciones, tendrá la opción de seleccionar el problema en todas las listas automáticamente.

Descripción del estado del dispositivo

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.

Estados de componentes en aplicaciones administradas

En la sección **Estados de componentes en aplicaciones administradas**, puede configurar los criterios que se usarán para incluir dispositivos en la selección basándose en 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 (*No hay datos del dispositivo, 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 (*No hay datos del dispositivo*, *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 (*No hay datos del dispositivo, Detenida, Iniciándose, En pausa, En ejecución, Error).*

- Estado de Sensor de Endpoint

Buscar dispositivos basándose en el estado del componente Sensor de Endpoint (*No hay datos del dispositivo, Detenida, Iniciándose, En pausa, En ejecución, Error*).

Componentes de las aplicaciones

En esta sección, se enumeran los componentes de aquellas aplicaciones que tienen instalado un complemento de administración en la Consola de administración.

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 una 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: *No hay datos del dispositivo*, *Detenido*, *Iniciándose*, *En pausa*, *En ejecución*, *Error de funcionamiento* y *Sin instalar*. 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:

  - *Iniciándose*: el componente está en proceso de iniciarse.
  - *En ejecución*: el componente está habilitado y funciona correctamente.
  - *En pausa*: el componente se encuentra suspendido (por ejemplo, porque el usuario pausó la protección en la aplicación administrada).
  - *Error de funcionamiento*: ocurrió un error durante el funcionamiento del componente.
  - *Detenido*: el componente está deshabilitado y no se encuentra en funcionamiento.
  - *Sin instalar*: el usuario no optó por instalar el componente al realizar una instalación personalizada de la aplicación.

  A diferencia de los demás estados, *No hay datos del dispositivo* 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. Tal situación puede presentarse, por ejemplo, si el componente seleccionado no pertenece a ninguna de las aplicaciones instaladas en el dispositivo o si 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 la versión del componente seleccionado deberá ser igual, anterior o posterior a ese valor. También puede configurar la búsqueda de todas las versiones excepto la especificada.

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.

Para encontrar la información que necesita en la guía de referencia de OpenAPI, puede utilizar el campo de búsqueda ubicado en la parte derecha de la pantalla.

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 puede llamar a métodos OpenAPI y realizar automáticamente varias tareas para proteger su red, por ejemplo, crear una jerarquía "primario/secundario", ejecutar tareas en Kaspersky Security Center, 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:

1. Descargue el archivo KlAkOAPI.tar.gz. Este archivo incluye el paquete KlAkOAPI y las muestras (puede copiarlas del archivo o de la guía de referencia de OpenAPI).

2. Instale el paquete KlAkOAPI del archivo KlAkOAPI.tar.gz en un dispositivo donde esté instalado el Servidor de administración.

   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.

Coincidencia entre escenarios de usuario y ejemplos de métodos OpenAPI de Kaspersky Security Center

Ejemplo	Propuesta del ejemplo	Escenario
Registro KlAkParams	Puede extraer y procesar datos utilizando 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
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.	Supervisar la ejecución de tareas
Crear y ejecutar una tarea	Puede crear una tarea. Especifique los siguientes parámetros de la tarea en la muestra: • Tipo	Crear una tarea

	• Método de ejecución • Nombre • 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.	
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.	Seleccionar la cuenta para iniciar el Servidor de administración
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.	Administrar cuentas de usuario

Aplicaciones que interactúan con Kaspersky Security Center a través de OpenAPI

Algunas aplicaciones interactúan con Kaspersky Security Center a través de OpenAPI. Ejemplo de ellas son Kaspersky Anti Targeted Attack Platform y Kaspersky Security for Virtualization. También pueden ser aplicaciones cliente personalizadas, desarrolladas por usted para utilizar OpenAPI.

Las aplicaciones que interactúan con Kaspersky Security Center a través de OpenAPI se conectan al Servidor de administración. Si configuró 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. Para saber si una aplicación utiliza OpenAPI, consulte la ayuda de esa aplicación.

