Contenido

Ayuda de Kaspersky Security Center 14 Linux

Novedades

Descubra las novedades de esta versión del programa.

Requisitos de hardware y software

Compruebe qué sistemas operativos y versiones de aplicación se admiten.

Instalación

Instale el Servidor de administración y Kaspersky Security Center 14 Web Console

Detección de dispositivos en red

Descubra los dispositivos existentes y nuevos en la red de su organización.

Aplicaciones de Kaspersky. Despliegue centralizado

Aplicaciones de Kaspersky. Licencia y activación

Active aplicaciones de Kaspersky en unos pasos.

Configuración de protección de la red

Administre la seguridad de la organización.

Aplicaciones de Kaspersky. Actualización de bases de datos y módulos de software

Mantener la fiabilidad del sistema de protección.

Supervisión e informes

Vea su infraestructura, estados de protección y las estadísticas.

Ajuste de puntos de distribución y/o puertas de enlace de conexión

 Desplegar aplicaciones de Kaspersky.

 Configurar puntos de distribución.

Novedades

Kaspersky Security Center 14 Linux

Kaspersky Security Center 14 Linux tiene varias mejoras y funciones 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 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 volumen de los datos descargados.
- Ahora puede utilizar la característica diff de archivos 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 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 ha añadido la tarea *Verificación de actualizaciones*. Al utilizar esta tarea, puede verificar automáticamente la operatividad y los errores de las actualizaciones descargadas antes de instalarlas en los dispositivos administrados.

Acerca de 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 conocido como Kaspersky Security Center) está diseñado para implementar y administrar la protección de dispositivos Linux mediante el 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 de una red corporativa, ejecutar tareas de análisis y actualización de forma remota y administrar las políticas de seguridad de las aplicaciones administradas. Como administrador, puede usar un panel detallado que proporciona una instantánea de los estados de los dispositivos corporativos, informes detallados y configuraciones granulares en las políticas de protección.

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

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

Con Kaspersky Security Center puede realizar lo siguiente:

- Crear una jerarquía de Servidores de administración para gestionar la red de la organización, así como las redes de oficinas remotas u organizaciones cliente.

  La *organización cliente* es una organización que tiene asegurada la protección antivirus por un proveedor de servicio.
- Crear una jerarquía de grupos de administración para administrar una selección de dispositivos cliente como un todo.
- Administre un sistema de protección antivirus creado según las aplicaciones Kaspersky.
- Realice la instalación remota de aplicaciones de Kaspersky y otros proveedores de software.
- Lleve 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 aplicaciones y de dispositivos.
- Recibir notificaciones sobre eventos críticos durante la operación de aplicaciones Kaspersky.
- Realizar el inventario del hardware conectado a la red de la organización.
- Administrar de forma centralizada los archivos que las aplicaciones de seguridad han trasladado a Cuarentena o Copia de seguridad, así como administrar archivos cuyo procesamiento por parte de las aplicaciones de seguridad se ha pospuesto.

Kit de distribución

Puede adquirir la aplicación en las tiendas online de Kaspersky (por ejemplo, https://www.kaspersky.es) o a empresas asociadas.

Si compra Kaspersky Security Center Linux en una tienda en línea, tiene que bajar la aplicación del sitio web de esta. La información necesaria para la activación de la aplicación se le envía por correo electrónico tras la realización del pago.

Requisitos de hardware y software

Servidor de administración

Requisitos mínimos de hardware:

- CPU con frecuencia de operación de 1 GHz o superior. Para un sistema operativo de 64 bits, la frecuencia de CPU mínima 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 / 64 bits.
- Debian GNU/Linux 10.x (Buster) de 32 bits / 64 bits.
- Debian GNU/Linux 9.x (Stretch) de 32 bits / 64 bits.
- Ubuntu Server 20.04 LTS (Focal Fossa) 64 bits.
- Ubuntu Server 18.04 LTS (Bionic Beaver) de 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 Packs) 64 bits.
- SUSE Linux Enterprise Server 15 (todos los Service Packs) 64 bits.
- Astra Linux Special Edition 1.7 (incluido el modo de entorno de software cerrado y el modo obligatorio) de 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 plataformas de virtualización siguientes:

- 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.
- Máquina virtual basada en kernel. Compatible con 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) de 64 bits.
  - Debian GNU/Linux 11.x (Bullseye) 32 bits / 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 (se pueden instalar en un dispositivo diferente):

- MySQL 5.7 Community de 32 bits / 64 bits.
- MySQL 8.0 Community de 32 / 64 bits.
- MariaDB 10.5.x de 32 bits / 64 bits.
- MariaDB 10.4.x de 32 bits / 64 bits.
- MariaDB 10.3.22 y superior de 32 bits / 64 bits.
- El servidor MariaDB 10.3 de 32 bits o 64 bits con motor de almacenamiento InnoDB.
- MariaDB 10.1.30 y superior de 32 bits / 64 bits.

Kaspersky Security Center 14 Web Console

Servidor de Kaspersky Security Center 14 Web Console

Requisitos mínimos de hardware:

- CPU: 4 núcleos, frecuencia de operación 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 Packs).
- SUSE Linux Enterprise Server 15 (todos los Service Packs).
- SUSE Linux Enterprise Desktop 15 (Service Pack 3) ARM 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.

Entre las plataformas de virtualización, la máquina virtual basada en kernel es compatible con 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) de 64 bits.
- Debian GNU/Linux 11.x (Bullseye) 32 bits / 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 un dispositivo cliente, el uso de Kaspersky Security Center 14 Web Console solo requiere un navegador.

Los requisitos de hardware y software del dispositivo son idénticos a los del navegador utilizado para Kaspersky Security Center 14 Web Console.

Navegadores:

- Mozilla Firefox Extended Support Release 91.8.0 o superior (la versión 91.8.0 se lanzó el 5 de abril de 2022).
- Mozilla Firefox Release 99.0 o superior (la versión 99.0 se lanzó el 5 de abril de 2022).
- Google Chrome 100.0.4896.88 o superior (compilación oficial).
- Microsoft Edge 100 o superior.
- Safari 15 en macOS.

Agente de red

Requisitos mínimos de hardware:

- CPU con frecuencia de operación de 1 GHz o superior. Para un sistema operativo de 64 bits, la frecuencia de CPU mínima 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 / 64 bits.
- Debian GNU/Linux 10.x (Buster) de 32 bits / 64 bits.
- Debian GNU/Linux 9.x (Stretch) de 32 bits / 64 bits.
- Ubuntu Server 20.04 LTS (Focal Fossa) de 32 bits / 64 bits.
- Ubuntu Server 20.04.04 LTS (Focal Fossa) ARM 64 bits.
- Ubuntu Server 18.04 LTS (Bionic Beaver) de 32 bits / 64 bits.
- Ubuntu Desktop 20.04 LTS (Focal Fossa) de 32 bits / 64 bits.
- Ubuntu Desktop 18.04 LTS (Bionic Beaver) de 32 bits / 64 bits.
- CentOS 8.x 64 bits.
- CentOS 7.x 64 bits.
- CentOS 7.x ARM 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 de 32 bits / 64 bits.
- SUSE Linux Enterprise Server 12 (todos los Service Packs) 64 bits.
- SUSE Linux Enterprise Server 15 (todos los Service Packs) 64 bits.
- SUSE Linux Enterprise Desktop 15 (todos los Service Packs) 64 bits.
- SUSE Linux Enterprise Desktop 15 (Service Pack 3) ARM 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) de 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 de 32 bits / 64 bits.
- Alt Workstation 9.2 de 32 bits / 64 bits.
- Alt 8 SP Server (LKNV.11100-01) 64 bits.
- Alt 8 SP Server (LKNV.11100-02) 64 bits.
- Alt 8 SP Server (LKNV.11100-03) 64 bits.
- Alt 8 SP Workstation (LKNV.11100-01) de 32 bits / 64 bits.

- Alt 8 SP Workstation (LKNV.11100-02) de 32 bits / 64 bits.
- Alt 8 SP Workstation (LKNV.11100-03) de 32 bits / 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 superior 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 de 64 bits.
- ROSA Enterprise Linux Desktop 7.3 de 64 bits.
- ROSA COBALT Workstation 7.3 de 64 bits.
- ROSA COBALT Server 7.3 de 64 bits.
- Lotos (Linux core versión 4.19.50, DE: MATE) de 64 bits.

Se admiten las plataformas de virtualización siguientes:

- 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.
- Máquina virtual basada en kernel. Compatible con 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) de 64 bits.
  - Debian GNU/Linux 11.x (Bullseye) 32 bits / 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 una red protegida por aplicaciones de Kaspersky.

Al usar la aplicación, puede realizar lo siguiente:

- Administrar el estado del sistema de seguridad de la organización.
- Instalar aplicaciones de Kaspersky en dispositivos de su red y administrar aplicaciones instaladas.
- Administrar directivas creadas para dispositivos de su red.
- Administrar cuentas de usuario.
- Administrar tareas de aplicaciones instaladas en sus dispositivos de red.
- Ver informes del estado de seguridad del sistema.
- Administrar el envío de informes a administradores de sistemas y a otros especialistas de TI.

Kaspersky Security Center 14 Web Console proporciona una interfaz web que garantiza la comunicación 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 con los dispositivos de su red a través de canales protegidos con Secure Socket Layer (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.

Esto es lo que debe hacer para usar Kaspersky Security Center 14 Web Console:

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

Kaspersky Security Center 14 Web Console es una aplicación multilingüe. Puede cambiar el idioma de la interfaz en cualquier momento, sin volver a abrir la aplicación. Cuando instala Kaspersky Security Center 14 Web Console junto con Kaspersky Security Center, Kaspersky Security Center 14 Web Console tiene el mismo idioma de la 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 es compatible con el idioma del archivo de instalación o del sistema operativo, se establece el idioma inglés de forma predeterminada.

Lista de aplicaciones de Kaspersky compatibles

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, usted instala el Servidor de administración en un dispositivo Windows y la solución basada en Linux tiene una 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 al funcionar 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 donde se instala el Servidor de administración	Windows	Linux
Tipo de consola de administración	En las instalaciones y basado en la web	Basado en la web
Sistema operativo para donde se instala la consola de administración basada en la web	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	10 0000	20 000
Protección de dispositivos administrados: Windows, macOS y Linux	✓	— (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	✓	✓
Administración 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 políticas 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 hacen posible administrar en remoto las aplicaciones Kaspersky instaladas en los dispositivos cliente.

Los dispositivos que tengan instalado el componente Servidor de administración se denominarán *Servidores de administración* (también *Servidores*). Los Servidores de administración se deben proteger, 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 parámetros:

- Con el nombre "Servidor de administración de Kaspersky Security Center".
- Configurar para que se inicie automáticamente cuando se inicie el sistema operativo.
- Con la cuenta **LocalSystem** o la cuenta de usuario seleccionada durante la instalación del Servidor de administración.

El Servidor de administración realiza las siguientes funciones:

- Almacena la estructura de los grupos de administración.
- Almacenamiento de la información acerca de la configuración de los dispositivos cliente.
- Organización de repositorios para los paquetes de distribución de aplicaciones.
- Instalación remota de aplicaciones en dispositivos del cliente y eliminación de aplicaciones.
- Actualiza las bases de datos de la aplicación y los módulos de software de las aplicaciones de Kaspersky.
- Administración de directivas y tareas en los dispositivos cliente.
- Almacenamiento de la información acerca de los eventos que se han producido en los dispositivos cliente.
- Generación de informes sobre el funcionamiento de las aplicaciones Kaspersky.
- Despliega las claves de licencia en dispositivos cliente y almacena la información sobre claves de licencia.
- Reenvía notificaciones sobre el progreso de tareas (por ejemplo, la detección de virus en un dispositivo cliente).

Nombres de administración los Servidores de administración en la interfaz de la aplicación

En la interfaz de Kaspersky Security Center 14 Web Console, los Servidores de administración pueden tener los siguientes nombres:

- Nombre del dispositivo del Servidor de administración, por ejemplo: "*nombre_del_dispositivo*" o "Servidor de administración: *nombre_del_dispositivo*".
- Dirección IP del dispositivo del Servidor de administración, por ejemplo: "*Dirección IP*" o "Servidor de administración: *dirección IP*".
- Los Servidores de administración secundarios y los Servidores de administración virtuales tienen nombres personalizados, que usted especifica cuando conecta un Servidor de administración virtual o secundario al Servidor de administración principal.
- Si usa Kaspersky Security Center 14 Web Console instalado en un dispositivo Linux, la aplicación muestra los nombres de los Servidores de administración que especificó como fiables en el archivo de respuesta.

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

Jerarquía de Servidores de administración

Los Servidores de administración pueden organizarse en una jerarquía. Cada Servidor de administración puede tener varios Servidores de administración secundarios (conocidos como *Servidores secundarios*) en distintos niveles de anidamiento de la jerarquía. El nivel de anidamiento para los Servidores secundarios no está limitado. 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 virtual* son un caso particular de Servidores de administración secundarios.

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

La jerarquía de los Servidores de administración se puede utilizar para hacer lo siguiente:

- Disminuir la carga en el Servidor de administración (comparado con un único Servidor de administración instalado en toda la red).
- Minimizar el tráfico de la Intranet y simplificar el trabajo con las oficinas remotas. No tiene que establecer conexiones entre el Servidor de administración principal y todos los dispositivos de la red, que pueden estar ubicados en diferentes regiones, por ejemplo. Es suficiente instalar un Servidor de administración secundario en cada segmento de red, distribuir los dispositivos entre los grupos de administración de Servidores secundarios y establecer las conexiones entre los Servidores secundarios y el Servidor principal a través de canales de comunicación rápidos.
- Distribuir las responsabilidades entre los administradores de la seguridad antivirus. Todas las posibilidades para la administración centralizada y el control del estado de la seguridad antivirus en las redes corporativas permanecen disponibles.
- Cómo de los proveedores de servicios utilizan Kaspersky Security Center. El proveedor de servicio solo necesita 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 servicio puede añadir Servidores de administración virtuales a la jerarquía de Servidores de administración.

Cada dispositivo incluido en la jerarquía de los grupos de administración se puede conectar a un solo Servidor de administración. Debe supervisar independientemente la conexión de dispositivos a los Servidores de administración. Para hacerlo, puede usar la función de búsqueda de dispositivos según atributos de red en los grupos de administración de diferentes servidores.

Servidor de administración virtual

El Servidor de administración virtual (también denominado *servidor virtual*) es un componente de Kaspersky Security Center Linux diseñado para administrar la protección antivirus de la red de una organización cliente.

El Servidor de administración virtual es un tipo concreto de Servidor de administración secundario y, en comparación con un Servidor de administración físico, tiene las siguientes restricciones:

- El Servidor de administración virtual solo se puede crear en un Servidor de administración principal.
- Durante su funcionamiento, el Servidor de administración Virtual utiliza la base de datos del Servidor de administración principal. Las tareas de copia de seguridad y restauración de datos, así como las tareas de exploración y descarga de actualizaciones, no son compatibles con un Servidor de administración virtual.
- El Servidor virtual no permite la creación de Servidores de administración secundarios (incluidos los Servidores virtuales).

Además, el Servidor de administración virtual tiene las siguientes restricciones:

- En la ventana de propiedades del Servidor de administración virtual el número de secciones es limitado.
- Para llevar a cabo la instalación remota de las aplicaciones de Kaspersky en dispositivos cliente administrados por el Servidor de administración virtual, debe asegurarse que el Agente de red esté instalado en uno de los dispositivos cliente a fin de garantizar la comunicación con el Servidor de administración virtual. La primera vez que se conecta al Servidor de administración virtual, se designa al dispositivo como punto de distribución de manera automática, por lo que funciona como puerta de enlace para la conexión entre el Servidor de administración virtual y los dispositivos cliente.
- Un Servidor virtual solo puede sondear la red a través de puntos de distribución.
- Para reiniciar un Servidor virtual que no funciona correctamente, Kaspersky Security Center Linux reinicia el Servidor de administración principal y todos los Servidores de administración virtuales.

El administrador de un Servidor de administración virtual dispone de todos los privilegios en ese Servidor virtual.

Servidor Web

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

Al crear un paquete de instalación independiente, se publica automáticamente en el Servidor Web. El enlace para descargar el paquete independiente se muestra en la lista de paquetes de instalación independiente creados. Si fuera necesario, puede cancelar la publicación del paquete independiente o publicarlo de nuevo en el Servidor Web.

La carpeta compartida se usa para el almacenamiento de información disponible para todos los usuarios cuyos dispositivos se administran mediante el Servidor de administración. Si un usuario no tiene acceso directo a la carpeta compartida, se le puede proporcionar información de dicha carpeta mediante el Servidor Web.

Para proporcionar a los usuarios información de una carpeta compartida mediante el Servidor Web, el administrador debe crear una subcarpeta denominada "pública" en la carpeta compartida y pegar en ella la información pertinente.

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. Un 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 la subcarpeta o el archivo al que puede acceder el usuario.

El administrador puede enviar el nuevo enlace al usuario de cualquier forma que convenga; por ejemplo, por correo electrónico.

Al hacer clic en el enlace, el usuario puede descargar la información necesaria en un dispositivo local.

Agente de red

La interacción entre el Servidor de administración y los dispositivos se realiza mediante el componente *Agente de red* de Kaspersky Security Center. El Agente de red se debe instalar en todos los dispositivos en los que Kaspersky Security Center se utilice para administrar las aplicaciones de Kaspersky.

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

- Con el nombre "Agente de red de Kaspersky Security Center 14 Linux".
- Configurar para que se inicie automáticamente cuando se inicie el sistema operativo.
- Usando la cuenta LocalSystem.

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

- Paquete de instalación en el almacenamiento del Servidor de administración (debe tener el Servidor de administración instalado).
- Paquete de instalación ubicado en los servidores web de Kaspersky.

No tiene que instalar el Agente de red en el dispositivo donde instale el Servidor de administración, ya que la versión del servidor 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 sincroniza el dispositivo administrado con el Servidor de administración. Recomendamos que establezca el intervalo de sincronización (también conocido como *heartbeat*) 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 combinados en función de un rasgo específico para la administración de dispositivos agrupados en una única unidad dentro de Kaspersky Security Center.

Todos los dispositivos administrados dentro de un grupo de administración están configurados para hacer lo siguiente:

- Use la misma configuración de la aplicación (que puede especificar en las directivas de grupo).
- Utilice un modo común de funcionamiento de las aplicaciones, mediante la creación de tareas de grupo con parámetros específicos. Por ejemplo, crear e instalar un paquete de instalación común para actualizar las bases de datos y los módulos de la aplicación, analizar el dispositivo bajo petición y activar la protección en tiempo real.

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

Puede crear jerarquías que tengan cualquier grado de anidamiento para los Servidores de administración los grupos. Un solo nivel de jerarquía puede incluir Servidores de administración secundarios y virtuales, grupos y dispositivos administrados. Puede mover dispositivos de un grupo a otro sin moverlos físicamente. Por ejemplo, si la posición de un trabajador en la empresa cambia de la de contador a desarrollador, puede mover el equipo de este trabajador del grupo de administración de Contadores al grupo de administración de Desarrolladores. A partir de entonces, el equipo recibirá automáticamente la configuración de la aplicación requerida para los desarrolladores.

Dispositivo administrado

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

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

Un dispositivo puede estar administrado por un solo Servidor de administración. Un Servidor de administración puede admitir hasta 20 000 dispositivos.

Dispositivo no asignados

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

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 que tienen instalado Kaspersky Security Center 14 Web Console Server se denominan *estaciones de trabajo del administrador*. Los administradores pueden utilizar esos dispositivos para una administración centralizada a distancia de las aplicaciones Kaspersky instaladas en los dispositivos cliente.

No hay restricciones para el número de estaciones de trabajo del administrador. En la red se pueden administrar simultáneamente grupos de administración de varios Servidores de administración desde cualquier estación de trabajo del administrador. Se puede conectar una estación de trabajo del administrador a un Servidor de administración (ya sea físico o virtual) de cualquier nivel de la jerarquía.

Se puede incluir una 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 funcionar como cliente del Servidor de administración, como Servidor de administración o como estación de trabajo del administrador.

Complementos 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. De aquí en adelante, un complemento web de administración se denomina también *complemento de administración*. Un complemento de administración es una interfaz entre Kaspersky Security Center 14 Web Console y una aplicación específica de Kaspersky. Con un complemento de administración, puede configurar tareas y directivas para la aplicación.

Puede descargar complementos web de administración desde la Página web de servicio al cliente de Kaspersky.

El complemento de administración proporciona lo siguiente:

- Interfaz para crear y editar tareas y configuraciones de aplicaciones
- Interfaz para crear y editar directivas y perfiles de directivas para la configuración remota y centralizada de las aplicaciones y dispositivos de Kaspersky
- La transmisión de eventos generados por la 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 configuraciones de aplicaciones de Kaspersky que se aplican a un grupo de administración y sus subgrupos. Puede instalar varias aplicaciones de Kaspersky en los dispositivos de un grupo de administración. Kaspersky Security Center proporciona una directiva única para cada aplicación de Kaspersky en un grupo de administración. Una política tiene uno de los siguientes estados:

El estado de la directiva

Estado	Descripción
Activo	La directiva actual que se aplica al dispositivo. Solo una directiva puede estar activa para una aplicación de Kaspersky en cada grupo de administración. Los dispositivos aplican los valores de configuración de una directiva activa para una aplicación de Kaspersky.
Inactiva	Una directiva que no se aplica actualmente a un dispositivo.
Fuera de la oficina	Si se selecciona esta opción, la directiva se activa cuando un dispositivo sale de la red corporativa.

Las directivas funcionan según las siguientes reglas:

- Se pueden configurar varias directivas con diferentes valores para una única aplicación.
- Solo una directiva puede estar activa para la aplicación actual.
- Una directiva puede tener directivas secundarias.

Generalmente, puede utilizar las directivas como preparación para situaciones de emergencia, como el ataque de un virus. Por ejemplo, si se trata de un ataque a través de unidades flash, puede activar una directiva que bloquee el acceso a las unidades flash. En este caso, la directiva activa actual se vuelve inactiva automáticamente.

Para evitar el mantenimiento de varias directivas, por ejemplo, cuando en diferentes ocasiones se supone el cambio de varias configuraciones únicamente, puede utilizar perfiles de directivas.

Un *perfil de directiva* es un subconjunto con nombre de valores de configuración de directiva que reemplaza los valores de configuración de una directiva. Un perfil de directiva afecta la formación de configuraciones efectivas en un dispositivo administrado. Las *configuraciones efectivas* son un conjunto de configuraciones de directivas, configuraciones de perfiles de directivas y configuraciones de aplicaciones locales que están aplicadas en ese momento en el dispositivo.

Los perfiles de directivas funcionan según las siguientes reglas:

- Un perfil de directiva entra en vigor cuando se produce una condición de activación específica.
- Los perfiles de directivas contienen valores de configuración que difieren de la configuración de la directiva.

- La activación de un perfil de directiva cambia la configuración efectiva del dispositivo administrado.
- Una directiva puede incluir un máximo de 100 perfiles de directivas.

Perfiles de directiva

A veces, puede ser necesario crear varias instancias de una sola directiva para diferentes grupos de administración; también podría desear modificar la configuración de esas directivas centralmente. Estas instancias pueden diferir solo en una o dos configuraciones. Por ejemplo, todos los contadores en una empresa trabajan bajo la misma directiva, pero los contadores sénior tienen permiso para usar unidades flash, mientras que los contadores junior no. En este caso, la aplicación de directivas a los dispositivos solo a través de la jerarquía de grupos de administración puede ser inconveniente.

Para ayudarle a evitar la creación de varias instancias de una sola directiva, Kaspersky Security Center le permite crear *perfiles de directivas*. Los perfiles de directivas son necesarios si desea que los dispositivos dentro de un solo grupo de administración se ejecuten bajo diferentes configuraciones de directivas.

Un perfil de directiva es un subconjunto de parámetros de la directiva denominado. Este subconjunto se distribuye en dispositivos de destino junto con la directiva, y se complementa en una condición específica denominada la *Condición de activación de perfil*. Los perfiles solo contienen parámetros que se diferencian de la directiva "básica", que está activa en el dispositivo administrado. La activación de un perfil modifica la configuración de la directiva "básica" que inicialmente estaba activa 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 dispositivos mediante la creación y ejecución de *tareas*. Las tareas son necesarias 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.

Las tareas se pueden realizar en el Servidor de administración y en los dispositivos.

Las siguientes tareas se realizan en el Servidor de administración:

- Distribución automática de informes
- Descarga de actualizaciones al repositorio del Servidor de administración
- Copia de seguridad de los datos del Servidor de administración
- Mantenimiento de bases 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 realizan en dispositivos:

- *Tareas locales*: tareas que se realizan en un dispositivo específico

  El administrador puede modificar las tareas locales mediante de Kaspersky Security Center 14 Web Console o el usuario de un dispositivo remoto (por ejemplo, a través de la interfaz de la aplicación de seguridad). Si una tarea local ha sido modificada simultáneamente por el administrador y el usuario de un dispositivo administrado, los cambios hechos por el administrador entrarán en vigor, ya que tienen una prioridad más alta.

- *Tareas de grupo*: tareas que se realizan 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. Las tareas de grupo también afectan (opcionalmente) los dispositivos que se han conectado a Servidores de administración virtuales y secundarios desplegados en ese grupo o cualquiera de sus subgrupos.

- *Tareas globales*: tareas que se realizan en un conjunto de dispositivos, independientemente de si se incluyen en algún grupo

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

Puede realizar cambios en la configuración de tareas, ver el progreso de las tareas y copiar, exportar, importar y eliminar tareas.

Una tarea se inicia en un dispositivo solo si la aplicación para la que se creó la tarea se está en ejecución.

Los resultados de las tareas se guardan en el registro de eventos de Syslog y en el registro de eventos de Kaspersky Security Center, tanto de manera central en el Servidor de administración como de manera local en cada dispositivo.

No incluya datos confidenciales en la configuración de la tarea. Por ejemplo, no especifique la contraseña del administrador de dominio.

Cobertura de la tarea

La *cobertura de una tarea* es el conjunto de dispositivos en los que se realiza la tarea. Los tipos de cobertura son los siguientes:

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

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

- Especificar determinados dispositivos manualmente.

  Puede utilizar una dirección IP (o un rango IP) o un nombre DNS como la dirección del dispositivo.

- Importación de una lista de dispositivos desde un archivo .txt con las direcciones del dispositivo que se añadirán (cada dirección debe ubicarse en una línea individual).

  Si importa una lista de dispositivos desde un archivo o la crea manualmente, y si los dispositivos se identifican por sus nombres, la lista solo podrá contener dispositivos para los cuales ya se haya introducido información en la base de datos del Servidor de administración. Además, la información debe haberse introducido cuando se conectaron esos dispositivos o durante la detección de dispositivos.

- Especificar selección de dispositivos.

  Con el tiempo, la cobertura de la tarea cambia a medida que el conjunto de dispositivos incluidos en la selección cambia. Puede realizarse una selección de dispositivos sobre la base de atributos del dispositivo, incluido el software instalado en un dispositivo y sobre la base de etiquetas asignadas a dispositivos. La selección de dispositivos es la forma más flexible de especificar la cobertura de una tarea.

  Las tareas para selecciones de dispositivos siempre se ejecutan de forma programada por el Servidor de administración. Estas tareas no se pueden ejecutar en dispositivos que carecen de conexión con el Servidor de administración. Las tareas cuya cobertura 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 en la hora local de un dispositivo; en su lugar, se ejecutan en la hora local del Servidor de administración. Las tareas cuya cobertura se especifica mediante otros métodos se ejecutan en la hora local de un dispositivo.

Cómo se relaciona la configuración de la aplicación local con las directivas

Se pueden utilizar directivas para establecer valores idénticos de la configuración de la aplicación para todos los dispositivos de un grupo.

Los valores de los ajustes especificados por una directiva pueden ser redefinidos para dispositivos individuales de un grupo utilizando los ajustes de la aplicación local. Se pueden establecer solo los valores de los parámetros que la directiva permite modificar, es decir, los parámetros desbloqueados.

El valor de un ajuste que una aplicación utiliza en un dispositivo cliente (consulte la figura siguiente) se determina por la posición del candado (🔒) para ese parámetro en la directiva:

- Si la modificación del parámetro está bloqueada, el mismo valor definido en la directiva se utiliza en todos los dispositivos cliente.
- Si el parámetro de modificación está desbloqueado, la aplicación utiliza un valor de configuración local en cada dispositivo cliente en lugar del valor especificado en la directiva. Así, se puede cambiar el parámetro en los parámetros de aplicación locales.

Esto significa que cuando una tarea se ejecuta en el dispositivo cliente, la aplicación aplica los parámetros definidos de dos maneras diferentes:

- Por parámetros de tarea y configuración de la aplicación local si el parámetro no está bloqueado contra cambios en la directiva.
- Por directiva de grupo si el parámetro está bloqueado contra cambios.

La configuración de aplicación local se cambia una vez que se aplica por primera vez la directiva, de acuerdo con los parámetros de la 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 la distribución de actualizaciones, la instalación remota de aplicaciones y la recuperación de información relativa a dispositivos en red. Un punto de distribución puede realizar las siguientes funciones:

- Distribuir las actualizaciones y los paquetes de instalación que se reciben del Servidor de administración a los dispositivos cliente del grupo (incluida la multidifusión mediante UDP). Las actualizaciones se pueden recuperar del Servidor de administración o de 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 del Servidor de administración.

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

- Ejercer de pasarela a los dispositivos de un grupo de administración para que se conecten con el Servidor de administración.

  Si no se puede establecer una conexión directa entre los dispositivos administrados del grupo y el Servidor de administración, se puede utilizar el punto de distribución como puerta de enlace de conexión al Servidor de administración para este grupo. En este caso, los dispositivos administrados se conectarán a la puerta de enlace de conexión, que se conectará a su vez al Servidor de administración.

  La presencia de un punto de distribución que ejerce como puerta de enlace de conexión no excluye la opción de conexión directa entre los dispositivos administrados y el Servidor de administración. Si la puerta de enlace de conexión no está disponible, pero técnicamente se puede establecer una conexión directa con el Servidor de administración, los dispositivos administrados se conectarán directamente al servidor.

- Sondear la red para detectar dispositivos nuevos y actualizar la información sobre los existentes. Un punto de distribución puede aplicar los mismos métodos de detección de dispositivos que el Servidor de administración.

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

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

Los archivos se transmiten desde el Servidor de administración a un punto de distribución mediante HTTP o, si está activada la conexión SSL, mediante HTTPS. La utilización del HTTP o HTTPS se traduce en un rendimiento más alto, comparado con SOAP, gracias a la reducción del tráfico.

Los dispositivos que tienen instalado Agente de red se pueden designar como puntos de distribución manualmente (por parte del administrador) o de forma automática (por parte del Servidor de administración). La lista completa de los puntos de distribución para los grupos de administración especificados se muestra en el informe sobre la lista de puntos de distribución.

La cobertura de un punto de distribución es definida por el administrador. La cobertura incluye el grupo de administración asignado y sus subgrupos, de todos los niveles de anidamiento. Si se han asignado varios puntos de distribución a la jerarquía de los grupos de administración, el Agente de red del dispositivo administrado se conecta al punto de distribución más cercano en la jerarquía.

Si el Servidor de administración asigna puntos de distribución automáticamente, lo hace por dominios de difusión, no por grupos de administración. Esto tiene lugar si se conocen todos los dominios de difusión. El Agente de red intercambia mensajes con otros Agentes de red de la misma subred; a continuación, envía al Servidor de administración información sobre sí mismo y otros Agentes de red. El Servidor de administración puede utilizar dicha información para agrupar Agentes de red por dominios de difusión. El Servidor de administración conoce los dominios de difusión tras haber sondeado a más del 70 % de los Agentes de red en grupos de administración. El Servidor de administración sondea dominios de difusión cada dos horas. Después de asignar puntos de distribución por 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 un perfil de conexión activo no participan en la detección de dominios de difusión.

Kaspersky Security Center Linux asigna a cada Agente de red una dirección IP de difusión múltiple única que se diferencia del resto de direcciones. Esto permite evitar una sobrecarga de red debida a superposiciones de IP. Las direcciones IP de difusión múltiple que se asignaron en versiones anteriores de la aplicación no se cambiarán.

Si dos o más puntos de distribución se asignan a una sola área de red o un solo grupo de administración, uno de ellos se convierte en el punto de distribución activo y los demás, en puntos de distribución en espera. El punto de distribución activo descarga actualizaciones y paquetes de instalación directamente del Servidor de administración; por su parte, los puntos de distribución en espera solo reciben actualizaciones del punto de distribución activo. En este caso, los archivos se descargan una sola vez del Servidor de administración y después se distribuyen entre los puntos de distribución. Si el punto de distribución activo deja de estar disponible por cualquier motivo, uno de los que están en espera se convierte en punto de distribución activo. El Servidor de administración asigna automáticamente un punto de distribución para que funcione en modo de espera.

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

Un punto de distribución necesita como mínimo 4 GB de espacio libre en disco. Si el espacio libre en disco del punto de distribución es menor 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 punto de distribución requiere espacio libre adicional en disco. El volumen de espacio libre en el disco debe superar el tamaño total de todos los paquetes de instalación que se instalarán.

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

Los dispositivos que funcionan como puntos de distribución se deben proteger, incluida la protección física, contra cualquier acceso no autorizado.

Puerta de enlace de conexión

Una *puerta de enlace de conexión* es un Agente de red que actúa en un modo especial. Una puerta de enlace de conexión acepta conexiones de otros Agentes de red y las conecta al Servidor de administración a través de su propia conexión con el Servidor. A diferencia de un Agente de red normal, una puerta de enlace de conexión espera las conexiones del Servidor de administración en lugar de establecer conexiones con el Servidor de administración.

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

Tiene dos opciones para usar puertas de enlace de conexión:

- Le recomendamos que instale una puerta de enlace de conexión en una zona desmilitarizada (DMZ). Para otros Agentes de red instalados en dispositivos fuera de la oficina, debe configurar especialmente una conexión al Servidor de administración a través de 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 estos datos en ningún búfer y, por lo tanto, no puede aceptar datos de un Agente de red y luego reenviarlos al Servidor de administración. Si el Agente de red intenta conectarse al Servidor de administración a través de la puerta de enlace de conexión, pero la puerta de enlace de la conexión no puede conectarse al Servidor de administración, el Agente de red asume que el Servidor de administración está inaccesible. 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 a través de otra puerta de enlace de conexión. Significa que el Agente de red no puede ser al mismo tiempo una puerta de enlace de conexión y usar una puerta de enlace de conexión para conectarse al Servidor de administración.

  Todas las puertas de enlace de conexión están incluidas en la lista de puntos de distribución en las propiedades del Servidor de administración.

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

Licencias

Esta sección proporciona información acerca de los conceptos generales relacionados con la licencia de Kaspersky Security Center 14 Linux.

Acerca del Contrato de licencia de usuario final

El Contrato de licencia de usuario final (Contrato de licencia o EULA) es un acuerdo obligatorio entre AO Kaspersky Lab y usted que estipula las condiciones según las 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 las condiciones del Contrato de licencia de usuario final para Kaspersky Security Center Linux utilizando 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 las condiciones del Contrato de licencia de usuario final para Agente de red para Linux utilizando los siguientes métodos:

- Mientras se descarga de 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 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.

- Leyendo 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 de Agente de red para Linux.

Acepta las condiciones del Contrato de Licencia de Usuario Final si así lo confirma al instalar la aplicación. Si no acepta las condiciones del Contrato de licencia, cancele la instalación de la aplicación y no la utilice.

Información acerca de la licencia

Una *licencia* es un derecho de uso de la aplicación durante un tiempo limitado que se concede en las condiciones del Contrato de licencia de usuario final.

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

- Uso de la aplicación de acuerdo con las condiciones del Contrato de licencia de usuario final.
- Obtención de soporte técnico.

La cobertura de los servicios y el periodo de validez dependen del tipo de licencia bajo la cual se activó la aplicación.

Se proporcionan los siguientes tipos de licencia:

- *Evaluación*: licencia gratuita para evaluar la aplicación.

  La licencia de evaluación suele tener una duración limitada. Al caducar la licencia de prueba, se desactivan todas las funciones de Kaspersky Security Center Linux. Para continuar usando la aplicación, debe comprar la licencia comercial.

  Solo puede activar una vez la aplicación con una licencia de prueba.

- *Comercial*: licencia de pago concedida con la compra de la aplicación.

  Cuando la licencia comercial expira, la aplicación continúa ejecutándose con una funcionalidad limitada (por ejemplo, las actualizaciones de la base de datos de Kaspersky Security Center no están disponibles). Para continuar usando todas las funciones de Kaspersky Security Center, debe renovar su licencia comercial.

Le recomendamos que renueve la licencia antes de que caduque, a fin de garantizar la máxima protección frente a todas las amenazas de seguridad.

Sobre el certificado de licencia

El *certificado de licencia* es un documento que recibe junto con un archivo clave o un código de activación.

Un certificado de licencia contiene la siguiente información sobre la licencia proporcionada:

- Clave de licencia o número de pedido.
- Información sobre el usuario al que se le ha concedido la licencia.
- Información sobre la aplicación que se puede activar según la licencia proporcionada.
- Límite del número de unidades de licencia (por ejemplo, los dispositivos en los que se puede utilizar la aplicación según la licencia proporcionada).
- Fecha de inicio de la validez de la licencia.
- Periodo de vigencia o fecha de caducidad de la licencia.
- Tipo de licencia.

Sobre la clave de licencia

La *clave de licencia* es una secuencia de bits que puede usar para activar y utilizar la aplicación de acuerdo con las condiciones del Contrato de licencia de usuario final. Las claves de licencia las generan los especialistas de Kaspersky.

Puede añadir una clave de licencia a la aplicación con uno de los siguientes métodos: aplicando un *archivo clave* o introduciendo un *código de activación*. La clave de licencia se mostrará en la interfaz de la aplicación como una secuencia alfanumérica única cuando la añada a la aplicación.

Kaspersky puede bloquear una clave de licencia si se infringen las condiciones del Contrato de licencia. Si se bloquea una clave de licencia, deberá añadir otra para poder utilizar la aplicación.

Las claves de licencia pueden ser activas o adicionales (o de reserva).

Una *clave de licencia activa* es una clave que actualmente utiliza la aplicación. Se puede añadir 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 da derecho al usuario a usar la aplicación, pero actualmente no está en uso. La clave de licencia adicional se activa automáticamente cuando caduca la licencia asociada a la clave de licencia activa actual. Se puede añadir una clave de licencia adicional solo si se ha agregado ya una clave de licencia activa.

Se puede añadir una clave de licencia para una licencia de prueba como clave de licencia activa. No se puede añadir una clave de licencia para una licencia de prueba como clave de licencia adicional.

Consulta de 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:

- Puede leer la Política de privacidad antes 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 desde el 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.

Las siguientes funciones están disponibles:

- 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 un conjunto.
- 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.
- Configuración centralizada de aplicaciones instaladas en dispositivos cliente.
- Visualización y modificación de 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 ha pospuesto.
- Administración de funciones de usuario.

Acerca del archivo clave

Un *archivo clave* es un archivo con la extensión .key que Kaspersky le proporciona. Los archivos clave están diseñados para activar la aplicación agregando una clave de licencia.

Recibirá un archivo clave en la dirección de correo electrónico que proporcionó cuando compró Kaspersky Security Center o solicitó la versión de prueba de Kaspersky Security Center.

No es necesario que se conecte a los servidores de activación de Kaspersky para activar la aplicación con un archivo clave.

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

Para restaurar su archivo clave, realice una de las siguientes acciones:

- Contacte con el vendedor de la licencia.
- Obtener un archivo clave a través del sitio web de Kaspersky utilizando 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 Linux está diseñado para la ejecución centralizada de las tareas básicas de administración y de mantenimiento en la red de una organización. Kaspersky Security Center Linux proporciona al administrador acceso a información detallada sobre el nivel de seguridad de la red de la organización; Kaspersky Security Center Linux le permite al administrador configurar todos los componentes de protección de las aplicaciones de Kaspersky. Kaspersky Security Center Linux realiza las siguientes funciones principales:

- Detectar dispositivos y sus usuarios en la red de la organización.
- Crear una jerarquía de grupos de administración para la administración de dispositivos.
- Instalar aplicaciones de Kaspersky en dispositivos.
- Administrar la configuración y las tareas de las aplicaciones instaladas.
- Activar aplicaciones de Kaspersky en dispositivos.
- Administración de cuentas de usuario.
- Mostrar información sobre el funcionamiento de las aplicaciones de Kaspersky en dispositivos.
- Ver informes.

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

- Información sobre los dispositivos en la red de la organización recibida como resultado de la detección de dispositivos en la red mediante el escaneo de intervalos de IP. El Servidor de administración recibe datos por sí mismo o recibe datos del Agente de red.
- Detalles de los dispositivos administrados. Agente de red transfiere los datos que se enumeran a continuación desde el dispositivo hasta el Servidor de administración. El usuario introduce el nombre para mostrar y la descripción del dispositivo en la interfaz de Kaspersky Security Center 14 Web Console:
  - Especificaciones técnicas del dispositivo administrado y sus componentes necesarios para la identificación del dispositivo: nombre y descripción para mostrar del dispositivo, dominio DNS y nombre DNS, dirección IPv4, dirección IPv6, ubicación de red, dirección MAC, tipo de sistema operativo, si el dispositivo es una máquina virtual junto con el tipo de hipervisor y si el dispositivo es una máquina virtual dinámica como parte de 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 en dispositivos administrados: fecha y hora de la última actualización; hora a la que el dispositivo estuvo visible por última vez en la red; estado de espera de reinicio, hora a la que se encendió el dispositivo.
  - Detalles de cuentas de usuario del dispositivo y sus sesiones.
- Estadísticas de operación del punto de distribución, si el dispositivo es un punto de distribución. Agente de red transfiere los 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 desde el dispositivo al Servidor de administración a través de 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 protección en tiempo real, fecha y hora del último análisis del dispositivo, número de amenazas detectadas, número de

objetos que no se desinfectaron, disponibilidad y estado del componentes de la aplicación, detalles de las configuraciones y tareas de la aplicación Kaspersky, información sobre las claves de licencia activas y de reserva, fecha de instalación e Id. de la aplicación.

- Estadísticas de operación de la aplicación: eventos relacionados con cambios en el estado de los componentes de la aplicación Kaspersky del dispositivo administrado y el desempeño de las tareas iniciadas por los componentes de la aplicación.
- Estado del dispositivo definido por la aplicación Kaspersky.
- Etiquetas asignadas por la aplicación Kaspersky.

- Datos contenidos en los eventos de los componentes de Kaspersky Security Center Linux y las aplicaciones de Kaspersky administradas. Agente de red transfiere los datos del dispositivo al Servidor de administración.
- Configuración de los componentes de Kaspersky Security Center Linux y las aplicaciones administradas de Kaspersky presentadas en las directivas y los perfiles de las directivas El Usuario ingresa los datos en la interfaz de Kaspersky Security Center 14 Web Console.
- Configuración de las tareas de los componentes de Kaspersky Security Center Linux y las aplicaciones administradas de Kaspersky El Usuario ingresa los 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 usuario de aplicaciones. El Usuario ingresa los datos en la interfaz de Kaspersky Security Center 14 Web Console.
- Detalles de los archivos ejecutables detectados en dispositivos administrados por la función Control de aplicaciones. La aplicación administrada transfiere datos desde el dispositivo al Servidor de administración a través de Agente de red. Se proporciona una lista completa de datos en los archivos de Ayuda de la aplicación correspondiente.
- Detalles de los archivos colocados en la Copia de seguridad. La aplicación administrada transfiere datos desde el dispositivo al Servidor de administración a través de Agente de red. Se proporciona una lista completa de datos en los archivos de Ayuda de la aplicación correspondiente.
- Detalles de los archivos colocados en cuarentena. La aplicación administrada transfiere datos desde el dispositivo al Servidor de administración a través de Agente de red. Se proporciona una lista completa de 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 desde el dispositivo al Servidor de administración a través de Agente de red. Se proporciona una lista completa de datos en los archivos de Ayuda de la aplicación correspondiente.
- Detalles de dispositivos externos (unidades de memoria, herramientas de transferencia de información, herramientas de copia impresa de información y buses de conexión) instalados o conectados al dispositivo administrado y detectados por la función Control de dispositivos. La aplicación administrada transfiere datos desde el dispositivo al Servidor de administración a través de Agente de red. Se proporciona una lista completa de datos en los archivos de Ayuda de la aplicación correspondiente.
- Lista de controladores lógicos programables administrados (PLC). La aplicación administrada transfiere datos desde el dispositivo al Servidor de administración a través de Agente de red. Se proporciona una lista completa de datos en los archivos de Ayuda de la aplicación correspondiente.
- Detalles de los códigos de activación introducidos. El Usuario ingresa los datos en la interfaz de Consola de administración o 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 los datos en la interfaz de Kaspersky Security Center 14 Web Console.
- Historial de revisión de objetos de administración. El Usuario ingresa los datos en la interfaz de Kaspersky Security Center 14 Web Console.
- Registro de objetos de administración eliminados. El Usuario ingresa los datos en la interfaz de Kaspersky Security Center 14 Web Console.
- Paquetes de instalación creados a partir del archivo, así como configuración de instalación. El Usuario ingresa los datos en la interfaz de Kaspersky Security Center 14 Web Console.
- Datos necesarios para mostrar los anuncios de Kaspersky en Kaspersky Security Center 14 Web Console. El Usuario ingresa los datos en la interfaz de Kaspersky Security Center 14 Web Console.
- Datos necesarios para el funcionamiento de los complementos de aplicaciones administradas en Kaspersky Security Center 14 Web Console y guardados por los complementos en la base de datos del Servidor de administración durante su operación de rutina. La descripción y las formas de proporcionar los datos se proporcionan en los archivos de Ayuda de la aplicación correspondiente.
- Configuración de usuario de Kaspersky Security Center 14 Web Console: idioma de localización y tema de la interfaz, configuración de visualización del panel de monitoreo, información sobre el estado de las notificaciones (Leídas/No leídas), estado de las columnas en las hojas de cálculo (Mostrar/Ocultar), progreso del modo Formación. El Usuario ingresa los datos en la interfaz de Kaspersky Security Center 14 Web Console.
- Componentes de Registro de eventos de Kaspersky for Kaspersky Security Center Linux y la aplicación administrada de Kaspersky. El Registro de eventos de Kaspersky se almacena en cada dispositivo y no se transfieren nunca al Servidor de administración.
- Certificado para la conexión segura de dispositivos administrados a los componentes de Kaspersky Security Center Linux El Usuario ingresa los datos en la interfaz de Kaspersky Security Center 14 Web Console.

- Cualquier dato que el Usuario ingrese en la interfaz de Kaspersky Security Center 14 Web Console.
- Cualquier dato que el Usuario ingrese en la interfaz de Kaspersky Security Center 14 Web Console.

Los datos enumerados anteriormente pueden estar presentes en Kaspersky Security Center Linux si se aplica uno de los siguientes métodos:

- El Usuario ingresa los 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 mediante la aplicación de Kaspersky administrada y los transfiere al Servidor de administración. Las listas de datos que procesan las aplicaciones de Kaspersky administradas se proporciona en los archivos de Ayuda de las aplicaciones correspondientes.
- El Servidor de administración y el Agente de red asignados a un punto de distribución recibe información sobre los dispositivos en red.

Los datos enumerados se almacenan en la base de datos del Servidor de administración. Los nombres de usuario y contraseñas se almacenan en forma cifrada.

Todos los datos procesados de forma local solo pueden transferirse a Kaspersky a través de archivos de volcado, archivos de seguimiento o archivos de registro de componentes de Kaspersky Security Center Linux, entre ellos archivos de registro creados por instaladores y utilidades.

Kaspersky protege cualquier información recibida de acuerdo con la ley y las reglas aplicables de Kaspersky. Los datos se transmiten a través de un canal seguro.

Al seguir los enlaces de la Consola de administración o de Kaspersky Security Center 14 Web Console, el usuario acepta la transferencia automática de los siguientes datos:

- Código de Kaspersky Security Center Linux.
- Versión de Kaspersky Security Center Linux.
- Localización de Kaspersky Security Center Linux.
- Id. de licencia.
- Tipo de licencia.
- Si la licencia se compró a través de un socio.

La lista de datos proporcionada a través de cada enlace depende de la finalidad y la ubicación de este.

Kaspersky utiliza cualquier información recibida de forma anónima y solo como estadísticas generales. Las estadísticas resumidas se generan automáticamente a partir de la información recibida originalmente y no contienen ningún dato personal o confidencial. Tan pronto como se acumulan nuevos datos, los datos anteriores se borran (una vez al año). Los resúmenes de estadísticas se almacenan indefinidamente.

Acerca de la suscripción

Una *Suscripción a Kaspersky Security Center Linux* es una solicitud para usar la aplicación con las opciones seleccionadas (fecha de vencimiento de la suscripción, cantidad de dispositivos protegidos). Puede registrar la suscripción a Kaspersky Security Center Linux con su proveedor de servicios (por ejemplo, su proveedor de Internet). La suscripción se puede renovar de forma manual o automática; también se puede cancelar.

Una suscripción puede ser limitada (por ejemplo, de 1 año) o ilimitada (sin fecha de caducidad). Para seguir utilizando Kaspersky Security Center tras la caducidad de una suscripción limitada, debe renovarla. Una suscripción ilimitada se renueva automáticamente si se ha pagado previamente al proveedor de servicios en el plazo de vencimiento.

Cuando caduca una suscripción limitada, se le puede proporcionar un periodo de gracia para la renovación durante el cual la aplicación continúa funcionando. El proveedor de servicios determina la disponibilidad y la duración del periodo de gracia.

Para utilizar Kaspersky Security Center Linux con suscripción, debe aplicar el código de activación facilitado por el proveedor de servicios.

Puede aplicar otro código de activación para Kaspersky Security Center Linux solo cuando caducado la suscripción caduque o usted la cancele.

Las acciones posibles en la administración de suscripciones pueden variar en función del proveedor de servicios. Puede suceder que el proveedor de servicios no conceda ningún periodo de gracia para la renovación de la suscripción, con lo cual la aplicación deja de estar operativa.

Los códigos de activación adquiridos mediante suscripción no son válidos para activar versiones anteriores de Kaspersky Security Center.

Cuando la aplicación se utiliza bajo suscripción, Kaspersky Security Center Linux intenta acceder automáticamente al servidor de activación a intervalos de tiempo especificados, hasta que caduque la suscripción. Puede renovar la suscripción en el sitio web del proveedor de servicios.

Eventos de límite de licencias superado

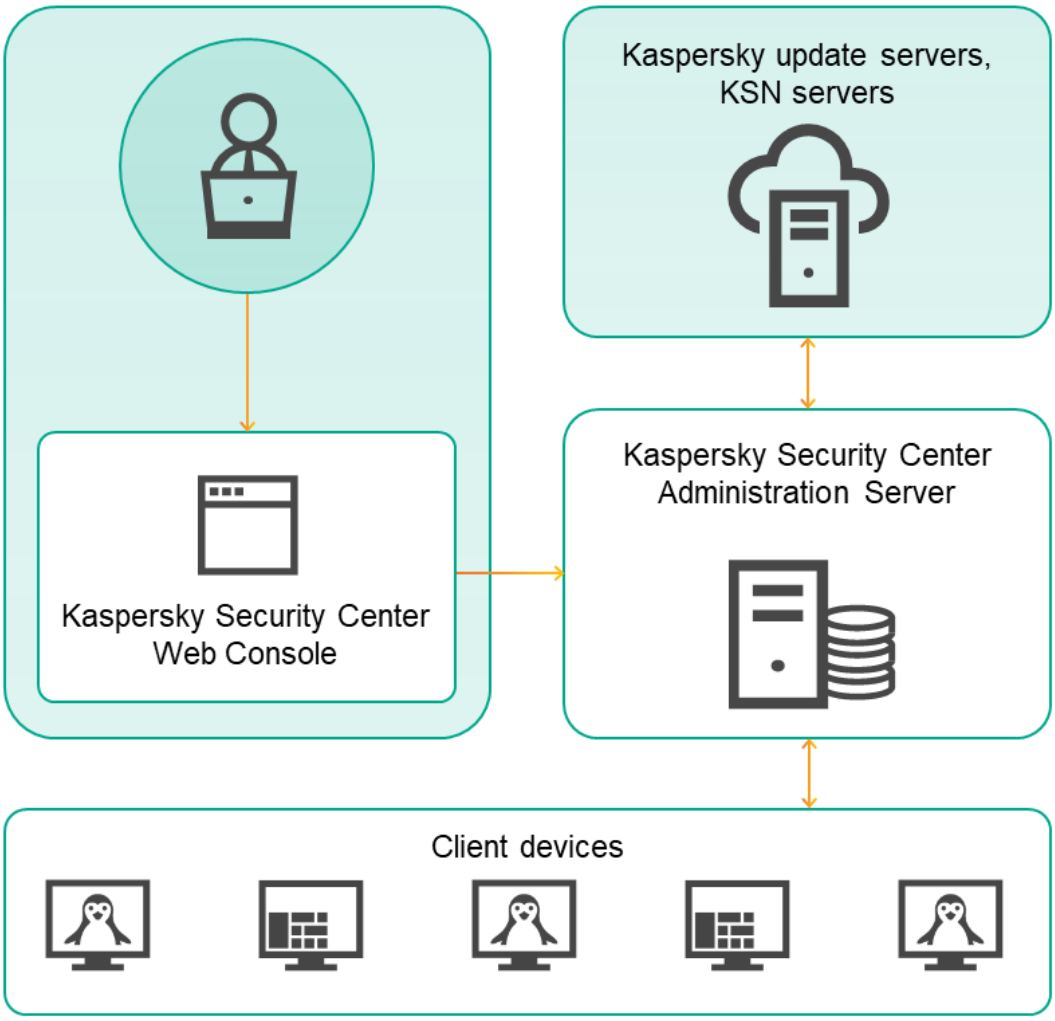
Kaspersky Security Center Linux permite obtener información sobre los eventos que ocurren cuando el Servidor de administración y otras aplicaciones Kaspersky instaladas en dispositivos cliente exceden determinados límites de licencias.

El nivel de importancia de eventos sobre superación de restricciones de licencia se define según las reglas siguientes:

- Si las unidades usadas en un momento dado y cubiertas por una única licencia constituye entre el 90 % y 100 % del número total de unidades cubiertas por dicha licencia, el evento se publica con el nivel de importancia **Información**.
- Si las unidades usadas en un momento dado y cubiertas por una única licencia constituye entre el 100% y 110% del número total de unidades cubiertas por dicha licencia, el evento se publica con el nivel de importancia **Advertencia**.
- Si el número de unidades usadas en un momento dado y cubiertas por una única licencia supera el 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 contiene 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 la información sobre las aplicaciones instaladas en la red de la organización y sobre cómo administrarlas.
- **Servidores de actualización de Kaspersky**. Servidores HTTP(S) de Kaspersky desde los que las aplicaciones Kaspersky descargan las actualizaciones para las bases de datos y los módulos de la aplicación.
- **Servidores de KSN**. Servidores que contienen una base de datos de Kaspersky con información actualizada constantemente sobre la reputación de los archivos, recursos web y software. Kaspersky Security Network garantiza respuestas más rápidas de las aplicaciones Kaspersky a las amenazas, mejora el rendimiento de algunos componentes de protección y reduce la probabilidad de falsos positivos.

- **Dispositivos 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.

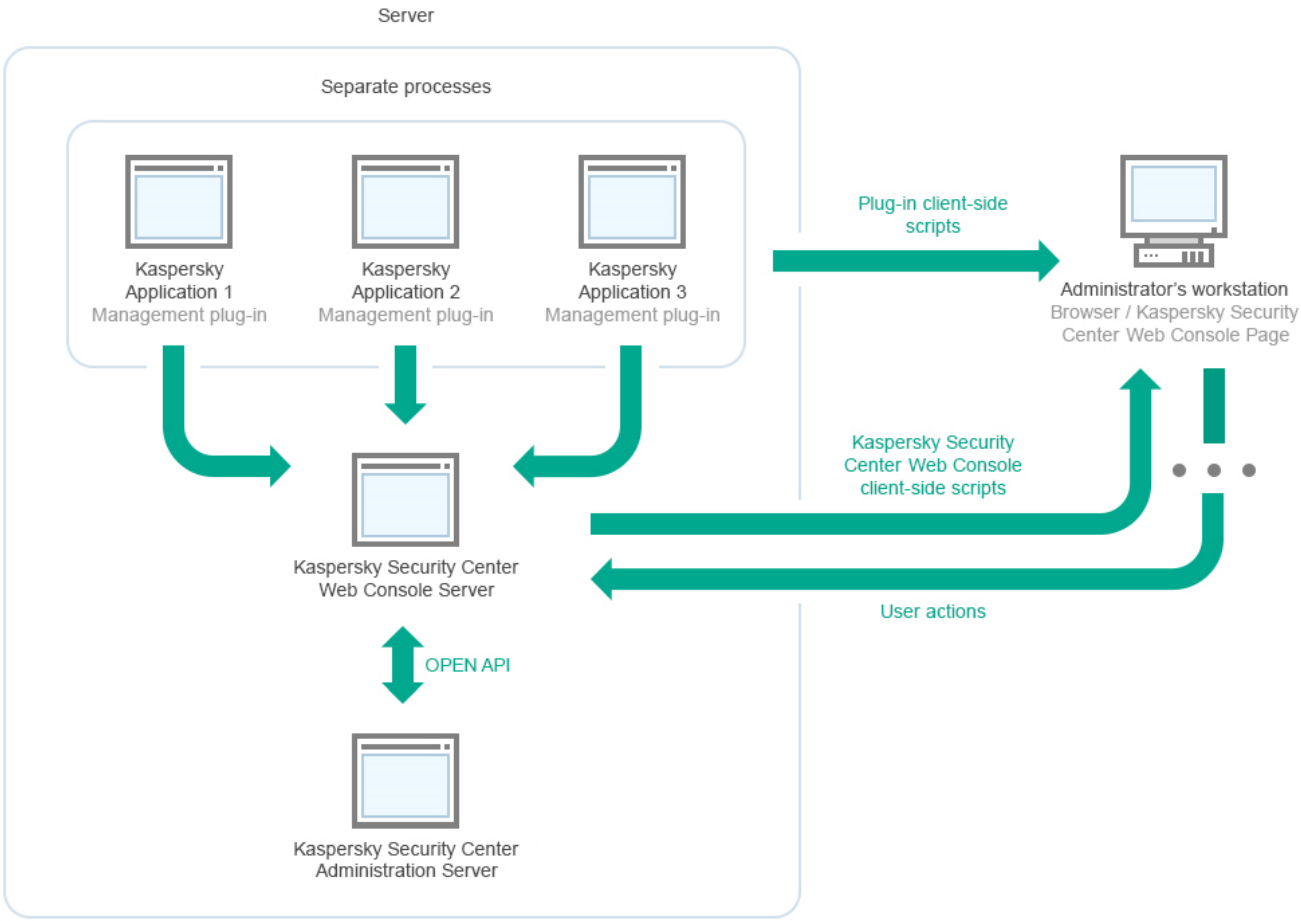


Diagrama de despliegue del Servidor de administración de Kaspersky Security Center y Kaspersky Security Center 14 Web Console

Los complementos de administración para aplicaciones de Kaspersky instaladas en dispositivos protegidos (un complemento para cada aplicación) se despliegan junto con el servidor de Kaspersky Security Center 14 Web Console.

Como administrador, usted accede a Kaspersky Security Center 14 Web Console mediante un navegador en su estación de trabajo.

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

Puertos utilizados 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 cada uno de los números de puerto predeterminados.

Puerto utilizado por el Servidor de administración de Kaspersky Security Center Linux

Número de puerto	Nombre del proceso que abre el puerto	Protocolo	Objetivo del puerto	Cobertura
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 Agentes de red y Servidores de administración secundarios; también se usa en Servidores de administración secundarios para recibir conexiones del Servidor de administración principal (por ejemplo, si el Servidor de administración secundarios está en la DMZ)	Administración de dispositivos cliente y Servidores de administración secundarios. Puede cambiar el número del 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 número del puerto predeterminado para recibir conexiones de los servidores de administración secundarios al crear una jerarquía de servidores de administración.
13000	klserver	UDP	Recepción de información sobre dispositivos que se apagaron desde Agentes de red	Administración de dispositivos cliente. Puede cambiar el número de puerto predeterminado en los ajustes de la directiva del Agente de red.
13299	klserver	TCP (TLS)	Recibiendo conexiones desde Kaspersky Security Center 14 Web Console al Servidor de administración; recibiendo conexiones al Servidor de administración sobre 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 al crear una jerarquía de Servidores de administración.
14000	klserver	TCP	Recepción de conexiones de Agentes de red	Administración de dispositivos cliente. Puede cambiar el número de puerto predeterminado al configurar puertos de conexión durante la instalación de Kaspersky Security Center Linux o al conectar manualmente un dispositivo cliente al Servidor de administración.
13111 (solo si el servicio de Proxy de KSN se ejecuta en el dispositivo)	ksnproxy	TCP	Recepción de solicitudes de dispositivos administrados al servidor proxy de KSN	Servidor proxy de KSN. Puede cambiar el número de puerto predeterminado en la ventana de propiedades del Servidor de administración.
15111 (solo si el servicio de Proxy de KSN se ejecuta en el dispositivo)	ksnproxy	UDP	Recepción de solicitudes de 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 aplicaciones de dispositivos administrados	Activación del Servidor proxy para dispositivos administrados. Puede cambiar el número de puerto predeterminado en la ventana de propiedades del Servidor de administración (en la sección secundaria **Puertos adicionales** en la sección **General**).
19170	klserver	HTTPS (TLS)	Uso de la utilidad klsctunnel para tunelizar conexiones a dispositivos administrados	Conexión remota a dispositivos administrados mediante 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 MariaDB Server). Consulte la documentación del DBMS para obtener la información necesaria.

La siguiente tabla muestra el puerto que debe estar abierto en Kaspersky Security Center Linux Web Console Server. Puede ser el mismo dispositivo donde está instalado el Servidor de administración o un dispositivo diferente.

Puerto utilizado por Kaspersky Security Center Linux Web Console Server

Número de puerto	Nombre del proceso que abre el puerto	Protocolo	Objetivo del puerto	Cobertura
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 al instalar Kaspersky Security Center 14 Web Console. Si instala Kaspersky Security Center 14 Web Console en el sistema operativo Linux ALT, debe especificar un número de puerto que no sea 8080, ya que el sistema operativo usa el puerto 8080.

La siguiente tabla muestra el puerto que debe estar abierto en los dispositivos administrados donde está instalado el Agente de red.

Puertos utilizados por el Agente de red

Número de puerto	Nombre del proceso que abre el puerto	Protocolo	Objetivo del puerto	Cobertura
15000	klnagent	UDP	Señales de gestión del Servidor de administración a los Agentes de red	Administración de dispositivos cliente. Puede cambiar el número de puerto predeterminado en los ajustes de la directiva del Agente de red.
15000	klnagent	Transmisión UDP	Obtención de datos sobre otros Agentes de red dentro del mismo dominio de transmisión (los datos se envían al Servidor de administración)	Entrega de actualizaciones y paquetes de instalación.
15001	klnagent	UDP	Recepción de solicitudes de multidifusión desde un punto de distribución (si está en uso)	Recepción de actualizaciones y paquetes de instalación desde un punto de distribución. Puede cambiar el número de puerto predeterminado en la ventana propiedades del punto de distribución.

La siguiente tabla muestra los puertos que deben estar abiertos en un dispositivo administrado que tenga el Agente de red instalado actuando como un 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 utilizados por el Agente de red que funciona como punto de distribución

Número de puerto	Nombre del proceso que abre el puerto	Protocolo	Objetivo del puerto	Cobertura
13000	klnagent	TCP (TLS)	Recepción de conexiones de Agentes de red	Administración de dispositivos cliente, entrega de actualizaciones y paquetes de instalación Puede cambiar el número de puerto predeterminado en las propiedades del punto de distribución.
13111 (solo si el servicio de Proxy de KSN se ejecuta en el dispositivo)	ksnproxy	TCP	Recepción de solicitudes de dispositivos administrados al servidor proxy de KSN	Servidor proxy de KSN. Puede cambiar el número de puerto predeterminado en las propiedades del punto de distribución.
15111 (solo si el servicio de Proxy de KSN se ejecuta en el dispositivo)	ksnproxy	UDP	Recepción de solicitudes de 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 utilizados por Kaspersky Security Center 14 Web Console

La siguiente tabla enumera los puertos que deben estar abiertos en el dispositivo donde está instalado Kaspersky Security Center 14 Web Console Server (también conocido como Kaspersky Security Center 14 Web Console).

Puertos utilizados por Kaspersky Security Center 14 Web Console

Número de puerto	Nombre de servicio	Protocolo	Objetivo del puerto	Cobertura
2001	KSCWebConsolePlugin	HTTPS	Puerto de API que utilizan los procesos del complemento de administración para	Ejecución de procesos node.exe de complementos de

			recibir solicitudes provenientes de KSCWebConsoleManagementService	administración
1329, 2003	KSCWebConsoleManagementService	HTTPS	Puertos API que se utilizan para recibir solicitudes del servicio KSCWebConsole que se ejecuta en el mismo dispositivo	Actualización de los componentes de Kaspersky Security Center 14 Web Console
2005	KSCWebConsole	HTTPS	Puerto API que se utiliza para recibir solicitudes del servicio KSCWebConsoleManagementService que se ejecuta en el mismo dispositivo	Ejecución de proceso node.exe de Kaspersky Security Center 14 Web Console
8200	—	HTTP	Puerto API que se utiliza para generar certificados mediante HashiCorp Vault (para obtener más detalles, consulte el sitio web de HashiCorp Vault)	Instalación de Kaspersky Security Center 14 Web Console y actualización de los componentes de Kaspersky Security Center 14 Web Console
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	Interacción entre Kaspersky Security Center 14 Web Console y complementos de administración

Instalación

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

Escenario de instalación principal

Siguiendo estas instrucciones, puede instalar el Servidor de administración de Kaspersky Security Center 14 Linux y Kaspersky Security Center 14 Web Console, 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

Debe tener una clave de licencia (código de activación) para Kaspersky Security Center for Buisness o 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. **Selección de una estructura para la protección de una organización**

   Más información sobre los componentes de Kaspersky Security Center Linux. Según la configuración de red y el rendimiento de los canales de comunicación, debe definir el número de Servidores de administración que se usarán y cómo deben distribuirse entre sus oficinas (en caso de que gestione una red distribuida).

   Defina si se utilizará una jerarquía de Servidores de administración en su organización. Para hacer esto, debe evaluar si es posible y oportuno abarcar todos los dispositivos cliente con un solo Servidor de administración o si es necesario construir una jerarquía de Servidores de administración. También es posible que deba construir una jerarquía de Servidores de administración que sea idéntica a la estructura de la organización cuya red quiera proteger.

2. **Preparación para el uso de certificados personalizados**

   Si la infraestructura de clave pública (PKI) de su organización requiere que utilice certificados personalizados emitidos por una autoridad de certificación (CA) específica, prepare esos certificados y asegúrese de que cumplan con 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. **Configuración de puertos**

   Asegúrese de que todos los puertos necesarios estén abiertos para la interacción entre los componentes de acuerdo con la estructura de seguridad que haya seleccionado.

Si debe proporcionar acceso a Internet al Servidor de administración, configure los puertos y especifique la configuración de conexión, según la configuración de red.

5 Instalar 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 automáticmente junto con el Servidor de administración.

6 Instalar Kaspersky Security Center 14 Web Console y 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 14 Web Console en el dispositivo. Puede instalar Kaspersky Security Center 14 Web Console en el mismo dispositivo donde 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 Instalar 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 que instale Kaspersky Endpoint Security para Linux y 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 comienza automáticamente. Realice la configuración inicial del Servidor de administración según los requisitos existentes. Durante la etapa de configuración inicial, el Asistente usa la configuración predeterminada para crear las directivas y las tareas que son necesarias para desplegar la protección. Sin embargo, las configuraciones predeterminadas pueden no ser óptimas para las necesidades de su organización. Puede editar la configuración de directivas y tareas si es necesario.

9 Detección de dispositivos de red

Detecte los dispositivos manualmente. Kaspersky Security Center Linux recibe las direcciones y los nombres de todos los dispositivos detectados en la red. A continuación, puede usar Kaspersky Security Center Linux para instalar aplicaciones y software de Kaspersky desde otros proveedores en los dispositivos detectados. Cada cierto tiempo, Kaspersky Security Center Linux inicia una detección de dispositivos, 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 dispositivos en red de la forma más cómoda puede puede ser necesario dividir el conjunto completo de dispositivos en grupos de administración, tomando en cuenta la estructura de la organización. Puede crear reglas de movimiento para distribuir dispositivos entre grupos o puede distribuir dispositivos manualmente. Puede asignar tareas de grupo para grupos de administración, definir la cobertura 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 de que ya no haya dispositivos no asignados en la red.

11 Asignando los puntos de distribución

Los puntos de distribución se asignan automáticamente a los grupos de administración, pero también puede asignarlos manualmente, si es necesario. Recomendamos que use puntos de distribución en redes a gran escala para reducir la carga en el Servidor de administración y en redes que tengan una estructura distribuida para proporcionar al Servidor de administración acceso a los dispositivos (o grupos de dispositivos) comunicados mediante canales con velocidades de rendimiento reducidas.

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

La implementación de protección en una red empresarial implica la instalación del Agente de red y aplicaciones de seguridad y en dispositivos que el Servidor de administración ha detectado durante el descubrimiento de dispositivos.

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

Las aplicaciones de seguridad protegen los dispositivos frente a virus y otros programas que suponen una amenaza. El Agente de red garantiza la comunicación entre el dispositivo y el Servidor de administración. Los ajustes del Agente de red se configuran automáticamente de forma predeterminada.

Antes de iniciar la instalación del Agente de red y las aplicaciones de seguridad en los dispositivos de la red, asegúrese de que pueda acceder a estos dispositivos (es decir, que estén encendidos).

13 Despliegue de claves de licencia en dispositivos cliente

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

14 Configuración de las directivas de aplicaciones de Kaspersky

Para aplicar diferentes configuraciones de aplicaciones a diferentes dispositivos, puede usar la administración de seguridad centrada en el dispositivo y/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 administración de bases de datos

Instale el sistema de administración de bases de datos (DBMS) que utilizará Kaspersky Security Center. Puede elegir una de las DBMS admitidas.

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

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

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

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

Configuración recomendada para el archivo my.cnf

Para configurar el archivo my.cnf:

1. Abra el archivo my.cnf en un editor de textos.

2. Introduzca 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=< value >
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
```

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

Se recomienda utilizar el valor del parámetro `innodb_flush_log_at_trx_commit=0`, porque los valores "1" o "2" afectan negativamente a la velocidad de funcionamiento de MariaDB.

De forma predeterminada, los complementos del optimizador `join_cache_incremental`, `join_cache_hashed`, y `join_cache_bka` están activados. Si estos complementos no están habilitados, debe habilitarlos.

Para comprobar si los complementos del optimizador están habilitados:

1. En la consola del 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`, entonces los complementos del optimizador están activados.

Si estas líneas faltan o tienen el valor `off`, haga lo siguiente:

a. Abra el archivo my.cnf en un editor de textos.

b. Añada las siguientes líneas al archivo my.cnf:

```
optimizer_switch='join_cache_incremental=on'
optimizer_switch='join_cache_hashed=on'
optimizer_switch='join_cache_bka=on'
```

Los complementos `join_cache_incremental`, `join_cache_hash`, and `join_cache_bka` están habilitados.

Instalar Kaspersky Security Center

Este procedimiento describe cómo instalar Kaspersky Security Center.

Antes de la instalación:

- Instale un sistema de administración de bases de datos.
- Asegúrese de que el dispositivo donde desea instalar Kaspersky Security Center esté ejecutando una de las distribuciones de Linux compatibles.

Utilice el archivo de instalación — ksc64_[version_number]_amd64.deb o ksc64-[version_number].x86_64.rpm — que corresponda a la distribución de Linux instalada en su dispositivo. 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 los siguientes comandos en secuencia:
   ```
   # 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. Lea 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 lo solicite, ingrese los siguientes valores:
   a. Ingrese `y` si entiende y acepta los términos del EULA. Ingrese `n` si no acepta los términos del EULA. Para usar Kaspersky Security Center, debe aceptar las condiciones del EULA.
   b. Ingresar `y` si comprende y acepta los términos de la Política de privacidad, y acepta que sus datos se manejarán y transmitirán (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 lo solicite, ingrese los siguientes ajustes:
   a. Ingrese el nombre DNS o la dirección IP estática del Servidor de administración.
   b. Introduzca el número de puerto del Servidor de administración. De forma predeterminada, se utiliza el puerto 14000.
   c. Introduzca el número de puerto SSL del Servidor de administración. De forma predeterminada, se utiliza el puerto 13000.
   d. Evalúe el número aproximado de dispositivos que desea 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 forma predeterminada, se utiliza el puerto 3306.
   j. Introduzca el nombre de la base de datos.
   k. Introduzca el inicio de sesión de la cuenta root de la base de datos que utiliza para acceder a la base de datos.

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

Espere a que los servicios se añadan 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:
  - Mayúsculas (A-Z)
  - Minúsculas (a-z)
  - Números (0-9)
  - Caracteres especiales (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

Se añade 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 Kaspersky Security Center 14 Web Console (también denominado 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 a 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 instala Kaspersky Security Center 14 Web Console en el sistema operativo Linux ALT, debe especificar un número de puerto que no sea 8080, ya que el sistema operativo usa el puerto 8080.

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

4. Con una cuenta con privilegios root, use la línea de comandos para ejecutar el archivo de instalación con la extensión .deb o .rpm, dependiendo de su distribución de Linux.

   - Para instalar o actualizar Kaspersky Security Center 14 Web Console desde 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 uno de los siguientes comandos:
     ```
     $ sudo rpm -ivh --nodeps ksc-web-console-[número_de_compilación].x86_64.rpm
     ```
     o bien
     ```
     $ sudo alien -i ksc-web-console-[número_de_compilación].x86_64.rpm
     ```
   - Para actualizar desde una versión anterior de Kaspersky Security Center Web Console, ejecute uno de los siguientes 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 empezará a desempaquetar el archivo de instalación. Espere hasta que finalice la instalación. Kaspersky Security Center 14 Web Console se instala en el siguiente directorio: /var/opt/kaspersky/ksc-web-console.

5. Ejecute el siguiente comando para reiniciar todos los servicios de Kaspersky Security Center 14 Web Console:
   ```
   $ 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 Kaspersky Security Center 14 Web Console en dispositivos que ejecutan Linux, debe crear un archivo de respuesta: un archivo .json que contenga 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": "Grupo1:Usuario3",
  "pluginAccount": "Grupo1:Usuario4",
  "messageQueueAccount": "Grupo1:Usuario5"
}
```

Cuando instala Kaspersky Security Center 14 Web Console en el sistema operativo Linux ALT, debe especificar un número de puerto que no sea 8080, ya que el sistema operativo usa 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 disponibles
`dirección`	Dirección del servidor Kaspersky Security Center 14 Web Console (obligatorio)	Valor de cadena.
`puerto`	Número de puerto que utiliza el servidor 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 idioma inglés (en-US).
`enableLog`	Activar o no activar el registro de actividad de Kaspersky Security Center 14 Web Console	Valor booleano: • `true` — el registro está activado (seleccionado de forma predeterminada) • `false` — 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 debe estar definido con los siguientes parámetros: • Dirección de Servidor de administración • Puerto OpenAPI que utiliza Kaspersky Security Center 14 Web Console para conectarse al Servidor de administración (por defecto, 13299) • Ruta al certificado del Servidor de administración • Nombre del Servidor de administración que se mostrará en la ventana de inicio de sesión	Valor de cadena en el siguiente formato: `" server address|port|certificate path|server name "`. Ejemplo: `"X.X.X.X|13299|/cert/server-1.cer|Server 1||Y.Y.Y.Y|13299|/cert/server-2.cer|Server 2"`.

	Los parámetros se separan con barras verticales. Si se especifican varios Servidores de administración, sepárelos con dos barras verticales (plecas).	
`acceptEula`	Aceptar o no aceptar las 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: • `true`: He leído, y entiendo y acepto completamente los términos del Contrato de licencia de usuario final. • `false:` no acepto los términos del Contrato de licencia (seleccionado por defecto).
`certDomain`	Si desea generar un nuevo certificado, use este parámetro para especificar el nombre de dominio para el que se generará el nuevo certificado.	Valor de cadena.
`certPath`	Si desea usar un certificado existente, use este parámetro para especificar la ruta al archivo del certificado	Valor de cadena. Especificar la ruta `"/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"` para utilizar el certificado existente. Para un certificado personalizado, especifique la ruta donde se almacena este certificado personalizado.
`keyPath`	Si desea usar un certificado existente, use este parámetro para especificar la ruta al archivo clave.	Valor de cadena.
`webConsoleAccount`	Nombre de la cuenta en la que se está ejecutando el servicio KSCWebConsole.	Valor de cadena en el siguiente formato: `"nombre del grupo:nombre de usuario"`. Ejemplo: `"Grupo1:Usuario1"`. Si no se especifica ningún valor, el instalador de Kaspersky Security Center 14 Web Console crea una nueva cuenta con el nombre predeterminado `user_management_%uid%`.
`managementServiceAccount`	Nombre de la cuenta privilegiada bajo la cual se ejecuta el servicio KSCWebConsoleManagement.	Valor de cadena en el siguiente formato: `"nombre del grupo:nombre de usuario"`. Ejemplo: `"Grupo1:Usuario1"`. Si no se especifica ningún valor, el instalador de Kaspersky Security Center 14 Web Console crea una nueva cuenta con el nombre predeterminado `user_nodejs_%uid%`.
`serviceWebConsoleAccount`	Nombre de la cuenta en la que se está ejecutando el servicio KSCWebConsole.	Valor de cadena en el siguiente formato: `"nombre del grupo:nombre de usuario"`. Ejemplo: `"Grupo1:Usuario1"`. Si no se especifica ningún valor, el instalador de Kaspersky Security Center 14 Web Console crea una nueva cuenta con el nombre predeterminado `user_svc_nodejs_%uid%`.
`pluginAccount`	Nombre de la cuenta en la que se está ejecutando el servicio KSCWebConsolePlugin.	Valor de cadena en el siguiente formato: `"nombre del grupo:nombre de usuario"`. Ejemplo: `"Grupo1:Usuario1"`. Si no se especifica ningún valor, el instalador de Kaspersky Security Center 14 Web Console crea una nueva cuenta con el nombre predeterminado `user_web_plugin_%uid%`.
`messageQueueAccount`	Nombre de la cuenta en la que se está ejecutando el servicio KSCWebConsoleMessageQueue.	Valor de cadena en el siguiente formato: `"nombre del grupo:nombre de usuario"`. Ejemplo: `"Grupo1:Usuario1"`. Si no se especifica ningún valor, el instalador de Kaspersky Security Center 14 Web Console crea una nueva cuenta con el nombre predeterminado `user_message_queue_%uid%`.

Si especifica los parámetros `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount`, 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 escogidas para trabajar con MariaDB DBMS.

El *DBMS local* es un DBMS instalado en el mismo dispositivo que el Servidor de administración. El *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 remoto.	Local o remoto.
Quién crea la base de datos KAV	El instalador (automáticamente).	Administrador (manualmente).
Cuenta en la que se está ejecutando el programa de instalación	Local o de dominio, con derechos de administrador local.	Local o de dominio, con derechos de administrador local.
Cuenta de servicio del Servidor de administración	Local o dominio.	Local o 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 tanto información general sobre el clúster de conmutación por error de Kaspersky, como las 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 fallo. 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 un nodo pasivo. El nodo activo gestiona la protección de los dispositivos del cliente, mientras que el pasivo está preparado para asumir todas las funciones del nodo activo en caso de que este falle. Cuando se produce un fallo, el nodo pasivo pasa a ser activo y el nodo activo pasa a ser pasivo.

Requisitos previos

Dispone de hardware que cumple los requisitos del clúster de conmutación por error.

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

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

   Cree una nueva cuenta de usuario de dominio o seleccione una existente, bajo la cual se ejecutarán los servicios de Kaspersky Security Center. Añada 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 componente del clúster de conmutación por error de Kaspersky. Asegúrese de que el servidor de archivos cumple 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: Preparar un servidor de archivos para el clúster de conmutación por error de Kaspersky

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

   Prepare dos equipos con hardware y software idénticos para que funcionen como un nodo activo y pasivo.

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

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

   Tiene dos opciones:

   - Si desea utilizar MariaDB Galera Cluster, no necesita una computadora dedicada para la DBMS. Instale MariaDB Galera Cluster en cada uno de los nodos.
   - Si desea utilizar cualquier otra DBMS compatible, instale la DBMS seleccionada 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, en el pasivo.

6 **Prueba del clúster de conmutación por error**

Compruebe que ha configurado correctamente el clúster de conmutación por error y que funciona como debe. Por ejemplo, puede detener uno de los servicios de Kaspersky Security Center en el nodo activo: kladminserver, klnagent, ksnproxy, klactprx o klwebsrv. Una vez detenido el servicio, la administración de la protección debe pasar automáticamente al nodo pasivo.

Resultados

El clúster de conmutación por error de Kaspersky queda desplegado. 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 fallo. 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 un nodo pasivo. El nodo activo gestiona la protección de los dispositivos del cliente, mientras que el pasivo está preparado para asumir todas las funciones del nodo activo en caso de que este falle. Cuando se produce un fallo, el nodo pasivo pasa a ser activo y el nodo activo pasa a ser 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 hardware y software idénticos. 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 actúe como servidor de archivos.

  Asegúrese de que ha proporcionado un gran ancho de banda de red entre el servidor de archivos y los nodos activos y pasivos.

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

Condiciones de los interruptores

El clúster de conmutación por error cambia la administración de la protección de los dispositivos cliente del nodo activo al nodo pasivo si se produce alguno de los siguientes eventos en el nodo activo:

- El nodo activo está roto debido a un fallo de software o hardware.
- El nodo activo se detuvo temporalmente por actividades de mantenimiento.
- Al menos uno de los servicios (o procesos) de Kaspersky Security Center falló o fue cancelado deliberadamente por el usuario. Los servicios de Kaspersky Security Center son los siguientes: kladminserver, klnagent, klactprx y klwebsrv.
- Se interrumpió o terminó la conexión de red entre el nodo activo y el almacenamiento en el servidor de archivos.

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:

1. Asegúrese de que el servidor de archivos cumple 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 núcleo 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 mantener la 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. Usted especificará las rutas a las carpetas compartidas mientras configura la instalación de Kaspersky Security Center.

   Ejecute los siguientes comandos:

   ```
   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
   ```

   Active el inicio automático ejecutando el siguiente comando:

   ```
   sudo systemctl enable rpcbind
   ```

4. Reinicie el servidor de archivos.

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

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

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

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

1. Asegúrese de que tienes dos equipos que cumplen 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 instalar nfs-utils
   ```

3. Cree puntos de montaje con 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 los siguientes comandos:

   ```
   sudo mount -t nfs -o vers=4,nolock,local_lock=none,auto,user,rw {server}:{ruta a la carpeta KlFocStateShare}
   /mnt/KlFocStateShare
   sudo mount -t nfs -o vers=4,nolock,local_lock=none,noauto,user,rw {server}:{ruta a la carpeta
   KlFocDataShare_klfoc} /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}:{ruta a la carpeta KlFocStateShare} /mnt/KlFocStateShare nfs vers=4,nolock,local_lock=none,auto,user,rw
   0 0
   {server}:{ruta a la carpeta KlFocDataShare_klfoc} /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 ejecutando 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 virtuales de ambos nodos deben tener la misma dirección IP.

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

     Ejecute los siguientes comandos:

     ```
     ip link set macvlan1 up
     ifconfig
     ```

     e. Desactive 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. Establezca el nodo activo como servidor principal y el nodo pasivo como servidor de reserva.

     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 desplegar el clúster de conmutación por error de Kaspersky, siga las demás instrucciones 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. Se instala Kaspersky Security Center en ambos nodos del clúster de conmutación por error de Kaspersky por separado. Primero se instala la aplicación en el nodo activo y luego en el pasivo. Durante la instalación, elige el nodo que será el activo y el que será el pasivo.

Utilice el archivo de instalación — ksc64_[version_number]_amd64.deb o ksc64-[version_number].x86_64.rpm — que corresponda a la distribución de Linux instalada en su dispositivo. 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 donde 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. Lea 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 lo solicite, ingrese los siguientes valores:

   a. Ingrese `y` si entiende y acepta los términos del EULA. Ingrese `n` si no acepta los términos del EULA. Para usar Kaspersky Security Center, debe aceptar las condiciones del EULA.

   b. Ingresar `y` si comprende y acepta los términos de la Política de privacidad, y acepta que sus datos se manejarán y transmitirán (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 modo de instalación del Servidor de administración.

7. Cuando se lo solicite, ingrese los siguientes ajustes:

   a. Ingrese la ruta local al punto de montaje de la carpeta compartida de estados del disco.

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

   c. Elija un modo de conectividad del 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 su nombre.

   e. Cuando se le solicite ingresar el nombre DNS o la dirección IP estática del Servidor de administración, 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 forma predeterminada, se utiliza el puerto 14000.

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

   h. Evalúe el número aproximado de dispositivos que desea 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 forma predeterminada, se utiliza el puerto 3306.

   n. Introduzca el nombre de la base de datos.

   o. Introduzca el inicio de sesión de la cuenta root de la base de datos que utiliza para acceder a la base de datos.