Integración entre Kaspersky Security Center 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 Endpoint Detection and Response y Kaspersky Managed Detection and Response.

Configurando el acceso a KATA/KEDR Web Console

Kaspersky Anti Targeted Attack (KATA) y Kaspersky Endpoint Detection and Response (KEDR) son dos bloques funcionales de Kaspersky Anti Targeted Attack Platform. Puede administrar estos bloques funcionales a través de Web Console for Kaspersky Anti Targeted Attack Platform (KATA/KEDR Web Console). Si usa tanto Kaspersky Security Center 14 Web Console como KATA/KEDR Web Console, puede configurar el acceso a KATA/KEDR Web Console de KEDR directamente desde la interfaz de Kaspersky Security Center 14 Web Console.

Para configurar el acceso a KATA/KEDR Web Console:

1. En la ventana principal de la aplicación, haga clic en **Configuración de la consola** en la parte superior de la pantalla.
2. En el menú desplegable, seleccione **Integración**.

   Se abre la ventana Configuración de la consola.
3. En la pestaña **Integración**, escriba la URL de KATA/KEDR Web Console en el campo **URL a KATA / KEDR Web Console**.
4. Haga clic en el botón **Guardar**.

La lista desplegable **Administración avanzada** se agrega a la ventana principal de la aplicación. Puede usar este menú para abrir KATA/KEDR Web Console. Después de que haga clic en **Seguridad cibernética avanzada**, se abre una nueva pestaña en su navegador con la URL que especificó.

Establecer una conexión en segundo plano

Para configurar la interacción entre Kaspersky Security Center y otra aplicación o solución de Kaspersky, por ejemplo, Kaspersky Managed Detection and Response (también conocido como MDR), debe establecer una conexión en segundo plano entre Kaspersky Security Center Web Console y Administration Server. 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 basada en Windows de Kaspersky Security Center.

Para establecer una conexión en segundo plano:

1. En la lista desplegable **Configuración de la consola**, seleccione **Integración**.

   Se abre la ventana **Configuración de la consola**.
2. Seleccione la pestaña **Integración**.

3. En la pestaña **Integración**, seleccione la sección **Integración**.

4. Cambie el botón de activación para establecer una conexión en segundo plano a la posición: **Establecer una conexión en segundo plano para la integración HABILITADO**.

5. En la sección **El servicio que establece una conexión en segundo plano se iniciará en el servidor de Kaspersky Security Center Web Console** 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 y esta cuenta se utiliza como cuenta de servicio para mantener la interacción entre Kaspersky Security Center y otra aplicación o solución de Kaspersky. El nombre de esta cuenta de servicio contiene el prefijo NWCSvcUser. Por motivos de seguridad, el Servidor de administración cambia automáticamente cada 30 días la contraseña de la cuenta del servicio. No puede eliminar la cuenta del servicio manualmente. El Servidor de administración elimina esta cuenta automáticamente cuando se deshabilita una conexión de servicios cruzados. El Servidor de administración crea una única cuenta de servicio para cada Kaspersky Security Center 14 Web Console y cada Consola de administración y asigna todas las cuentas de servicio al grupo de seguridad con el nombre ServiceNwcGroup. El Servidor de administración crea automáticamente este grupo de seguridad durante el proceso de instalación de Kaspersky Security Center. No puede eliminar este grupo de seguridad manualmente.

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 encuentra una solución a su problema en la documentación de Kaspersky Security Center Linux o en ninguna de las fuentes de información sobre Kaspersky Security Center Linux, comuníquese con el Servicio de 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 Linux.