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

   Espere a que los servicios se añadan 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 añade 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 donde 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. Lea 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 lo solicite, ingrese los siguientes valores:
   a. Ingrese `y` si entiende y acepta los términos del EULA. Ingrese `n` si no acepta los términos del EULA. Para usar Kaspersky Security Center, debe aceptar las condiciones del EULA.
   b. Ingresar `y` si comprende y acepta los términos de la Política de privacidad, y acepta que sus datos se manejarán y transmitirán (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 modo de instalación del Servidor de administración.
7. Cuando se lo solicite, ingrese la ruta local al punto de montaje de la carpeta compartida de estados del disco.

Kaspersky Security Center queda instalado en el nodo pasivo.

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.

Inicio y detención manual de nodos del clúster

Es posible que tenga que detener todo el clúster de conmutación por error de Kaspersky o separar temporalmente uno de los nodos del clúster para su mantenimiento. En este caso, siga las instrucciones de esta sección. No intente iniciar o detener los servicios o procesos relacionados con el clúster de conmutación por error con cualquier otro medio. Esto puede causar la pérdida de datos.

Inicio y detención de todo el clúster de conmutación por error para su mantenimiento detención

Para iniciar o detener todo el clúster de conmutación por error:

1. En el nodo activo, vaya a /opt/kaspersky/ksc64/sbin.

2. Abra la línea de comandos y ejecute uno de los siguientes comandos:

   - Para detener el clúster, ejecute: `klfoc -stopcluster --stp klfoc`
   - Para iniciar el clúster, ejecute: `klfoc -startcluster --stp klfoc`

Se inicia o se detiene el clúster de conmutación por error, dependiendo del comando que se ejecute.

Mantenimiento de uno de los nodos

Para el mantenimiento de uno de los nodos:

1. En el nodo activo, detenga el clúster de conmutación por error con el comando `klfoc -stopcluster --stp klfoc`.
2. En el nodo que desea mantener, vaya a /opt/kaspersky/ksc64/sbin.
3. Abra la línea de comandos y, a continuación, separe el nodo del clúster con el comando `detach_node.cmd`.
4. En el nodo activo, inicie el clúster de conmutación por error con el comando `klfoc -startcluster --stp klfoc`.
5. Actividades de mantenimiento.
6. En el nodo activo, detenga el clúster de conmutación por error con el comando `klfoc -stopcluster --stp klfoc`.
7. En el nodo que mantuvo, vaya a /opt/kaspersky/ksc64/sbin.
8. Abra la línea de comandos y, a continuación, adjunte el nodo al clúster ejecutando el comando `attach_node.sh`.
9. En el nodo activo, inicie el clúster de conmutación por error con 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 describe cómo emitir y reemplazar certificados para Kaspersky Security Center 14 Web Console 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

Kaspersky Security Center utiliza los siguientes tipos de certificados para permitir una interacción segura entre los componentes de la aplicación:

- Certificado del Servidor de administración
- Certificado del Servidor web
- Certificado de Kaspersky Security Center 14 Web Console

De forma predeterminada, Kaspersky Security Center utiliza certificados autofirmados (es decir, emitidos por el propio Kaspersky Security Center), pero puede reemplazarlos por certificados personalizados para cumplir mejor con los requisitos de la red de su organización y cumplir con los estándares de seguridad. Una vez que el Servidor de administración verifica si un certificado personalizado cumple con todos los requisitos aplicables, este certificado asume el mismo alcance funcional que un certificado autofirmado. La única diferencia es que un certificado personalizado no se vuelve a emitir automáticamente al expirar. Puede reemplazar certificados autofirmados por personalizados mediante la utilidad klsetsrvcert o mediante la sección de propiedades del Servidor de administración en la Kaspersky Security Center 14 Web Console, según el tipo de certificado. Cuando usa la utilidad klsetsrvcert, debe especificar un tipo de certificado usando uno de los siguientes valores:

- C: Certificado común para los puertos 13000 y 13291.
- CR: Certificado de reserva común 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 14 Web Console
- 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 del Servidor de administración y se guarda 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. Este certificado se denomina común ("C").

El certificado del Servidor de administración es válido por 397 días. Kaspersky Security Center genera automáticamente un certificado de reserva común ("CR") 90 días antes de que caduque el certificado común. El certificado de reserva común se utiliza más tarde para sustituir el certificado del Servidor de administración. Cuando el certificado común está a punto de caducar, el certificado de reserva común se utiliza para mantener la conexión con las instancias del Agente de red instaladas en los dispositivos administrados. Con este propósito, el certificado de reserva común se convierte automáticamente en el nuevo certificado común 24 horas antes de que expire el antiguo certificado común.

Si especifica un período de validez superior a 397 días para el certificado del Servidor de administración, el navegador web devuelve un error.

Si es necesario, puede asignar un certificado personalizado para el 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 de certificado. Al reemplazar el certificado, todos los Agentes de red que estaban conectados anteriormente al Servidor de administración a través de SSL perderán su conexión y devolverán el "error de autenticación del Servidor de administración". Para eliminar este error, tendrá que restaurar la conexión después del reemplazo del certificado.

Si se pierde el certificado del Servidor de administración, para recuperarlo debe volver a instalar el componente Servidor de administración y restaurar los datos.

También puede realizar una copia de seguridad del certificado del Servidor de administración por separado de otras configuraciones del Servidor de administración para mover el Servidor de administración de un dispositivo a otro sin pérdida de datos.

Certificado del Servidor web

Servidor web, un componente de Servidor de administración de Kaspersky Security Center, utiliza un tipo especial de certificado. Este certificado es necesario para publicar paquetes de instalación del Agente de red que usted descargará posteriormente en los dispositivos administrados. Para ello, Servidor web puede utilizar varios certificados.

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

1. Certificado de servidor web personalizado que ha especificado manualmente mediante Kaspersky Security Center 14 Web Console
2. Certificado del Servidor de administración común ("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. Esta advertencia aparece porque el certificado de la Web Console está autofirmado y fue generado automáticamente por Kaspersky Security Center. Para eliminar esta advertencia, puede realizar una de las acciones siguientes:

- Reemplace el certificado de Web Console por uno personalizado (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. Le 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

La siguiente tabla muestra los requisitos para los certificados personalizados especificados para diferentes componentes de Kaspersky Security Center.

Requisitos para 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 la clave: • Firma digital • Firma de certificados	El parámetro Extended Key Usage es opcional. El valor de la restricción de longitud de ruta puede ser un número entero diferente de "Ninguna", pero no menos de 1.

	• Cifrado de claves • Firma de CRL Uso extendido de claves (opcional): autenticación de servidor, autenticación de cliente.	
Certificado del Servidor web	Extended Key Usage: autenticación de servidor. El contenedor PKCS # 12 / PEM desde el que se especifica el certificado incluye toda la cadena de claves públicas. El nombre alternativo del sujeto (SAN) del certificado está presente; es decir, el valor del campo `subjectAltName` es válido. El certificado cumple con los requisitos efectivos que los navegadores web imponen a los certificados de servidor, así como con los requisitos básicos actuales del CA/Browser Forum.	No aplica.
Certificado de Kaspersky Security Center 14 Web Console	El contenedor PEM desde el que se especifica el certificado incluye la cadena completa de claves públicas. El nombre alternativo del sujeto (SAN) del certificado está presente; es decir, el valor del campo `subjectAltName` es válido. El certificado cumple con los requisitos efectivos que los navegadores web imponen a los certificados de servidor, así como con los requisitos básicos actuales del CA/Browser Forum.	Los certificados cifrados no son compatibles con Kaspersky Security Center 14 Web Console.

Reemplazar el certificado para Kaspersky Security Center 14 Web Console

La mayoría de los navegadores imponen un límite en el 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 se limita a 397 días. Puede reemplazar un certificado existente recibido de una autoridad de certificación (CA) al emitir un nuevo certificado autofirmado de forma manual. Como alternativa, puede volver a emitir su certificado caducado de Kaspersky Security Center 14 Web Console.

Cuando abre Web Console, el navegador le informa que la conexión a Web Console no es privada y que el certificado de Web Console no es válido. Esta advertencia aparece porque el certificado de la Web Console está autofirmado y fue 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. Le 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, siga estos pasos:

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, ejecute 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.

Reemplazar certificado para Kaspersky Security Center 14 Web Console

De forma predeterminada, cuando instala el Servidor de Kaspersky Security Center 14 Web Console (también conocido como Kaspersky Security Center 14 Web Console), se genera automáticamente un certificado de navegador para la aplicación. Puede reemplazar el certificado generado automáticamente por uno personalizado.

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

1. Cree 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 el parámetro `certPath` y el parámetro `keyPath`.
3. Especifique el nuevo archivo de respuesta para volver a instalar Kaspersky Security Center 14 Web Console. 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, ejecute el comando de actualización.

Kaspersky Security Center 14 Web Console funciona con el certificado especificado.

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

   ```
   openssl pkcs12 -in <filename.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > key.pem
   ```

2. Asegúrese de que el archivo de certificado y la clave privada se generen en el mismo directorio donde está almacenado el archivo .pfx.

3. Kaspersky Security Center 14 Web Console no es compatible con certificados protegidos con contraseña. Por tanto, ejecute el siguiente comando en una utilidad multiplataforma basada en OpenSSL para eliminar una contraseña del archivo .pem:

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   No use el mismo nombre para los archivos .pem de entrada y salida.

   Como resultado, el nuevo archivo .pem se descifra. No tiene que introducir una contraseña para usarlo.

Los archivos .crt y .pen están listos para usarse, 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 clave pública (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 especifica un período de validez superior a 397 días para el certificado del Servidor de administración, el navegador web devuelve un error.

Requisitos previos

El nuevo certificado debe crearse en el formato PKCS#12 (por ejemplo, mediante la PKI de la organización) y debe ser emitido por una autoridad de certificación (CA) de confianza. Además, el nuevo certificado debe incluir toda la cadena de confianza y una clave privada, que debe almacenarse en el archivo con la extensión pfx o p12. Para el nuevo certificado, se deben cumplir los requisitos enumerados a continuación.

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 diferente de "Ninguna", pero no menos de 1.
- Uso de la clave:
  - Firma digital
  - Firma de certificados
  - Cifrado de claves
  - Firma de CRL
- Uso extendido de claves (EKU): autenticación de servidor y autenticación de cliente. El EKU es opcional, pero si su certificado lo contiene, los datos de autenticación del servidor y del cliente deben especificarse en el EKU.

Los certificados emitidos por una CA pública no tienen el permiso de firma de certificados. Para utilizar dichos certificados, asegúrese de haber instalado la versión 13, o una posterior, del Agente de red en los puntos de distribución o las 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. **Sustitución del certificado del Servidor de administración**

   Para ello, use la línea de comandos utilidad klsetsrvcert.

2. **Especificación de un nuevo certificado y restauración de la conexión de los Agentes de red con el 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 el "error de autenticación del Servidor de administración". Para especificar el nuevo certificado y restaurar la conexión, use la línea de comandos utilidad klmover.

Resultados

Cuando termina el escenario, el certificado del Servidor de administración se reemplaza y el servidor es autenticado por los Agentes de red 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. Está incluida 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 <type>`	Tipo de certificado para reemplazar. Posibles valores del parámetro `<type>`: • `C`: Reemplace el certificado para los puertos 13000 y 13291. • `CR`: Reemplace el certificado de reserva común para los puertos 13000 y 13291.
`-f <time>`	Programación de cambio del certificado, en 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 <inputfile>`	Contenedor con el certificado y una clave privada con formato PKCS#12 (archivo con la extensión .p12 o .pfx).
`-p <password>`	Contraseña usada para la protección del contenedor p12. El certificado y una 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 <dnsname>`	Un nuevo certificado se creará para el nombre de DNS especificado.
`-r <calistfile>`	Lista de autoridades de certificación raíz de confianza, formato PEM.

`-l <logfile>`	Archivo de salida de resultados. De forma predeterminada, la salida se redirige al flujo de 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 comandos 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 comandos utilidad klsetsrvcert, debe establecer la conexión SSL entre los Agentes de red y el Servidor de administración porque la conexión está interrumpida.

Para especificar el nuevo certificado del Servidor de administración y restaurar la conexión, haga lo siguiente:

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 de 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 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 por el que se establecerá la conexión no cifrada al Servidor de administración. El número de puerto predeterminado es el 14000.
`-ps <número de puerto SSL>`	Número del puerto SSL por el que se establecerá la conexión cifrada al Servidor de administración, con protocolo 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 de certificado>`	Utilizar 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 de vez en cuando en el despliegue del Agente de red.

Se debe desactivar la distinción entre mayúsculas y minúsculas para la carpeta compartida.

Acerca del proceso de actualización 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, se prohíbe estrictamente que el Servidor de administración y otra aplicación hagan uso concurrente de la DBMS.

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

- Mediante el Archivo de instalación de Kaspersky Security Center

- Mediante la creación de la Copia de seguridad de datos del Servidor de administración, la instalación de una nueva versión del Servidor de administración y la restauración de 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.

Al actualizar Kaspersky Security Center Linux desde una versión anterior, se conservan todos los complementos instalados de 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.

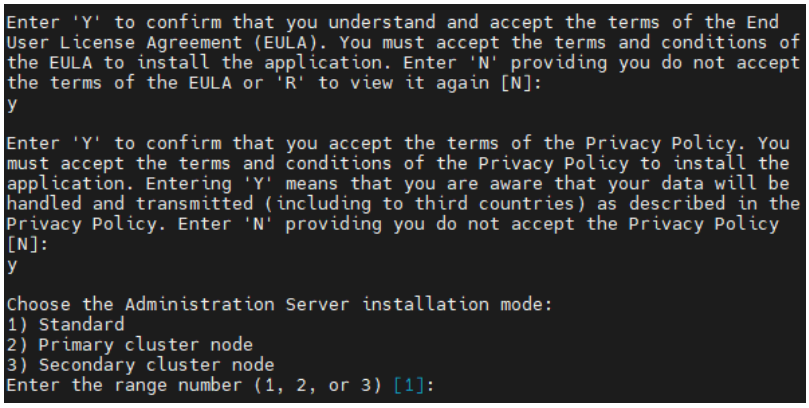
Para actualizar una versión anterior del Servidor de administración a la versión 14 mediante el archivo de instalación:

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 el terminal de línea de comandos en una cuenta con privilegios de root:
   - 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. En la terminal se muestra el mensaje correspondiente.
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 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 en su totalidad los términos y condiciones del EULA.
   b. Ingrese 'Y' nuevamente para confirmar que ha leído, entendido y aceptado en su totalidad la Política de privacidad que describe el manejo de datos.

   La instalación de la aplicación en su dispositivo continuará después de haber ingresado '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 CLUF y la Política de privacidad, y seleccionar el modo de instalación estándar del Servidor de administración en el terminal de línea de comandos

   A continuación, el script configura y finaliza la actualización del Servidor de administración. Durante la actualización, no puede cambiar los ajustes del Servidor de administración que haya configurado antes de la actualización.
6. Para dispositivos que tienen instalada una versión posterior 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.

Al completarse la tarea de instalación remota, se actualiza la versión del Agente de red.

Actualizar 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 restaurarlos después de instalar la nueva versión de Kaspersky Security Center. Si se presentan problemas durante la instalación, puede restaurar la versión anterior del Servidor de administración usando la copia de seguridad del Servidor de administración creada antes de la actualización.

Para actualizar una versión anterior del Servidor de administración a la versión 14 mediante copia de seguridad, realice lo siguiente:

1. Antes de la actualización, haga una copia de seguridad de los datos del Servidor de administración con la versión anterior de la aplicación.
2. Desinstale la versión anterior de Kaspersky Security Center.
3. Instale Kaspersky Security Center versión 14 en el anterior Servidor de administración.
4. Restaure los datos del Servidor de administración de la copia de seguridad creada antes de la actualización.
5. Para los dispositivos en los que estaba instalada la versión anterior del Agente de red, cree y ejecute la tarea para la instalación remota de 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.

Al completarse la tarea de instalación remota, se actualiza la versión del Agente de red.

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

Puede iniciar sesión en 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 Linux 14 Web Console y usarla 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 realizar los siguientes cambios en la aplicación:

- Añadir archivos claves o ingresar códigos de activación que se pueden distribuir automáticamente a los dispositivos de grupos de administración.
- Configurar el envío de notificaciones por correo electrónico sobre eventos que tienen lugar durante el funcionamiento del Servidor de administración y las aplicaciones administradas (para que el envío de notificaciones sea correcto, el servicio de mensajería se debe ejecutar en el Servidor de administración y en todos los dispositivos destinatarios).
- Crear una directiva de protección para estaciones de trabajo y servidores, así como tareas del 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 ninguna tarea si ya existe alguna tarea con el mismo nombre en el nivel superior de jerarquía de los dispositivos administrados.

La aplicación automáticamente solicita que se ejecute el Asistente de inicio rápido tras la instalación del Servidor de administración la primera vez que se realiza la conexión con él. También puede iniciar el Asistente de inicio rápido manualmente en cualquier momento.

Para iniciar manualmente el Asistente de inicio rápido, haga lo siguiente:

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

   Se abre la ventana Propiedades del Servidor de administración.
2. En la pestaña **Control de aplicaciones**, seleccione la sección **Control de aplicaciones**.
3. Haga clic en **Iniciar Asistente de inicio rápido**.

El Asistente le solicita a realizar la configuración inicial del Servidor de administración. Siga las instrucciones del Asistente. Avance a través del Asistente utilizando el botón **Siguiente**.

Paso 1. Especificar la configuración de la conexión a Internet

Expandir todo | Contraer todo

Especificar la configuración del acceso a Internet de Kaspersky Security Center Linux.

Seleccione la casilla **Usar servidor proxy** si desea usar un servidor proxy al conectarse a Internet. Si se selecciona esta casilla, los campos están disponibles para introducir la configuración. Especifique la configuración siguiente para la conexión con el servidor proxy:

- **Dirección**
- **Número de puerto**
- No utilizar el servidor proxy para direcciones locales

  No se utilizará un servidor proxy para conectarse a los dispositivos de 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 si la casilla **Usar servidor proxy** está seleccionada.
- Nombre de usuario (este campo está disponible si la casilla de verificación **Autenticación del servidor proxy** está seleccionada)

  La cuenta de usuario en la que se establece la conexión al servidor proxy (este campo está disponible si la casilla **Autenticación del servidor proxy** está seleccionada).
- Contraseña (este campo está disponible si la casilla de verificación **Autenticación del servidor proxy** está seleccionada)

  La contraseña configurada por el usuario bajo cuya cuenta se establece la conexión del servidor proxy (este campo está disponible si la casilla **Autenticación del servidor proxy** está seleccionada).

  Para ver la contraseña introducida, mantenga pulsado el botón **Mostrar** todo el tiempo que sea necesario.

Paso 2. Selección del método de activación de la aplicación

Expandir todo | Contraer todo

Seleccione una de las siguientes opciones de activación de Kaspersky Security Center Linux:

- **Introducir su código de activación**

  El *código de activación* es una secuencia única de 20 caracteres alfanuméricos. Introduzca un código de activación para añadir una clave que active Kaspersky Security Center Linux. Recibirá el código de activación a través de la dirección de correo electrónico que especificó después de adquirir Kaspersky Security Center.

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

  Si ha seleccionado esta opción de activación, puede activar la opción **Desplegar clave de licencia automáticamente en dispositivos administrados**.

  Si esta opción está activada, la clave de licencia se desplegará automáticamente en los dispositivos administrados.

  Si esta opción está desactivada, puede implementar la clave de licencia en los dispositivos administrados más adelante en la sección **OPERACIONES → LICENCIAS → LICENCIAS DE KASPERSKY** del menú principal.

- **Especifique un archivo clave**

  Un *archivo clave* es un archivo con la extensión .key que Kaspersky le proporciona. Sirve para añadir archivo clave que active la aplicación.

  Recibirá su archivo clave a través de la dirección de correo electrónico que especificó después de adquirir Kaspersky Security Center.

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

  Si ha seleccionado esta opción de activación, puede activar la opción **Desplegar clave de licencia automáticamente en dispositivos administrados**.

  Si esta opción está activada, la clave de licencia se desplegará automáticamente en los dispositivos administrados.

  Si esta opción está desactivada, puede implementar la clave de licencia en los dispositivos administrados más adelante en la sección **OPERACIONES → LICENCIAS → LICENCIAS DE KASPERSKY** del menú principal.

- Posponer la activación de aplicaciones

Si decide posponer la activación de la aplicación, puede agregar una clave de licencia más adelante en cualquier momento en **OPERACIONES → LICENCIAS**.

Cuando trabaja con Kaspersky Security Center desplegado desde una AMI de pago o para un SKU facturado mensualmente según el uso, no puede especificar un archivo clave ni introducir un código.

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

Puede consultar la lista de directivas y tareas que se crean.

Espere a que se complete la creación de directivas y tareas antes de ir al paso siguiente del Asistente.

Paso 4. Configuración de notificaciones por correo electrónico

Expandir todo | Contraer todo

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:

- **Destinatarios (direcciones de correo electrónico)**

  Las direcciones de correo electrónico de usuarios a quien la aplicación enviará notificaciones. Puede introducir una o más direcciones; si introduce 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 introduce más de una dirección, sepárelas con un punto y coma. Puede usar los siguientes valores:

  - 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**

  Activa la compatibilidad con autenticación de ESMTP. Cuando la casilla está seleccionada, en los campos **Nombre de usuario** y **Contraseña**, puede especificar la configuración de la autorización de ESMTP. De forma predeterminada, esta casilla está vacía y los parámetros de autenticación ESMTP no están disponibles.

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

Paso 5. Cerrar el Asistente de inicio rápido

Para cerrar 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 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 la instalación de la aplicación (si no se creó antes). El paquete de instalación se encuentra en **DETECCIÓN Y DESPLIEGUE → DESPLIEGUE Y ASIGNACIÓN → PAQUETES DE INSTALACIÓN**. Puede usar este paquete de instalación para la instalación de la aplicación en el futuro.
- Crea y ejecuta una tarea de instalación remota para dispositivos específicos o para un grupo de administración. La tarea de instalación remota recién creada se almacena en la sección **Tareas**. Más tarde podrá iniciar esta tarea manualmente. El tipo de tarea es **Instalar aplicación en remoto**.

Si desea instalar Agente de red en dispositivos con el sistema operativo SUSE Linux Enterprise Server 15, instale el paquete insserv-compat primero para configurar el Agente de red.

Iniciar Asistente de despliegue de la protección

También puede iniciar el Asistente de despliegue de la protección manualmente en cualquier momento.

Para iniciar manualmente el Asistente de despliegue de la protección,

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

Comienza el Asistente de despliegue de la protección. Avance a través del Asistente utilizando el botón **Siguiente**.

Paso 1. Seleccionar paquete de instalación

Seleccione el paquete de instalación de la aplicación que desea instalar.

Si el paquete de instalación de la aplicación requerida no está en la lista, haga clic en el botón **Añadir** y luego seleccione la aplicación de la lista.

Paso 2. Seleccionar un método para la distribución de archivos claves o códigos de activación

Expandir todo | Contraer todo

Seleccione un método para la distribución de la archivo clave o el código de activación:

- **No añadir la clave de licencia al paquete de instalación**

  La clave se distribuye automáticamente a todos los dispositivos con los que es compatible:
  - Si se ha activado la distribución automática en las propiedades de la clave.

- Si se ha creado la tarea **Agregar clave**.

- **Añadir clave de licencia al paquete de instalación**

  La clave se distribuye a dispositivos junto 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 incluye un archivo clave o un código de activación, se muestra esta ventana, pero solo contiene la información de la clave de licencia.

Paso 3. Seleccionar versión del Agente de red

Si seleccionó el paquete de instalación de una aplicación que no sea el agente de red, también debe 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. Selección de dispositivos

Expandir todo | Contraer todo

Especifique una lista de dispositivos en los que se instalará la aplicación:

- **Instalar en dispositivos administrados**

  Si se selecciona esta opción, la tarea de instalación remota se creará para un grupo de dispositivos.

- **Seleccionar dispositivos para la instalación**

  La tarea se asigna a los dispositivos incluidos en una selección de dispositivos. Puede especificar una de las selecciones existentes.

  Por ejemplo, es posible que desee utilizar esta opción para ejecutar una tarea en dispositivos con una versión específica del sistema operativo.

Paso 5. Especificar la configuración de tarea de instalación remota

Expandir todo | Contraer todo

En la página **Configuración de tarea Instalación remota**, especifique la configuración de la instalación remota de la aplicación.

En el grupo de ajustes **Forzar la descarga del paquete de instalación**, especifique cómo los archivos necesarios para la instalación de la aplicación se distribuirán a los dispositivos cliente:

- **Usando el Agente de red**

  Si esta opción está habilitada, el Agente de red instalado en dispositivos cliente entrega los paquetes de instalación a dichos dispositivos cliente.

  Si esta opción está desactivada, los paquetes de instalación se entregan mediante las herramientas del sistema operativo Linux.

  Recomendamos que habilite esta opción si la tarea se ha asignado a dispositivos que tienen instalados Agentes de red.

  Esta opción está activada de forma predeterminada.

- **Usando los recursos del sistema operativo mediante puntos de distribución**

  Si esta opción está habilitada, los paquetes de instalación se transmiten a los dispositivos cliente mediante herramientas del sistema operativo a través de los puntos de distribución. Se puede seleccionar esta opción si existe al menos un punto de distribución en la red.

  Si la opción **Usando el Agente de red** está habilitada, los archivos se entregan mediante herramientas del sistema operativo solo si los recursos del Agente de red no están disponibles.

  De forma predeterminada, esta opción está habilitada para tareas de instalación remotas creadas en un Servidor de administración virtual.

Defina la configuración adicional:

No reinstalar la aplicación si ya se encuentra instalada

Si esta opción está habilitada, la aplicación seleccionada no se volverá a instalar si ya está instalada en el dispositivo cliente.

Si esta opción está deshabilitada, la aplicación se instalará igualmente.

Esta opción está activada de forma predeterminada.

Paso 6. Eliminar aplicaciones incompatibles antes de la instalación

Este paso solo está presente si se conoce que la aplicación que despliega es incompatible con otras aplicaciones.

Seleccione esta 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 esta opción, la aplicación solo se instalará en dispositivos que no tengan aplicaciones incompatibles.

Paso 7. Mover dispositivos móviles a dispositivos administrados

Expandir todo | Contraer todo

Especifique si los dispositivos deben moverse a un grupo de administración después de la instalación del Agente de red.

- **No mover dispositivos**

  Los dispositivos permanecen en los grupos en los que se localizan actualmente. Los dispositivos que no se han localizado en ningún grupo permanecen sin asignar.

- **Mover dispositivos no asignados al grupo**

  Los dispositivos se mueven al grupo de administración que seleccione.

La opción **No mover dispositivos** está preseleccionada. Por razones de seguridad, quizá quiera mover los dispositivos manualmente.

Paso 8. Selección de cuentas para acceder a dispositivos

Expandir todo | Contraer todo

Si es necesario, agregue las cuentas que se utilizarán para iniciar la tarea de instalación remota:

- **No es necesaria una cuenta (Agente de red instalado)**

  Si se selecciona esta opción, no tiene que especificar la cuenta bajo la que se ejecutará el instalador de aplicación. La tarea se ejecutará en la cuenta en la que se está ejecutando el servicio del Servidor de administración.

  Si el Agente de red no se ha instalado en dispositivos cliente, esta opción no está disponible.

- **Se necesita una cuenta (para la instalación sin Agente de red)**

  Si se selecciona esta opción, puede especificar la cuenta bajo la que se ejecutará el instalador de aplicación. Puede especificar la cuenta de usuario si el Agente de red no se ha instalado en los dispositivos para los cuales está asignada la tarea.

  Puede especificar varias cuentas de usuario si, por ejemplo, ninguna de ellas tiene todos los derechos requeridos en todos los dispositivos a los que se asignó esta tarea. En este caso, todas las cuentas que se han agregado se utilizan para ejecutar la tarea, en orden consecutivo de arriba abajo.

  Si no se agrega ninguna cuenta, la tarea se ejecutará en la cuenta en la que se está ejecutando 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** se ha creado y configurado correctamente.

La opción **Ejecutar tarea después de que finalice el Asistente** no está seleccionada de forma predeterminada. 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. Más tarde podrá iniciar esta tarea manualmente.

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 icono 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 **Control de aplicaciones**, seleccione la sección **Puertos de conexión**.

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

Configurar una lista de direcciones IP permitidas para iniciar sesión en Kaspersky Security Center

De manera predeterminada, los usuarios pueden iniciar sesión en Kaspersky Security Center desde cualquier dispositivo en el que puedan abrir Kaspersky Security Center 14 Web Console (en adelante, Web Console). Sin embargo, puede configurar el Servidor de administración para que los usuarios puedan conectarse a él solo desde dispositivos con las direcciones IP permitidas. En este caso, incluso si un intruso roba una cuenta de Kaspersky Security Center, no podrá iniciar sesión en Kaspersky Security Center porque la dirección IP del dispositivo del intruso no está en la lista de permitidos.

La dirección IP se verifica cuando un usuario inicia sesión en Kaspersky Security Center o ejecuta una aplicación que interactúa con el Servidor de administración a través de Kaspersky Security Center OpenAPI. 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 admitidos, se produce un error de autenticación y el evento KLAUD_EV_SERVERCONNECT notifica que no se ha establecido una conexión con el Servidor de administración.

Requisitos para una lista de direcciones IP permitidas

Las direcciones IP se verifican solo cuando las siguientes aplicaciones intentan conectarse al Servidor de administración:

- Servidor de Web Console

  Si inicia sesión en Kaspersky Security Center a través de Web Console, puede configurar un firewall en el dispositivo donde está instalado el servidor de Web Console utilizando los medios estándar del sistema operativo. Después, si alguien intenta iniciar sesión en Kaspersky Security Center en un dispositivo y el servidor de consola web está instalado en otro dispositivo, un firewall ayuda a evitar que los intrusos interfieran.

- Aplicaciones que interactúan con el Servidor de administración a través de objetos de automatización 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 lo tanto, especifique las direcciones de los dispositivos en los que están instaladas las aplicaciones enumeradas anteriormente.

Puede establecer direcciones IPv4 e IPv6. No puede especificar rangos de direcciones IP.

Cómo establecer una lista de direcciones IP permitidas

Si no ha establecido una lista de direcciones permitidas antes, siga las instrucciones a continuación.

Para establecer la lista de direcciones IP permitidas para iniciar sesión en Kaspersky Security Center, haga lo siguiente:

1. En el dispositivo del Servidor de administración, ejecute 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, usando derechos de administrador:
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<direcciones IP>" -t s`

   Especifique direcciones IP que cumplan con los requisitos enumerados anteriormente. Las direcciones IP deben estar separadas por un punto y coma.

   Ejemplo de cómo permitir que solo un 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 de cómo 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.

Puede averiguar si configuró correctamente la lista de direcciones IP permitidas en el Registro de eventos de Syslog en el Servidor de administración.

Cómo cambiar una lista de direcciones IP permitidas

Puede cambiar una lista de direcciones permitidas tal como lo hizo cuando la estableció por primera vez. Para ello, ejecute el mismo comando y especifique una nueva lista de permitidas:

```
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, introduzca 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 restablecer una lista de direcciones IP permitidas ya configurada

Para restablecer una lista de direcciones IP permitidas ya configurada:

1. Introduzca el siguiente comando en el símbolo del sistema, usando 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.

Después de hacerlo, las direcciones IP dejan de verificarse.

Visualización del registro de conexiones con el 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 icono de **Configuración** () junto al nombre del Servidor de administración requerido.

   Se abre la ventana Propiedades del Servidor de administración.
2. En la pestaña **Control de aplicaciones**, seleccione la sección **Puertos de conexión**.
3. Active la opción **Registrar eventos de conexión 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 especifica el número máximo de eventos, la aplicación calcula una cantidad aproximada de espacio de almacenamiento requerido para el número especificado. Puede usar 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 45 millones de eventos.

Si el número de eventos en la base de datos llega al valor máximo especificado por el administrador, la aplicación elimina los eventos más antiguos sobrescribiéndolos con los nuevos. Cuando el Servidor de administración elimina eventos antiguos, no puede guardar eventos nuevos 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 luego se guardan en la base de datos una vez que se completa la operación de eliminación.

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 icono 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 **Control de aplicaciones**, seleccione la sección **Repositorio de eventos**. Especifique el número máximo de eventos almacenados en la base de datos.
3. Haga clic en el botón **Guardar**.

Copia de seguridad y restauración de datos del servidor de administración

La copia de seguridad de datos permite trasladar un Servidor de administración de un dispositivo a otro sin perder los datos. Mediante la copia de seguridad, puede restaurar datos cuando traslada la base de datos de un Servidor de administración a otro dispositivo o cuando se pasa 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:

- Creando y ejecutando un tarea de copia de seguridad de datos a través de Kaspersky Security Center 14 Web Console.
- Ejecutando la utilidad klbackup en el dispositivo que tenga instalado el Servidor de administración. La utilidad se incluye en el kit de distribución de Kaspersky Security Center. Después de la instalación del Servidor de administración, la utilidad se ubica en la raíz de la carpeta de destino especificada durante la instalación de la aplicación (por lo general, /opt/kaspersky/ksc64/sbin/klbackup).

Los siguientes datos se guardan 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 la instalación remota.
- Certificado del Servidor de administración.

La recuperación de datos del Servidor de administración solo es posible mediante la utilidad klbackup.

Crear una tarea de creación de copias de seguridad de los datos del Servidor de administración:

Las tareas de creación de copias de seguridad son tareas del Servidor de administración creadas por el Asistente de inicio rápido. Si se ha eliminado una tarea de creación de copias de seguridad creada por el Asistente de inicio rápido, puede crear una manualmente.

La tarea *Copia de seguridad de los datos del Servidor de administración* solo puede crearse en una copia individual. Si la tarea de creación de copias de seguridad de los datos del Servidor de administración ya se ha creado, no aparecerá en la ventana de selección de tipo de tarea.

Para crear una tarea de creación de copias de seguridad de los datos del Servidor de administración:

1. Vaya a **DISPOSITIVOS** → **TAREAS**.
2. Haga clic en **Añadir**.
   Se inicia el Asistente para añadir tareas.
3. En la primera página del Asistente, en la lista **Aplicación**, seleccione **Proveedor**, y en la lista **Tipo de tarea**, seleccione **Copia de seguridad de los datos del Servidor de administración**.
4. En la página correspondiente del Asistente, especifique la siguiente configuración:
   - Carpeta para el almacenamiento de copias de seguridad
   - Contraseña de la copia de seguridad (opcional)
   - Número máximo de copias de seguridad para guardar
5. Si en la página **Finalizar la creación de tareas**, activa la opción **Abrir los detalles de la tarea cuando se complete la creación**, puede modificar la configuración de tarea predeterminada. Si no activa esta opción, la tarea se creará con las configuraciones predeterminadas. Puede modificar la configuración predeterminada más tarde, en cualquier momento.
6. Haga clic en el botón **Finalizar**.

La tarea se crea y se muestra en la lista de tareas.

Utilidad de creación de copias de seguridad y recuperación de datos (klbackup)

Puede hacer copias de seguridad de los datos del Servidor de administración para su almacenamiento y futura recuperación mediante la utilidad klbackup, que es parte del kit de distribución de Kaspersky Security Center.

La utilidad klbackup puede ejecutarse en cualquiera de los dos modos siguientes:

- Interactivo
- No interactivo

Creación de copias de seguridad y recuperación de datos en modo interactivo

Expandir todo | Contraer todo

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 copias de seguridad y restauración.

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

   Si marca la opción **Restaurar o crear copia de seguridad solamente del 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 luego 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). Inicie la utilidad con la misma cuenta con la que instaló el Servidor de administración.

   Se inicia el Asistente de copias de seguridad y restauración.

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

   Si selecciona la opción **Restaurar o crear copia de seguridad solamente del certificado del Servidor de administración**, el Servidor de administración solo se recuperará.

   Haga clic en **Siguiente**.

3. En la ventana **Restaurar la configuración** del Asistente:

   - Especifique la carpeta que contiene una copia de seguridad de los datos del Servidor de administración. Debe asegurarse de que el archivo se denomine backup.zip.
   - Especifique la contraseña introducida durante la creación de copias de seguridad de los datos.

     Al restaurar datos, debe indicar la misma contraseña que se introdujo durante la creación de copias de seguridad. Si la ruta de una carpeta compartida cambió tras realizar la copia de seguridad, compruebe el funcionamiento de las tareas que utilizan datos restaurados (tareas de restablecimiento y tareas de instalación remota). Si fuera necesario, edite 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 con la que se inicia la utilidad klbackup debe tener total acceso a la carpeta compartida.

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

Creación de copias 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,

Ejecute la utilidad klbackup con el conjunto de claves requeridas desde la línea de comandos del dispositivo en el que esté instalado el Servidor de administración.

Sintaxis de línea de comandos de la utilidad:

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

Si no hay ninguna contraseña especificada en la línea de comandos de la utilidad klbackup, la utilidad le solicitará introducir la contraseña de forma interactiva.

Descripciones de las claves:

- `-path BACKUP_PATH`: Guardar información en la carpeta BACKUP_PATH o utilizar datos de la carpeta BACKUP_PATH para la recuperación (parámetro obligatorio).
- `-logfile LOGFILE`: Guardar un informe sobre la creación de copias de seguridad y recuperación de los datos del Servidor de administración.

  Se concederá acceso a la cuenta del servidor de bases de datos y a la utilidad klbackup para la modificación de datos en 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 ha especificado ninguna clave, la información se guarda en la raíz de la carpeta BACKUP_PATH.

  Cuando se intenta guardar información en una carpeta que ya tiene almacenada una copia de seguridad, aparece un mensaje de error. No se actualizará ninguna información.

  La disponibilidad de la clave `-use_ts` permite conservar 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`: Recupera datos del Servidor de administración. La recuperación de datos se realiza según la información incluida en la carpeta BACKUP_PATH. Si no hay ninguna clave disponible, se hace una copia de seguridad de los datos en la carpeta BACKUP_PATH.
- `-password PASSWORD`: Guarda o recupera el certificado del Servidor de administración. Para cifrar y descifrar el certificado, utilice la contraseña especificada por el parámetro PASSWORD.

  > Una contraseña olvidada no se puede recuperar. No hay requisitos para la contraseña. La longitud de la contraseña es ilimitada y también es posible la longitud cero (sin contraseña).

  Al restaurar datos, debe indicar la misma contraseña que se introdujo durante la creación de copias de seguridad. Si la ruta de una carpeta compartida cambió tras realizar la copia de seguridad, compruebe el funcionamiento de las tareas que utilizan datos restaurados (tareas de restablecimiento y tareas de instalación remota). Si fuera necesario, edite 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 con la que se inicia la utilidad klbackup debe tener total acceso a la carpeta compartida.
- `-online`: Hace una copia de seguridad de los datos del Servidor de administración, mediante la creación de una instantánea de volumen para minimizar el tiempo sin conexión del Servidor de administración. Cuando utiliza la utilidad para recuperar datos, esta opción se ignora.

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 base de datos a un nuevo dispositivo.
- Mantenga el servidor de 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 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 14 Web Console o ejecutar la utilidad klbackup.
2. Seleccione un nuevo dispositivo en el que 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 14 Web Console y Agente de red. Además, compruebe que están disponibles los puertos que se usan en el Servidor de administración.
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 nuevo dispositivo.

   Tenga en cuenta que si mueve el servidor de la base de datos al nuevo dispositivo, debe especificar la dirección local como la dirección IP del dispositivo en el que está instalada la base de datos (el elemento "h" en la instrucción Instalación de Kaspersky Security Center). 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 la instrucción Instalar Kaspersky Security Center.
5. Una vez completada la instalación, recupere los datos del Servidor de administración en el nuevo dispositivo mediante el 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 14 Web Console y conéctese al Servidor de administración.

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

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

Creación de un Servidor de administración virtual

Puede crear Servidores de administración virtuales y añadirlos a grupos de administración.

Para crear y añadir un Servidor de administración virtual:

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

2. En la página que se abre, vaya a la pestaña **Servidores de administración**.

3. Seleccione el grupo de administración al que quiere añadir el Servidor de administración virtual.
   El Servidor de administración virtual administrará los dispositivos del grupo seleccionado (incluidos los subgrupos).

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 especificar el nombre o la dirección IP de su 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**.

El nuevo Servidor de administración virtual se crea, se añade al grupo de administración y se muestra 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 añadir 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 configuración de conexión**.
  5. En la página **Servidores de administración de confianza**, añada el Servidor de administración secundario necesario.
  6. En la última página del Asistente, haga clic en **Modificar** para aplicar la nueva configuración.
  7. Después de que la reconfiguración de la aplicación se complete correctamente, haga clic en el botón **Terminar**.

- Use Kaspersky Security Center 14 Web Console para conectarse directamente al Servidor de administración secundario donde se ha creado 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 resultar incómodo administrar varios Servidores de administración independientes, por lo tanto, se puede aplicar una jerarquía.

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

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

- Un Servidor de administración secundario hereda directivas y tareas del Servidor de administración principal, lo que evita la copia de la configuración.
- Las selecciones de dispositivos en el Servidor de administración principal pueden incluir dispositivos de Servidores de administración secundarios.
- Los informes sobre el Servidor de administración principal pueden contener datos (incluida información detallada) de Servidores de administración secundarios.

Creación de una jerarquía de Servidores de administración: adición de un Servidor de administración secundario

Expandir todo | Contraer todo

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

Adición de un Servidor de administración secundario (operación realizada en el futuro Servidor de administración principal)

Puede añadir un Servidor de administración como Servidor de administración secundario y establecer así una jerarquía "principal/secundario".

Para añadir 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 icono 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 del Servidor de administración secundario de conexión.
6. En la primera página del Asistente, complete los siguientes campos:

   - **Nombre a mostrar del Servidor de administración secundario**

     Un nombre con el que se mostrará en la jerarquía el Servidor de administración secundario. Si lo desea, puede introducir la dirección IP como nombre, o puede usar un nombre como, por ejemplo, "Servidor secundario para el grupo 1".
   - **Dirección del Servidor de administración secundario (opcional)**

     Especifique 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 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 Servidor de administración principal a 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.

Cuando el Asistente concluye, se crea la jerarquía "principal/secundario". La conexión entre los Servidores de administración principal y secundario se establece a través del puerto 13000. Se reciben y aplican 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 añadió.

Adición de un Servidor de administración secundario (operación realizada en el futuro Servidor de administración secundario)

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

Para añadir en calidad de secundario un Servidor de administración que no esté disponible para conectarse mediante Kaspersky Security Center 14 Web Console, haga lo siguiente:

1. Envíe el archivo de certificado del futuro Servidor de administración principal al administrador del sistema de la oficina donde se encuentra el supuesto 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 icono de la **Configuración** ( ).

   b. En la página de propiedades que se abre, vaya a la sección **Jerarquía de Servidores de administración** de la pestaña **Control de aplicaciones**.

   c. Seleccione la opción **Este Servidor de administración es secundario en la jerarquía**.

   d. En el campo **Dirección del Servidor de administración principal**, especifique el nombre de la red del futuro Servidor de administración principal.

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

   f. Si es necesario, seleccione la casilla **Conectar Servidor de administración principal a 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**.

Se construye la jerarquía "principal/secundario". El Servidor de administración principal comienza recibiendo conexión de Servidor de administración secundario utilizando el puerto 13000. Se reciben y aplican 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 añadió.

Visualización de 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 ubicado junto al icono de **Configuración** ( ).

Se muestra la lista desplegable de los Servidores de administración secundarios (incluidos los virtuales).

Puede ir a cualquiera de estos Servidores de administración haciendo clic en su nombre.

Los grupos de administración también se muestran, pero están 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 añadir 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 configuración de conexión**.
5. En la página **Servidores de administración de confianza**, añada el Servidor de administración secundario necesario.
6. En la última página del Asistente, haga clic en **Modificar** para aplicar la nueva configuración.
7. Después de que la reconfiguración de la aplicación se complete correctamente, haga clic en el botón **Terminar**.

- Use Kaspersky Security Center 14 Web Console para conectarse directamente al Servidor de administración secundario donde se ha creado 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.

Activar la protección de la cuenta de modificaciones no autorizadas

Puede habilitar una opción adicional para proteger una cuenta de usuario de modificaciones no autorizadas. Si esta opción está activada, 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 la cuenta contra modificaciones no autorizadas:

1. Vaya a **USUARIOS Y FUNCIONES → USUARIOS**.
2. Haga clic en el nombre de la cuenta de usuario interna en la que desea especificar la protección de la cuenta frente a modificaciones no autorizadas.
3. En la ventana de configuración de usuario que se abre, seleccione la pestaña **Seguridad de la autenticación**.
4. En la pestaña **Seguridad de la autenticación**, seleccione la opción **Solicitar autenticación para verificar el permiso para modificar las cuentas de usuario** si desea solicitar credenciales cada vez que se cambia o modifica 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 usar 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 activar la verificación en dos pasos para todos los usuarios y cómo excluir las 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 activar la verificación en dos pasos para su propia cuenta.

Si habilitó la verificación en dos pasos para su cuenta, puede proceder a activar la verificación en dos pasos para todos los usuarios.

Requisitos previos

Antes de empezar:

- Asegúrese de que su cuenta de usuario tenga derechos de Modificar ACL de objeto del área funcional **Funciones 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 activación 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 única basada en tiempo.

2. **Sincronización de 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. **Activación de la verificación en dos pasos para su cuenta y recepción de la clave secreta de su cuenta**

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

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

   Los usuarios que tengan activada la verificación en dos pasos deben usarla para iniciar sesión en el Servidor de administración.

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

   Si tiene varios Servidores de administración con nombres similares, es posible que deba cambiar los nombres de los emisores del código de seguridad para reconocer mejor los diferentes Servidores de administración.

6. **Exclusión de las cuentas de usuario para las que no necesita activar la verificación en dos pasos**

   Si es necesario, puede excluir 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 queda activada para su cuenta.
- La verificación en dos pasos queda activada para todas las cuentas de usuario del Servidor de administración, excepto para las cuentas de usuario que fueron excluidas.

Acerca de la verificación en dos pasos de una cuenta

Kaspersky Security Center Linux proporciona verificación en dos pasos para los usuarios de Kaspersky Security Center 14 Web Console. Cuando la verificación en dos pasos está activada para su propia cuenta, cada vez que inicie sesión en Kaspersky Security Center 14 Web Console, debe introducir 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 un 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 un identificador del Servidor de administración en la aplicación de autenticación. Si cambia el nombre del emisor del código de seguridad, debe volver a 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 que tenga activada la verificación en dos pasos puede volver a emitir su propia clave secreta. Cuando un usuario se autentica con la clave secreta reemitida y la usa para iniciar sesión, el Servidor de administración guarda la nueva clave secreta de la cuenta de usuario. Si un usuario introduce la clave secreta de forma incorrecta al formulario de autenticación, el Servidor de administración no guarda la nueva clave secreta y conserva la validez de la clave secreta vigente para la autenticación posterior.

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

Insistimos en recomendarle que instale una aplicación de autenticación en más de un dispositivo móvil. Guarde la clave secreta (o el código QR) y conservelos en un lugar seguro. Esto le ayudará a restaurar el acceso a Kaspersky Security Center 14 Web Console si pierde el acceso a su dispositivo móvil.

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

Puede excluir cuentas de la verificación en dos pasos. Esto 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 según las siguientes reglas:

- Solo una cuenta de usuario que tenga los derechos Modificar objeto ACL en el área funcional **Funciones generales: Permisos de usuario** puede activar 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 activar la verificación en dos pasos solo para su propia cuenta.
- Una cuenta de usuario que tiene el derecho Modificar las LCA de objetos en el área funcional **Características generales: permisos de usuario** y está conectado a Kaspersky Security Center 14 Web Console mediante la verificación en dos pasos puede deshabilitar la verificación en dos pasos: a) para cualquier otro usuario solo si la verificación en dos pasos para todos los usuarios está deshabilitada; b) para un usuario excluido de la lista de verificación en dos pasos que esté 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 para el Servidor de administración con el que está trabajando en un momento dado. Si activa esta opción en el Servidor de administración, también activa esta opción para las cuentas de usuario de sus Servidores de administración virtuales y no activa la verificación en dos pasos para las cuentas de usuario de los Servidores de administración secundarios.

Si la verificación en dos pasos está activada para una cuenta de usuario en el Servidor de administración de Kaspersky Security Center versión 13 o posterior, el usuario no podrá conectarse a las versiones 12, 12.1 o 12.2 de Kaspersky Security Center Web Console.

Activar la verificación en dos pasos para su propia cuenta

Puede activar la verificación en dos pasos solo para su propia cuenta.

Antes de empezar a activar la verificación en dos pasos para su cuenta, asegúrese de 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 se instaló el Servidor de administración.

Para activar la verificación en dos pasos en una cuenta de usuario:

1. Vaya a **USUARIOS Y FUNCIONES → USUARIOS**.
2. Haga clic en el nombre de su cuenta.
3. En la ventana de configuración de usuario que se abre, seleccione la pestaña **Protección de cuenta**.
4. En la pestaña **Protección de cuenta**:
   - 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, introduzca la clave secreta en la aplicación de autenticación o escanee el código QR y reciba un código de seguridad por única vez.

       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 luego haga clic en el botón **Comprobar y aplicar**.
5. Haga clic en el botón **Guardar**.

La verificación en dos pasos queda activada para su cuenta.

Activación de la verificación en dos pasos para todos los usuarios

Puede activar la verificación en dos pasos para todos los usuarios del Servidor de administración si su cuenta tiene el derecho Modificar ACL de objetos en el área funcional **Funciones generales: Permisos de usuario** y si está autenticado mediante 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 propia cuenta.

Para activar la verificación en dos pasos para todos los usuarios:

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

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Seguridad de la autenticación** de la ventana de propiedades, deslice el botón de alternancia de la opción **verificación en dos pasos para todos los usuarios** a la posición "activada".

La verificación en dos pasos queda activada para todos los usuarios. A partir de ahora, los usuarios del Servidor de administración, incluidos los usuarios que se agregaron después de activar la verificación en dos pasos, tienen que configurar la verificación en dos pasos para sus cuentas. La excepción son los usuarios cuyas cuentas estén excluidas de la verificación en dos pasos.

Desactivación de la verificación en dos pasos de una cuenta de usuario

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

Puede desactivar la verificación en dos pasos de la cuenta de otro usuario si su cuenta tiene el derecho Modificar LCA de objeto del área funcional **Características generales: Permisos de usuario**.

Para desactivar la verificación en dos pasos de una cuenta de usuario:

1. Vaya a **USUARIOS Y FUNCIONES → USUARIOS**.
2. Haga clic en el nombre de la cuenta de usuario interno para la que desea desactivar la verificación en dos pasos. Esta puede ser su propia cuenta o la cuenta de cualquier otro usuario.
3. En la ventana de configuración de usuario que se abre, seleccione la pestaña **Protección de cuenta**.
4. En la pestaña **Protección de cuenta**, seleccione la opción **Solicitar solo nombre de usuario y contraseña** si desea desactivar la verificación en dos pasos para una cuenta de usuario.
5. Haga clic en el botón **Guardar**.

La verificación en dos pasos queda desactivada para la cuenta de usuario.

Desactivar la verificación en dos pasos para todos los usuarios

Puede desactivar la verificación en dos pasos para todos los usuarios si la verificación en dos pasos está activada para su cuenta y su cuenta tiene el derecho Modificar LCA de objetos en el área funcional **Características generales: permisos de usuario**. Si la verificación en dos pasos no está habilitada para su cuenta, debe activar la verificación en dos pasos para su cuenta antes de desactivarla para todos los usuarios.

Para desactivar la verificación en dos pasos para todos los usuarios:

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

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Seguridad de la autenticación** de la ventana de propiedades, deslice el botón de alternancia de la opción **verificación en dos pasos para todos los usuarios** a la posición "desactivada".
3. Introduzca las credenciales de su cuenta en la ventana de autenticación.

La verificación en dos pasos queda desactivada para todos los usuarios.

Exclusión de cuentas de la verificación en dos pasos

Puede excluir cuentas de usuario de la verificación en dos pasos si tiene el derecho Modificar LCA 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 desea excluir algunas cuentas de usuario de la verificación en dos pasos, haga lo siguiente:

1. En la ventana principal de la aplicación, haga clic en el icono de **Configuración** () junto al nombre del Servidor de administración requerido.
   Se abre la ventana Propiedades del Servidor de administración.
2. En la pestaña **Seguridad de la autenticación** de la ventana de propiedades, en la tabla de exclusiones de la verificación de dos pasos, haga clic en el botón **Añadir**.
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 mediante la verificación en dos pasos.

Para generar una nueva clave secreta para una cuenta de usuario, haga lo siguiente:

1. Vaya a **USUARIOS Y FUNCIONES → 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 de configuración de usuario que se abre, seleccione la pestaña **Protección de cuenta**.
4. En la pestaña **Protección de cuenta**, haga clic en el enlace **Generar una nueva clave secreta**.
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 **Comprobar 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.

Modificar el nombre de un emisor del código de seguridad

Puede tener varios identificadores (se denominan emisores) para diferentes Servidores de administración. Puede cambiar el nombre de un emisor de código de seguridad en el caso de que, por ejemplo, el Servidor de administración ya utilice un nombre similar de emisor de código de seguridad para otro Servidor de administración. De forma predeterminada, el nombre del emisor del código de seguridad es el mismo que el del Servidor de administración.

Después de cambiar el nombre del emisor del código de seguridad, debe 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:

1. En la ventana principal de la aplicación, haga clic en el icono de **Configuración** () junto al nombre del Servidor de administración requerido.
   Se abre la ventana Propiedades del Servidor de administración.
2. En la ventana de configuración de usuario que se abre, seleccione la pestaña **Protección de cuenta**.
3. En la pestaña **Protección de cuenta**, haga clic en el enlace **Editar**.
   Se abre la sección **Editar emisor del código de seguridad.**
4. Especifique el nuevo nombre de emisor de código de seguridad.
5. Haga clic en el botón **Aceptar**.

Se especifica un nuevo nombre de emisor de 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. Para la utilidad klscflag, ejecute el siguiente comando:

   ```
   sudo /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n SrvSplPpcLogonAttempts -t d -v N
   ```

   donde N es el 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.

Cambiar las credenciales de DBMS

A veces, es posible que 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 la utilidad 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 la DBMS.
4. Introduzca una nueva contraseña.
5. Especifique la nueva contraseña para su confirmación.

Se cambian las credenciales de la DBMS.

Eliminación de una jerarquía de Servidores de administración

Si ya no desea tener una jerarquía de Servidores de administración, puede desconectarlos de esta jerarquía.

Para eliminar una jerarquía de Servidores de administración:

1. En la parte superior de la pantalla, haga clic en el icono de la **Configuración** ( ) al lado del nombre del Servidor de administración principal.
2. En la página que se abre, vaya a la pestaña **Servidores de administración**.
3. En el grupo de administración del que desea eliminar el Servidor de administración secundario, seleccione el Servidor de administración secundario.
4. En la línea del menú, haga clic en **Eliminar**.
5. En la ventana que se abre, haga clic en **Aceptar** para eliminar el Servidor de administración secundario.

El Servidor de administración principal anterior y el Servidor de administración secundario anterior ahora son independientes el uno del otro. La jerarquía ya no existe.

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 de acuerdo con el conjunto de funciones utilizado actualmente:

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 necesarias.

4. Hacer clic en **Guardar**.

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

Detección de dispositivos en red

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

Kaspersky Security Center permite encontrar dispositivos según los criterios especificados. Puede guardar los resultados de la búsqueda 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: Detección de dispositivos en red

Debe realizar la detección de dispositivos antes de instalar las aplicaciones de seguridad. Cuando se detecten todos los dispositivos en red, puede obtener información sobre ellos y administrarlos a través de directivas. Se necesitan sondeos de red regulares para detectar si hay dispositivos nuevos y si los dispositivos detectados todavía están en la red.

La detección de dispositivos en red se realiza en etapas:

1. **Detección inicial de dispositivos**

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

2. **Configuración de futuros sondeos**

   Asegúrese de que Sondeo de rangos IP esté activado 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 Sondeo de configuración cero si su red incluye dispositivos IPv6.

3. **La configuración de reglas para agregar dispositivos detectados a grupos de administración (opcional)**

   Si aparecen nuevos dispositivos de la red, que se detectan durante las sondeos 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 configurar reglas de retención.

   Si omite este paso que configura la regla, todos los dispositivos recién detectados van al grupo **Dispositivos no asignados** y se quedan allí. Si lo desea, puede mover estos dispositivos al grupo de **Dispositivos administrados** manualmente. Si mueve estos 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

Al completar el escenario se obtienen 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 rangos IP

Expandir todo | Contraer todo

Kaspersky Security Center intenta realizar una resolución de nombres inversa para cada dirección IPv4 desde el rango especificado a un nombre de DNS usando solicitudes de DNS estándar. Si esta operación se realiza correctamente, el servidor envía una `ICMP ECHO REQUEST` (comando similar a "ping") al nombre recibido. Si el dispositivo responde, la información se añade a la base de datos de Kaspersky Security Center. La resolución de nombres inversa es necesaria para excluir los dispositivos de red que pueden tener una dirección IP pero no son equipos, por ejemplo, impresoras o rúteres.

Este método de sondeo se basa en un servicio DNS local configurado correctamente. Debe tener una zona de búsqueda inversa. Si esta zona no está configurada, el sondeo de subred 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 activado el sondeo de rangos de IP, Kaspersky Security Center detecta dispositivos solo con direcciones IPv4. Si su red incluye dispositivos IPv6, active el Sondeo de configuración cero de dispositivos

Visualización y modificación de los parámetros para el sondeo de rangos IP

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

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

   Se abrirá la ventana de propiedades de sondeo de IP.
3. Habilite o deshabilite el sondeo de IP con el botón de activación **Permitir sondeo**.
4. Configurar la programación del sondeo. De forma predeterminada, el sondeo IP se ejecuta cada 420 minutos (siete horas).

   Al especificar el intervalo de sondeo, asegúrese de que esta configuración no exceda el valor del parámetro de duración de la dirección IP. Si una dirección IP no se verifica mediante sondeo durante el tiempo de vida de la dirección IP, esta dirección IP se eliminará automáticamente de los resultados del sondeo. De forma predeterminada, la vida útil de los resultados del sondeo es de 24 horas, porque las direcciones IP dinámicas (asignadas mediante el Protocolo de configuración dinámica de host (DHCP)) cambian cada 24 horas.

   Opciones de planificación de sondeo:

   - **Cada N días**

     El sondeo se ejecuta regularmente, con el intervalo especificado en días, a partir de la fecha y la hora especificadas.

     De forma predeterminada, el sondeo se ejecuta cada día, a partir de la fecha y la hora actuales del sistema.
   - **Cada N minutos**

     El sondeo se ejecuta regularmente, con el intervalo especificado en minutos, a partir de la fecha y la hora especificadas.
   - **Por días de la semana**

     El sondeo se ejecuta regularmente, en los días especificados de la semana y en el momento especificado.
   - **Cada mes, en días concretos de las semanas seleccionadas**

     El sondeo se realiza regularmente, en los días especificados de cada mes y en el momento especificado.
   - **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 que se encienda o esperar el siguiente sondeo programado.

     Si esta opción está activada, el Servidor de administración inicia el sondeo inmediatamente después de encenderse.

     Si esta opción está desactivada, el Servidor de administración espera el siguiente sondeo programado.

     Esta opción está desactivada de forma predeterminada.
5. Haga clic en el botón **Guardar**.

Las propiedades se guardan y se aplican a todos los rangos de IP.

Ejecución manual de la encuesta

Para ejecutar la encuesta de inmediato,

haga clic en **Iniciar sondeo**.

Adición y modificación de un rango 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 rangos de IP definidos automáticamente o añadir rangos de IP personalizados.

Puede crear un rango Solo para direcciones IPv4. Si activa el Sondeo de Zeroconf, Kaspersky Security Center sondeará toda la red.

Para agregar un nuevo rango de IP:

1. Vaya a **DETECCIÓN Y DESPLIEGUE → DETECCIÓN → RANGOS IP**.
2. Para añadir un nuevo rango IP, haga clic en el botón **Añadir**.
3. En la ventana que se abre, especifique la siguiente configuración:
   - **Nombre del rango IP**

     Un nombre del rango IP. Es posible que desee especificar el rango IP como su nombre, 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 (horas)**

     Al especificar este parámetro, asegúrese de que exceda el intervalo de sondeo establecido en el programa de sondeo. Si una dirección IP no se verifica mediante sondeo durante el tiempo de vida de la dirección IP, esta dirección IP se eliminará automáticamente de los resultados del sondeo. De forma predeterminada, la vida útil de los resultados del sondeo es de 24 horas, porque las direcciones IP dinámicas (asignadas mediante el Protocolo de configuración dinámica de host, DHCP) cambian cada 24 horas.
4. Seleccione **Activar sondeos de rangos IP** si desea sondear la subred o el intervalo que ha añadido. De lo contrario, la subred o el intervalo que ha añadido no se sondearán.
5. Haga clic en el botón **Guardar**.

El nuevo rango IP se agrega a la lista de rangos IP.

Puede ejecutar el sondeo de cada rango IP por separado usando el botón **Iniciar sondeo**. Cuando se completa el sondeo, puede ver la lista de dispositivos descubiertos utilizando el botón **Dispositivos**. De forma predeterminada, la vida útil de los resultados del sondeo es de 24 horas y es igual a la configuración de duración de la dirección IP.

Para agregar una subred a un rango IP existente:

1. Vaya a **DETECCIÓN Y DESPLIEGUE → DETECCIÓN → RANGOS IP**.
2. Haga clic en el nombre del rango de IP al que desea agregar una subred.
3. En la ventana que se abre, haga clic en el botón **Añadir**.
4. Especifique una subred usando su dirección y máscara o usando la primera y la última dirección IP en el rango IP. O, añada 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 añadir tantas subredes como necesite. Los rangos IP con nombre no pueden superponerse pero las subredes sin nombre dentro de un rango IP no tienen tales restricciones. Puede habilitar y deshabilitar el sondeo de forma independiente para cada rango IP.

Sondeo de Zeroconf

Este tipo de sondeo solo es compatible con los puntos de distribución basados en Linux.

Kaspersky Security Center puede sondear 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, ya sea el Servidor de administración o un punto de distribución.

Para activar el sondeo de Zeroconf:

1. Vaya a **DETECCIÓN Y DESPLIEGUE → DETECCIÓN → RANGOS IP**.
2. Haga clic en el botón **Propiedades**.
3. En la ventana abierta, active el botón **Usar Zeroconf para sondear las redes IPv6**.

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

Etiquetas del dispositivo

Esta sección describe las etiquetas de dispositivos y proporciona instrucciones para crearlas y modificarlas, así como para etiquetar dispositivos de forma manual o automática.

Acerca de las etiquetas del dispositivo

Kaspersky Security Center permite que usted *etiquete* dispositivos. Una etiqueta es un identificador de un dispositivo que se puede utilizar para agrupar, describir o encontrar dispositivos. Las etiquetas asignadas a dispositivos se pueden utilizar para crear selecciones, para encontrar dispositivos y para distribuir dispositivos entre grupos de administración.

Puede etiquetar dispositivos manualmente o automáticamente. Puede utilizar el etiquetado manual cuando desee etiquetar un dispositivo particular. Kaspersky Security Center realiza el etiquetado automático de acuerdo con las reglas de etiquetado especificadas.

Los dispositivos se etiquetan automáticamente cuando las reglas especificadas se cumplen. Una regla particular equivale a cada etiqueta. Las reglas se aplican a las propiedades de la red del dispositivo, sistema operativo, aplicaciones instaladas en el dispositivo y otras propiedades del dispositivo. Por ejemplo, puede configurar una regla que asignará la etiqueta `[CentOS]` a todos los dispositivos con el sistema operativo CentOS. A continuación, puede usar esta etiqueta al crear una selección de dispositivos. Esto le ayudará a clasificar todos los dispositivos CentOS y a asignarles una tarea.

Una etiqueta se elimina automáticamente desde un dispositivo en los siguientes casos:

- Cuando el dispositivo deja de cumplir las condiciones de la regla que asigna la etiqueta.
- Cuando la regla que asigna la etiqueta se desactiva o elimina.

La lista de etiquetas y la lista de reglas de cada Servidor de administración son independientes de todos los demás Servidores de administración, incluido un Servidor de administración principal o Servidores de administración virtuales subordinados. Una regla se aplica solo a los dispositivos del mismo Servidor de administración en el que se crea la regla.

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 **Añadir**.
   Una nueva ventana de etiqueta se abre.
3. En el campo **Etiqueta**, escriba un nombre de 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 renombrar una etiqueta del dispositivo:

1. En el menú principal, vaya a **DISPOSITIVOS → ETIQUETAS → ETIQUETAS DEL DISPOSITIVO**.
2. Haga clic en el nombre de la etiqueta que desea renombrar.
   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 del dispositivo.

Eliminar una etiqueta de dispositivo

Eliminar una etiqueta del dispositivo:

1. En el menú principal, vaya a **DISPOSITIVOS → ETIQUETAS → ETIQUETAS DEL DISPOSITIVO**.
2. En la lista, seleccione el botón de opción junto a la etiqueta del dispositivo que desea eliminar.
3. Haga clic en el botón **Eliminar**.
4. En la ventana que se abre, haga clic en **Sí**.

Se elimina la etiqueta del dispositivo. La etiqueta eliminada se elimina automáticamente de todos los dispositivos a los que fue asignada.

> La etiqueta que eliminó se elimina automáticamente de las reglas de etiquetado automático. Después de eliminar la etiqueta, se asignará a un nuevo dispositivo solo cuando el dispositivo cumpla las condiciones de una regla que asigne la etiqueta.

Visualización de dispositivos a los que se asigna una etiqueta

Para ver los dispositivos a los que se asigna una etiqueta:

1. En el menú principal, vaya a **DISPOSITIVOS → ETIQUETAS → ETIQUETAS DEL DISPOSITIVO**.
2. Haga clic en el enlace **Ver dispositivos** al lado de la etiqueta para la cual desea ver los dispositivos asignados.
   Si no ve el enlace **Ver dispositivos** al lado de una etiqueta, la etiqueta no se asigna a ningún dispositivo.

La lista de dispositivos que aparece muestra solo los dispositivos a los que se asigna la etiqueta.

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

Visualización de etiquetas asignadas a un dispositivo

Para visualizar etiquetas asignadas a un dispositivo:

1. En el menú principal, vaya a **DISPOSITIVOS → DISPOSITIVOS ADMINISTRADOS**.
2. Haga clic en el nombre de la directiva cuyos etiquetas desea ver.
3. En la ventana de propiedades del dispositivo que se abre, seleccione la pestaña **Etiquetas**.

Se muestra la lista de etiquetas asignadas al dispositivo seleccionado.

Puede asignar otra etiqueta al dispositivo o eliminar una etiqueta ya asignada. También puede ver todas las etiquetas del dispositivo que existen en el Servidor de administración.

Etiquetar un dispositivo manualmente

Para asignar una etiqueta a un dispositivo manualmente:

1. Ver las etiquetas asignadas al dispositivo al que desea eliminar una etiqueta.
2. Haga clic en **Añadir**.
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 después especifique el nombre de la nueva etiqueta.
   - Para seleccionar una etiqueta existente, seleccione **Asignar etiqueta existente** y después seleccione la etiqueta necesaria en la lista desplegable.
4. Haga clic en **Correcto** para aplicar los cambios.

5. Haga clic en **Guardar** para guardar los cambios.

La etiqueta seleccionada está asignada al dispositivo.

Eliminación de una etiqueta asignada de un dispositivo

Para eliminar una etiqueta del dispositivo:

1. Vea las etiquetas asignadas al dispositivo al que desea eliminar una etiqueta.
2. Seleccione la casilla al lado de las etiquetas que desea eliminar.
3. Haga clic en el botón **Desasignar etiqueta**.
4. En la ventana que se abre, haga clic en **Sí**.

La etiqueta se elimina del dispositivo.

> La etiqueta del dispositivo no asignado no se elimina. Si lo desea, puede borrarlo manualmente.

Visualización de reglas de etiquetado automático de dispositivos

Para visualizar las reglas para etiquetar dispositivos automáticamente,

Realice una 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**.

Aparece la lista de reglas para los dispositivos de etiquetado automático.

Modificación de una regla de etiquetado automático de dispositivos

Para editar una regla para etiquetar dispositivos automáticamente:

1. Vea las reglas de etiquetado automático en dispositivos.
2. Haga clic en el nombre de la etiqueta que desea editar.
   Se abrirá una ventana de configuración de reglas.
3. Editar las propiedades generales de la regla:
   a. En el campo **Nombre de la regla**, cambie el nombre de regla.
      El nombre no puede tener más de 256 caracteres.
   b. Realice una de las siguientes acciones:
      - Habilite la regla cambiando el botón de activación a **Regla activada**.
      - Deshabilite la regla cambiando el botón de activación a **Regla desactivada**.
4. Realice una de las siguientes acciones:
   - Si desea agregar una nueva condición, haga clic en el botón **Añadir** y especifique la configuración de la nueva condición en la ventana que se abre.
   - Si desea editar una condición existente, haga clic en el nombre de la condición que desea editar y luego edite la configuración de la condición.
   - Si desea eliminar una condición, seleccione la casilla de verificación al lado del nombre de la condición que desea eliminar, y luego haga clic en **Eliminar**.
5. Haga clic en **Aceptar** en la ventana de configuración de las condiciones.
6. Haga clic en **Guardar** para guardar los cambios.

La regla editada se muestra en la lista.

Creación de una regla de etiquetado automático de dispositivos

Para crear una regla de etiquetado automático en dispositivos:

1. Vea las reglas de etiquetado automático en dispositivos.
2. Haga clic en **Añadir**.

   Se abre una nueva ventana de configuración de regla.
3. Configure las propiedades generales de la regla:

   a. En el campo **Nombre de la regla**, introduzca un nombre de regla.

   El nombre no puede tener más de 256 caracteres.

   b. Realice una de las siguientes acciones:

   - Habilite la regla cambiando el botón de activación a **Regla activada**.
   - Deshabilite la regla cambiando el botón de activación a **Regla desactivada**.

   c. En el campo **Etiqueta**, introduzca el nuevo nombre de etiqueta del dispositivo o seleccione una de las etiquetas del dispositivo existentes en la lista.

   El nombre no puede tener más de 256 caracteres.
4. En la sección de condiciones, haga clic en el botón **Añadir** para añadir una nueva condición.

   Se abre una nueva ventana de configuración de condiciones.
5. Introduzca el nombre de la condición.

   El nombre no puede tener más de 256 caracteres. El nombre debe ser único en una regla.
6. Configure la activación de la regla de acuerdo con las condiciones siguientes. Puede seleccionar varias condiciones.

   - **Red**: Propiedades de red del dispositivo, como el nombre DNS del dispositivo o la inclusión del dispositivo en una subred IP.
   - **Aplicaciones**: Presencia del Agente de red en el dispositivo, tipo del sistema operativo, versión y arquitectura.
   - **Máquinas virtuales**: El dispositivo pertenece a un tipo concreto de máquina virtual.