Kaspersky brinda soporte para Kaspersky Security Center Linux durante su ciclo de vida (consulte la página del ciclo de vida de soporte del producto). 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
- Puede enviar una solicitud al servicio de soporte técnico a través del portal Kaspersky CompanyAccount

Obtenga soporte técnico por teléfono

Puede llamar a los especialistas de soporte técnico desde gran parte del mundo. Puede encontrar información sobre cómo obtener soporte técnico en su región e información de contacto para soporte técnico en el Sitio web de atención al cliente de Kaspersky.

Antes de comunicarse con el servicio de soporte técnico, lea las reglas de soporte técnico.

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 seguir el estado de sus solicitudes en línea y también para almacenar un historial de 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.

Fuentes de información acerca de la aplicación

Página de Kaspersky Security Center en el sitio web de Kaspersky

En la página de Kaspersky Security Center en el sitio web de Kaspersky, puede ver información general sobre la aplicación, sus funciones y características.

Página de Kaspersky Security Center 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 en la Base de conocimiento pueden proporcionar respuestas a preguntas relacionadas tanto con Kaspersky Security Center como con otras aplicaciones de Kaspersky. Estos artículos también pueden contener noticias vinculadas al 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.

Dentro del foro, puede ver temas de discusión existentes, publicar comentarios y crear nuevos temas de discusión.

> 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.

Problemas conocidos

Kaspersky Security Center Linux tiene una serie de limitaciones que no son críticas para el funcionamiento de la aplicación:

- 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 no requerirá que ingrese las credenciales.

- La tarea *Cambiar servidor de administración* no se inicia automáticamente después de establecer la opción **Inmediatamente** en la programación de tareas y guardar los cambios.

- Si define los ajustes de un servidor proxy dentro de las propiedades del Servidor de administración y luego habilita la opción **No usar servidor proxy** en la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*, la opción no se tendrá en cuenta y la conexión se establecerá a través del servidor proxy de todos modos.

- Si abre Kaspersky Security Center 14 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.

- Cuando se intenta restaurar un objeto desde el repositorio **COPIA DE SEGURIDAD** (**OPERACIONES → REPOSITORIOS → COPIA DE SEGURIDAD**), ocurre un error. Lo mismo sucede si se intenta enviar ese objeto a Kaspersky.

- Los ajustes de configuración bloqueados en una directiva principal de Kaspersky Endpoint Security for Linux son heredados por las directivas secundarias, pero no quedan bloqueados en esas directivas.

- Es posible que la información de hardware enviada desde un dispositivo administrado al Servidor de administración no esté completa; es posible que no se especifiquen algunos elementos de hardware.

- Es posible eliminar categorías de aplicaciones agregadas en la función Control de aplicaciones de una directiva de Kaspersky Endpoint Security for Linux.

- 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 ha utilizado para conectarse al Servidor de administración.

- Si especifica cuentas de usuario personalizadas en los parámetros webConsoleAccount y managementServiceAccount en un archivo de respuesta para la instalación de Kaspersky Security Center 14 Web Console y estas cuentas pertenecen a diferentes grupos de seguridad, Kaspersky Security Center 14 Web Console no funciona después de la instalación.

- En la edición Astra Linux de 64 bits, el paquete klnagent-astra no se puede actualizar con el paquete klnagent64_14: se eliminará el paquete antiguo klnagent64-astra y el nuevo paquete klnagent64 se instalará en lugar de actualizarlo, por lo que se añadirá un nuevo ícono para el dispositivo con el paquete klnagent64_14. Puede eliminar el icono anterior de este dispositivo.

Glosario

Actualización

Procedimiento de sustitución o adición de nuevos archivos (bases de datos o módulos de software) descargados de los servidores de actualizaciones 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

La persona que administra el funcionamiento de las aplicaciones a través del sistema de administración remota y centralizada Kaspersky Security Center.

Administrador del cliente

Miembro del personal de una organización cliente que es responsable de supervisar el estado de la protección 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 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 que permite la interacción entre el Servidor de administración y las aplicaciones de Kaspersky instaladas en un nodo de red específico (estación de trabajo o servidor). Este componente es el mismo para todas las aplicaciones para Microsoft® Windows® de la empresa. Existen versiones independientes del Agente de red para las aplicaciones de Kaspersky desarrolladas para macOS y sistemas operativos de tipo Unix.