   - **Registro de aplicaciones**: Presencia de aplicaciones de proveedores diferentes en el dispositivo.
7. Haga clic en **Aceptar** para guardar los cambios.

   Si es necesario, puede establecer varias condiciones para una sola regla. En este caso, la etiqueta se asignará a un dispositivo si cumple al menos una condición.
8. Haga clic en **Guardar** para guardar los cambios.

Las regla recién creada se hace cumplir en dispositivos administrados por el Servidor de administración seleccionado. Si la configuración de un dispositivo cumple las condiciones de la regla, se asigna la etiqueta al dispositivo.

Más adelante, la regla se aplica en los siguientes casos:

- Automática y periódicamente, según la cantidad de trabajo del servidor.
- Después de que edite la regla.
- Cuando ejecute la regla manualmente.
- Después de que el Servidor de administración detecte un cambio en la configuración de un dispositivo que cumpla las condiciones de la regla o la configuración de un grupo que contenga dicho dispositivo.

Puede crear varias reglas de etiquetado. Pueden asignarse varias etiquetas a un solo dispositivo si ha creado varias reglas de etiquetado y si las condiciones respectivas de estas reglas se cumplen simultáneamente. Puede ver la lista de todas las etiquetas asignadas en las propiedades del dispositivo.

Ejecución de reglas de etiquetado automático de dispositivos

Cuando se ejecuta una regla, la etiqueta especificada en las propiedades de esta regla se asigna a los dispositivos que cumplen con las condiciones especificadas en las propiedades de la misma regla. Solo puede ejecutar reglas activas.

Para ejecutar reglas para dispositivos de etiquetado automático:

1. Vea las reglas de etiquetado automático en dispositivos.
2. Seleccione las casillas de verificación junto a las reglas activas que desea ejecutar.
3. Haga clic en el botón **Ejecutar regla**.

Se ejecutan las reglas seleccionadas.

Eliminación de una regla de etiquetado automático de dispositivos

Para eliminar una regla para etiquetar dispositivos automáticamente:

1. Vea las reglas de etiquetado automático en dispositivos.
2. Seleccione la casilla de verificación al lado de las etiquetas que desea eliminar.
3. Haga clic en **Eliminar**.
4. En la ventana que se abre, haga clic de nuevo en **Eliminar**.

Se eliminar la regla seleccionada. La etiqueta que se especificó en las propiedades de esta regla no está asignada a todos los dispositivos a los que fue asignada.

La etiqueta del dispositivo no asignado no se elimina. Si lo desea, puede borrarlo manualmente.

Etiquetas de aplicaciones

Esta sección describe las etiquetas de aplicaciones y proporciona instrucciones para crearlas y modificarlas, así como para etiquetar aplicaciones de terceros.

Acerca de las etiquetas de aplicación

Kaspersky Security Center Linux le permite etiquetar aplicaciones de terceros (aplicaciones creadas por vendedores de software diferentes a Kaspersky). Una etiqueta es la etiqueta de una aplicación que puede ser utilizada para agrupar o encontrar aplicaciones. Una etiqueta asignada a las aplicaciones puede servir como una condición en las selecciones de dispositivos.

Por ejemplo, puede crear la etiqueta `[Navegadores]` y asignar a todos los navegadores, como Microsoft Internet Explorer, Google Chrome, Mozilla Firefox.

Creación de una etiqueta de aplicación

Creación de una categoría de aplicación:

1. En el menú principal, vaya a **OPERACIONES → APLICACIONES DE TERCEROS → ETIQUETAS DE LA APLICACIÓN**.
2. Haga clic en **Añadir**.
   Una nueva ventana de etiqueta se abre.
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.

Renombramiento de una etiqueta de aplicación

Para renombrar una etiqueta de aplicación:

1. En el menú principal, vaya a **OPERACIONES → APLICACIONES DE TERCEROS → ETIQUETAS DE LA APLICACIÓN**.
2. Seleccione la casilla de verificación junto a la etiqueta que quiere renombrar 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 aplicaciones.

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 desea asignar etiquetas.
3. Seleccione la pestaña **Etiquetas**.

   La pestaña muestra todas las etiquetas de aplicación que existen en el Servidor de administración. Para etiquetas asignadas a la aplicación seleccionada, la casilla de verificación en la columna **Etiqueta asignada** está seleccionada.
4. Para etiquetas que quiera asignar, seleccione las casillas de verificación en la columna **Etiqueta asignada**.
5. Haga clic en **Guardar** para guardar los cambios.

Las etiquetas están asignadas a la aplicación.

Eliminación de etiquetas asignadas desde una aplicación

Para eliminar una o varias etiquetas de 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 de la que desea eliminar etiquetas.
3. Seleccione la pestaña **Etiquetas**.

   La pestaña muestra todas las etiquetas de aplicación que existen en el Servidor de administración. Para etiquetas asignadas a la aplicación seleccionada, la casilla de verificación en la columna **Etiqueta asignada** está seleccionada.
4. Para etiquetas que quiera eliminar, quite la selección de las casillas de verificación en la columna **Etiqueta asignada**.
5. Haga clic en **Guardar** para guardar los cambios.

Las etiquetas se retiran de la aplicación.

Las etiquetas de aplicación retiradas 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 LA APLICACIÓN**.
2. En la lista, seleccione la etiqueta de la aplicación que quiere eliminar.
3. Haga clic en el botón **Eliminar**.
4. En la ventana que se abre, haga clic en **Aceptar**.

Se elimina la etiqueta de la aplicación. La etiqueta eliminada se elimina automáticamente de todas las aplicaciones a las que fue asignada.

Despliegue de las aplicaciones de Kaspersky

Esta sección describe cómo desplegar aplicaciones de Kaspersky en dispositivos cliente de su organización por medio de Kaspersky Security Center 14 Web Console.

Escenario: despliegue de aplicaciones de Kaspersky

Este escenario explica cómo desplegar aplicaciones de Kaspersky mediante 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 realiza en etapas:

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

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

2. **Descargar y crear paquetes de instalación para Agente de red**

   Descargue el paquete de distribución del Agente de red desde el sitio web de Kaspersky, y luego cree 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 el 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 cree un paquete de instalación de Kaspersky Endpoint Security para Linux.

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

   Si no puede instalar las aplicaciones de Kaspersky mediante Kaspersky Security Center Linux en algunos dispositivos, (por ejemplo, en dispositivos de empleados remotos) 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 descritas a continuación.

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

   Este paso forma parte del Asistente de despliegue de la protección. 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 se hayan detectado todos los dispositivos en su red; a continuación, ejecute la tarea (o tareas) de instalación remota.

   > Si desea instalar Agente de red en dispositivos con el sistema operativo SUSE Linux Enterprise Server 15, instale el paquete insserv-compat primero para configurar el Agente de red.

6. **Creación y configuración de tareas**

   La tarea *Instalar actualización* de Kaspersky Endpoint Security for 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. **Creación de directivas**

   Cree la política para Kaspersky Endpoint Security for Linux de forma manual 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 el despliegue se completó correctamente: tiene directivas y tareas para cada aplicación y estas aplicaciones están instaladas en los dispositivos administrados.

Resultados

Al completar el escenario se obtienen 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 para aplicaciones de Kaspersky

Para desplegar una aplicación Kaspersky, como Kaspersky Endpoint Security for Linux, debe añadir e instalar el complemento de administración de la aplicación.

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

1. Descargue el complemento web de administración para Kaspersky Endpoint Security para Linux del sitio web de Kaspersky.

2. Abra 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 **Añadir desde archivo**.

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

   Kaspersky Security Center verifica los archivos cargados y luego añade e instala el complemento web.
10. Cuando la instalación se haya completado, haga clic en **Aceptar**.

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

Crear paquetes de instalación a partir de un archivo

Puede utilizar paquetes de instalación personalizada para hacer lo siguiente:

- Para instalar cualquier aplicación (como un editor de texto) en un dispositivo cliente, por ejemplo, mediante una tarea.
- Para crear un paquete de instalación independiente.

Un paquete de instalación personalizada es una carpeta con un conjunto de archivos. La fuente para crear un paquete de instalación personalizada es un *archivo de almacenamiento*. El archivo de almacenamiento contiene un archivo o archivos que deben incluirse en el paquete de instalación personalizada.

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 personalizada:

1. Realice una de las siguientes acciones:
   - Vaya a **DETECCIÓN 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 **Añadir**.

   Se inicia el Asistente de nuevo paquete. Avance a través del Asistente utilizando el botón **Siguiente**.
3. En la primera página del Asistente, seleccione la opción **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 desde un archivo SFX (archivo autoextraíble).

   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) de la aplicación. Para continuar, debe aceptar el EULA. Seleccione la opción **Aceptar los términos y las 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. Seleccionar la opción **Acepto la Política de privacidad** solo si entiende y está de acuerdo con que sus datos serán manejados y transmitidos (incluso a terceros países) como se describe en la Política de privacidad.
7. En la página siguiente del Asistente, seleccione un archivo (de la lista de archivos extraídos del archivo de almacenamiento seleccionado) 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 informa cuando finaliza 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. Después de la descarga, el paquete de instalación aparece 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 enlace 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 empaquetada en el paquete de instalación personalizado.
  - **Versión**. Versión de la aplicación.
  - **Idioma**. Idioma de la aplicación empaquetada en 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 del paquete de instalación.
- Cambie los parámetros de la línea de comandos.

Crear 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 usted puede almacenar en el servidor web, en una carpeta compartida, enviar por correo electrónico o transferir al dispositivo cliente de otra manera. En el dispositivo cliente, el usuario puede ejecutar el archivo recibido localmente para instalar una aplicación sin utilizar Kaspersky Security Center Linux. Puede crear paquetes de instalación independientes de aplicaciones de Kaspersky y de aplicaciones de terceros. Para crear un paquete de instalación independiente para una aplicación de terceros, debe crear un paquete de instalación personalizada.

Asegúrese de que el paquete de instalación independiente no esté disponible para terceras personas.

Para crear un paquete de instalación independiente:

1. Realice una de las siguientes acciones:
   - Vaya a **DETECCIÓN 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, encima de la lista, haga clic en el botón **Desplegar**.
3. Seleccione la opción **Mediante un paquete independiente**.

   Se inicia el Asistente para crear paquete de instalación independiente. Avance a través del Asistente utilizando el botón **Siguiente**.
4. En la primera página del Asistente, asegúrese de seleccionar la opción **Instalar Agente de red junto con esta aplicación** si desea instalar el Agente de red junto con la aplicación seleccionada.

   Esta opción está activada de forma predeterminada. Le recomendamos que active 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 desactiva esta opción, el Agente de red no se instalará en el dispositivo y este quedará no administrado.

Si la aplicación seleccionada ya cuenta con un paquete de instalación independiente en el Servidor de administración, el Asistente se lo informa. En este caso, debe seleccionar una de las siguientes acciones:

- **Crear un paquete de instalación independiente**. Seleccione esta opción, por ejemplo, si desea crear un paquete de instalación independiente para una nueva versión de la aplicación y también conservar un paquete de instalación independiente que haya creado para una versión de la aplicación anterior. El nuevo paquete de instalación independiente se ubicará en otra carpeta.
- **Utilizar paquete de instalación independiente existente**. Seleccione esta opción si desea utilizar un paquete de instalación independiente existente. El proceso para crear paquetes no se iniciará.
- **Crear de nuevo un paquete de instalación independiente existente**. 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 del Asistente **Mover a lista de dispositivos administrados**, la opción **No mover dispositivos** está seleccionada de forma predeterminada. Si no desea mover el dispositivo cliente a ningún grupo de administración después de la instalación del Agente de red, no cambie la selección de la opción.

   Si desea mover los dispositivos cliente después de la instalación del Agente de red, seleccione la opción **Mover dispositivos no asignados a este grupo** y especifique el grupo de administración al que desea mover el dispositivo cliente. De manera predeterminada, el dispositivo se mueve al grupo de **Dispositivos administrados**.

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

   Asistente para crear 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 encima de la lista de paquetes de instalación.

Ver la lista de paquetes de instalación independientes

Puede ver la lista de paquetes de instalación independiente y las propiedades de cada paquete de instalación independiente.

Para ver la lista de paquetes de instalación independientes para todos los paquetes de instalación:

Encima de la lista, haga clic en el botón **Ver la lista de paquetes independientes**.

En la lista de paquetes de instalación independientes, se muestran las siguientes propiedades:

- **Nombre del paquete**. Nombre del paquete de instalación independiente que se forma automáticamente como el nombre de la aplicación incluida en el paquete y la versión de la aplicación.
- **Nombre de la aplicación**. 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 solo si el Agente de red está incluido en el paquete de instalación independiente.
- **Versión del Agente de red**. La propiedad se muestra solo si el Agente de red está incluido en el paquete de instalación independiente.
- **Tamaño**. Tamaño de RAM, 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 la creación del paquete de instalación independiente.
- **Modificado**. Fecha y hora de la modificación del paquete de instalación independiente.
- **Ruta**. Ruta completa a la carpeta donde se ubica el paquete de instalación independiente.
- **Dirección web**. Dirección web de la ubicación del paquete de instalación independiente.
- **Archivo hash**. La propiedad se utiliza para certificar que el paquete de instalación independiente no fue modificado por terceros 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 determinados paquetes de instalación:

Seleccione el paquete de instalación en la lista y, encima de esta, haga clic en el botón **Ver la lista de paquetes independientes**.

En la lista de paquetes de instalación independientes puede:

- Publicar un paquete de instalación independiente en el servidor web si hace clic en el botón **Publicar**. El paquete de instalación independiente publicado queda disponible para que lo descarguen los usuarios a quienes ha enviado el enlace a dicho paquete.
- Cancelar la publicación de un paquete de instalación independiente en el servidor web si hace clic en el botón **Anular la publicación**. El paquete de instalación independiente que no se publica estará disponible solo para que usted y otros administradores lo descarguen.
- Descargar un paquete de instalación independiente en su dispositivo haciendo clic en el botón **Descargar**.
- Enviar un correo electrónico con el enlace a un paquete de instalación independiente si hace clic en el botón **Enviar por correo electrónico**.
- Eliminar un paquete de instalación independiente haciendo clic en el botón **Eliminar**.

Instalación de aplicaciones con una tarea de instalación remota

Kaspersky Security Center Linux permite instalar aplicaciones en dispositivos remotamente con tareas de instalación remota. Esas tareas se crean y se asignan a dispositivos a través de un Asistente dedicado. Para asignar una tarea a dispositivos de modo más fácil y rápido, puede especificar dispositivos en la ventana del Asistente de una de estas formas:

- **Seleccionar dispositivos de red detectados por el Servidor de administración**. En este caso, la tarea se asigna a dispositivos específicos. Los dispositivos específicos pueden incluir dispositivos en grupos de administración así como dispositivos no asignados.
- **Especificar direcciones de dispositivo manualmente o importar direcciones desde una lista**. Puede especificar nombres DNS, direcciones IP y subredes IP de dispositivos a los cuales debe asignar la tarea.
- **Asignar tarea a una selección de dispositivos**. En este caso, la tarea se asigna a dispositivos incluidos en una selección creada anteriormente. Puede especificar la selección predeterminada o una personalizado que haya creado.
- **Asignar tarea a un grupo de administración**. En este caso, la tarea se asigna a dispositivos incluidos en un grupo de administración creado anteriormente.

Para realizar la instalación remota en un dispositivo en el que no se ha instalado el Agente de red, se deben abrir los siguientes puertos: (a) TCP 139 y 445; (b) UDP 137 y 138. De forma predeterminada, se abren los puertos en todos los dispositivos incluidos en el dominio. Se abren automáticamente mediante la utilidad de preparación de instalación remota.

Instalar la aplicación en dispositivos específicos

Expandir todo | Contraer todo

Esta sección contiene información sobre cómo instalar una aplicación de forma remota en un grupo de administración, en dispositivos con direcciones IP específicas o en 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 correspondientes.
2. En el menú principal, vaya a **DISPOSITIVOS → TAREAS**.
3. Haga clic en **Añadir**.
   Se inicia el Asistente para añadir tareas.
4. En el campo **Tipo de tarea**, seleccione **Instalar aplicación en remoto**.
5. Seleccione una de las siguientes opciones:

   - Asignar tarea a un grupo de administración

     La tarea se asigna a los dispositivos incluidos en un grupo de administración. Puede especificar uno de los grupos existentes o crear uno nuevo.

     Por ejemplo, es posible que desee utilizar esta opción para ejecutar una tarea de envío de un mensaje a los usuarios si el mensaje es específico para dispositivos incluidos en un grupo de administración específico.

   - Especificar direcciones de dispositivo manualmente o importar direcciones desde una lista

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

     Es posible que desee utilizar esta opción para ejecutar una tarea para una subred específica. Por ejemplo, es posible que desee instalar una aplicación determinada en dispositivos de contadores o analizar dispositivos en una subred que probablemente esté infectada.

   - Asignar tarea a una selección de dispositivos

La tarea se asigna a los dispositivos incluidos en una selección de dispositivos. Puede especificar una de las selecciones existentes.

Por ejemplo, es posible que desee utilizar esta opción para ejecutar una tarea en dispositivos con una versión específica del sistema operativo.

6. Siga las instrucciones del Asistente.

   El Asistente para añadir tareas crea una tarea para la instalación remota de la aplicación seleccionada en el Asistente en dispositivos especificados. Si seleccionó la opción **Asignar tarea a un grupo de administración** la tarea es de grupo.

7. Ejecute la tarea manualmente o espere a que se inicie de acuerdo con la programación que ha especificado en la configuración de la tarea.

Al completarse la tarea de instalación remota, la aplicación seleccionada queda instalada en los dispositivos especificados.

Instalación de una aplicación mediante directivas de grupo de Active Directory

Kaspersky Security Center permite usar directivas de grupo de Active Directory para instalar aplicaciones Kaspersky en dispositivos administrados.

Puede instalar aplicaciones mediante directivas de grupo de Active Directory solo desde los paquetes de instalación que incluyan el Agente de red.

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

1. Ejecute el Asistente de despliegue de la protección. Siga las instrucciones del Asistente.
2. En la página **Configuración de tarea Instalación remota** del Asistente de despliegue de la protección, active la opción **Asignar instalación del paquete en las directivas de grupo de Active Directory**.
3. En la página Seleccionar cuentas para acceder a los dispositivos, seleccione la opción **Se necesita una cuenta (para la instalación sin Agente de red)**.
4. Añada la cuenta con privilegios de administrador en el dispositivo donde se instala Kaspersky Security Center o la cuenta incluida en el grupo de dominio Propietarios del creador de directivas de grupo.
5. Otorgue los permisos 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 con el dominio requerido.
   c. Haga clic en la sección **Delegación**.
   d. En la lista desplegable **Permiso**, seleccione **Vincular Objetos de directivas de grupo**.
   e. Haga clic en **Añadir**.
   f. En la ventana **Seleccionar usuario, equipo o grupo** que se abre, seleccione la cuenta necesaria.
   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 añadir y después haga clic en **Avanzado → Avanzado**.
   i. En la lista de **Entradas de permisos**, haga doble clic en la cuenta que acaba de añadir.
   j. Otorgue los siguientes permisos:
      - **Crear objetos de grupo**
      - **Eliminar objetos de grupo**
      - **Crear objetos contenedores de directivas de grupo**
      - **Borrar objetos contenedores de directivas de grupo**
   k. Haga clic en **Aceptar** para guardar los cambios.
6. Defina otras configuraciones siguiendo las instrucciones del Asistente.
7. Ejecute manualmente la tarea de instalación remota creada o espere a que se produzca el inicio programado.

Se inicia la siguiente secuencia de instalación remota:

1. Durante la ejecución de la tarea, se crean los siguientes objetos en cada dominio que incluye los dispositivos cliente del conjunto especificado:
   - Objeto de directiva de grupo (Group policy object, GPO) con el nombre **Kaspersky_AK{GUID}**.
   - Un grupo de seguridad que equivale al GPO. Este grupo de seguridad incluye dispositivos cliente cubiertos por la tarea. El contenido del grupo de seguridad define la cobertura del GPO.
2. Kaspersky Security Center instala las aplicaciones seleccionadas en los dispositivos cliente directamente desde la carpeta de red compartida Compartir de la aplicación. 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. Cuando se añaden nuevos dispositivos al alcance de la tarea, se los añade también al grupo de seguridad al iniciarse la siguiente tarea. Si la opción **Ejecutar tareas no realizadas** está seleccionada en la planificación de tareas, los dispositivos se añadirán al grupo de seguridad inmediatamente.
4. Cuando los dispositivos se eliminan del alcance de la tarea, se borran del grupo de seguridad durante el siguiente inicio de la tarea.
5. Cuando se elimina una tarea de Active Directory, se eliminan también el GPO, el enlace del GPO y el grupo de seguridad correspondiente.

Si quiere aplicar algún otro esquema de instalación mediante Active Directory, puede configurar manualmente los parámetros requeridos. Puede ser necesario en los siguientes casos:

- Cuando el administrador de la protección antivirus no tiene permisos para realizar cambios en Active Directory de ciertos dominios
- Cuando el paquete de instalación original debe almacenarse en un recurso de red independiente
- Cuando es necesario vincular un GPO a unidades de Active Directory específicas

Están disponibles las siguientes opciones para utilizar una planificación de instalación alternativa a través de Active Directory:

- Si la instalación debe realizarse directamente desde la carpeta compartida de Kaspersky Security Center, deberá especificar en las propiedades del GPO el archivo .msi ubicado en la subcarpeta exec de la carpeta del paquete de instalación para la aplicación requerida.
- Si el paquete de instalación debe localizarse en otro recurso de red, deberá copiar todo el contenido de la carpeta exec en este, ya que, además del archivo con la extensión .msi, la carpeta contiene archivos de configuración generados cuando se creó el paquete. Para instalar la clave de licencia con la aplicación, copie también el archivo clave en esta carpeta.

Instalación de aplicaciones en Servidores de administración secundarios

Para instalar una aplicación en los Servidores de administración secundarios:

1. Establezca una conexión con el Servidor de administración que controla los Servidores de administración secundarios.
2. Asegúrese de que el paquete de instalación correspondiente 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. Cree una tarea de instalación de una aplicación remota en Servidores de administración secundarios. Seleccione el tipo de tarea **Instalar la aplicación en Servidor de administración secundario de forma remota**.

   El Asistente para añadir tareas crea una tarea para la instalación remota de la aplicación seleccionada en el Asistente en servidores de administración secundarios específicos.
4. Ejecute la tarea manualmente o espere a que se inicie de acuerdo con la programación que ha especificado en la configuración de la tarea.

Al completarse la tarea de instalación remota, la aplicación seleccionada queda instalada en los Servidores de administración secundarios.

Especificación de la configuración para la instalación remota en dispositivos Unix

Expandir todo | Contraer todo

Cuando instala una aplicación en un dispositivo Unix mediante una tarea de instalación remota, puede especificar la configuración específica de Unix para la tarea. Esta configuración está disponible en las propiedades de la tarea después de que se crea la tarea.

Para especificar la configuración específica de Unix para una tarea de instalación remota, haga lo siguiente:

1. En el menú principal, vaya a **DISPOSITIVOS** → **TAREAS**.
2. Haga clic en el nombre de la tarea de instalación remota para la que desea especificar la configuración específica de Unix.

   Se abrirá la ventana de propiedades de la tarea.
3. Vaya a **Configuración de la aplicación** → **Configuraciones específicas de Unix**.
4. Especifique los siguientes parámetros:

- **Establecer una contraseña para la cuenta raíz (solo para el despliegue a través de SSH)**

  Si el comando `sudo` no se puede usar en el dispositivo de destino sin especificar la contraseña, seleccione esta opción y luego especifique la contraseña para la cuenta raíz. Kaspersky Security Center Linux transmite la contraseña en forma cifrada al dispositivo de destino, descifra la contraseña y luego inicia el procedimiento de instalación en nombre de la cuenta raíz con la contraseña especificada.

  Kaspersky Security Center Linux no utiliza la cuenta ni la contraseña especificada para crear una conexión SSH.

- **Especifique la ruta a la carpeta temporal con permisos de ejecución en el dispositivo de destino (solo para el despliegue a través de SSH)**

  Si el directorio /tmp en el dispositivo de destino no tiene el permiso de ejecución, seleccione esta opción y luego especifique la ruta al directorio con el permiso de ejecución. Kaspersky Security Center Linux utiliza el directorio especificado como directorio temporal para acceder a través de SSH. La aplicación coloca el paquete de instalación en el directorio y ejecuta el procedimiento de instalación.

5. Haga clic en el botón **Guardar**.

La configuración de la tarea especificada se guarda.

Sustitución 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

Puede habilitar la opción **Desinstalar automáticamente las aplicaciones incompatibles** al configurar la instalación remota de una aplicación de seguridad 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 prácticas: Eliminar aplicaciones incompatibles antes de la instalación

Eliminación de aplicaciones incompatibles mediante una tarea dedicada

Para eliminar las aplicaciones incompatibles, use la tarea **Desinstalar aplicación en remoto**. Esta tarea debería ejecutarse en dispositivos antes de la tarea de instalación de la aplicación de seguridad. Por ejemplo, en la tarea de instalación, puede seleccionar el tipo de la programación **Al completar otra tarea**, donde la otra tarea es **Desinstalar aplicación en remoto**.

Este método de desinstalación es útil cuando el instalador de la aplicación de seguridad no puede eliminar correctamente una aplicación incompatible.

Instrucciones: Crear una directiva

Eliminar aplicaciones o actualizaciones de software de forma remota

Expandir todo | Contraer todo

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 **Añadir**.

   Se inicia el Asistente para añadir tareas. Avance por el Asistente utilizando el botón **Siguiente**.
3. Para la aplicación Kaspersky Security Center, seleccione el tipo de tarea **Desinstalar aplicación en remoto**.
4. Especifique el nombre para la tarea que está creando.

   El nombre de la tarea no puede contener más de 100 caracteres y no puede incluir ningún carácter especial (como "*<>?\:|).
5. Seleccione los dispositivos a los que se asignará la tarea.
6. Seleccione qué tipo de software desea eliminar y luego seleccione las aplicaciones, las actualizaciones o los parches específicos que desee eliminar:

   - **Desinstalar aplicación administrada**

Se muestra una lista de aplicaciones de Kaspersky. Seleccione la aplicación que desee eliminar.

- Desinstalar aplicación incompatible

  Se muestra una lista de aplicaciones incompatibles con las aplicaciones de seguridad de Kaspersky o Kaspersky Security Center. Seleccione las casillas de verificación al lado de las aplicaciones que desea eliminar.

- Desinstalar 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 que se va a 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 comando de desinstalación automáticamente**

      Si la aplicación tiene un comando de desinstalación definido por el proveedor de la aplicación, Kaspersky Security Center usa este comando. Le recomendamos que seleccione esta opción.

    - **Especificar 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 comando de desinstalación automáticamente**. Si falla 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:

      Usar este comando para desinstalación únicamente cuando el comando predeterminado no se detecte 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 la desinstalación de la aplicación**.

      Le recomendamos que active esta opción.

  - Reiniciar después de la desinstalación correcta de la aplicación

    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:

- Usando el Agente de red

  Los archivos se entregan a los dispositivos cliente mediante el Agente de red instalado en dichos dispositivos cliente.

  Si esta opción está desactivada, los archivos se entregan mediante las herramientas del sistema operativo Linux.

  Recomendamos que esta opción si la tarea se ha asignado a dispositivos que tienen instalados Agentes de red.

- Usando los recursos del sistema operativo mediante el Servidor de administración

La opción está obsoleta. En su lugar, utilice la opción **Usando el Agente de red** o **Usando los recursos del sistema operativo mediante puntos de distribución**.

Los archivos se transmiten a los dispositivos cliente mediante las herramientas del sistema operativo del Servidor de administración. Puede activar esta opción si no hay ningún Agente de red instalado en el dispositivo cliente, pero el dispositivo cliente está en la misma red que el Servidor de administración.

- **Usando los recursos del sistema operativo mediante puntos de distribución**

  Los archivos se transmiten a los dispositivos cliente mediante el uso de herramientas del sistema operativo a través de los puntos de distribución. Se puede activar esta opción si existe al menos un punto de distribución en la red.

  Si se activa la opción **Usando el Agente de red**, los archivos se entregan mediante herramientas del sistema operativo solo si los recursos del Agente de red no están disponibles.

- **Número máximo de descargas concurrentes**

  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 es mayor.

- **Número máximo de intentos de desinstalación**

  Si, al ejecutar la tarea *Desinstalar aplicación en remoto*, Kaspersky Security Center no logra desinstalar una aplicación en un dispositivo administrado dentro del número de intentos de instalación especificado por el parámetro, Kaspersky Security Center deja de enviar la utilidad de Desinstalación a este dispositivo administrado y ya no inicia el instalador en el dispositivo.

  El parámetro **Número máximo de intentos de desinstalación** le permite guardar los recursos del dispositivo administrado y reducir el tráfico (desinstalación, ejecución de archivos MSI y mensajes de error).

  Los intentos de inicio de tarea reiterados 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 reiniciar la tarea (manualmente o mediante una programación).

  Si finalmente no se logra realizar la desinstalación, el problema se considera irresoluble y cualquier otro inicio de tarea se percibe como costoso en cuanto a consumo innecesario de recursos y tráfico.

  Cuando se crea la tarea, el contador de intentos se fija en `0`. Cada intento del instalador que devuelve un error en el dispositivo aumenta la lectura del contador.

  Si se ha superado el número de intentos especificados en el parámetro y el dispositivo está listo para la desinstalación de la aplicación, puede aumentar el valor del parámetro **Número máximo de intentos de desinstalación** e iniciar la tarea de desinstalación de la aplicación. O bien, puede crear una nueva tarea *Desinstalar aplicación en remoto*.

- **Verificar el tipo de sistema operativo antes de descargar**

  Antes de transmitir los archivos a los dispositivos cliente, Kaspersky Security Center verifica si la configuración de la utilidad de Desinstalación puede aplicarse al sistema operativo del dispositivo cliente. Si la configuración no puede aplicarse, 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, a continuación, activar esta opción para omitir los dispositivos que ejecutan un sistema operativo distinto del requerido.

8. Especifique la configuración de reinicio del sistema operativo:

- **No reiniciar el dispositivo**

  Los dispositivos cliente no se reinician automáticamente después de la operación. Para completar la operación, debe reiniciar un dispositivo (por ejemplo, manualmente o a través de la tarea de administración de un dispositivo). La información sobre el reinicio requerido se guardará en los resultados de la tarea y en el estado del dispositivo. Esta opción es conveniente para las tareas en servidores y otros dispositivos donde la operación continua tiene importancia crítica.

- **Reiniciar el dispositivo**

  Los dispositivos cliente siempre se reinician automáticamente si se requiere un reinicio para completar la operación. Esta opción es útil para las tareas en dispositivos que ofrecen pausas habituales en su funcionamiento (cierre o reinicio).

- **Forzar el cierre de las aplicaciones en sesiones bloqueadas**

  La ejecución de aplicaciones puede impedir el reinicio del dispositivo cliente. Por ejemplo, si se está editando un documento en una aplicación de procesamiento de textos y no se lo guarda, la aplicación no permitirá que el dispositivo se reinicie.

  Si esta opción está activada, dichas aplicaciones en un dispositivo bloqueado son forzadas a cerrar antes de reiniciar el dispositivo. Como resultado, los usuarios pueden perder los cambios no guardados.

  Si esta opción está desactivada, no se reiniciará un dispositivo bloqueado. El estado de la tarea en este dispositivo indica que se requiere un reinicio del dispositivo. Los usuarios tienen que cerrar de forma manual todas las aplicaciones que se ejecutan en dispositivos bloqueados y reiniciar estos dispositivos.

  Esta opción está desactivada de forma predeterminada.

9. Si es necesario, añada las cuentas que se utilizarán para iniciar la tarea de desinstalación remota:

   - **No es necesaria una cuenta (Agente de red instalado)**

     Si se selecciona esta opción, no tiene que especificar la cuenta bajo la que se ejecutará el instalador de aplicación. La tarea se ejecutará en la cuenta en la que se está ejecutando el servicio del Servidor de administración.

     Si el Agente de red no se ha instalado en dispositivos cliente, esta opción no está disponible.

   - **Se necesita una cuenta (para la instalación sin Agente de red)**

     Si se selecciona esta opción, puede especificar la cuenta bajo la que se ejecutará el instalador de aplicación. Puede especificar la cuenta de usuario si el Agente de red no se ha instalado en los dispositivos para los cuales está asignada la tarea.

     Puede especificar varias cuentas de usuario si, por ejemplo, ninguna de ellas tiene todos los derechos requeridos en todos los dispositivos a los que se asignó esta tarea. En este caso, todas las cuentas que se han agregado se utilizan para ejecutar la tarea, en orden consecutivo de arriba abajo.

     Si no se agrega ninguna cuenta, la tarea se ejecutará en la cuenta en la que se está ejecutando el servicio del Servidor de administración.

10. Si desea modificar la configuración de tareas predeterminada, active la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de tareas**. Si no activa esta opción, la tarea se creará con las configuraciones predeterminadas. Puede modificar la configuración predeterminada más tarde, en cualquier momento.

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

    La tarea se crea y se muestra en la lista de tareas.

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

13. En la ventana de propiedades de la tarea, especifique la configuración general de la tarea.

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

15. Ejecute la tarea manualmente o espere a que se inicie de acuerdo con la programación que especificó en la configuración de la tarea.

    Al finalizar la tarea de desinstalación remota, se eliminará la aplicación seleccionada 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 le 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 a la vez. Por ejemplo, puede usar Puppet, Ansible, Chef o puede crear su propio script; use cualquier método que le resulte conveniente.

Después de preparar el dispositivo SUSE Linux Enterprise Server 15, implemente e instale el Agente de red.

Aplicaciones de Kaspersky: licencia 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 para las aplicaciones Kaspersky en dispositivos cliente, supervisar su uso y renovar las licencias.

Al agregar una clave de licencia mediante Kaspersky Security Center, los parámetros de la clave de licencia se almacenan en el Servidor de administración. En función de esta información, la aplicación genera un informe de uso de claves de licencia y envía notificaciones al administrador cuando caducan las licencias y cuando se infringen las restricciones de las licencias especificadas en las propiedades de las claves de licencia. Puede configurar notificaciones del uso de claves de licencia en los parámetros del Servidor de administración.

Obtención de licencias de aplicaciones administradas

Las aplicaciones de Kaspersky instaladas en los dispositivos administrados se deben licenciar aplicando un archivo clave o código de activación a cada una de las aplicaciones. Los archivos clave o códigos de activación se pueden desplegar de las siguientes formas:

- Despliegue automático
- El paquete de instalación de una aplicación administrada
- La tarea Agregar clave de licencia para una aplicación administrada
- Activación manual de una aplicación administrada

Puede añadir 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 añade 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 añadir una nueva clave de licencia.

Despliegue automático

Si usa diferentes aplicaciones administradas y tiene que desplegar un archivo clave o un código de activación específicos en los dispositivos, opte por otras formas de desplegar ese código de activación o archivo clave.

Kaspersky Security Center le permite desplegar automáticamente las claves de licencia disponibles en los dispositivos. Por ejemplo, en el repositorio del Servidor de administración se almacenan tres claves de licencia. Ha habilitado la opción **Clave de licencia distribuida automáticamente** para las tres claves de licencia. En los dispositivos de la organización se ha instalado una aplicación de seguridad de Kaspersky, por ejemplo, Kaspersky Endpoint Security for Linux. Se detecta un nuevo dispositivo en el que se debe desplegar una clave de licencia. La aplicación determina, por ejemplo, que dos de las claves de licencia del repositorio se pueden instalar 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 en el dispositivo. En este caso, no se puede predecir cuál de las dos claves de licencia se instalará en el dispositivo porque el despliegue automático de claves de licencia no prevé 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 en 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, se asignará a todos los dispositivos que no estaban cubiertos por la licencia el estado *Crítico*.

Antes del despliegue, se deben añadir el archivo clave o el código de activación al repositorio del Servidor de administración.

Instrucciones:

- Adición de una clave de licencia al repositorio del Servidor de administración
- Distribución automática de una clave de licencia

Adición de un archivo clave o un código de activación al paquete de instalación de una aplicación administrada

Por motivos de seguridad, esta opción no se recomienda. El archivo 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 clave en este paquete de instalación o en la directiva de la aplicación. La clave de licencia se desplegará en los dispositivos administrados en la próxima sincronización del dispositivo con el Servidor de administración.

Instrucciones: añadir una clave de licencia a un paquete de instalación

Despliegue al ejecutar la tarea de añadir clave de licencia a una aplicación administrada

Si opta por usar la tarea Agregar clave de licencia a una aplicación administrada, puede seleccionar la clave de licencia que debe instalarse en 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 añadir el archivo clave o el código de activación al repositorio del Servidor de administración.

Instrucciones:

- Adición de una clave de licencia al repositorio del Servidor de administración
- Despliegue de una clave de licencia en dispositivos cliente

Adición de un código de activación o un archivo clave manualmente a los dispositivos

Puede activar la aplicación Kaspersky instalada localmente, usando las herramientas provistas en la interfaz de la aplicación. Por favor, consulte la documentación de la aplicación instalada.

Adición de una clave de licencia al repositorio del Servidor de administración

Para añadir una clave de licencia al repositorio del Servidor de administración, realice lo siguiente:

1. En el menú principal, vaya a **OPERACIONES → LICENCIAS → LICENCIAS DE KASPERSKY**.
2. Haga clic en el botón **Añadir**.
3. Elija lo que quiera agregar:
   - **Añadir archivo clave**
     Haga clic en el botón **Seleccionar archivo clave** del archivo y vaya al archivo .key que desea añadir.
   - **Introducir el código de activación**
     Especifique el código de activación en el campo de texto y haga clic en el botón **Enviar**.
4. Haga clic en el botón **Cerrar**.

La clave o varias claves de licencia se añaden al repositorio del Servidor de administración.

Despliegue de una clave de licencia en dispositivos cliente

Kaspersky Security Center 14 Web Console permite distribuir una clave de licencia a los dispositivos cliente mediante la tarea de *Distribución de clave de licencia*.

Para distribuir una clave de licencia en los dispositivos cliente, realice lo siguiente:

1. En el menú principal, vaya a **DISPOSITIVOS → TAREAS**.
2. Haga clic en **Añadir**.
   Se inicia el Asistente para añadir tareas.
3. Seleccione la aplicación para la que desea añadir una clave de licencia.
4. De la lista **Tipo de tarea**, seleccione **Añadir clave de licencia**.
5. Siga las instrucciones del Asistente.
6. Si desea modificar la configuración de tareas predeterminada, active la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de tareas**. Si no activa esta opción, la tarea se creará con las configuraciones predeterminadas. Puede modificar la configuración predeterminada más tarde, en cualquier momento.
7. Haga clic en el botón **Crear**.
   La tarea se crea y se muestra en la lista de tareas.
8. Para ejecutar la tarea, selecciónela en la lista de tareas y haga clic en el botón **Iniciar**.

Cuando se realiza la tarea, la clave de licencia se despliega en los dispositivos seleccionados.

Distribución automática de una clave de licencia

Kaspersky Security Center Linux permite la distribución automática de claves de licencias en dispositivos administrados si estas se encuentran en el repositorio de claves del Servidor de administración.

Para distribuir una clave de licencia automáticamente en dispositivos administrados:

1. En el menú principal, vaya a **OPERACIONES → LICENCIAS → LICENCIAS DE KASPERSKY**.
2. Haga clic en el nombre de la clave que desee para distribuir automáticamente a dispositivos.
3. En la ventana de propiedades de la clave de licencia que se abre, seleccione la casilla **Distribuir automáticamente la clave de licencia 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 por medio 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 del número de licencias que se pueden asignar a los dispositivos. El límite de licencias está configurado en las propiedades de la clave de licencia. Si se alcanza el límite de licencias, esta clave de licencia se deja de distribuir automáticamente en dispositivos.

Si elige la casilla de verificación **Distribuir automáticamente la clave de licencia 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 manualmente una clave de licencia más tarde.

Visualización de información sobre claves de licencias 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**.

La lista que se muestra contiene los archivos clave y códigos de activación que se añadieron 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 requerida.

En la ventana de propiedades de claves de licencia que se abre, puede:

- En la pestaña **Control de aplicaciones**: información principal sobre la clave de la licencia
- En la pestaña **Dispositivos**: La lista de dispositivos cliente donde se usó la clave de licencia para la activación de la aplicación 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 requerido.
3. En la ventana de propiedades del dispositivo que se abre, seleccione 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 **Control de aplicaciones** y después abra la sección **Licencia**.

Se muestra la información principal sobre las claves de licencia activas y de reserva.

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.

Eliminación de una clave de licencia del repositorio

Cuando elimina la clave de licencia activa desplegada en un dispositivo administrado, la aplicación continua trabajando en el dispositivo administrado.

Para eliminar un archivo clave o un código de activación del repositorio del Servidor de administración, haga lo siguiente:

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

El archivo clave seleccionado o el código de activación se eliminan del repositorio.

Puede volver a añadir una clave de licencia eliminada o bien otra nueva.

Revocación de consentimiento con el Contrato de licencia de usuario final

Si decide dejar de proteger algunos de sus dispositivos cliente, puede revocar el Contrato de licencia de usuario final (EULA) para cualquier aplicación Kaspersky administrada. Debe desinstalar la aplicación seleccionada antes de revocar su EULA.

Para revocar un EULA para aplicaciones Kaspersky administradas:

1. Abra la ventana de propiedades del Servidor de administración y en la pestaña **Control de aplicaciones**, seleccione la sección **Contratos de licencia de usuario final**.

   Se muestra una lista de EULA, aceptada tras la creación de paquetes de instalación, la instalación sin problemas de actualizaciones o el despliegue de Kaspersky Security for Mobile.
2. En la lista, seleccione el EULA que quiere revocar.

   Puede ver las siguientes propiedades del EULA:

   - Fecha en la que se aceptó el EULA.
   - Nombre del usuario que aceptó el EULA.
3. Haga clic en la fecha de aceptación de cualquier EULA para abrir su ventana de propiedades, que muestra los siguientes datos:
   - Nombre del usuario que aceptó el EULA.
   - Fecha en la que se aceptó el EULA.
   - Identificador único (UID) del EULA.
   - Texto completo del EULA.
   - Lista de objetos (paquetes de instalación, actualizaciones integradas, aplicaciones móviles) vinculados al EULA y sus respectivos nombres y tipos.
4. En la parte inferior de la ventana de propiedades del EULA, haga clic en el botón **Revocar el Contrato de licencia**.

   > Si existen objetos (paquetes de instalación y sus respectivas tareas) que impidan la revocación del EULA, se muestra la notificación correspondiente. No puede continuar con la revocación hasta que elimine estos objetos.

   En la ventana que se abre, se le informa que primero debe desinstalar la aplicación Kaspersky correspondiente al EULA.
5. Haga clic en el botón para confirmar la revocación.

El EULA se ha revocado. Ya no se lo muestra en la lista de Acuerdos de licencia en la sección **Contratos de licencia de usuario final**. La ventana de propiedades del EULA se cierra y la aplicación ya no está instalada.

Renovación de licencias para aplicaciones de Kaspersky

Puede renovar una licencia de una aplicación de Kaspersky que haya caducado o que esté a punto de caducar (en menos de 30 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 enlace **Ver licencias que caducan** 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** que aparece junto a la licencia requerida.

   Al hacer clic en un enlace de renovación de licencia, acepta transferir a Kaspersky la siguiente información sobre Kaspersky Security Center: la versión, la localización que está utilizando, el ID de la licencia de 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. En la ventana del servicio de renovación de licencia que se abre, siga las instrucciones para renovar una licencia.

   La licencia queda renovada.

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 del vencimiento
- 7 días antes del vencimiento
- 3 días antes del vencimiento
- 24 horas antes del vencimiento
- Cuando una licencia ha caducado

Utilizar Kaspersky Marketplace para elegir soluciones empresariales de Kaspersky

MERCADO es una sección en el menú principal que le permite ver toda la gama de soluciones empresariales de Kaspersky, seleccionar las que necesita y proceder a la compra en el sitio web de Kaspersky. Puede utilizar filtros para ver solo las soluciones que se ajustan a su organización y a los requisitos de su sistema de seguridad de la información. Cuando selecciona una solución, Kaspersky Security Center Linux le redirige a la página web relacionada en el sitio web de Kaspersky para obtener más información sobre esa solución. Cada página web le permite continuar la compra o contiene instrucciones sobre el proceso de compra.

En la sección **MERCADO**, puede filtrar las soluciones de Kaspersky con los siguientes criterios:

- Número de dispositivos (puntos finales, 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:
  - **Bases**

    Este nivel es típico de las empresas que solo tienen un equipo de TI. Se bloquea el máximo número posible de amenazas automáticamente.
  - **Óptimo**

    Este nivel es típico de las empresas que tienen una función específica de seguridad informática dentro del equipo de TI. A este nivel, las empresas requieren soluciones que les permitan contrarrestar las amenazas de productos básicos y las amenazas que evitan los mecanismos de prevención existentes.
  - **Experto**

    Este nivel es típico de las empresas con entornos complejos y distribuidos de TI. El equipo de seguridad de TI es maduro o la empresa tiene un equipo SOC (Centro de Operaciones de Seguridad). Las soluciones requeridas permiten a las empresas contrarrestar amenazas complejas y ataques dirigidos.
- Tipos de activos que desea proteger:
  - **Puntos finales**: estaciones de trabajo de 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
  - **Servicio**: servicios relacionados con la seguridad proporcionados por Kaspersky

Para encontrar y adquirir una solución empresarial de Kaspersky:

1. En la ventana principal, vaya a **MERCADO**.

De forma predeterminada, la sección muestra todas las soluciones empresariales disponibles de Kaspersky.

2. Para ver solo las soluciones que se adaptan a su organización, seleccione los valores necesarios en los filtros.

3. Haga clic en la solución que desea adquirir o sobre la que desea obtener más información.

Será redirigido a la página web de la solución. Puede seguir las instrucciones en pantalla para proceder a la compra.

Configuración de protección de la red

En esta sección, encontrará información sobre la configuración manual de las directivas y las tareas, sobre las funciones del usuario y sobre la creación de una estructura de grupos de administración y jerarquía de tareas.

Escenario: Configuración de protección de la red

El Asistente de inicio rápido crea directivas y tareas con la configuración predeterminada. Estas configuraciones pueden resultar subóptimas o, incluso, inadmisibles para la organización. Por lo tanto, le recomendamos que ajuste estas directivas y tareas, y cree otras en caso de ser necesarias para su red.

Requisitos previos

Antes de comenzar, asegúrese de haber hecho lo siguiente:

- Instalado el Servidor de administración de Kaspersky Security Center
- Instalación de Kaspersky Security Center 14 Web Console
- Completado 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 de **Dispositivos administrados**:
  - Directiva de Kaspersky Endpoint Security
  - Tarea de grupo para actualizar Kaspersky Endpoint Security
  - Directiva del Agente de red

La configuración de la protección de red se realiza en etapas:

1. **Configuración y propagación de directivas de aplicación Kaspersky y perfiles de directiva**

   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. **Configuración de tareas para la administración remota de aplicaciones Kaspersky**

   Verifique las tareas creadas con el Asistente de inicio rápido y afínelas, si es necesario.

   Instrucciones: Configurar de la tarea de grupo para actualizar Kaspersky Endpoint Security

   Si es necesario, cree tareas adicionales para administrar las aplicaciones Kaspersky instaladas en los dispositivos cliente.

3. **La evaluación y la limitación del evento se cargan en la base de datos**

   Se transfiere la información sobre eventos 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 en el Servidor de administración, evalúe y limite el número máximo de eventos que se pueden almacenar en la base de datos.

   Instrucciones prácticas: Configurar el número máximo de eventos

Resultados

Cuando complete este escenario, su red estará protegida gracias a la configuración de las aplicaciones de Kaspersky, tareas y eventos recibidos por el Servidor de administración:

- Las aplicaciones de Kaspersky se configuran de acuerdo con las directivas y los perfiles de directiva
- Las aplicaciones se administran a través de un conjunto de tareas
- Se establece el número máximo de eventos que se pueden almacenar en la base de datos

Cuando se completa la configuración de protección de la red, puede proceder a configurar actualizaciones periódicas de las bases de datos y aplicaciones de Kaspersky.

Acerca de los enfoques de administración de seguridad centrados en el dispositivo y centrados en el usuario

Puede administrar la configuración de seguridad desde el punto de vista de las funciones del dispositivo y desde el punto de vista de los roles de usuario. El primer enfoque se denomina *administración de seguridad centrada en el dispositivo* y el segundo se denomina *administración de seguridad centrada en el usuario*. Para aplicar diferentes configuraciones de aplicaciones a diferentes dispositivos, puede usar uno o ambos tipos de administración en combinación.

La administración de seguridad centrada en el dispositivo le permite aplicar distintas configuraciones de la aplicación de seguridad a los dispositivos administrados según las funciones específicas del dispositivo. Por ejemplo, puede aplicar distintas configuraciones a los dispositivos asignados en diferentes grupos de administración.

La administración de seguridad centrada en el usuario le permite aplicar distintas configuraciones de la aplicación de seguridad a diferentes funciones de usuario. Puede crear varias funciones de usuario, asignar una función de usuario adecuada para cada usuario y definir diferentes configuraciones de la aplicación para los dispositivos de usuarios con diferentes funciones. Por ejemplo, es posible que desee aplicar diferentes configuraciones de aplicaciones a los dispositivos de contadores y especialistas del departamento de recursos humanos (HR). Como resultado, cuando se implementa la administración de seguridad centrada en el usuario, cada departamento (el departamento de contabilidad y el departamento de recursos humanos) tiene su propia configuración de opciones para las aplicaciones de Kaspersky. Una configuración define qué opciones de la aplicación pueden cambiar los usuarios y cuáles impone y bloquea el administrador.

Al utilizar la administración de seguridad centrada en el usuario, puede aplicar configuraciones de aplicaciones específicas incluso para usuarios individuales. Esto puede ser necesario cuando un empleado tiene un rol único en la empresa o cuando desea monitorear incidentes de seguridad relacionados con dispositivos de una persona específica. Dependiendo de la función de este empleado en la empresa, puede ampliar o limitar los derechos de esta persona para cambiar la configuración de la aplicación. Por ejemplo, es posible que desee ampliar los derechos de un administrador del sistema que administra los dispositivos cliente en una oficina local.

También puede combinar los enfoques de administración de seguridad centrados en el dispositivo y centrados en el usuario. Por ejemplo, puede configurar una directiva de aplicación específica para cada grupo de administración y luego crear perfiles de directivas para una o varias funciones de usuario de su empresa. En este caso, las directivas y los perfiles de directiva se aplican en el siguiente orden:

1. Se aplican las directivas creadas para la administración de seguridad centrada en el dispositivo.
2. Son modificados por los perfiles de directiva de acuerdo con las prioridades del perfil de directiva.
3. Las directivas son modificadas por los perfiles de directiva asociados con roles de usuario.

Configuración y propagación de directivas: enfoque centrado en el dispositivo

Cuando complete este escenario, las aplicaciones se configurarán en todos los dispositivos administrados de acuerdo con las directivas de aplicación y los perfiles de directiva que 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. También es posible que desee considerar la administración de seguridad centrada en el usuario como una opción alternativa o adicional al enfoque centrado en el dispositivo. Más información sobre dos enfoques de administración.

Etapas

El escenario de administración centrada en el dispositivo de las aplicaciones de Kaspersky consiste en los siguientes pasos:

1. **Configuración de directivas de aplicación**

   Configure los ajustes para las aplicaciones de Kaspersky instaladas en los dispositivos administrados mediante la creación de una directiva para cada aplicación. El conjunto de directivas se propagará 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 for Linux. Si completó el proceso de configuración utilizando este Asistente, no tiene que crear una nueva directiva para esta aplicación.

   Si tiene una estructura jerárquica de varios Servidores de administración y/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 parámetros configurados en la directiva ascendente. Si desea que solo una parte de la configuración se herede a la fuerza, puede bloquearla en la directiva ascendente. El resto de configuraciones desbloqueadas estarán disponibles para modificación en las directivas posteriores. La jerarquía de directivas creada le permitirá administrar efectivamente los dispositivos en los grupos de administración.

   Instrucciones: Creación de una directiva

2. **Creación de perfiles de directivas (opcional)**

Si desea que los dispositivos dentro de un solo grupo de administración se ejecuten bajo diferentes configuraciones de directivas, cree perfiles de directivas para esos dispositivos. Un perfil de directiva es un subconjunto de parámetros de la directiva denominado. Este subconjunto se distribuye en dispositivos de destino junto con la directiva, y se complementa en una condición específica denominada la *Condición de activación de perfil*. Los perfiles solo contienen parámetros que se diferencian de la directiva "básica", que está activa en el dispositivo administrado.

Al utilizar las condiciones de activación del perfil, puede aplicar diferentes perfiles de directivas, por ejemplo, a los dispositivos que tienen configuración de hardware específica o marcados con etiquetas específicas. Utilice etiquetas para filtrar dispositivos que cumplan criterios específicos. Por ejemplo, puede crear una etiqueta llamada *CentOS*, marcar todos los dispositivos que ejecutan el sistema operativo CentOS con esta etiqueta y luego especificar esta etiqueta como condición de activación para un perfil de directiva. Como resultado, las aplicaciones de Kaspersky instaladas en todos los dispositivos que ejecutan CentOS serán administradas por su propio perfil de directiva.

Instrucciones:

- Crear perfil de directiva
- Creación de una regla de activación de perfil de directiva

3. **Propagación de directivas y perfiles de directiva a los dispositivos administrados**

   De forma predeterminada, Kaspersky Security Center sincroniza automáticamente el Servidor de administración con los dispositivos administrados cada 15 minutos. Durante la sincronización, las directivas nuevas o modificadas y los perfiles de directivas se propagan a los dispositivos administrados. Puede evitar la sincronización automática y ejecutar la sincronización manualmente utilizando el comando Forzar sincronización. Una vez que se complete la sincronización, las directivas y los perfiles de las directivas se entregan y aplican a las aplicaciones instaladas de Kaspersky.

   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

Cuando se completa el escenario centrado en el dispositivo, las aplicaciones de Kaspersky se configuran de acuerdo con la configuración especificada y propagada a través de la jerarquía de directivas.

Las directivas de aplicación configuradas y los perfiles de directivas se aplicarán automáticamente a los nuevos dispositivos añadidos a los grupos de administración.

Configuración y propagación de directivas: enfoque centrado en el usuario

Esta sección describe el escenario de enfoque centrado en el usuario para la configuración centralizada de las aplicaciones de Kaspersky instaladas en los dispositivos administrados. Cuando complete este escenario, las aplicaciones se configurarán en todos los dispositivos administrados de acuerdo con las directivas de aplicación y los perfiles de directiva que 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. También es posible que desee considerar la administración de seguridad centrada en el dispositivo como una opción alternativa o adicional al enfoque centrado en el usuario. Más información sobre dos enfoques de administración.

Proceso

El escenario de administración centrada en el usuario de las aplicaciones de Kaspersky consta de los siguientes pasos:

1. **Configuración de directivas de aplicación**

   Configure los ajustes para las aplicaciones de Kaspersky instaladas en los dispositivos administrados mediante la creación de una directiva para cada aplicación. El conjunto de directivas se propagará 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 tiene que crear una nueva directiva para esta aplicación.

   Si tiene una estructura jerárquica de varios Servidores de administración y/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 parámetros configurados en la directiva ascendente. Si desea que solo una parte de la configuración se herede a la fuerza, puede bloquearla en la directiva ascendente. El resto de configuraciones desbloqueadas estarán disponibles para modificación en las directivas posteriores. La jerarquía de directivas creada le permitirá administrar efectivamente los dispositivos en los grupos de administración.

   Instrucciones: Creación de una directiva

2. **Especificación de propietarios de los dispositivos**

   Asigne los dispositivos administrados a los usuarios correspondientes.

   Instrucciones: Designación del usuario como propietario del dispositivo

3. **Definición de funciones de usuario típicas de su empresa**

   Piense en los diferentes tipos de trabajo que normalmente realizan los empleados de su empresa. Debe dividir a todos los empleados de acuerdo con sus funciones. Por ejemplo, puede dividirlos por departamentos, profesiones o cargos. Después de eso, deberá crear una función de usuario para cada grupo. Tenga en cuenta que cada función de usuario tendrá su propio perfil de directiva que contiene la configuración de la aplicación específica para esta función.

4. **Creación de funciones 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. Las funciones de usuario contendrán un conjunto de derechos de acceso a las características de la aplicación.

   Instrucciones: Creación de una función de usuario

5. **Definición de la cobertura de cada función de usuario**

   Para cada uno de las funciones de usuario creadas, defina usuarios y/o grupos de seguridad y grupos de administración. La configuración asociada con una función de usuario se aplica solo a los dispositivos que pertenecen a usuarios que tienen esta función y solo si estos dispositivos pertenecen a grupos asociados con esta función, incluidos los grupos secundarios.

   Instrucciones: Edición de la cobertura de una función de usuario

6. **Crear perfiles de directiva**

   Crear un perfil de directiva para cada función de usuario en su empresa. Los perfiles de directivas definen qué configuración se aplicará a las aplicaciones instaladas en los dispositivos de los usuarios en función de la función de cada usuario.

   Instrucciones: Creación de un perfil de directiva

7. **Asociación de perfiles de directivas de funciones de usuario**

   Asocie los perfiles de directiva creados con las funciones de usuario. Después de eso: el perfil de la directiva se activa para un usuario que tiene la función especificada. Los parámetros configurados en el perfil de la directiva se aplicarán a las aplicaciones de Kaspersky instaladas en los dispositivos del usuario.

   Instrucciones: Asociación de perfiles de directivas con funciones

8. **Propagación de directivas y perfiles de directiva a los dispositivos administrados**

   De forma predeterminada, Kaspersky Security Center sincroniza automáticamente el Servidor de administración con los dispositivos administrados cada 15 minutos. Durante la sincronización, las directivas nuevas o modificadas y los perfiles de directivas se propagan a los dispositivos administrados. Puede evitar la sincronización automática y ejecutar la sincronización manualmente utilizando el comando Forzar sincronización. Una vez que se complete la sincronización, las directivas y los perfiles de las directivas se entregan y aplican a las aplicaciones instaladas de Kaspersky.

   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

Cuando se completa el escenario centrado en el dispositivo, las aplicaciones de Kaspersky se configuran de acuerdo con la configuración especificada y propagada a través de la jerarquía de directivas y perfiles de directivas.

Para un nuevo usuario, tendrá que crear una nueva cuenta, asignar al usuario una de las funciones de usuario creados y asignar los dispositivos al usuario. Las directivas de aplicación configuradas y los perfiles de la directiva se aplicarán automáticamente a los dispositivos de este usuario.

Configuración manual de la tarea de actualización de grupo para Kaspersky Endpoint Security

La opción de programación óptima y recomendada para Kaspersky Endpoint Security es **Cuando se descargan nuevas actualizaciones en el repositorio** cuando la casilla de verificación **Usar el retraso aleatorio automáticamente para el inicio de tareas** está seleccionada.

Configuración de la directiva del Agente de red

Expandir todo | Contraer todo

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 esta pestaña puede modificar el estado de la directiva y especificar la herencia de la configuración de la directiva:

- En el bloque **Estado de la directiva**, puede seleccionar uno de los modos de la directiva:
  - **Directiva activa**

    Si se selecciona esta opción, se activa la directiva.

    Esta opción está seleccionada de forma predeterminada.

  - **Directiva inactiva**

    Si se selecciona esta opción, se inactiva la directiva, pero sigue almacenada en la carpeta **Directivas**. Si fuera necesario, se puede activar la directiva.

- En la sección de grupo **Herencia de configuración**, se puede configurar la herencia de directivas:
  - **Heredar configuración de la directiva primaria**

    Si se activa esta opción, los valores de la configuración de la directiva se heredan de la directiva de grupos de nivel superior y, por lo tanto, quedan bloqueados.

    Esta opción está activada de forma predeterminada.

  - **Forzar la herencia de la configuración en las directivas secundarias**

    Si se activa esta opción, después de aplicar modificaciones a las directivas, se realizarán las siguientes acciones:
    - Los valores de los parámetros de las directivas se distribuirán a las directivas de los grupos de administración anidados, es decir, a las directivas secundarias.
    - En el bloque **Herencia de configuración** de la sección **General** de la ventana de propiedades de cada directiva secundaria, se activará automáticamente la opción **Heredar configuración de la directiva primaria**.

    Si se activa esta opción, la configuración de las directivas secundarias queda bloqueada.

    Esta opción está desactivada de forma predeterminada.

Configuración de eventos

En esta pestaña, puede configurar el registro de eventos y la notificación de eventos. Los eventos se distribuyen según el nivel de importancia en las siguientes secciones en la pestaña **Configuración de eventos**:

- **Fallo operativo**
- **Advertencia**
- **Información**

En cada sección, la lista muestra los tipos de eventos y el plazo de almacenamiento de eventos predeterminado en el Servidor de administración (en días). Después de hacer clic en un tipo de evento, puede especificar la configuración del registro de eventos y las notificaciones relativas a los eventos elegidos en la lista. De forma predeterminada, la configuración de la notificación común especificada para el Servidor de administración completo se utiliza para todos los tipos de evento. Sin embargo, puede cambiar la configuración específica para los tipos de evento requeridos.

Por ejemplo, en la sección **Advertencia**, puede configurar el tipo de evento **Se ha producido un incidente**. Este tipo de eventos pueden ocurrir, por ejemplo, cuando el espacio libre en 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 **Se ha producido un incidente**, haga clic en este y especifique dónde almacenar los eventos ocurridos y cómo notificarlos.

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

Configuración de la aplicación

Configuración

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

- Tamaño máximo de la cola del evento, en MB

  En este campo se puede especificar el espacio máximo en disco que puede ocupar una cola de eventos.

  El valor predeterminado es de 2 Megabytes (MB).

- La aplicación podrá obtener información adicional sobre la directiva en el dispositivo

  El Agente de red instalado en un dispositivo administrado transfiere información sobre la directiva de aplicación de seguridad aplicada a la aplicación de seguridad (por ejemplo, Kaspersky Endpoint Security for Linux). Puede ver la información transferida en la interfaz de la aplicación de seguridad.

  El Agente de red transfiere la siguiente información:

  - Hora de entrega de la directiva al dispositivo administrado
  - Nombre de la directiva activa o fuera de la oficina en el momento de la entrega de la directiva al dispositivo administrado
  - Nombre y ruta completa al grupo de administración que contenía el dispositivo administrado en el momento de la entrega de la directiva al dispositivo administrado
  - Lista de perfiles de directivas activas

    Puede utilizar la información para asegurarse de que se aplique la directiva correcta al dispositivo y para solucionar problemas. Esta opción está desactivada de forma predeterminada.

Repositorios

En la sección **Repositorios**, puede seleccionar los tipos de objetos cuya información se enviará desde el Agente de red hasta el Servidor de administración. Si la modificación de algunos parámetros de esta sección está prohibida por la directiva del Agente de red, no se los podrá modificar.

- Detalles de las aplicaciones instaladas

  Si esta opción está activada, la información sobre las aplicaciones instaladas en los dispositivos cliente se envía al Servidor de administración.

  Esta opción está activada de forma predeterminada.

- Detalles de registro de hardware

  El Agente de red instalado en un dispositivo envía información sobre el hardware del dispositivo al Servidor de administración. Puede ver los detalles del hardware en las propiedades del dispositivo.

Red

La sección **Red** incluye tres subsecciones:

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

En la subsección **Conectividad**, puede configurar la conexión con el Servidor de administración, activar el uso de un puerto UDP y especificar el número de puerto UDP.

- El grupo de configuración **Conectar al Servidor de administración** le permite configurar la conexión al Servidor de administración y especificar el período para la sincronización de los dispositivos cliente y el Servidor de administración:

  - Intervalo de sincronización (min)

    El Agente de red sincroniza el dispositivo administrado con el Servidor de administración. Recomendamos que establezca el intervalo de sincronización (también conocido como heartbeat) en 15 minutos por cada 10 000 dispositivos administrados.

    Si el intervalo de sincronización está configurado en menos de 15 minutos, la sincronización se realiza 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 se selecciona esta opción, aumentará la velocidad de transferencia de datos del Agente de red, disminuirá la cantidad de información que se transfiere y disminuirá la carga en el Servidor de administración.

Puede incrementarse la carga de trabajo de la CPU del dispositivo cliente.

De forma predeterminada, esta opción está activada.

- Usar conexión SSL

  Si esta opción está activada, la conexión al Servidor de administración se establece a través de un puerto seguro a través de SSL.

  Esta opción está activada de forma predeterminada.

- Usar puerta de enlace de conexión del punto de distribución (si está disponible) en la configuración de la conexión predeterminada

  Si se selecciona esta opción, la puerta de enlace de conexión en el punto de distribución se utilizará con la configuración especificada en las propiedades del grupo de administración.

  Esta opción está activada de forma 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 activada de forma predeterminada. El puerto UDP predeterminado de conexión al servidor proxy de KSN es 15111.

- Número de puerto UDP

  En este campo se introduce el nombre del puerto UDP. El número de puerto predeterminado es el 15000.

  Se usa el sistema decimal para los registros.

En la subsección **Perfiles de conexión** de la sección **Red**, puede especificar la configuración de ubicación de red y habilitar el modo fuera de la oficina cuando el Servidor de administración no esté disponible. La configuración en la sección **Perfiles de conexión** está disponible solo en dispositivos que ejecutan Windows:

- Configuración de la ubicación de red

  La configuración de la ubicación de red define las características de la red a la que está conectado el dispositivo cliente y especifica las reglas para el cambio del Agente de red de un perfil de conexión Servidor de administración a otro cuando se alteran esas características de red.

- Perfiles de conexión al Servidor de administración

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

  Puede ver y añadir perfiles para la conexión del Agente de red al Servidor de administración. En esta sección, también puede crear reglas para cambiar el Agente de red a Servidores de administración diferentes cuando ocurren los siguientes eventos:

  - Cuando un dispositivo cliente se conecta a otra red local
  - Cuando un dispositivo pierde conexión con la red local de la organización
  - Cuando se cambia la dirección de la puerta de enlace de conexión o se modifica 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 **Añadir** está inactivo. Los perfiles de conexión preestablecidos tampoco se pueden modificar.

- Activar modo Fuera de la oficina cuando el Servidor de administración no esté disponible

Si se selecciona esta opción y en el caso de que la conexión se realice con este perfil, las aplicaciones instaladas en el dispositivo cliente utilizan los perfiles de directivas para dispositivos en modo fuera de la oficina, además de directivas fuera de la oficina. Si no se ha definido una directiva fuera de la oficina en la aplicación, se utilizará la directiva activa.

Si esta opción está desactivada, las aplicaciones utilizarán las directivas activas.

Esta opción está desactivada de forma predeterminada.

En la subsección **Programación de conexiones**, se pueden especificar los intervalos de tiempo en los que el Agente de red envía los datos al Servidor de administración:

- **Conectar cuando sea necesario**

  Si se selecciona esta opción, la conexión se establecerá cuando el Agente de red tenga que enviar datos al Servidor de administración.

  Esta opción está seleccionada de forma predeterminada.

- **Conectarse en los intervalos de tiempo especificados**

  Si se selecciona esta opción, el Agente de red se conectará al Servidor de administración a una hora concreta. Se pueden añadir varios períodos de tiempo de conexión.

Sondeo de la red realizado por los puntos de distribución

En la sección **Sondeo de la red realizado por los puntos de distribución**, puede configurar el sondeo automático de la red. Puede utilizar las siguientes opciones para habilitar el sondeo y establecer su frecuencia:

- **Zeroconf**

  Si esta opción está activada, 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 activados 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 desactivada, el punto de distribución no sondea las redes con dispositivos IPv6.

  Esta opción está desactivada de forma predeterminada.

- **Rangos IP**

  Si esta opción está activada, el Servidor de administración sondea automáticamente los rangos de IP de acuerdo con la programación que ha configurado al hacer clic en el enlace **Programar sondeo**.

  Si esta opción está desactivada, el Servidor de administración no sondea los rangos de IP.

  La frecuencia de sondeos de rangos IP en las versiones del Agente de red anteriores a 10.2 se puede configurar en el campo **Intervalo de sondeo (min)**. El campo está disponible si la opción está activada.

  Esta opción está desactivada de forma predeterminada.

Configuración de red para puntos de distribución

En la sección **Configuración de red para puntos de distribución**, puede especificar la configuración de acceso a Internet:

- **Usar servidor proxy**
- **Dirección**
- **Número de puerto**
- **No utilizar el servidor proxy para direcciones locales**

  Si se selecciona esta opción, no se utilizará el servidor proxy para conectarse a los dispositivos de la red local.

  Esta opción está desactivada de forma predeterminada.

- Autenticación del servidor proxy

  Si se activa esta casilla, podrá especificar las credenciales para la autenticación del servidor proxy en los campos de entrada.

  De forma predeterminada, esta opción está desactivada.

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

Actualizaciones (puntos de distribución)

En la sección **Actualizaciones (puntos de distribución)**, puede activar 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 revisión

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

Cambio de prioridad de las reglas de movimiento de dispositivos

Todas las reglas de movimiento de dispositivos tienen prioridades.

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

use el ratón para desplazar la regla hacia arriba o hacia abajo en la lista, respectivamente.

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 dispositivos mediante la creación y ejecución de *tareas*. Las tareas son necesarias 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.

Las tareas se pueden realizar en el Servidor de administración y en los dispositivos.

Las tareas que se realizan en el Servidor de administración incluyen lo siguiente:

- Distribución automática de informes
- Descargar actualizaciones en el repositorio
- Copia de seguridad de los datos del Servidor de administración
- Mantenimiento de bases de datos

Los siguientes tipos de tareas se realizan en dispositivos:

- *Tareas locales*: tareas que se realizan en un dispositivo específico

  Las tareas locales pueden ser modificadas por el administrador usando herramientas de Kaspersky Security Center 14 Web Console, o por el usuario de un dispositivo remoto (por ejemplo, a través de la interfaz de la aplicación de seguridad). Si una tarea local ha sido modificada simultáneamente por el administrador y el usuario de un dispositivo administrado, los cambios hechos por el administrador entrarán en vigor, ya que tienen una prioridad más alta.

- *Tareas de grupo*: tareas que se realizan 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. Las tareas de grupo también afectan (opcionalmente) los dispositivos que se han conectado a Servidores de administración virtuales y secundarios desplegados en ese grupo o cualquiera de sus subgrupos.

- *Tareas globales*: tareas que se realizan en un conjunto de dispositivos, independientemente de si se incluyen en algún grupo.

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

Puede realizar cambios en la configuración de tareas, ver el progreso de las tareas y copiar, exportar, importar y eliminar tareas.

Una tarea se inicia en un dispositivo solo si la aplicación para la que se creó la tarea se está en ejecución.

Los resultados de la ejecución de tareas se guardan en el registro de eventos del sistema operativo de cada dispositivo, el registro de eventos del sistema operativo del Servidor de administración, y en la base de datos del Servidor de administración.

No incluya datos confidenciales en la configuración de la tarea. Por ejemplo, no especifique la contraseña del administrador de dominio.

Acerca de la cobertura de la tarea

La *cobertura de una tarea* es el conjunto de dispositivos en los que se realiza la tarea. Los tipos de cobertura son los siguientes:

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

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

- Especificar determinados dispositivos manualmente.

  Puede utilizar una dirección IP (o un rango IP) o un nombre DNS como la dirección del dispositivo.
- Importación de una lista de dispositivos desde un archivo .txt con las direcciones del dispositivo que se añadirán (cada dirección debe ubicarse en una línea individual).

  Si importa una lista de dispositivos desde un archivo o la crea manualmente, y si los dispositivos se identifican por sus nombres, la lista solo podrá contener dispositivos para los cuales ya se haya introducido información en la base de datos del Servidor de administración. Además, la información debe haberse introducido cuando se conectaron esos dispositivos o durante la detección de dispositivos.
- Especificar selección de dispositivos.

  Con el tiempo, la cobertura de la tarea cambia a medida que el conjunto de dispositivos incluidos en la selección cambia. Puede realizarse una selección de dispositivos sobre la base de atributos del dispositivo, incluido el software instalado en un dispositivo y sobre la base de etiquetas asignadas a dispositivos. La selección de dispositivos es la forma más flexible de especificar la cobertura de una tarea.

  Las tareas para selecciones de dispositivos siempre se ejecutan de forma programada por el Servidor de administración. Estas tareas no se pueden ejecutar en dispositivos que carecen de conexión con el Servidor de administración. Las tareas cuya cobertura 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 en la hora local de un dispositivo; en su lugar, se ejecutan en la hora local del Servidor de administración. Las tareas cuya cobertura se especifica mediante otros métodos se ejecutan en la hora local de un dispositivo.

Creación de una tarea

Para crear una tarea:

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

   Se inicia el Asistente para añadir tareas. Siga sus instrucciones.
3. Si desea modificar la configuración de tareas predeterminada, active la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de tareas**. Si no activa esta opción, la tarea se creará con las configuraciones predeterminadas. Puede modificar la configuración predeterminada más tarde, en cualquier momento.
4. Haga clic en el botón **Finalizar**.

La tarea se crea y se muestra en la lista de tareas.

Inicio de una tarea de forma manual

La aplicación inicia las tareas según la configuración de programación especificada en las propiedades de cada tarea. Puede iniciar una tarea de forma manual en cualquier momento.

Para iniciar una tarea manualmente, haga lo siguiente:

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

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

Visualización de 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 según los nombres de las aplicaciones con las que están relacionadas. Por ejemplo, la tarea Instalar aplicación en remoto está relacionada con el Servidor de administración, mientras que la tarea *Actualizar* corresponde 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 se con varias pestañas con nombre. Por ejemplo, **Tipo de tarea** se muestra en la pestaña **Control de aplicaciones** y la programación de tareas, en la pestaña **Programación**.

Configuración general de la tareas

Expandir todo | Contraer todo

Esta sección indica los ajustes que puede ver y especificar para las tareas.

Configuraciones especificadas durante la creación de tareas

Puede especificar los siguientes ajustes al crear una tarea. Algunos de estos ajustes también se pueden modificar en las propiedades de la tarea creada.

- Configuración de reinicio del sistema operativo:
  - **No reiniciar el dispositivo**

    Los dispositivos cliente no se reinician automáticamente después de la operación. Para completar la operación, debe reiniciar un dispositivo (por ejemplo, manualmente o a través de la tarea de administración de un dispositivo). La información sobre el reinicio requerido se guardará en los resultados de la tarea y en el estado del dispositivo. Esta opción es conveniente para las tareas en servidores y otros dispositivos donde la operación continua tiene importancia crítica.

  - **Reiniciar el dispositivo**

    Los dispositivos cliente siempre se reinician automáticamente si se requiere un reinicio para completar la operación. Esta opción es útil para las tareas en dispositivos que ofrecen pausas habituales en su funcionamiento (cierre o reinicio).

  - **Forzar el cierre de las aplicaciones en sesiones bloqueadas**

    La ejecución de aplicaciones puede impedir el reinicio del dispositivo cliente. Por ejemplo, si se está editando un documento en una aplicación de procesamiento de textos y no se lo guarda, la aplicación no permitirá que el dispositivo se reinicie.

    Si esta opción está activada, dichas aplicaciones en un dispositivo bloqueado son forzadas a cerrar antes de reiniciar el dispositivo. Como resultado, los usuarios pueden perder los cambios no guardados.

    Si esta opción está desactivada, no se reiniciará un dispositivo bloqueado. El estado de la tarea en este dispositivo indica que se requiere un reinicio del dispositivo. Los usuarios tienen que cerrar de forma manual todas las aplicaciones que se ejecutan en dispositivos bloqueados y reiniciar estos dispositivos.

    Esta opción está desactivada de forma predeterminada.

- Configuración de programación de la tarea:
  - **Inicio programado**

Seleccione la programación según la cual se ejecuta la tarea y configure la programación seleccionada.

- **Cada N horas**

  La tarea se ejecuta regularmente, con el intervalo especificado en horas, a partir de la fecha y hora especificadas.

  De forma predeterminada, la tarea se ejecuta cada seis horas, a partir de la fecha y hora actuales del sistema.

- **Cada N días**

  La tarea se ejecuta regularmente, con el intervalo especificado en días. Además, puede especificar una fecha y hora de la primera tarea ejecutada. Estas opciones adicionales estarán disponibles si son compatibles con la aplicación para la que crea la tarea.

  De forma predeterminada, la tarea se ejecuta cada día, a partir de la fecha y hora actuales del sistema.

- **Cada N semanas**

  La tarea se ejecuta regularmente, con el intervalo especificado en semanas, en el día especificado de la semana y en el tiempo especificado.

  De forma predeterminada, la tarea se ejecuta todos los lunes a la hora actual del sistema.

- **Cada N minutos**

  La tarea se ejecuta regularmente, con el intervalo especificado en minutos, a partir de la hora especificada en el día en que se crea la tarea.

  De forma predeterminada, la tarea se ejecuta cada 30 minutos, a partir de la hora actuales del sistema.

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

  La tarea se ejecuta regularmente, con el intervalo especificado en días. Este programa no admite el cumplimiento del horario de verano (DST). Esto significa que cuando los relojes saltan una hora hacia adelante o hacia atrás al comienzo o al final del horario de verano, la hora de inicio de la tarea actual no cambia.

  No recomendamos que utilice este horario. Es necesario para la compatibilidad con versiones anteriores de Kaspersky Security Center Linux.

  De forma predeterminada, la tarea se ejecuta cada día a la hora actual del sistema.

- **Semanalmente**

  La tarea se ejecuta cada semana en el día especificado y a la hora especificada.

- **Por días de la semana**

  La tarea se ejecuta regularmente, en el día de la semana especificado y a la hora especificada.

  De forma predeterminada, la tarea se ejecuta todos los viernes a las 18:00:00 h.

- **Mensualmente**

  La tarea se ejecuta regularmente, en el día del mes especificado y a la hora especificada.

  En los meses que faltan el día especificado, la tarea se ejecuta el último día.

  De forma predeterminada, la tarea se ejecuta el primer día de cada mes, a la hora actual del sistema.

- **Manualmente**

  La tarea no se ejecuta automáticamente. Solo lo puede iniciar de forma manual.

  Esta opción está activada de forma predeterminada.

- **Cada mes, en días concretos de las semanas seleccionadas**

La tarea se ejecuta regularmente, en el día de cada mes especificado y a la hora especificada.

De forma predeterminada, no se seleccionan días del mes; la hora de inicio predeterminada es las 18:00:00 h.

- Cuando se descargan nuevas actualizaciones en el repositorio

  La tarea se ejecuta después de descargar las actualizaciones en el repositorio. Por ejemplo, es posible que desee utilizar esta programación para la tarea *Actualizar*.

- Al completar otra tarea

  La tarea actual se inicia después de que se complete otra tarea. Puede seleccionar cómo debe completarse la tarea anterior (satisfactoriamente o con errores) para activar el inicio de la tarea actual.

- Ejecutar tareas no realizadas

  Esta opción determina el comportamiento de una tarea si un dispositivo cliente no está visible en la red cuando la tarea vaya a comenzar.

  Si esta opción está activada, el sistema intentará iniciar la tarea la próxima vez que la aplicación Kaspersky se ejecute en un dispositivo cliente. Si la programación de la tarea es **Manualmente**, **Una vez** o **Inmediatamente**, la tarea se inicia inmediatamente después de que el dispositivo se haga visible en la red o inmediatamente después de que el dispositivo se incluya en la cobertura de la tarea.

  Si esta opción está desactivada, solo se ejecutarán en dispositivos cliente las tareas programadas; para **Manualmente**, **Una vez** e **Inmediatamente**, las tareas solo se ejecutarán en aquellos dispositivos cliente que estén visibles en la red. Por ejemplo, es posible que desee desactivar esta opción para una tarea que consuma recursos que desee ejecutar solo fuera del horario comercial.

  Esta opción está activada de forma predeterminada.

- Usar el retraso aleatorio automáticamente para el inicio de tareas

  Si esta opción está activada, la tarea se inicia aleatoriamente en los dispositivos cliente, dentro del intervalo de tiempo especificado, es decir, se trata de un *inicio distribuido de tarea*. El inicio distribuido de tareas ayuda a evitar que los dispositivos cliente hagan una elevada cantidad de peticiones simultáneas al Servidor de administración cuando se inicia una tarea programada.

  La hora de inicio distribuido se calcula automáticamente cuando se crea una tarea según el número de dispositivos cliente a los que se la asigna. Más tarde, la tarea se inicia siempre a la hora de inicio calculada. Sin embargo, cuando la configuración de la tarea se edita o la tarea se inicia de forma manual, el valor calculado de la hora de inicio de la tarea cambia.

  Si esta opción está desactivada, la tarea se inicia en los dispositivos cliente de acuerdo con la programación.

- Usar el retraso aleatorio para el inicio de tareas con un intervalo de (min)

  Si esta opción está activada, la tarea se inicia en los dispositivos cliente aleatoriamente dentro del intervalo de tiempo especificado. El inicio distribuido de tareas ayuda a evitar que los dispositivos cliente hagan una elevada cantidad de peticiones simultáneas al Servidor de administración cuando se inicia una tarea programada.

  Si esta opción está desactivada, la tarea se inicia en los dispositivos cliente de acuerdo con la programación.

  Esta opción está desactivada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

- Dispositivos a los que se asignará la tarea:

  - Seleccionar dispositivos de red detectados por el Servidor de administración

    La tarea se asigna a dispositivos específicos. Los dispositivos específicos pueden incluir dispositivos en grupos de administración así como dispositivos no asignados.

    Por ejemplo, es posible que desee usar esta opción en una tarea de instalación del Agente de red en dispositivos no asignados.

  - Especificar direcciones de dispositivo manualmente o importar direcciones de la lista

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

    Es posible que desee utilizar esta opción para ejecutar una tarea para una subred específica. Por ejemplo, es posible que desee instalar una aplicación determinada en dispositivos de contadores o analizar dispositivos en una subred que probablemente esté infectada.

  - Asignar tarea a una selección de dispositivos

    La tarea se asigna a los dispositivos incluidos en una selección de dispositivos. Puede especificar una de las selecciones existentes.

Por ejemplo, es posible que desee utilizar esta opción para ejecutar una tarea en dispositivos con una versión específica del sistema operativo.

- **Asignar tarea a un grupo de administración**

  La tarea se asigna a los dispositivos incluidos en un grupo de administración. Puede especificar uno de los grupos existentes o crear uno nuevo.

  Por ejemplo, es posible que desee utilizar esta opción para ejecutar una tarea de envío de un mensaje a los usuarios si el mensaje es específico para dispositivos incluidos en un grupo de administración específico.

- Configuraciones de la cuenta:

  - **Cuenta preconfigurada**

    La tarea se ejecutará bajo la misma cuenta donde se ejecuta la aplicación de esta tarea.

    Esta opción está seleccionada de forma predeterminada.

  - **Especificar una cuenta**