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.

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.

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 que utiliza el Servidor de administración para los siguientes fines:

- Autenticación del Servidor de administración al conectarse a Kaspersky Security Center Web Console 14

- Interacción segura entre el Servidor de administración y los Agentes de red en los dispositivos administrados
- Autenticación de los Servidores de administración al conectar un Servidor de administración principal a un Servidor de administración secundario

El certificado se crea automáticamente cuando se instala el Servidor de administración y queda almacenado en el Servidor de administración.

Clave activa

Una clave que está siendo utilizada por la aplicación.

Clave de suscripción adicional

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 que tiene instalado el Agente de red y que tiene aplicaciones de Kaspersky administradas en ejecución.

Configuración de la tarea

Ajustes de una aplicación que son específicos para cada tipo de tarea.

Configuración de programa

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).

Consola de administración

Un componente de Kaspersky Security Center basado en Windows (también llamado Consola de administración basada en MMC). La Consola de administración proporciona una interfaz de usuario a los servicios de administración del Servidor de administración y del Agente de red. La Consola de administración es un análogo de Kaspersky Security Center Web Console 14.

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 datos 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 múltiples directivas para las aplicaciones instaladas en los equipos de cada grupo de administración, solamente puede haber una directiva aplicada a cada aplicación dentro de cada grupo de administración.

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

Un dispositivo desde el que se abre Kaspersky Security Center Web Console 14. La Consola de administración es un componente que brinda una interfaz para administrar Kaspersky Security Center.

La estación de trabajo del administrador se utiliza para configurar y administrar el lado del servidor de Kaspersky Security Center. El administrador utiliza esta estación de trabajo para crear y gestionar un sistema de protección antivirus centralizado para una LAN corporativa basado en las aplicaciones de Kaspersky.

Estado de protección

Estado de protección registrado en un momento dado. Refleja el nivel de seguridad del equipo.

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. Para determinar el estado de protección de la red, se consideran factores como las aplicaciones de seguridad instaladas, el uso de claves de licencia y el número y tipo de amenazas detectadas.

Gravedad de un evento

Propiedad de un evento registrado durante la ejecución de una aplicación de Kaspersky. Los niveles de gravedad posibles son los siguientes:

- 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 aplicaciones con licencia

Grupo de aplicaciones que el administrador crea sobre la base de distintos criterios (p. ej., por proveedor). El sistema mantiene estadísticas sobre la instalación de las aplicaciones de estos grupos en los dispositivos clientes.

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.

Instalación local

Método para instalar una aplicación de seguridad en un dispositivo conectado a una red corporativa. El método supone iniciar la instalación manualmente utilizando, o bien el paquete de distribución de la aplicación de seguridad, o bien un paquete de instalación publicado que se haya descargado en el dispositivo de antemano.

Instalación manual

Instalación de una aplicación de seguridad en un dispositivo de la red corporativa utilizando 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 Private Security Network (KSN Privada)

Kaspersky Private Security Network es una solución que permite acceder a las bases de datos de reputación de Kaspersky Security Network y a otros datos estadísticos desde un dispositivo sin que se envíen datos a Kaspersky Security Network desde ese dispositivo. Kaspersky Private Security Network está 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.

Kaspersky Security Center System Health Validator (SHV)

Componente de Kaspersky Security Center diseñado para verificar la operatividad del sistema operativo cuando Kaspersky Security Center y Microsoft NAP funcionan simultáneamente.

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

Periodo de tiempo durante el cual se tiene acceso a las funciones de la aplicación y a otros 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.

Protección antivirus para redes

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 de una red aumenta cuando se utilizan aplicaciones y servicios de seguridad, y cuando existe y se hace cumplir una política corporativa que regula la seguridad de los datos.