    Rellene los campos **Cuenta** y **Contraseña** para especificar los detalles de la cuenta en la que se ejecuta la tarea. La cuenta debe tener los derechos suficientes para esta tarea.

  - **Cuenta**

    Cuenta bajo la que se ejecuta la tarea.

  - **Contraseña**

    La contraseña de la cuenta bajo la cual la tarea se ejecutará.

Configuraciones especificadas después de la creación de tareas

Puede especificar la siguiente configuración solo después de crear una tarea.

- Ajustes de la tarea de grupo:

  - **Distribuir a subgrupos**

    Esta opción solo está disponible en la configuración de las tareas de grupo.

    Cuando esta opción está activada, la cobertura de la tarea incluye:

    - El grupo de administración que seleccionó al crear la tarea.
    - Los grupos de administración subordinados al grupo de administración seleccionado en cualquier nivel inferior al de la jerarquía del grupo.

    Cuando esta opción está desactivada, el alcance de la tarea incluye solo el grupo de administración que seleccionó al crear la tarea.

    Esta opción está activada de forma predeterminada.

  - **Distribuir a Servidores de administración secundarios y virtuales**

    Cuando esta opción está activada, la tarea que es efectiva en el Servidor de administración principal también se aplica en los Servidores de administración secundarios (incluidos los virtuales). Si ya existe una tarea del mismo tipo en el Servidor de administración secundario, ambas tareas se aplican en el Servidor de administración secundario: el existente y el heredado del Servidor de administración principal.

    Esta opción solo está disponible cuando está activada la opción **Distribuir a subgrupos**.

    Esta opción está desactivada de forma predeterminada.

- Configuración de programación avanzada:

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

El sistema operativo en el dispositivo se inicia a la hora especificada antes de que se inicie la tarea. El intervalo de tiempo predeterminado es de cinco minutos.

Active esta opción si desea que la tarea se ejecute en todos los dispositivos cliente desde el ámbito de la tarea, incluidos aquellos dispositivos que están apagados cuando la tarea está a punto de comenzar.

Si desea que el dispositivo se apague automáticamente una vez completada la tarea, habilite la opción **Cerrar el dispositivo cuando se complete la tarea**. Esta opción se puede encontrar en la misma ventana.

Esta opción está desactivada de forma predeterminada.

- Apagar el dispositivo después de completar la tarea

  Por ejemplo, es posible que desee activar esta opción para una tarea de actualización de instalación que instale actualizaciones en los dispositivos cliente todos los viernes después del horario comercial y después apagar estos dispositivos para el fin de semana.

  Esta opción está desactivada de forma predeterminada.

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

  Una vez que el periodo de tiempo especificado expira, la tarea se detiene automáticamente, ya esté completa o no.

  Active esta opción si desea interrumpir (o detener) las tareas que tardan mucho en ejecutarse.

  Esta opción está desactivada de forma predeterminada. El tiempo de ejecución de la tarea predeterminado es de 120 minutos.

- Configuración de la notificación:
  - Bloque **Historial de la tarea de la tienda**:
    - Almacenar en la base de datos del Servidor de administración durante (días)

      Los eventos de la aplicación relacionados con la ejecución de la tarea en todos los dispositivos cliente del ámbito de la tarea se almacenan en el Servidor de administración durante el número de días especificado. Cuando transcurre este periodo, la información se elimina del Servidor de administración.

      Esta opción está activada de forma predeterminada.

    - Almacenar en el registro de eventos del SO del dispositivo

      Los eventos de la aplicación relacionados con la ejecución de la tarea se almacenan localmente en el Registro de eventos de Syslog de cada dispositivo cliente.

      Esta opción está desactivada de forma predeterminada.

    - Almacenar en el registro de eventos del SO del Servidor de administración

      Los eventos de la aplicación relacionados con la ejecución de la tarea en todos los dispositivos cliente del ámbito de la tarea se almacenan de forma centralizada en el Registro de eventos de Syslog del sistema operativo (SO) del Servidor de administración.

      Esta opción está desactivada de forma predeterminada.

    - Guardar todos los eventos

      Si se selecciona esta opción, todos los eventos relacionados con la tarea se guardan en los registros del evento.

    - Guardar eventos sobre el progreso de la tarea

      Si se selecciona esta opción, solo los eventos relacionados con la ejecución de la tarea se guardan en los registros del evento.

    - Guardar solo los resultados de ejecución de la tarea

      Si se selecciona esta opción, solo los eventos relacionados con los resultados de la tarea se guardan en los registros del evento.

  - Notificar al administrador los resultados de la ejecución de tareas

Puede seleccionar los métodos por los cuales los administradores reciben notificaciones sobre los resultados de la ejecución de la tarea: por correo electrónico, por SMS y ejecutando un archivo ejecutable. Para configurar la notificación, haga clic en el enlace **Configuración**.

De forma predeterminada, todos los métodos de notificación están deshabilitados.

- Notificar solo de errores

  Si esta opción está habilitada, solo se notifica a los administradores cuando una ejecución de tarea se completa con un error.

  Si esta opción está desactivada, se notifica a los administradores después de cada finalización de la ejecución de la tarea.

  Esta opción está activada de forma predeterminada.

- Configuración de seguridad.
- Configuración de la cobertura de la tarea.

  Dependiendo de cómo se determine la cobertura de la tarea, están presentes las siguientes configuraciones:

  - Dispositivos

    Si la cobertura de una tarea está determinada por un grupo de administración, puede ver este grupo. No hay cambios disponibles aquí. Sin embargo, puede configurar **Exclusiones de la cobertura de la tarea**.

    Si la cobertura de una tarea está determinado por una lista de dispositivos, puede modificar esta lista añadiendo y eliminando dispositivos.

  - Selección de dispositivos

    Puede cambiar la selección de dispositivos a la que se aplicará la tarea.

  - Exclusiones de la cobertura de la tarea

    Puede especificar grupos de dispositivos a los que no se aplica la tarea. Los grupos que se excluyen solo pueden ser subgrupos del grupo de administración al que se aplica la tarea.

- **Historial de revisión.**

Inicio del Asistente para cambiar contraseñas de tareas

Para una tarea no local, puede especificar una cuenta en la que se debe ejecutar la tarea. Puede especificar la cuenta durante la creación de la tarea o en las propiedades de una tarea existente. 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 establece 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. Alternativamente, 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

Expandir todo | Contraer todo

Especifique las nuevas credenciales que sean 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 la nueva cuenta, seleccione una opción:

- Utilizar cuenta actual

El Asistente utiliza el nombre de la cuenta con la que ha iniciado sesión actualmente en Kaspersky Security Center 14 Web Console. Luego, especifique manualmente la contraseña de la cuenta en el campo **Contraseña actual para utilizar en tareas**.

- **Especificar una cuenta distinta**

  Especifique el nombre de la cuenta con la que se deben iniciar las tareas. Luego especifique la contraseña de la cuenta en el campo **Contraseña actual para utilizar en 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. Seleccione la casilla junto a la tarea para la que desee elegir una acción.
2. Realice una de las siguientes acciones:
   - Para eliminar la contraseña en las propiedades de la tarea, haga clic en **Eliminar credenciales**.

     La tarea cambia para ejecutarse con la cuenta predeterminada.
   - Para reemplazar la contraseña con la nueva, haga clic en **Aplicar el cambio de contraseña incluso si la contraseña anterior no se proporcionó o es incorrecta**.
   - Para cancelar el cambio de contraseña, haga clic en **No se seleccionó ninguna acción**.

Las acciones elegidas se aplican después de pasar 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 completar el Asistente, haga clic en el botón **Finalizar**.

Visualizar los resultados de ejecución de la tarea almacenados en el Servidor de administración

Kaspersky Security Center Linux le permite ver los resultados de las tareas de grupo, las tareas asignadas a dispositivos específicos y las tareas del Servidor de administración. No se pueden visualizar los resultados de ejecución de las tareas locales.

Para visualizar los resultados de tarea:

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

Administración de dispositivos cliente

Esta sección describe cómo administrar dispositivos en los grupos de administración.

Configuración de un dispositivo administrado

Expandir todo | Contraer todo

Para ver la configuración de un dispositivo administrado, siga estos pasos:

1. Seleccione **DISPOSITIVOS → DISPOSITIVOS ADMINISTRADOS**.

   Se muestra la lista de dispositivos administrados.
2. En la lista de dispositivos administrados, haga clic en el enlace con el nombre del dispositivo requerido.

Se muestra la ventana de propiedades del dispositivo seleccionado.

General

La sección **General** muestra información general sobre el dispositivo cliente. La información proporcionada se basa en los datos recibidos durante la última sincronización del dispositivo cliente con el Servidor de administración:

- Nombre

  En este campo se puede ver y modificar el nombre del dispositivo cliente en el grupo de administración.

- Descripción

  En este campo se puede introducir una descripción adicional para un dispositivo cliente.

- Grupo

  Grupo de administración que incluye 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 estuvo visible por última vez en la red.

- Conectado al Servidor de administración

  Fecha y hora en que el Agente de red instalado en el dispositivo cliente se conectó por última vez al Servidor de administración.

- No desconectar del Servidor de administración

  Si esta opción está activada, se mantiene la conectividad continua entre el dispositivo administrado y el Servidor de administración. Es posible que desee usar esta opción si no está utilizando servidores push, que proporcionan dicha conectividad.

  Si esta opción está desactivada y los servidores push no están en uso, el dispositivo administrado solo se conecta al Servidor de administración para sincronizar datos o transmitir información.

  El número total máximo de dispositivos con la opción **No desconectar del Servidor de administración** seleccionada es 300.

  Esta opción está desactivada de manera predeterminada en los dispositivos administrados. Esta opción está activada de manera predeterminada en el dispositivo donde está instalado el Servidor de administración y permanece así incluso si intenta desactivarla.

Red

La sección **Red** proporciona la siguiente información sobre las propiedades de la 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** ofrece información sobre el estado actual de la protección antivirus en un dispositivo cliente:

- Estado del dispositivo

  Estado del dispositivo cliente, asignado según los criterios definidos por el administrador para el estado de la protección antivirus en el dispositivo y la actividad del dispositivo en la red.

- Todos los problemas

  Esta tabla contiene una lista completa de problemas detectados por las aplicaciones administradas instaladas en el dispositivo cliente. Cada problema va acompañado de un estado, que la aplicación sugiere que asigne al dispositivo para este problema.

- Protección en tiempo real

  Este campo muestra el estado actual de la protección en tiempo real en el dispositivo cliente.

  Cuando el estado cambia en el dispositivo, el nuevo estado se muestra en la ventana de propiedades del dispositivo solo después de que el dispositivo cliente se sincronice con el Servidor de administración.

- Último análisis a petición

  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 fecha en que el contador de amenazas se puso a cero.

- Amenazas activas

  Número de archivos no procesados en el dispositivo cliente.

  Este campo omite 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 que está instalada en el dispositivo. El estado del dispositivo puede ser diferente al definido por Kaspersky Security Center Linux Cloud Console.

Aplicaciones

La sección **Aplicaciones** enumera todas las aplicaciones Kaspersky instaladas en el dispositivo cliente. Puede hacer clic en el nombre de la aplicación para consultar la información general sobre la aplicación, una lista de eventos que se han producido en el dispositivo y la configuración de la aplicación.

Directivas activas y perfiles de directivas

La sección **Directivas activas y perfiles de directivas** enumera las directivas y los perfiles de directivas que se encuentran activos en el dispositivo administrado.

Tareas

En la sección **Tareas**, puede administrar tareas del dispositivo cliente: ver la lista de tareas existentes, crear nuevas, eliminar, iniciar y detener tareas, modificar su configuración y ver resultados de ejecución. La lista de tareas se proporciona a partir de los datos recibidos durante la última sesión de sincronización del cliente con el Servidor de administración. El Servidor de administración solicita los detalles de estado de la tarea desde el dispositivo cliente. No se mostrará el estado si no se ha establecido conexión.

Eventos

La sección **Eventos** muestra eventos registrados en el Servidor de administración para el dispositivo cliente seleccionado.

Etiquetas

En la sección **Etiquetas** puede administrar la lista de palabras clave que se utilizan para buscar dispositivos cliente: ver la lista de etiquetas existentes, asignar etiquetas de la lista, configurar reglas de etiquetado automático, añadir etiquetas nuevas y cambiar el nombre de las antiguas y eliminar etiquetas.

Archivos ejecutables

La sección **Archivos ejecutables** muestra los archivos ejecutables encontrados en el dispositivo cliente.

Puntos de distribución

Esta sección proporciona una lista de puntos de distribución con los cuales interactúa el dispositivo.

- Exportar a archivo

  Haga clic en el botón **Exportar a archivo** para guardar a un archivo una lista de puntos de distribución con los cuales interacciona el dispositivo. De forma predeterminada, la aplicación exporta la lista de dispositivos a un archivo CSV.

- Propiedades

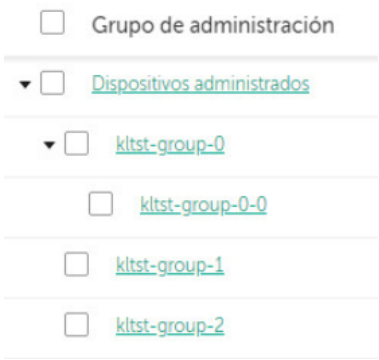
  Haga clic en el botón **Propiedades** para ver y configurar el punto de distribución con el cual interactúa el dispositivo.

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 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 (ver la figura de abajo).



Visualización de la jerarquía de los 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 que quiere incluir en el nuevo grupo de administración.
3. Haga clic en el botón **Añadir**.

4. En la ventana **Nombre del nuevo grupo de administración** que se abre, introduzca un nombre para el grupo y haga clic en el botón **Añadir**.

Aparece un nuevo grupo de administración con el nombre especificado en la jerarquía de los grupos de administración.

Para crear una estructura de grupos de administración:

1. Vaya a **DISPOSITIVOS → JERARQUÍA DE GRUPOS**.
2. Haga clic en el botón **Importar**.

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 mediante *reglas de movimiento de dispositivos*. Una regla de movimiento de dispositivo 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.

Todas las reglas de movimiento de dispositivos tienen prioridades. El Servidor de administración comprueba los atributos del dispositivo en cuanto a si cumplen la condición de ejecución de cada regla, en orden ascendente de prioridad. Si los atributos del dispositivo cumplen la condición de ejecución de una regla, el dispositivo se mueve al grupo de destino, por lo que el procesamiento de la regla está completo para ese dispositivo. Si los atributos del dispositivo cumplen las condiciones de varias reglas, el dispositivo se mueve al grupo de destino de la regla con la prioridad más alta (es decir, el que tiene el rango más alto 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 el Agente de red se instala en él. Además, el administrador de Kaspersky Security Center Linux puede crear reglas de movimiento de dispositivos explícitamente en la sección **DISPOSITIVOS → REGLAS DE MOVIMIENTO**.

De forma predeterminada, una regla de movimiento de dispositivo está destinada para la asignación inicial única de dispositivos a grupos de administración. La regla mueve dispositivos del grupo dispositivos no asignados solo una vez. Si esta regla movió un dispositivo una vez, la regla nunca lo moverá nuevamente, aun si devuelve el dispositivo al grupo dispositivos no asignados manualmente. Esta es la forma recomendada de aplicar reglas de movimiento.

Puede mover dispositivos que ya se hayan asignado a algunos de los grupos de administración. Para hacer esto, en las propiedades de una regla, borre la casilla de verificación **Mover solo dispositivos que no pertenezcan a ningún grupo de administración**.

Aplicar reglas de movimiento a dispositivos que ya se han asignado a algunos de los grupos de administración aumenta considerablemente la carga en el Servidor de administración.

Puede crear una regla de movimiento que afectaría un solo dispositivo repetidamente.

Recomendamos encarecidamente que evite mover un dispositivo solo desde un grupo a 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 Servidor de administración y el tráfico de red a un grado extremo. Estas situaciones también entran en conflicto con los principios de funcionamiento de Kaspersky Security Center Linux (en particular, en el área de derechos de acceso, eventos e informes). Otra solución se debe encontrar, por ejemplo, a través del uso de perfiles de directiva, tareas para selecciones de dispositivos, asignación de Agentes de red según el escenario estándar, etcétera.

Crear reglas de movimiento de dispositivos

Expandir todo | Contraer todo

Puede configurar reglas de movimiento de dispositivos; es decir, reglas que asignan automáticamente dispositivos a grupos de administración.

Para crear una regla móvil:

1. En el menú principal, vaya a la pestaña **DISPOSITIVOS → REGLAS DE MOVIMIENTO**.
2. Haga clic en **Añadir**.
3. En la ventana que se abre, especifique la siguiente información en la pestaña **Control de aplicaciones**:

- **Nombre de la regla**

  Introduzca un nombre para la nueva regla.

Si está copiando una regla, la nueva regla recibe el mismo nombre que la regla de origen, pero se añade un índice en formato () al nombre, por ejemplo: (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 en cada dispositivo.

    La regla se aplica una vez para cada dispositivo que coincida con sus criterios.

  - Ejecutar una vez en cada dispositivo y luego cada vez que vuelva a instalar el Agente de red.

    La regla se aplica una vez para cada dispositivo que coincida con sus criterios, luego solo cuando el Agente de red se reinstala en estos dispositivos.

  - Regla aplicada continuamente.

    La regla se aplica de acuerdo con el programa que el Servidor de administración configura automáticamente (generalmente cada varias horas).

- Mover solo dispositivos que no pertenezcan a ningún grupo de administración

  Si esta opción está activada, solo los dispositivos no asignados se moverán al grupo seleccionado.

  Si esta opción está desactivada, los dispositivos que ya pertenecen a otros grupos de administración, así como a los dispositivos no asignados, se moverán al grupo seleccionado.

- Activar regla

  Si esta opción está activada, la regla se activa y empieza a funcionar después de que se guarde.

  Si esta opción está desactivada, la regla se crea pero no se activa. No funcionará hasta que habilites esta opción.

4. En la pestaña **Condiciones de reglas**, 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 móvil. Se muestra en la lista de reglas móviles. Cuanto más alta sea la posición en la lista, mayor será la prioridad de la regla. Si los atributos del dispositivo cumplen las condiciones de varias reglas, el dispositivo se mueve al grupo de destino de la regla con la prioridad más alta (es decir, el que tiene el rango más alto en la lista de reglas).

Copiar reglas de movimiento de dispositivos

Expandir todo | Contraer todo

Puede copiar reglas en movimiento, por ejemplo, si desea tener varias reglas idénticas para diferentes grupos de administración de destino.

Para copiar una regla móvil existente:

1. En el menú principal, vaya a la pestaña **DISPOSITIVOS → REGLAS DE MOVIMIENTO**.

   También puede seleccionar **DETECCIÓN Y DESPLIEGUE → DESPLIEGUE Y ASIGNACIÓN** y después seleccionar **REGLAS DE MOVIMIENTO**.

   Se muestra la lista de reglas de movimiento.
2. Seleccione las casillas de verificación al lado de la regla que quiere copiar.
3. Haga clic en **Copiar**.
4. En la ventana que se abre, cambie la siguiente información en la pestaña **Control de aplicaciones** o no realice cambios si solo desea copiar la regla sin cambiar su configuración:

   - Nombre de la regla

     Introduzca un nombre para la nueva regla.

     Si está copiando una regla, la nueva regla recibe el mismo nombre que la regla de origen, pero se añade un índice en formato () al nombre, por ejemplo: (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 en cada dispositivo.

    La regla se aplica una vez para cada dispositivo que coincida con sus criterios.

  - Ejecutar una vez en cada dispositivo y luego cada vez que vuelva a instalar el Agente de red.

    La regla se aplica una vez para cada dispositivo que coincida con sus criterios, luego solo cuando el Agente de red se reinstala en estos dispositivos.

  - Regla aplicada continuamente.

    La regla se aplica de acuerdo con el programa que el Servidor de administración configura automáticamente (generalmente cada varias horas).

- **Mover solo dispositivos que no pertenezcan a ningún grupo de administración**

  Si esta opción está activada, solo los dispositivos no asignados se moverán al grupo seleccionado.

  Si esta opción está desactivada, los dispositivos que ya pertenecen a otros grupos de administración, así como a los dispositivos no asignados, se moverán al grupo seleccionado.

- **Activar regla**

  Si esta opción está activada, la regla se activa y empieza a funcionar después de que se guarde.

  Si esta opción está desactivada, la regla se crea pero no se activa. No funcionará hasta que habilites esta opción.

5. En la pestaña **Condiciones de reglas**, 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. Se muestra en la lista de reglas móviles.

Condiciones para una reglas de movimiento de dispositivos

Expandir todo | Contraer todo

Cuando usted crea o copia una regla para mover dispositivos cliente a grupos de administración, establece en la pestaña **Condiciones de reglas** 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 ficha, 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 activar las siguientes opciones:

- **Aplicar a los dispositivos que no tengan etiquetas especificadas**

Si esta opción está activada, 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 desactivada de forma predeterminada.

- Aplicar si coincide al menos una etiqueta especificada

  Si esta opción está activada, se aplica una regla de movimiento de dispositivos a los dispositivos cliente con al menos una de las etiquetas seleccionadas. Si esta opción está desactivada, la regla de movimiento de dispositivos se aplica a los dispositivos con todas las etiquetas seleccionadas.

  Esta opción está desactivada de forma predeterminada.

Pestaña Red

En esta pestaña, puede especificar los datos de red de los dispositivos a los que atañe una regla de movimiento de dispositivos:

- Nombre 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.

- Rango IP

  Si esta opción está activada, se pueden introducir las direcciones IP inicial y final del rango IP en el que se incluirán los dispositivos pertinentes.

  Esta opción está desactivada de forma predeterminada.

- Dirección IP para conectar con el Servidor de administración

  Si esta opción está activada, 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 desactivada de forma predeterminada.

- Perfil de conexión modificado

  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.
  - **No se ha seleccionado ningún valor**. La condición no se aplica.

- Administrado por otro Servidor de administración

  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.
  - **No se ha seleccionado ningún valor**. 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 está 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.
  - **No se ha seleccionado ningún valor**. 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 activa esta opción, la condición no se aplica. La opción está desactivada de forma predeterminada.

- Tamaño de bits del sistema operativo

  Puede seleccionar dispositivos cliente según el tamaño de bits del sistema operativo. En el bloque **Tamaño de bits 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 **Tamaño de bits del sistema operativo**, y haga clic en el botón **Guardar**.

     Después, se muestra el tamaño de bits del sistema operativo para cada dispositivo administrado.

- Versión del 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 forma predeterminada, no se especifica ningún valor de la versión.

- 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.
  - **No instalado**. La regla de movimiento de dispositivos solo se aplica a dispositivos móviles sin un certificado móvil.
  - **No se ha seleccionado ningún valor**. La condición no se aplica.

- Compilación del sistema operativo

Esta configuración solo se aplica a los sistemas operativos de Windows.

Puede especificar si el sistema operativo seleccionado debe tener un número de compilación igual, anterior o posterior. También puede configurar la búsqueda de una regla de movimiento para todos los números de compilación, excepto el especificado.

- Número de versión del sistema operativo

  Esta configuración solo se aplica a los sistemas operativos de 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):

- 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.

Adición de dispositivos al grupo de administración manualmente

Puede mover automáticamente dispositivos a grupos de administración creando reglas de movimiento de dispositivos o manualmente, moviendo dispositivos de un grupo de administración a otro o añadiendo dispositivos al grupo de administración seleccionado. Esta sección describe cómo añadir manualmente dispositivos a un grupo de administración.

Para añadir uno o más dispositivos a un grupo de administración seleccionado:

1. Vaya a **DISPOSITIVOS** → **DISPOSITIVOS ADMINISTRADOS**.
2. Haga clic en el enlace **Ruta actual:** `<ruta actual>` encima de la lista.
3. En la ventana que se abre, seleccione el grupo de administración al que desea añadir los dispositivos.
4. Haga clic en el botón **Añadir dispositivos**.
   Se inicia el Asistente para mover dispositivos.
5. Haga una lista de los dispositivos que desea añadir al grupo de administración.

   Solo se pueden añadir dispositivos cuya información se haya añadido a la base de datos del Servidor de administración o bien al conectarse el dispositivo o bien después de la detección de dispositivos.

Seleccione cómo desea añadir dispositivos a la lista:

- Haga clic en el botón **Añadir dispositivos** y luego especifique los dispositivos de una de las siguientes maneras:
  - Seleccione los dispositivos de la lista de dispositivos detectados por el Servidor de administración.
  - Especifique la dirección IP del dispositivo o un rango de IP.
  - Especifique el nombre DNS del dispositivo.

    El campo del nombre del dispositivo no debe contener caracteres de espacio, caracteres de retroceso, ni los siguientes caracteres prohibidos: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %
- Haga clic en el botón **Importar dispositivos desde un archivo** para importar una lista de dispositivos desde un archivo .txt. Cada dirección o nombre del dispositivo debe especificarse en una línea separada.

  El archivo no debe contener caracteres de espacio, caracteres de retroceso, ni los siguientes caracteres prohibidos: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %

6. Ver la lista de dispositivos que se añadirán al grupo de administración. Puede editar la lista añadiendo o quitando dispositivos.
7. Habiéndose asegurado de que la lista es correcta, haga clic en el botón **Siguiente**.

El Asistente procesa la lista de dispositivos y muestra el resultado. Los dispositivos correctamente procesados se incluyen en el grupo de administración y se muestran en la lista de dispositivos con nombres generados por el Servidor de administración.

Traslado manual de dispositivos al grupo de administración

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 donde se encuentran los dispositivos que desea mover. Puede hacerlo de una de las siguientes maneras:
   - Para abrir un grupo de administración, vaya a **DISPOSITIVOS** → **Grupos** → **<nombre del grupo>** → **DISPOSITIVOS ADMINISTRADOS**.
   - Para abrir el grupo **DISPOSITIVOS NO ASIGNADOS**, vaya a **DETECCIÓN Y DESPLIEGUE** → **DISPOSITIVOS NO ASIGNADOS**.
2. Seleccione las casillas de verificación junto a los dispositivos que desea mover a un grupo diferente.
3. Haga clic en el botón **Mover a un grupo**.
4. En la jerarquía de grupos de administración, seleccione la casilla de verificación junto al grupo de administración al que desea mover los dispositivos seleccionados.
5. Haga clic en el botón **Mover**.

Los dispositivos seleccionados se mueven al grupo de administración seleccionado.

Cambio del Servidor de administración de los dispositivos cliente

Para dispositivos cliente específicos, puede cambiar el Servidor de administración a otro. Para ello, utilice la tarea *Cambiar Servidor de administración*.

Para cambiar el Servidor de administración que gestiona los dispositivos cliente a otro servidor:

1. Conéctese al Servidor de administración que administra los dispositivos.
2. Cree la tarea de cambio del Servidor de administración.

   Se inicia el Asistente para añadir tareas. Siga las instrucciones del Asistente. En la ventana **Nueva tarea** del Asistente para añadir tareas, seleccione la aplicación **Proveedor** y el tipo de tarea **Cambiar Servidor de administración**. Después, especifique los dispositivos para los que desea cambiar el Servidor de administración:

   - Asignar tarea a un grupo de administración

     La tarea se asigna a los dispositivos incluidos en un grupo de administración. Puede especificar uno de los grupos existentes o crear uno nuevo.

Por ejemplo, es posible que desee utilizar esta opción para ejecutar una tarea de envío de un mensaje a los usuarios si el mensaje es específico para dispositivos incluidos en un grupo de administración específico.

- Especificar direcciones de dispositivo manualmente o importar direcciones desde una lista

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

  Es posible que desee utilizar esta opción para ejecutar una tarea para una subred específica. Por ejemplo, es posible que desee instalar una aplicación determinada en dispositivos de contadores o analizar dispositivos en una subred que probablemente esté infectada.

- Asignar tarea a una selección de dispositivos

  La tarea se asigna a los dispositivos incluidos en una selección de dispositivos. Puede especificar una de las selecciones existentes.

  Por ejemplo, es posible que desee utilizar esta opción para ejecutar una tarea en dispositivos con una versión específica del sistema operativo.

3. Ejecute la tarea creada.

Tras completarse la tarea, los dispositivos cliente para los que se la creó se ponen bajo la administración del Servidor de administración especificado en los parámetros de tarea.

Ver y configurar las acciones cuando los dispositivos muestran inactividad

Expandir todo | Contraer todo

Si los dispositivos cliente dentro de un grupo están inactivos, puede recibir notificaciones al respecto. También puede eliminar automáticamente dichos dispositivos.

Para ver o configurar las acciones cuando los dispositivos del grupo muestran inactividad:

1. En el menú principal, vaya a **DISPOSITIVOS → JERARQUÍA DE GRUPOS**.
2. Haga clic en el nombre del grupo de administración requerido.

   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 en esta sección se heredará del grupo primario en el que se incluye el dispositivo cliente. Si esta opción está activada, la configuración de **Actividad de los dispositivos en la red** se bloquea de cualquier cambio.

     Esta opción está disponible solo si el grupo de administración tiene un grupo primario.

     Esta opción está activada de forma predeterminada.

   - Forzar la herencia de la configuración en los grupos secundarios

     Los valores de configuración se distribuirán a grupos secundarios, pero en las propiedades de los grupos secundarios estas configuraciones están bloqueadas.

     Esta opción está desactivada de forma predeterminada.

5. En la sección **Actividad de los dispositivos**, active o desactive las siguientes opciones:

   - Notificar al administrador si el dispositivo ha estado inactivo durante más de (días)

     Si esta opción está activada, el administrador recibe notificaciones sobre dispositivos inactivos. Puede especificar el intervalo de tiempo después del cual se crea el **dispositivo inactivo en la red en un evento de larga duración**. De forma predeterminada, el intervalo de tiempo es 7 día.

     Esta opción está activada de forma predeterminada.

   - Quitar el dispositivo del grupo si ha estado inactivo durante más de (días)

Si esta opción está activada, puede especificar el intervalo de tiempo después del cual el dispositivo se eliminará automáticamente del grupo. De forma predeterminada, el intervalo de tiempo es 60 día.

Esta opción está activada de forma predeterminada.

6. Haga clic en **Guardar**.

Sus cambios están guardados y aplicados.

Acerca de los estados de los dispositivos

Kaspersky Security Center Linux asigna un estado a cada dispositivo administrado. El estado particular depende de si se cumplen 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*
- *Correcto* o *Correcto/Visible*

La tabla a continuación enumera las condiciones predeterminadas que se deben cumplir para asignar el estado *Crítico* o *Advertencia* a un dispositivo, con todos los valores posibles.

Condiciones para asignar 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 una aplicación de seguridad no está instalada.	• El botón está activado. • El botón está desactivado.
Demasiados virus detectados	Una tarea de detección de virus (por ejemplo, la tarea de análisis antivirus) ha detectado 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 es distinto del establecido por el administrador	El dispositivo es visible en la red, pero el nivel de la protección en tiempo real se diferencia del nivel configurado (en la condición) por el administrador para el estado del dispositivo.	• Detenido. • En pausa. • En ejecución.
No se ha realizado ningún análisis antivirus desde hace mucho tiempo	El dispositivo es visible en la red y una aplicación de seguridad está instalada en el dispositivo, pero la tarea de análisis antivirus no se ha ejecutado durante el intervalo de tiempo especificado. La condición se aplica solo a los dispositivos que se agregaron a la base de datos del Servidor de administración hace siete días o antes.	Más de 1 día.
Las bases de datos están desactualizadas	El dispositivo es visible en la red y una aplicación de seguridad está instalada en el dispositivo, pero las bases de datos antivirus no se han actualizado en este dispositivo durante el intervalo de tiempo especificado. La condición se aplica solo a los dispositivos que se agregaron a la base de datos del Servidor de administración hace un día o antes.	Más de 1 día.
No conectado durante mucho tiempo	El Agente de red está instalado en el dispositivo, pero el dispositivo no se ha conectado a un Servidor de administración durante el intervalo de tiempo especificado porque el dispositivo se desactivó.	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 requiere reiniciar	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 el inventario del software realizado a través del Agente de red ha detectado aplicaciones incompatibles instaladas en el dispositivo.	• El botón está desactivado.

		• El botón está activado.
La licencia comercial ha caducado	El dispositivo es visible en la red, pero la licencia ha caducado.	• El botón está desactivado. • El botón está activado.
la licencia caduca pronto	El dispositivo es visible en la red, pero la licencia caduca en el dispositivo en menos días que el número especificado de días.	Más de 0 días.
Incidentes sin procesar detectados	Se han detectado algunos incidentes no procesados en el dispositivo. Los incidentes se pueden crear automáticamente, mediante las aplicaciones administradas por Kaspersky que están instaladas en el dispositivo cliente, o el administrador las puede crear de forma manual.	• El botón está desactivado. • El botón está activado.
Estado del dispositivo definido por la aplicación	El estado del dispositivo se define por la aplicación administrada.	• El botón está desactivado. • El botón está activado.
El dispositivo no tiene espacio disponible en el disco	El espacio libre en disco en el dispositivo es menor que el valor especificado o el dispositivo no se pudo sincronizar con el Servidor de administración. El estado *Crítico* o *Advertencia* pasa al estado *Correcto* cuando el dispositivo se sincroniza correctamente con el Servidor de administración y el espacio libre en el dispositivo es mayor o igual al valor especificado.	Más de 0 MB.
Se ha perdido la conexión con el dispositivo	Durante la detección de dispositivos, el dispositivo se reconoció como visible en la red, pero más de tres intentos de sincronizar con el Servidor de administración fallaron.	• El botón está desactivado. • El botón está activado.
La protección está desactivada	El dispositivo es visible en la red, pero la aplicación de seguridad en el dispositivo se ha desactivado durante más tiempo que el intervalo de tiempo especificado.	Más de 0 minutos.
La aplicación de seguridad no se está ejecutando	El dispositivo es visible en la red y hay una aplicación de seguridad instalada en el dispositivo pero no se está ejecutando.	• El botón está desactivado. • El botón está activado.

Kaspersky Security Center Linux le permite configurar el cambio automático del estado de un dispositivo en un grupo de administración cuando las condiciones especificadas se cumplen. Cuando las condiciones especificadas se cumplen, se asigna al dispositivo cliente uno de los estados siguientes: *Crítico* o *Advertencia*. Cuando no se cumplen las condiciones especificadas, al dispositivo cliente se le asigna el estado *Correcto*.

Distintos estados pueden corresponder a distintos valores de una condición. Por ejemplo, de manera predeterminada, si 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 fuera **Más de 7 días**, se le asignaría 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 la condición) se tiene en cuenta el indicador de visibilidad. Por ejemplo, si a un dispositivo administrado se le ha asignado el estado *Crítico* porque se cumplió la condición Las bases de datos están desactualizadas, y luego se configuró el indicador de visibilidad para el dispositivo, entonces al dispositivo se le asigna el estado *Correcto*.

Configuración del cambio de estado de los dispositivos

Puede cambiar las condiciones para asignar el estado *Crítico* o *Advertencia* a un dispositivo.

Para activar el cambio del estado del dispositivo a Crítico:

1. Abra la ventana de propiedades de alguno de los siguientes modos:
   - 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 **Asignar Crítico si se especifican**, marque la casilla junto a una de las condiciones de la lista.

   Solo puede cambiar la configuración que no esté bloqueada en la directiva primaria.

4. Configure el valor requerido para la condición seleccionada.
   Puede establecer valores para algunas condiciones pero no para todas.
5. Haga clic en **Aceptar**.

Cuando se cumplen las condiciones especificadas, al dispositivo administrado se le asigna el estado *Crítico*.

Para activar el cambio del estado del dispositivo a Advertencia:

1. Abra la ventana de propiedades de alguno de los siguientes modos:
   - En la carpeta **Directivas** en el menú contextual de la 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 **Asignar Advertencia si se especifican**, marque la casilla junto a una de las condiciones de la lista.

   Solo puede cambiar la configuración que no esté bloqueada en la directiva primaria.

4. Configure el valor requerido para la condición seleccionada.
   Puede establecer valores para algunas condiciones pero no para todas.
5. Haga clic en **Aceptar**.

Cuando se cumplen las condiciones especificadas, al dispositivo administrado se le asigna el estado *Advertencia*.

Directivas y perfiles de directivas

En Kaspersky Security Center 14 Web Console, puede crear directivas para las aplicaciones de Kaspersky. Esta sección describe las directivas y los perfiles de directivas, y proporciona instrucciones para crearlos y modificarlos.

Acerca de las directivas y perfiles de directivas

Una *directiva* es un conjunto de configuraciones de aplicaciones de Kaspersky que se aplican a un grupo de administración y sus subgrupos. Puede instalar varias aplicaciones de Kaspersky en los dispositivos de un grupo de administración. Kaspersky Security Center proporciona una directiva única para cada aplicación de Kaspersky en un grupo de administración. Una política tiene uno de los siguientes estados:

El estado de la directiva

Estado	Descripción

Activo	La directiva actual que se aplica al dispositivo. Solo una directiva puede estar activa para una aplicación de Kaspersky en cada grupo de administración. Los dispositivos aplican los valores de configuración de una directiva activa para una aplicación de Kaspersky.
Inactiva	Una directiva que no se aplica actualmente a un dispositivo.
Fuera de la oficina	Si se selecciona esta opción, la directiva se activa cuando un dispositivo sale de la red corporativa.

Las directivas funcionan según las siguientes reglas:

- Se pueden configurar varias directivas con diferentes valores para una única aplicación.
- Solo una directiva puede estar activa para la aplicación actual.
- Una directiva puede tener directivas secundarias.

Generalmente, puede utilizar las directivas como preparación para situaciones de emergencia, como el ataque de un virus. Por ejemplo, si se trata de un ataque a través de unidades flash, puede activar una directiva que bloquee el acceso a las unidades flash. En este caso, la directiva activa actual se vuelve inactiva automáticamente.

Para evitar el mantenimiento de varias directivas, por ejemplo, cuando en diferentes ocasiones se supone el cambio de varias configuraciones únicamente, puede utilizar perfiles de directivas.

Un *perfil de directiva* es un subconjunto con nombre de valores de configuración de directiva que reemplaza los valores de configuración de una directiva. Un perfil de directiva afecta la formación de configuraciones efectivas en un dispositivo administrado. Las *configuraciones efectivas* son un conjunto de configuraciones de directivas, configuraciones de perfiles de directivas y configuraciones de aplicaciones locales que están aplicadas en ese momento en el dispositivo.

Los perfiles de directivas funcionan según las siguientes reglas:

- Un perfil de directiva entra en vigor cuando se produce una condición de activación específica.
- Los perfiles de directivas contienen valores de configuración que difieren de la configuración de la directiva.
- La activación de un perfil de directiva cambia la configuración efectiva del dispositivo administrado.
- Una directiva puede incluir un máximo de 100 perfiles de directivas.

Acerca del bloqueo y los ajustes bloqueados

Cada configuración de directiva tiene un icono de botón de bloqueo ( ). La siguiente tabla muestra los estados de los botones de bloqueo:

Estados de los botones de bloqueo

Estado	Descripción
Sin definir	Si se muestra un candado abierto junto a una configuración y el botón de alternar está desactivado, la configuración no está especificada en la directiva. El usuario puede cambiar esta configuración en la interfaz de la aplicación administrada. Este tipo de configuraciones se denominan *configuraciones desbloqueadas*.
Aplicar	Si se muestra un candado cerrado junto a una configuración y el botón de alternancia está activado, la configuración se aplica a los dispositivos donde se la directiva es obligatoria. Un usuario no podrá modificar los valores de esta configuración en la interfaz de la aplicación administrada. Este tipo de configuraciones se denominan *configuraciones bloqueadas*.

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 un botón de bloqueo para realizar las siguientes acciones:

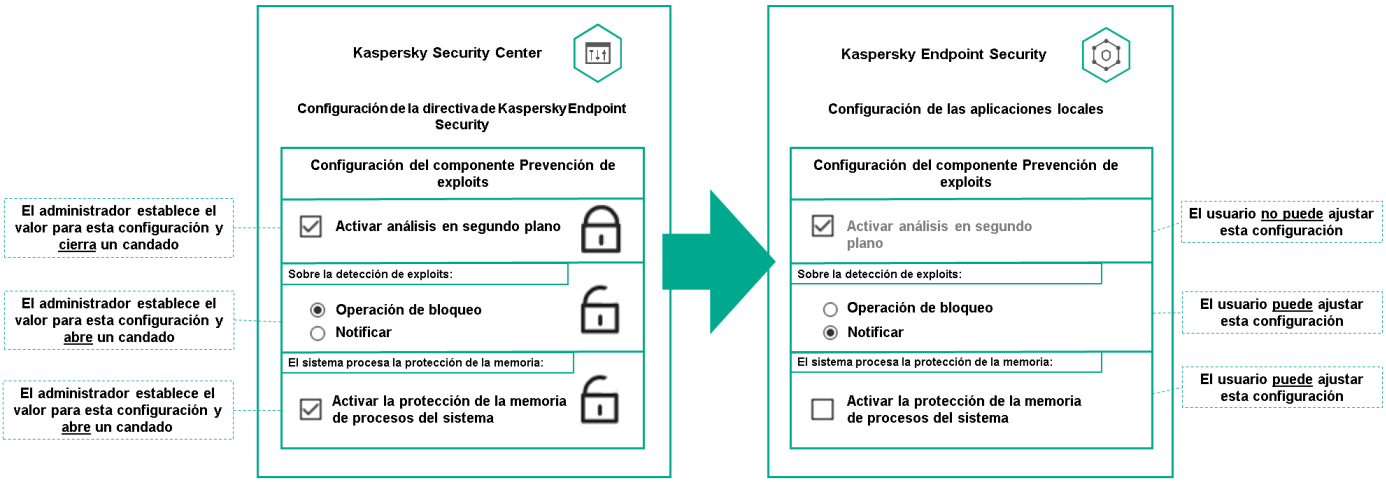
- Bloqueo de la configuración para una directiva de subgrupo de administración
- Bloqueo de la configuración de una aplicación de Kaspersky en un dispositivo administrado

Por lo tanto, una configuración bloqueada se utiliza para implementar configuraciones efectivas en un dispositivo administrado.

Un proceso de implementación efectiva de configuraciones incluye las siguientes acciones:

- El dispositivo administrado aplica los valores de configuración de la aplicación Kaspersky.
- El dispositivo administrado aplica los valores de configuración bloqueados de una directiva.

Una directiva y una aplicación de Kaspersky local contienen el mismo conjunto de configuraciones. Cuando ajusta la configuración de directiva, la configuración de la aplicación de Kaspersky cambia los valores en un dispositivo administrado. Usted no puede ajustar la configuración bloqueada en un dispositivo administrado (consulte la figura a continuación):



Configuración de bloqueos y aplicaciones de Kaspersky

Herencia de directivas y perfiles de directivas

Esta sección brinda información sobre la jerarquía y la herencia de directivas y perfiles de directivas.

Jerarquía de directivas

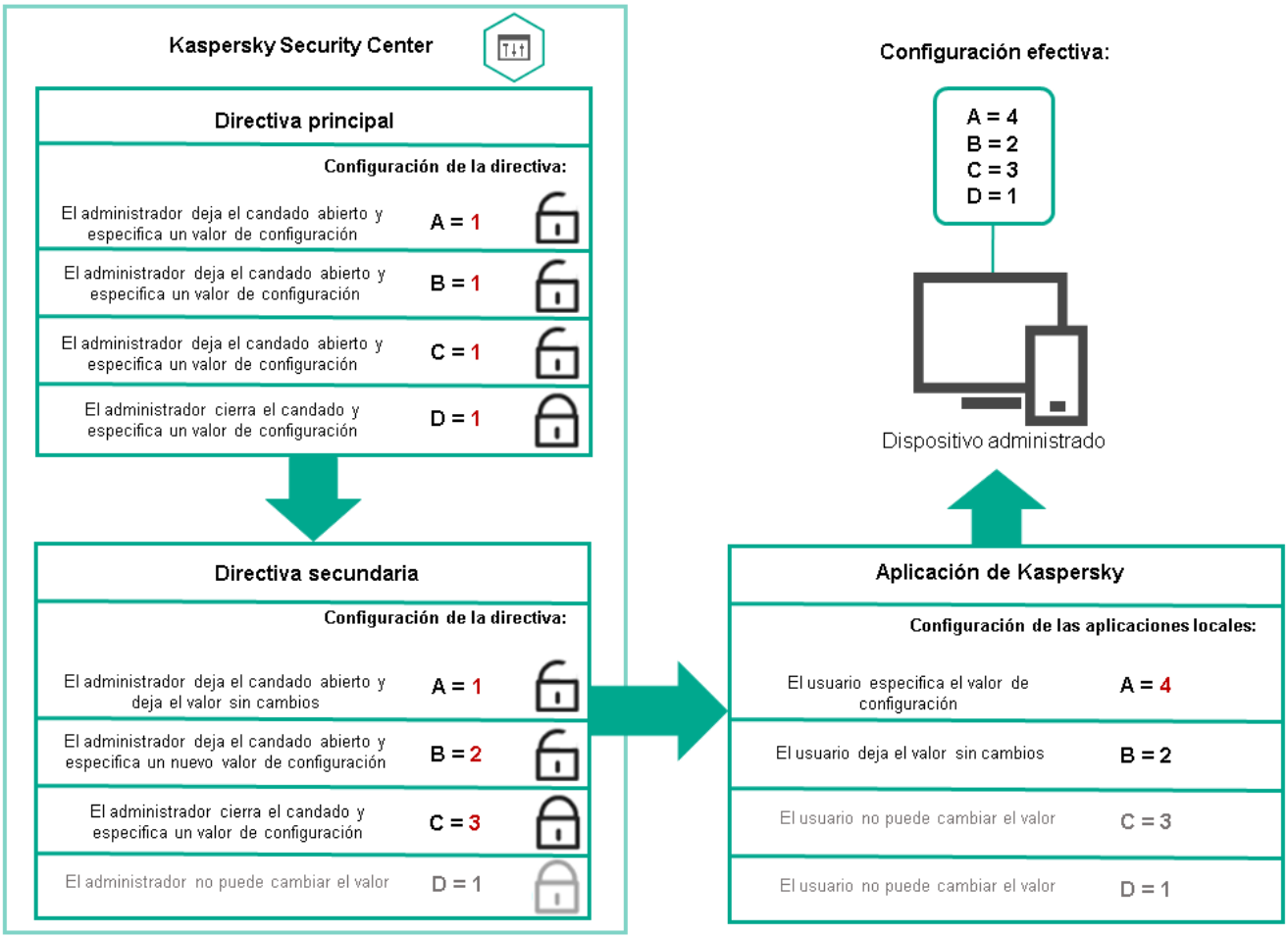
Si diferentes dispositivos necesitan diferentes configuraciones, puede organizar los dispositivos en grupos de administración.

Puede especificar una directiva para un grupo de administración único. La configuración de la directiva se puede *heredar*. Heredar una directiva significa recibir valores de configuración de directivas en subgrupos (grupos secundarios) de una directiva de un grupo de administración de nivel superior (principal).

En adelante, también se hará referencia a una directiva para un grupo primario como *directiva primaria*. Una directiva para un subgrupo (grupo secundario) también se denomina *directiva secundaria*.

De forma predeterminada, existe al menos un grupo de dispositivos administrados en el Servidor de administración. Si desea crear grupos personalizados, se crean como subgrupos (grupos secundarios) dentro del grupo de dispositivos administrados.

Las directivas de la misma aplicación actúan entre sí, de acuerdo con una jerarquía de grupos de administración. La configuración bloqueada de una directiva de un grupo de administración de nivel superior (principal) reasignará los valores de configuración de la directiva de un subgrupo (consulte la figura siguiente).

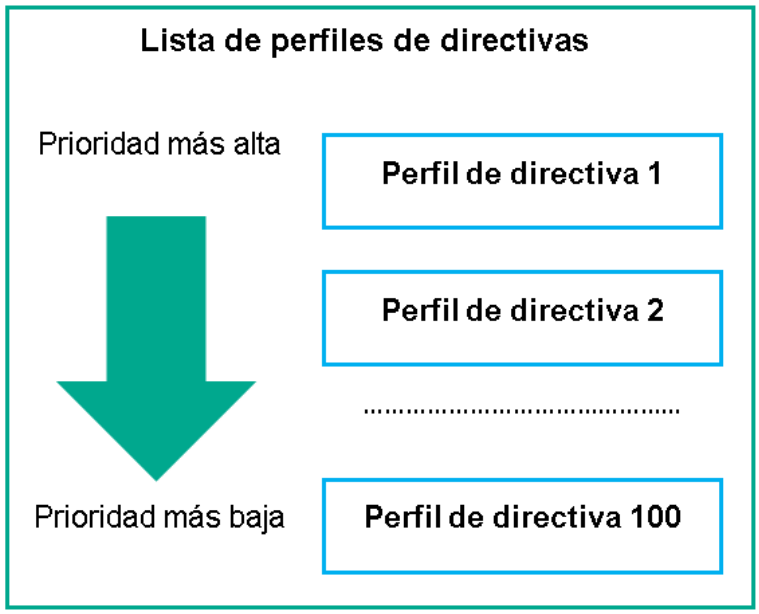


Jerarquía de directivas

Perfiles de directivas en una jerarquía de directivas

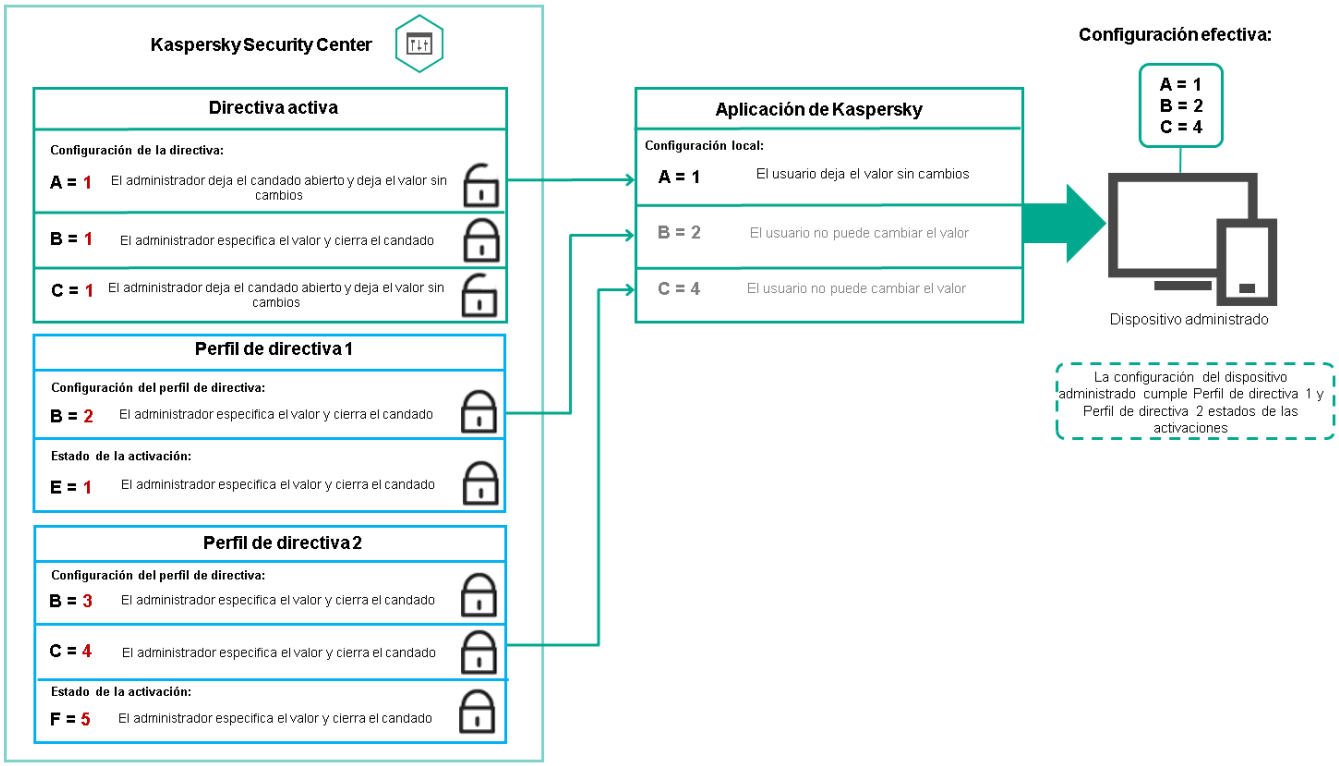
Los perfiles de directiva tienen las siguientes condiciones de asignación de prioridad:

- La posición de un perfil en una lista de perfiles de directivas indica su prioridad. Puede cambiar una prioridad de perfil de directiva. La posición más alta en una lista indica que la máxima prioridad (consulte la siguiente figura).



Definición de prioridades de un perfil de directiva

- Las condiciones de activación de los perfiles de directivas no dependen unas de otras. Se pueden activar varios perfiles de directivas simultáneamente. Si varios perfiles de directiva afectan la misma configuración, el dispositivo toma el valor de configuración del perfil de directiva con la prioridad más alta (consulte la siguiente figura).

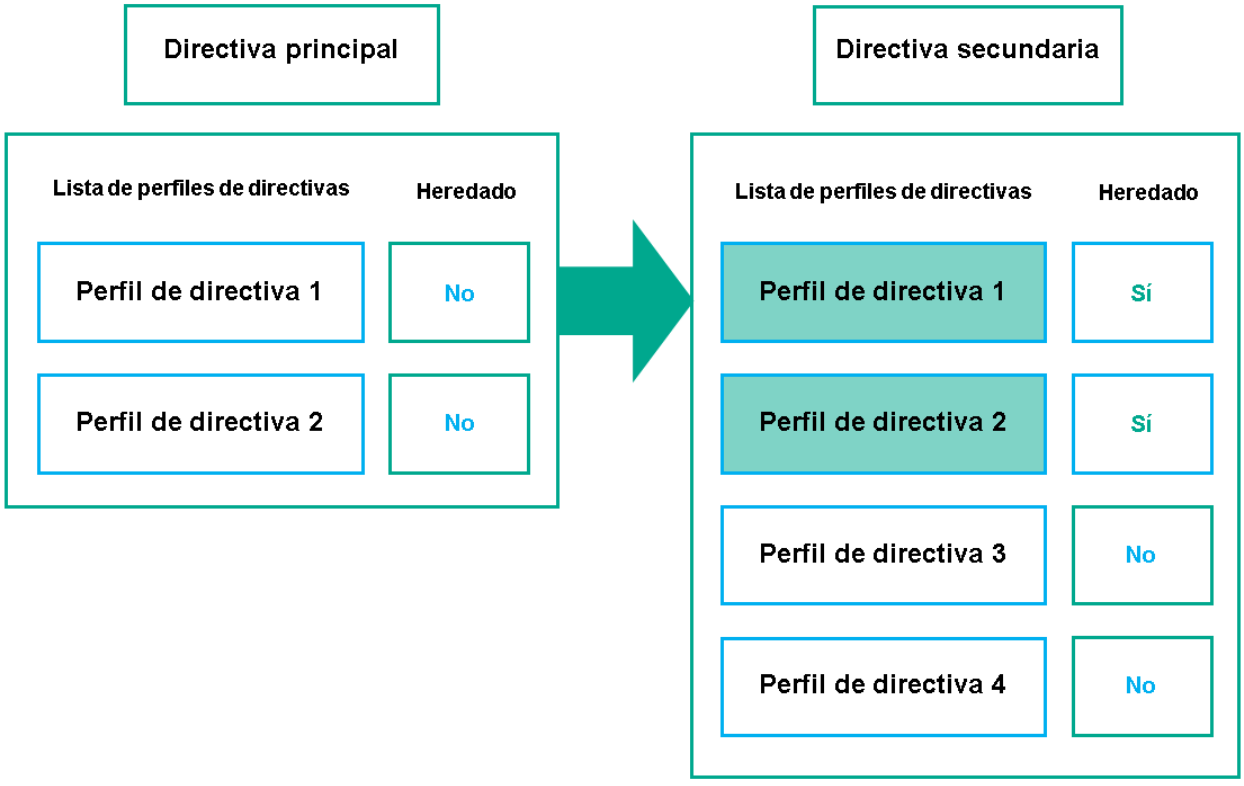


La configuración del dispositivo administrado cumple las condiciones de activación de varios perfiles de directivas

Perfiles de directivas en una jerarquía de herencia