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.

Punto de distribución

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. En versiones anteriores de la aplicación, los puntos de distribución se denominaban "agentes de actualización".

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 datos 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 equipos 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

Servidor de administración

Componente de Kaspersky Security Center que almacena centralmente información sobre las aplicaciones de Kaspersky instaladas en la red corporativa. También puede utilizarse para administrar esas aplicaciones.

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 diseñado para administrar el sistema de protección de la 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 web de Kaspersky Security Center

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, 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.

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 equipo 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

Uno de los componentes de Kaspersky Security Center. 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. Kaspersky Security Center otorga los permisos de usuarios reales a los usuarios internos de la aplicación.

Las cuentas de los usuarios internos se crean y utilizan solo para trabajar dentro de Kaspersky Security Center. No se transfiere ningún dato sobre estos usuarios internos al sistema operativo. Kaspersky Security Center se encarga de autenticar a los usuarios internos.

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 el código de terceros se encuentra en el archivo legal_notices.txt, en la carpeta 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, Shockwave y PostScript son marcas registradas o marcas comerciales de Adobe en los Estados Unidos y/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 en los Estados Unidos y/o en otros países.

Apache y el logotipo de la pluma de Apache son marcas registradas de The Apache Software Foundation.

AirPlay, AirDrop, AirPrint, App Store, Apple, 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., registradas en los EE. UU. y en otros países y regiones.

La palabra, la marca y los logotipos de Bluetooth son propiedad de Bluetooth SIG, Inc.

Ubuntu es una marca comercial registrada de Canonical Ltd.

Cisco, Cisco Systems y iOS son marcas comerciales registradas o marcas comerciales de Cisco Systems, Inc. y/o sus de empresas vinculadas en los Estados Unidos y en algunos otros países.

Citrix y XenServer son marcas comerciales de Citrix Systems, Inc. y/o de una o más de sus filiales y pueden estar registradas en la Oficina de Marcas y Patentes de los Estados Unidos y en 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.

Dropbox es una marca registrada de Dropbox, Inc.

Firebird es una marca registrada de Firebird Foundation.

Foxit es una marca registrada de Foxit Corporation.

FreeBSD es una marca registrada de The FreeBSD Foundation.

Android, Chrome, Chromium, Dalvik, Firebase, Google, Google Chrome, Google Earth, Google Play, Google Maps, Hangouts y YouTube son marcas comerciales de Google LLC.

FusionCompute y FusionSphere son marcas comerciales de Huawei Technologies Co., Ltd registradas en China y otros países.

Intel, Core y Xeon son marcas comerciales de Intel Corporation en los Estados Unidos y/o en otros países.

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.

Micro Focus es una marca comercial o una marca comercial registrada de Micro Focus (IP) Limited o sus filiales en el Reino Unido, los Estados Unidos y otros países.

Active Directory, ActiveSync, BitLocker, Excel, Forefront, Internet Explorer, InfoPath, Hyper-V, Microsoft, MultiPoint, MS-DOS, PowerShell, PowerPoint, SharePoint, SQL Server, 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, Thunderbird, Firefox son marcas registradas de Mozilla Foundation.

Novell es una marca registrada de Novell Enterprises Inc. en los Estados Unidos y en otros países.

Oracle, Java, JavaScript y TouchDown son marcas registradas de Oracle o de sus empresas vinculadas.

Parallels y el logotipo de Parallels son marcas comerciales o marcas comerciales registradas de Parallels International GmbH en Canadá, Estados Unidos y/o en otros lugares.

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, Ansible, CentOS, 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.

BlackBerry es propiedad de Research In Motion Limited y está registrada en los Estados Unidos y puede estar pendiente o registrada 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.

VMware, VMware vSphere y VMware Workstation son marcas comerciales registradas o marcas comerciales de VMware, Inc. en los Estados Unidos y/o en otras jurisdicciones.

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.