Los perfiles de directiva de las directivas de diferentes niveles de jerarquía cumplen con las siguientes condiciones:

- Una directiva de nivel inferior hereda los perfiles de directivas de una directiva de nivel superior. Un perfil de directiva heredado de una directiva de nivel superior tiene mayor prioridad que el nivel del perfil de directiva original.
- No puede cambiar la prioridad de un perfil de directiva heredado (consulte la figura siguiente).

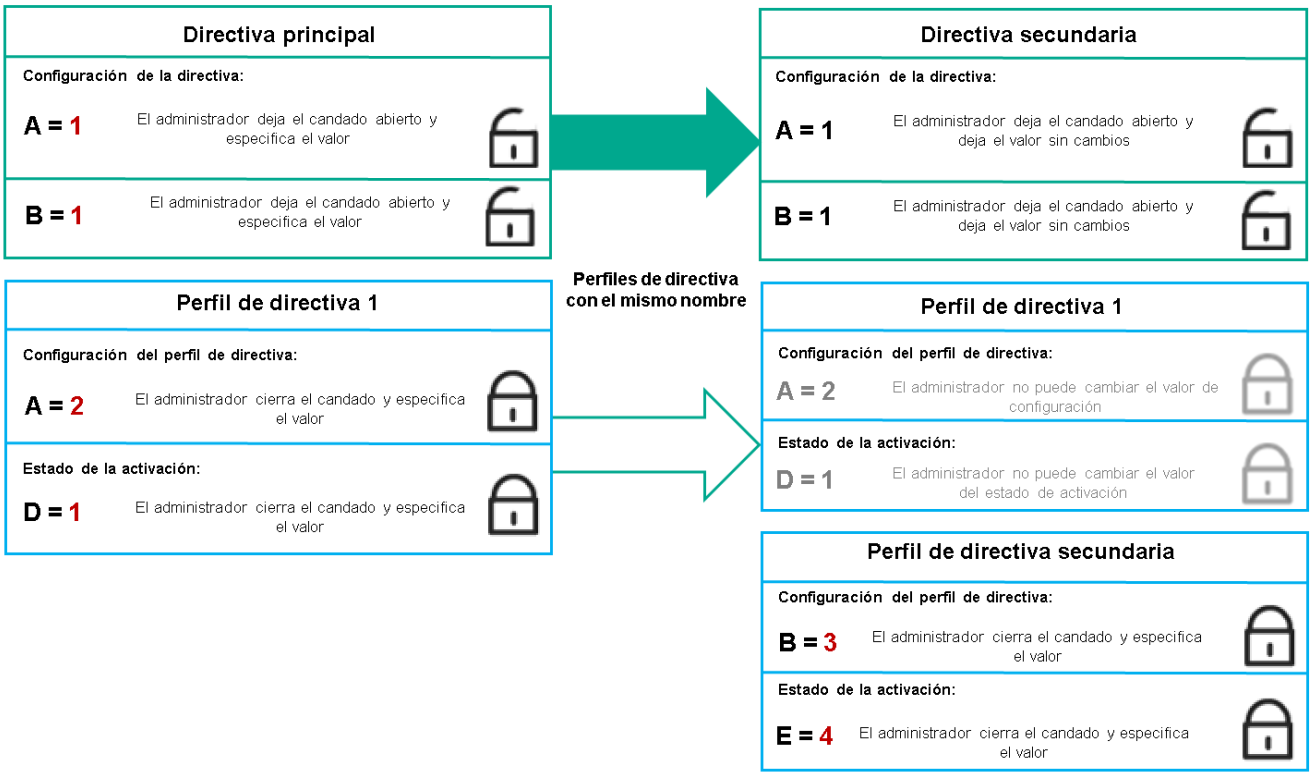


Herencia de los perfiles de directiva

Perfiles de directiva con el mismo nombre

Si hay dos directivas con el mismo nombre en diferentes niveles de jerarquía, estas directivas funcionan de acuerdo con las siguientes reglas:

- La configuración bloqueada y la condición de activación del perfil de un perfil de directiva de nivel superior cambian la configuración y la condición de activación del perfil de un perfil de directiva de nivel inferior (consulte la siguiente figura).



El perfil secundario hereda los valores de configuración de un perfil de directiva principal

- La configuración desbloqueada y la condición de activación del perfil de un perfil de directiva de nivel superior no cambian la configuración y la condición de activación del perfil de un perfil de directiva de nivel inferior.

Cómo se implementan las configuraciones en un dispositivo administrado

La implementación de configuraciones efectivas en un dispositivo administrado se puede describir de la siguiente manera:

- Los valores de todos los ajustes que no se han bloqueado se toman de la directiva.
- Luego se sobrescriben con los valores de los ajustes de la aplicación administrada.
- Y luego se aplican los valores de configuración bloqueados de la directiva efectiva. Los valores de los ajustes bloqueados cambian los valores de los ajustes efectivos desbloqueados.

Administrar directivas

Esta sección describe la gestión de directivas y proporciona información sobre cómo ver la lista de directivas, crear una directiva, modificar una directiva, copiar una directiva, mover una directiva, forzar la sincronización, ver el cuadro de estado de distribución de directivas y eliminar una directiva.

Visualización de la lista de directivas

Puede ver las listas de 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 del grupo de administración, seleccione el grupo de administración para el que desea ver la lista de directivas.

Aparece la lista de directivas en formato tabular. Si no hay directivas, la tabla está vacía. Puede mostrar o esconder las columnas de la tabla, cambiar su orden, ver solo las líneas que contienen un valor que especifique o utilizar la búsqueda.

Creación de una directiva

Puede crear directivas; también puede modificar y eliminar directivas existentes.

Para crear una directiva:

1. Vaya a **DISPOSITIVOS → DIRECTIVAS Y PERFILES**.
2. Haga clic en **Añadir**.

   Se abre la ventana **Seleccionar aplicación**.
3. Seleccione la aplicación para la que desea crear una directiva.
4. Haga clic en **Siguiente**.

   La ventana de propiedades de nueva directiva se abre con la pestaña **Control de aplicaciones** seleccionada.
5. Si lo desea, cambie el nombre predeterminado, el estado predeterminado y la configuración de herencia predeterminada de la directiva.
6. Seleccione la pestaña **Configuración de la aplicación**.

   O, puede hacer clic en **Guardar**. La directiva aparecerá en la lista de directivas, y podrá editar su configuración más adelante.
7. En la pestaña **Configuración de la aplicación**, en el panel izquierdo, seleccione la categoría que desea y, en el panel de resultados de la derecha, edite la configuración de la directiva. Puede editar la configuración de directivas 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
   - Configuración 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.

Configuración general de las directivas

Expandir todo | Contraer todo

Control de aplicaciones

En la pestaña **Control de aplicaciones**, puede modificar el estado de la directiva y especificar la herencia de la configuración de la directiva:

- En el bloque **Estado de la directiva**, puede seleccionar uno de los modos de la directiva:
  - **Activa**

    Si se selecciona esta opción, se activa la directiva.

    Esta opción está seleccionada de forma predeterminada.
  - **Fuera de la oficina**

    Si se selecciona esta opción, la directiva se activa cuando un dispositivo sale de la red corporativa.
  - **Inactiva**

    Si se selecciona esta opción, se inactiva la directiva, pero sigue almacenada en la carpeta **Directivas**. Si fuera necesario, se puede activar la directiva.
- En la sección de grupo **Herencia de configuración**, se puede configurar la herencia de directivas:
  - **Heredar configuración de la directiva primaria**

Si se activa esta opción, los valores de la configuración de la directiva se heredan de la directiva de grupos de nivel superior y, por lo tanto, quedan bloqueados.

Esta opción está activada de forma predeterminada.

- Forzar la herencia de la configuración en las directivas secundarias

  Si se activa esta opción, después de aplicar modificaciones a las directivas, se realizarán las siguientes acciones:

  - Los valores de los parámetros de las directivas se distribuirán a las directivas de los grupos de administración anidados, es decir, a las directivas secundarias.
  - En el bloque **Herencia de configuración** de la sección **General** de la ventana de propiedades de cada directiva secundaria, se activará automáticamente la opción **Heredar configuración de la directiva primaria**.

  Si se activa esta opción, la configuración de las directivas secundarias queda bloqueada.

  Esta opción está desactivada de forma predeterminada.

Configuración de eventos

La ficha **Configuración de eventos** le permite configurar el registro de eventos y la notificación de eventos. Los eventos se distribuyen en las fichas siguientes según el nivel de importancia:

- **Crítico**

  La ficha **Crítico** no se muestra en las propiedades de la directiva del Agente de red.
- **Fallo operativo**
- **Advertencia**
- **Información**

En cada sección, la lista muestra los tipos de eventos y el plazo de almacenamiento de eventos predeterminado en el Servidor de administración (en días). Al hacer clic en un tipo de evento le permite especificar la siguiente configuración:

- **Registro de eventos**

  Puede especificar cuántos días para almacenar el evento y seleccionar dónde almacenar el evento:

  - **Exportar al sistema SIEM a través de Syslog**
  - **Almacenar en el registro de eventos del SO del dispositivo**
  - **Almacenar en el registro de eventos del SO del Servidor de administración**
- **Notificaciones de 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 script o archivo ejecutable**
  - **Notificar por SNMP**

  De forma predeterminada, se utilizan las configuraciones de notificación especificadas en la pestaña de propiedades del Servidor de administración (como la dirección del destinatario). Si lo desea, puede cambiar esta configuración en la pestaña **Correo electrónico**, **SMS** y **Archivo ejecutable para lanzar**.

Historial de revisión

La pestaña **Historial de revisión** le permite ver la lista de revisiones de la directiva y revertir los cambios realizados en la directiva, si es necesario.

Modificación de una directiva

Para modificar una directiva:

1. Vaya a **DISPOSITIVOS → DIRECTIVAS Y PERFILES**.

2. Haga clic en la directiva que desea modificar.

   Se abre la ventana de configuración de directivas.

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
   - Configuración 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 esa aplicación.

4. Haga clic en **Guardar**.

Los cambios hechos a la directiva se guardarán en las propiedades de la directiva y aparecerán en la sección **Historial de revisión**.

Habilitar y deshabilitar una opción de herencia de directivas

Para activar o desactivar la opción de herencia en una directiva:

1. Abra la directiva requerida.
2. Abra la pestaña **Control de aplicaciones**.
3. Active o desactive la herencia de directivas:

   - Si activa **Heredar configuración de la directiva primaria** en una directiva secundaria y un administrador bloquea alguna configuración de la directiva primaria, no podrá cambiar esa configuración en la directiva secundaria.
   - Si desactiva **Heredar configuración de la directiva primaria** en una directiva secundaria, podrá cambiar toda la configuración de la directiva secundaria, incluso si hay parámetros bloqueados en la directiva primaria.
   - Si activa **Forzar la herencia de la configuración en las directivas secundarias** en el grupo primario, se activará **Heredar configuración de la directiva primaria** para cada directiva secundaria. En este caso, no puede desactivar esta opción para ninguna directiva secundaria. Todos los parámetros de configuración bloqueados en la directiva primaria se heredan obligatoriamente en los grupos secundarios y no puede cambiarlos en esos grupos.

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 activada para las directivas nuevas.

Si una directiva tiene perfiles, todas las directivas secundarias heredan estos perfiles.

Copia de 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. Seleccione la casilla de verificación junto a la directiva (o directivas) que desea copiar.
3. Haga clic en el botón **Copiar**.

   En el lado derecho de la pantalla, aparece el árbol de los grupos de administración.

4. En el árbol, seleccione el grupo objetivo, es decir, el grupo al que desea copiar la directiva (directivas).
5. Haga clic en el botón **Copiar** al final de la pantalla.
6. Haga clic en **Aceptar** para confirmar la operación.

La directiva (directivas) se copiarán al grupo objetivo con todos sus perfiles. El estado de cada directiva copiada en el grupo objetivo será **Inactiva**. Puede cambiar el estado a **Activa** en cualquier momento.

Si ya existe una directiva con el nombre idéntico al de la directiva recién movida en el grupo objetivo, el nombre de la directiva recién movida se expande con el índice (<siguiente número secuencial>); por ejemplo: (1).

Movimiento de una directiva

Puede mover directivas de un grupo de administración a otro. Por ejemplo, desea eliminar un grupo, pero desea utilizar sus directivas para otro grupo. En este caso, le recomendamos que mueva la directiva del grupo anterior al nuevo antes de eliminar el grupo anterior.

Para mover una directiva a otro grupo de administración:

1. En el menú principal, vaya a **DISPOSITIVOS → DIRECTIVAS Y PERFILES**.
2. Seleccione la casilla de verificación junto a la directiva (o directivas) que desea mover.
3. Haga clic en el botón **Mover**.

   En el lado derecho de la pantalla, aparece el árbol de los grupos de administración.
4. En el árbol, seleccione el grupo de destino, es decir, el grupo al que desea mover la directiva (o directivas).
5. Haga clic en el botón **Mover** al final de la pantalla.
6. Haga clic en **Aceptar** para confirmar la operación.

Si una directiva no se hereda del grupo de origen, se mueve al grupo objetivo con todos sus perfiles. El estado de la directiva en el grupo objetivo es **Inactiva**. Puede cambiar el estado a **Activa** en cualquier momento.

Si una directiva se hereda del grupo de origen, permanece en el grupo de origen. Se copia al grupo objetivo con todos sus perfiles. El estado de la directiva en el grupo objetivo es **Inactiva**. Puede cambiar el estado a **Activa** en cualquier momento.

Si ya existe una directiva con el nombre idéntico al de la directiva recién movida en el grupo objetivo, el nombre de la directiva recién movida se expande con el índice (<siguiente número secuencial>); por ejemplo: (1).

Forzar sincronización

Si bien Kaspersky Security Center Linux sincroniza el estado, la configuración, las tareas y las directivas para los dispositivos administrados automáticamente, en algunos casos, usted debe saber exactamente si la sincronización ya se ha realizado para un dispositivo específico en un momento dado.

Sincronización de 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 desea sincronizar con el Servidor de administración.

   Se abrirá una ventana de propiedades con la sección **Control de aplicaciones** seleccionada.
3. Haga clic en el botón **Forzar sincronización**.

La aplicación sincroniza el dispositivo seleccionado con el Servidor de administración.

Sincronización de múltiples dispositivos

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:
   - Vaya a **DISPOSITIVOS → DISPOSITIVOS ADMINISTRADOS → Grupos** y seleccione el grupo de administración que contiene los dispositivos que desea sincronizar.
   - Ejecute una selección de dispositivos para ver la lista de dispositivos.
2. Seleccione las casillas de verificación junto a los dispositivos que desea sincronizar con el Servidor de administración.
3. Haga clic en el botón **Forzar sincronización**.

   La aplicación sincroniza los dispositivos seleccionados con el Servidor de administración.
4. En la lista de dispositivos, puede ver que la hora de la última conexión al Servidor de administración de los dispositivos seleccionados ha cambiado a la hora actual. Si la hora no ha cambiado, actualice el contenido de la página haciendo clic en el botón **Actualizar**.

Los dispositivos seleccionados se sincronizan con el Servidor de administración.

Visualización del tiempo 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 hora en que se entregó una directiva de la aplicación a un dispositivo administrado, haga lo siguiente:

1. Vaya a **DISPOSITIVOS → DISPOSITIVOS ADMINISTRADOS**.
2. Haga clic en el nombre del dispositivo que desea sincronizar con el Servidor de administración.

   Se abrirá una ventana de propiedades con la sección **Control de aplicaciones** seleccionada.
3. Haga clic en la pestaña **Aplicaciones**.
4. Seleccione la aplicación para la que desea ver la fecha de sincronización de la directiva.

   La ventana de directiva de la aplicación se abre con la sección **Control de aplicaciones** seleccionada y la fecha y hora de entrega de la directiva mostradas.

Visualización del diagrama del estado de distribución de directivas

En Kaspersky Security Center, puede ver el estado de la aplicación de directivas en cada dispositivo en un gráfico del estado de distribución de directivas.

Para ver el estado de distribución de directivas en cada dispositivo:

1. Vaya a **DISPOSITIVOS → DIRECTIVAS Y PERFILES**.
2. Seleccione la casilla de verificación junto al nombre de la directiva cuyo estado de distribución en los dispositivos desea ver.
3. En el menú que aparece, seleccione el enlace **Distribución**.

   Se abre la ventana **Resultados de la distribución de <nombre de la directiva>**.
4. En la ventana **Resultados de la distribución de <nombre de la directiva>** que se abre, se muestra la **Descripción del estado** de la directiva.

Puede cambiar el número de resultados que se muestran en la lista con la distribución de directivas. El número predeterminado de eventos es de 100.000.

Para cambiar la cantidad de dispositivos que se muestran en la lista de resultados de la distribución de directivas:

1. Vaya a la sección **Opciones de interfaz** en la barra de herramientas.
2. En el **Límite de dispositivos que se muestran en los resultados de distribución de directivas**, ingrese la cantidad de dispositivos (hasta 100.000).

   El número de puerto predeterminado es 5000.
3. Haga clic en **Guardar**.

   Sus cambios quedan guardados y aplicados.

Eliminación de una directiva

Puede eliminar una directiva si ya no la necesita. Solo puede eliminar una directiva que no se herede en el grupo de administración especificado. Si se hereda una directiva, solo puede eliminarla en el grupo de nivel superior para el que se creó.

Para eliminar una directiva:

1. En el menú principal, vaya a **DISPOSITIVOS → DIRECTIVAS Y PERFILES**.
2. Seleccione la casilla de verificación junto a la directiva que desea eliminar y haga clic en **Eliminar**.

   El botón **Eliminar** no estará disponible (atenuado) si selecciona 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 describe la gestión de perfiles de directivas y proporciona información sobre cómo ver los perfiles de una directiva, cambiar la prioridad de un perfil de directiva, crear un perfil de directiva, copiar un perfil de directiva, crear una regla de activación de perfil de directiva y eliminar un perfil de directiva.

Visualización de perfiles de directiva

Ver 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 desea ver.

   La ventana de propiedades de la directiva se abre con la pestaña **Control de aplicaciones** 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 aparecerá vacía.

Cambiar una prioridad de perfil de directiva

Para cambiar una prioridad de perfil de directiva:

1. Vaya la lista de los perfiles de una directiva que desee.

   Aparece la lista de perfiles de directiva.
2. En la pestaña **Perfiles de directiva**, seleccione la casilla de verificación al lado del perfil de la directiva para el que desea cambiar la prioridad.
3. Establezca una nueva posición del perfil de directivas en la lista haciendo clic en **Priorizar** o **Desplorizar**.

   Cuanto mayor sea el perfil de una directiva en la lista, mayor será su prioridad.
4. Haga clic en el botón **Guardar**.

La prioridad del perfil de directivas seleccionado se cambia y se aplica.

Crear perfil de directiva

Crear perfil de directiva:

1. Vaya la lista de los perfiles de la directiva que desee.

   Aparece la lista de perfiles de directiva. Si la directiva no tiene perfiles, aparecerá una tabla vacía.
2. Haga clic en **Añadir**.
3. Si lo desea, cambie el nombre predeterminado y la configuración de herencia predeterminada del perfil.
4. Seleccione la pestaña **Configuración de la aplicación**.

   O bien, puede hacer clic en **Guardar** y salir. El perfil que ha creado aparece en la lista de perfiles de directivas y podrá editar su configuración más adelante.
5. En la pestaña **Configuración de la aplicación**, en el panel izquierdo, seleccione la categoría que desea y, en el panel de resultados de la derecha, edite la configuración del perfil. Puede editar la configuración del perfil de directiva en cada categoría (sección).

   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 directivas.

Copiar perfil de directiva

Puede copiar un perfil de directiva en la directiva actual o en otra, por ejemplo, si desea tener perfiles idénticos para directivas diferentes. También puede usar la copia si desea tener dos o más perfiles que se diferencien solo en un pequeño número de configuraciones.

Para copiar un perfil de directiva:

1. Vaya la lista de los perfiles de una directiva que desee.

   Aparece la lista de perfiles de directiva. Si la directiva no tiene perfiles, aparecerá una tabla vacía.
2. En la pestaña **Perfiles de directiva**, seleccione el perfil de la directiva que desea copiar.
3. Haga clic en **Copiar**.
4. En la ventana que se abre, seleccione la directiva en la que desea 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 la directiva se copia en la directiva que seleccionó. El perfil recién copiado obtiene la prioridad más baja. Si copia el perfil a la misma directiva, el nombre del perfil recién copiado se ampliará con el índice (), por ejemplo: (1), (2).

Más adelante, puede cambiar la configuración del perfil, incluyendo su nombre y su prioridad; el perfil de la directiva original no se cambiará en este caso.

Creación de una regla de activación de perfil de directiva

Expandir todo | Contraer todo

Para crear una regla de activación de perfil de directiva:

1. Vaya la lista de los perfiles de una directiva que desee.

   Aparece la lista de perfiles de directiva.

2. En la pestaña **Perfiles de directiva**, haga clic en el perfil de la directiva para el que tiene que crear una regla de activación.

   Si la lista de perfiles de directiva está vacía, puede crear un perfil de directiva.

3. En la pestaña **Reglas de activación**, haga clic en el botón **Añadir**.

   Se abrirá la ventana con las reglas de activación del perfil de la directiva.

4. Especifique un nombre para la regla.

5. Seleccione las casillas al lado de las condiciones que deben afectar a la activación del perfil de la directiva que está creando:

   - **Reglas generales de activación de perfiles de directivas**

     Seleccione esta casilla para configurar reglas de activación de perfiles de directiva del dispositivo según el estado del modo desconectado del dispositivo, la regla para la conexión con el Servidor de administración y las etiquetas asignadas al dispositivo.

     Para esta opción, especifique en el paso siguiente:

     - **Estado del dispositivo**

       Define la condición de 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.
       - **Desconectado**: El dispositivo está en una red externa, lo que significa que el Servidor de administración no está disponible.
       - **N/D**: No se aplica el criterio.

     - **La regla de conexión con el Servidor de administración está activa en este dispositivo**

       Elija la condición de activación del perfil de directiva (si la regla se ejecuta o no) y seleccione el nombre de la regla.

       La regla define la localización de la red del dispositivo para la conexión con el Servidor de administración, cuyas condiciones se deben cumplir (o no se debe cumplir) para la activación del perfil de la directiva.

       Se puede crear o configurarse una descripción de la ubicación de la red de dispositivos para la conexión con un Servidor de administración en una regla de conmutación de Agente de red.

   - **Reglas para un propietario del dispositivo específico**

     Para esta opción, especifique en el paso siguiente:

     - **Propietario del dispositivo**

       Seleccione esta opción para configurar y activar la regla de activación de perfil en el dispositivo según su propietario. En la lista desplegable de la casilla de verificación, puede seleccionar un criterio para la activación de perfil:

       - El dispositivo pertenece al propietario especificado (símbolo "=").
       - El dispositivo no pertenece al propietario especificado (símbolo "#").

         Si esta opción está activada, el perfil se activa en el dispositivo conforme al criterio configurado. Puede especificar el propietario del dispositivo cuando la opción está activada. Si esta opción está desactivada, el criterio de activación del perfil no se aplica. Esta opción está desactivada de forma predeterminada.

     - **El propietario del dispositivo está incluido en un grupo de seguridad interno**

Seleccione esta opción para configurar y activar la regla de activación de perfil en el dispositivo según la pertenencia del propietario del dispositivo a un grupo interno de seguridad de Kaspersky Security Center Linux. En la lista desplegable de la casilla de verificación, puede seleccionar un criterio para la activación de perfil:

- El propietario del dispositivo es un miembro del grupo de seguridad especificado (símbolo "=").
- El propietario del dispositivo no es un miembro del grupo de seguridad especificado (símbolo "#").

  Si esta opción está activada, el perfil se activa en el dispositivo conforme al criterio configurado. Puede especificar un grupo de seguridad de Kaspersky Security Center Linux. Si esta opción está desactivada, el criterio de activación del perfil no se aplica. Esta opción está desactivada de forma predeterminada.

- **Reglas para especificaciones de hardware**

  Seleccione esta casilla para configurar reglas de activación del perfil de la directiva en el dispositivo según el volumen de memoria y el número de procesadores lógicos.

  Para esta opción, especifique en el paso siguiente:

  - **Tamaño de RAM, en MB**

    Active esta opción para configurar y activar la regla de activación de perfil en el dispositivo según el volumen de RAM disponible en ese dispositivo. En la lista desplegable de la casilla de verificación, puede seleccionar un criterio para la activación de perfil:
    - El tamaño de la RAM del dispositivo es menor que el valor especificado (signo "<").
    - El tamaño de la RAM del dispositivo es mayor que el valor especificado (signo ">").

    Si esta opción está activada, el perfil se activa en el dispositivo conforme al criterio configurado. Puede especificar el volumen de RAM en el dispositivo. Si esta opción está desactivada, el criterio de activación del perfil no se aplica. Esta opción está desactivada de forma predeterminada.

  - **Número de procesadores lógicos**

    Active esta opción de verificación para configurar y activar la regla de activación de perfil en el dispositivo según el número de procesadores lógicos de dicho dispositivo. En la lista desplegable de la casilla de verificación, puede seleccionar un criterio para la activación de perfil:
    - El número de procesadores lógicos en el dispositivo es menor o igual que el valor especificado (signo "<").
    - El número de procesadores lógicos en el dispositivo es mayor o igual que el valor especificado (signo ">").

    Si esta opción está activada, el perfil se activa en el dispositivo conforme al criterio configurado. Puede especificar la cantidad de procesadores lógicos en el dispositivo. Si esta opción está desactivada, el criterio de activación del perfil no se aplica. Esta opción está desactivada de forma predeterminada.

- **Reglas para la asignación de funciones**

  Para esta opción, especifique en el paso siguiente:

  - **Activar perfil de directiva según la función específica del propietario del dispositivo**

    Seleccione esta opción para configurar y activar la regla de activación de perfil en el dispositivo según la función del propietario. Añada la función de manera manual desde la lista de funciones existentes.

    Si esta opción está activada, el perfil se activa en el dispositivo conforme al criterio configurado.

- **Reglas para el uso de etiquetas**

  Seleccione esta casilla para configurar reglas para la activación del perfil de la directiva en el dispositivo según las etiquetas asignadas al dispositivo. Puede activar el perfil de directiva tanto para los dispositivos que tienen las etiquetas seleccionadas, como para las que no las tienen.

  Para esta opción, especifique en el paso siguiente:

  - **Lista de etiquetas**

    En la lista de etiquetas, puede especificar la regla para incluir dispositivos en el perfil de la directiva seleccionando las casillas junto a las etiquetas correspondientes.

Puede añadir nuevas etiquetas a la lista al introducirlas en el campo sobre la lista y hacer clic en el botón **Añadir**.

El perfil de la directiva incluye los dispositivos con descripciones que contienen todas las etiquetas seleccionadas. El criterio no se aplica si las casillas están vacías. De forma predeterminada, estas casillas están en blanco.

- **Aplicar a los dispositivos que no tengan etiquetas especificadas**

  Active esta opción si tiene que cambiar su selección de etiquetas.

  Si se selecciona esta opción, el perfil de la directiva incluirá los dispositivos con descripciones que no contengan ninguna de las etiquetas seleccionadas. Si esta opción está desactivada, el software no se actualiza.

  Esta opción está desactivada de forma predeterminada.

El número de páginas adicionales del Asistente depende de la configuración que seleccione en el primer paso. Puede modificar las reglas de activación de perfil de la directiva más adelante.

6. Compruebe la lista de los parámetros configurados. Si la lista es correcta, haga clic en **Crear**.

El perfil se guardará. El perfil se activará en el dispositivo cuando se activen las reglas de activación.

Las reglas de activación del perfil de directiva creadas para el perfil se muestran en las propiedades del perfil de directiva en la pestaña **Reglas de activación**. Puede modificar o eliminar cualquier regla de activación de perfil de directiva.

Se pueden activar simultáneamente varias reglas de activación.

Eliminar perfil de directiva

Para eliminar el perfil de directiva:

1. Vaya la lista de los perfiles de una directiva que desee.

   Aparece la lista de perfiles de directiva.

2. En la pestaña **Perfiles de directiva**, seleccione la casilla de verificación al lado del perfil de directiva que desee eliminar y hacer 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. Esto se hace para eliminar un cambio significativo en la configuración de las aplicaciones administradas instaladas en los dispositivos de grupos de nivel inferior.

Usuarios y funciones de usuario

Esta sección describe los usuarios y las funciones de usuarios, y proporciona instrucciones para crearlos y modificarlos, para asignar funciones y grupos a los usuarios y para asociar los perfiles de directivas con las funciones.

Acerca de las funciones de usuario

Una *función de usuario* (también denominada *función*) es un objeto que contiene un conjunto de derechos y privilegios. Se puede asociar una función con la configuración de las aplicaciones de Kaspersky instaladas en un dispositivo de usuario. Puede asignar una función a un conjunto de usuarios o a un conjunto de grupos de seguridad en cualquier nivel en la jerarquía de grupos de administración.

Puede asociar funciones de usuario con perfiles de directiva. Si a un usuario se le asigna una función, este usuario obtiene la configuración de seguridad necesaria para realizar funciones de trabajo.

Una función de usuario se puede asociar con usuarios de dispositivos en un grupo de administración específico.

Cobertura de la función de usuario

Una *cobertura de la función de usuario* es una combinación de usuarios y grupos de administración. La configuración asociada con una función de usuario se aplica solo a los dispositivos que pertenecen a usuarios que tienen esta función y solo si estos dispositivos pertenecen a grupos asociados con esta función, incluidos los grupos secundarios.

Ventajas de utilizar funciones

Una ventaja de usar roles es que no tiene que especificar la configuración de seguridad para cada uno de los dispositivos administrados o para cada uno de los usuarios por separado. La cantidad de usuarios y dispositivos en una empresa puede ser bastante grande, pero la cantidad de funciones de trabajo diferentes que requieren configuraciones de seguridad diferentes es considerablemente menor.

Diferencias de utilizar perfiles de directivas

Los perfiles de directivas son propiedades de una directiva que se crea para cada aplicación de Kaspersky por separado. Una función está asociada con muchos perfiles de directivas creados para aplicaciones diferentes. Por lo tanto, una función es un método de unir configuraciones para un determinado tipo de usuario en un solo lugar.

Configuración de los derechos de acceso a las funciones de la aplicación. Control de acceso basado en funciones

Kaspersky Security Center Linux proporciona recursos para el acceso basado en funciones a las funciones de Kaspersky Security Center Linux o las aplicaciones administradas de Kaspersky.

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:

- Mediante la configuración por separado de los derechos de cada usuario o grupo de usuarios.
- Mediante la creación de funciones de usuario estándar con un conjunto de derechos preestablecido y la asignación de esas funciones a los usuarios según su ámbito de responsabilidad.

La aplicación de funciones de usuario tiene como objetivo simplificar y acortar los procedimientos de rutina para configurar los derechos de acceso de los usuarios a las funciones de la aplicación. Los derechos de acceso de una función se configuran según las tareas estándares y el ámbito de las responsabilidades de los usuarios.

A las funciones de usuario se les puede asignar nombres que se correspondan con sus respectivos propósitos. Puede crear un número ilimitado de funciones en la aplicación.

Puede utilizar las funciones de usuario predefinidas con un conjunto de derechos ya configurado, o crear nuevas funciones y configurar los derechos necesarios usted mismo.

Derechos de acceso a las funciones de la aplicación

La siguiente tabla muestra las funciones de Kaspersky Security Center Linux con los derechos de acceso para administrar las tareas, informes y configuraciones asociados y realizar las acciones de usuario asociadas.

Para realizar las acciones de usuario enumeradas en la tabla, un usuario debe tener el derecho especificado junto a la acción.

Los derechos de **lectura**, **modificación** y **ejecución** pueden aplicarse a cualquier tarea, informe o configuración. Además de estos derechos, el usuario debe tener el derecho de **Realizar operaciones en selecciones de dispositivos** para administrar tareas, informes o configuraciones en selecciones de dispositivos.

Todas las tareas, informes, configuraciones y paquetes de instalación que faltan 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	Otro
Características generales: Gestión de grupos de administración	**Modificación**	• Añadir dispositivos a un grupo de administración: **Modificación** • Eliminar dispositivos de un grupo de administración: **Modificación** • Agregar un grupo de administración a otro grupo de administración: **Modificación** • Eliminar un grupo de administración de otro	Ninguno	Ninguno	Ninguno

		grupo de administración: **Modificación**			
Características generales: **Acceder a objetos independientemente de sus ACL**	**Lectura**	Obtener acceso de lectura a todos los objetos: **Leer**	Ninguno	Ninguno	Ninguno
Características generales: **Funcionalidad básica**	• **Lectura** • **Modificación** • **Ejecución** • **Realizar operaciones en selecciones de dispositivos**	• Reglas de movimiento de dispositivos (crear, modificar o eliminar) para el Servidor virtual: **Modificación**, **realizar operaciones en selecciones de dispositivos** • Obtener certificado personalizado del protocolo móvil (LWNGT): **Lectura** • Establecer certificado personalizado del protocolo móvil (LWNGT): **Escritura** • Obtener lista de redes definidas por NLA: **Lectura** • Añadir, modificar o eliminar una lista de redes definida por NLA: **Modificación** • Ver lista de control de acceso de grupos: **Lectura** • Ver el registro de eventos de Kaspersky: **Lectura**	• "Descargar actualizaciones en el repositorio del Servidor de administración" • "Entregar informes" • "Distribuir paquetes de instalación" • "Instalar una aplicación de forma remota en Servidores de administración secundarios"	• "Informe del estado de la protección" • "Informe de amenazas" • "Informe sobre los dispositivos más infectados" • "Informe sobre el estado de las bases de datos antivirus" • "Informe de errores" • "Informe sobre ataques a la red" • "Informe resumido sobre las aplicaciones de defensa perimetral instaladas" • "Informe resumido sobre los tipos de aplicaciones instalados" • "Informe sobre usuarios de dispositivos infectados" • "Informe sobre incidentes" • "Informe sobre eventos" • "Informe sobre la actividad de los puntos de distribución" • "Informe sobre Servidores de administración" • "Informe sobre eventos de control de dispositivos"	Ninguno

				• "Informe sobre aplicaciones prohibidas" • "Informe de Control web" • "Informe sobre permisos de usuario vigentes" • "Informe sobre derechos"	
Características generales: **Objetos eliminados**	• **Lectura** • **Modificación**	• Ver objetos eliminados en la Papelera de reciclaje: **Lectura** • Eliminar objetos de la Papelera de reciclaje: **Modificación**	Ninguno	Ninguno	Ninguno
Características generales: **Procesamiento de eventos**	• **Eliminación de eventos** • **Edición de la configuración de notificación de eventos** • **Edición de la configuración del registro de eventos** • **Modificación**	• Cambiar la configuración del registro de eventos: **Edición de la configuración del registro de eventos** • Cambiar la configuración de notificación de eventos: **Edición de la configuración de notificación de eventos** • Eliminar eventos: **Eliminación de eventos**	Ninguno	Ninguno	Configuración: • Número máximo de eventos almacenados en la base de datos • Periodo de tiempo para almacenar eventos de los dispositivos eliminados
Características generales: **Operaciones en el Servidor de administración**	• **Lectura** • **Modificación** • **Ejecución** • **Modificación de las LCA de objetos** • **Realizar operaciones en selecciones de dispositivos**	• Especificar puertos del Servidor de administración para la conexión del Agente de red: **Modificación** • Especificar los puertos del Proxy de activación que se está ejecutando en el Servidor de administración: **Modificación** • Especificar los puertos del Proxy de activación de dispositivos móviles que se está ejecutando en el Servidor de administración: **Modificación** • Especificar los puertos del Servidor web para la distribución de paquetes independientes: **Modificación** • Especificar los puertos del Servidor web para la distribución de perfiles MDM: **Modificación**	• "Copia de seguridad de los datos del Servidor de administración" • "Mantenimiento de bases de datos"	Ninguno	Ninguno

		• Especificar los puertos SSL del Servidor de administración para la conexión a través de Web Console: **Modificación** • Especificar puertos del Servidor de administración para conexión de dispositivos móviles: **Modificación** • Especificar el número máximo de eventos que pueden almacenar en la base de datos del Servidor de administración: **Modificación** • Especificar el número máximo de eventos que el Servidor de administración puede enviar: **Modificación** • Especificar el periodo de tiempo durante el cual el Servidor de administración puede enviar eventos: **Modificación**			
Funciones generales: **despliegue del software de Kaspersky**	• **Administración de parches de Kaspersky** • **Lectura** • **Modificación** • **Ejecución** • **Realizar operaciones en selecciones de dispositivos**	Aprobar o rechazar la instalación del parche: **Administración de parches de Kaspersky**	Ninguno	• "Informe sobre el uso de claves de licencia por parte del Servidor de administración virtual" • "Informe de versiones de software de Kaspersky" • "Informe de aplicaciones incompatibles" • "Informe sobre las versiones de las actualizaciones del módulo de software de Kaspersky" • "Informe del despliegue de la protección"	Paquete de instalación: "Kaspersky"
Características generales: **Administración de claves**	• **Exportar archivo clave** • **Modificación**	• Exportar archivo clave: **Exportar archivo clave** • Modificar la configuración de la clave de licencia del Servidor de administración: **Modificación**	Ninguno	Ninguno	Ninguno

Características generales: **Administración de informes**	• **Lectura** • **Modificación**	• Crear informes independientemente de sus ACL: **Escritura** • Ejecutar informes independientemente de sus ACL: **Lectura**	Ninguno	Ninguno	Ninguno
Funciones generales: **Jerarquía de Servidores de administración**	**Configuración de jerarquía de Servidores de administración**	• Registrar, actualizar o eliminar Servidores de administración secundarios: **Configuración de la jerarquía del Servidor de administración**	Ninguno	Ninguno	Ninguno
Características generales: **Permisos de usuario**	**Modificación de las LCA de objetos**	• Cambiar las propiedades de "seguridad" de cualquier objeto: **Modificación de las LCA de objetos** • Administrar roles de usuario: **Modificación de las LCA de objetos** • Administrar usuarios internos: **Modificación de las LCA de objetos** • Administrar grupos de seguridad: **Modificación de las LCA de objetos** • Administrar alias: **Modificación de las LCA de objetos**	Ninguno	Ninguno	Ninguno
Características generales: **Servidores de administración virtuales**	• **Administración de Servidores de administración virtuales** • **Lectura** • **Modificación** • **Ejecución** • **Realizar operaciones en selecciones de dispositivos**	• Obtener lista de Servidores de administración: **Lectura** • Obtener información sobre el Servidor de administración virtual: **Lectura** • Crear, actualizar o eliminar un Servidor de administración virtual: **Administración de Servidores de administración virtuales** • Mover un Servidor de administración virtual a otro grupo: **Administración de Servidores de administración virtuales** • Establecer permisos de Servidor virtual de administración: **Administración de Servidores de administración virtuales**	Ninguno	Ninguno	Ninguno

Funciones de usuario predefinidas

Las funciones de usuario asignadas a los usuarios de Kaspersky Security Center Linux les proporcionan conjuntos de derechos de acceso a las funciones de la aplicación.

Puede utilizar las funciones de usuario predefinidas con un conjunto de derechos ya configurado, o crear nuevas funciones y configurar los derechos necesarios usted mismo. Algunas de las funciones de usuario predefinidas disponibles en Kaspersky Security Center Linux se pueden asociar con puestos de trabajo específicos, por ejemplo, **Auditor**, **Director de seguridad**, **Supervisor**. Los derechos de acceso de estas funciones están preconfiguradas de acuerdo con las tareas estándar y el alcance de las responsabilidades de los puestos asociados. La siguiente tabla muestra como las funciones pueden estar asociadas con puestos de trabajo específicos.

Ejemplos de funciones para puestos de trabajo específicos

Función	Comentario
Auditor	Permisos de todas las operaciones con todos los tipos de informes, todas las operaciones de visualización, incluyendo la visualización de objetos eliminados (concede los permisos **Leer** y **Editar** en el área de **objetos eliminados**). No permite otras operaciones. Puede asignar esta función a una persona que realice la auditoría de su organización.
Supervisor	Permite todas las operaciones de visualización, no permite otras operaciones. Puede asignar esta función a un director de seguridad y otros gerentes a cargo de la seguridad de TI en su organización.
Director de seguridad.	Permite todas las operaciones de visualización, permite la administración de informes; otorga permisos limitados en la **administración del sistema**: área de **Conectividad**. Puede asignar esta función a un responsable a cargo de la seguridad de TI en su organización.

La siguiente tabla muestra los derechos de acceso asignados a cada función de usuario predefinida.

Las características de las áreas funcionales **Administración de dispositivos móviles: general** y **Administración del sistema** no están disponibles en Kaspersky Security Center Linux. Un usuario con los roles **Administrador de administración de parches y vulnerabilidades/Operador**, y **Administrador de administración de dispositivos móviles/Operador** tienen acceso sólo por los derechos del área funcional **Características generales**: **Básicas**.

Derechos de acceso de las funciones de usuario predefinidas

Función	Descripción
Administrador del Servidor de administración	Permite todas las operaciones de las siguientes áreas funcionales, en **Funciones generales**: • **Funcionalidad básica** • **Procesamiento de eventos** • **Jerarquía de Servidores de administración** • **Servidores de administración virtual**
Operador del Servidor de administración	Otorga los derechos de **lectura** y **ejecución** en todas las áreas funcionales siguientes, en **Funciones generales**: • **Funcionalidad básica** • **Servidores de administración virtual**
Auditor	Permite todas las operaciones de las siguientes áreas funcionales, en **Funciones generales**: • **Acceder a objetos independientemente de sus ACL** • **Objetos eliminados** • **Gestión reforzada de informes** Puede asignar esta función a una persona que realice la auditoría de su organización.
Administrador de instalación	Permite todas las operaciones de las siguientes áreas funcionales, en **Funciones generales**: • **Funcionalidad básica** • **Despliegue del software de Kaspersky** • **Administración de claves de licencia** Otorga derechos de **lectura** y **ejecución** en el área funcional **Características Generales: Servidores de administración Virtual**.
Operador de instalación	Otorga los derechos de **lectura** y **ejecución** en todas las áreas funcionales siguientes, en **Funciones generales**: • **Funcionalidad básica**

	• **Despliegue del software de Kaspersky** (también otorga el derecho **Administrar parches de Kaspersky** en esta área) • **Servidores de administración virtual**
Administrador de Kaspersky Endpoint Security	Permite todas las operaciones en las siguientes áreas funcionales: • **Características generales: Funcionalidad básica** • Área de Kaspersky Endpoint Security, incluidas todas las funciones
Operador de Kaspersky Endpoint Security	Otorga los derechos de **lectura** y **ejecución** en todas las áreas funcionales siguientes: • **Características generales: Funcionalidad básica** • Área de Kaspersky Endpoint Security, incluidas todas las funciones
Administrador principal	Permite todas las operaciones en áreas funcionales, *excepto* en las siguientes áreas, en **Funciones generales**: • **Acceder a objetos independientemente de sus ACL** • **Gestión reforzada de informes**
Operador principal	Otorga los derechos de **lectura** y **ejecución** (cuando corresponda) en todas las áreas funcionales siguientes: • **Funciones generales**: • **Funcionalidad básica** • **Objetos eliminados** • **Operaciones en el Servidor de administración** • **Despliegue del software de Kaspersky** • **Servidores de administración virtual** • Área de Kaspersky Endpoint Security, incluidas todas las funciones
Administrador de Administración de dispositivos móviles	Permite todas las operaciones en el área funcional **Características generales: Funcionalidad básica**.
Director de seguridad.	Permite todas las operaciones de las siguientes áreas funcionales, en **Funciones generales**: • **Acceder a objetos independientemente de sus ACL** • **Gestión reforzada de informes** Otorga derechos de **Lectura**, **Modificación**, **Ejecución**, **Guardar archivos desde los dispositivos a la estación de trabajo del administrador** y **Realizar operaciones para las selecciones de dispositivos** en el área funcional **Administración del sistema: Conectividad**. Puede asignar esta función a un responsable a cargo de la seguridad de TI en su organización.
Usuario del 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 y versiones posteriores.
Supervisor	Otorga el derecho de **lectura** en las áreas funcionales **Funciones generales**: **Acceder a objetos, independientemente de sus ACL** y **Funciones generales**: **Gestión reforzada de informes**. Puede asignar esta función a un director de seguridad y otros gerentes a cargo de la seguridad de TI en su organización.

Añadir una cuenta de un usuario interno

Para añadir una nueva cuenta de usuario interno a Kaspersky Security Center Linux:

1. En el menú principal, vaya a **USUARIOS Y FUNCIONES → USUARIOS**.
2. Haga clic en **Añadir**.
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 a 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:
    - Mayúsculas (A-Z)
    - Minúsculas (a-z)
    - Números (0-9)
    - Caracteres especiales (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
  - La contraseña no debe contener espacios en blanco, caracteres Unicode o la combinación de "." y "@", cuando "." está colocado delante de "@".

  Para ver los caracteres que ha ingresado, haga clic y mantenga presionado el botón **Mostrar**.

  > El número de intentos de introducción de la contraseña es limitado. De forma predeterminada, el número máximo de intentos de introducción de la contraseña permitidos es 10. Puede cambiar el número permitido de intentos para introducir una contraseña, como se describe en "Cambiar el número de intentos de ingreso de contraseña permitidos".

  > Si el usuario introduce incorrectamente la contraseña el número especificado de veces, la cuenta de usuario quedará bloqueada durante una hora. Puede desbloquear la cuenta de usuario cambiando solo la contraseña.

- **Nombre completo**
- **Descripción**
- **Dirección de correo electrónico**
- **Teléfono**

4. Haga clic en **Correcto** 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 FUNCIONES** → **USUARIOS**.
2. Haga clic en **Añadir**.
3. Cuando se abre la ventana **Nueva entidad**, seleccione **Grupo**.
4. Especifique la siguiente configuración para el nuevo grupo de usuarios:
   - **Nombre del grupo**
   - **Descripción**
5. Haga clic en **Correcto** 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

Modificar una cuenta de usuario interna en Kaspersky Security Center Linux:

1. En el menú principal, vaya a **USUARIOS Y FUNCIONES → 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 **Control de aplicaciones**, cambie la configuración de la cuenta de usuario:
   - **Descripción**
   - **Nombre completo**
   - **Dirección de correo electrónico**
   - **Teléfono principal**
   - **Contraseña** para la conexión del usuario a 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:
       - Mayúsculas (A-Z)
       - Minúsculas (a-z)
       - Números (0-9)
       - Caracteres especiales (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - La contraseña no debe contener espacios en blanco, caracteres Unicode o la combinación de "." y "@", cuando "." está colocado delante de "@".

     Para ver la contraseña introducida, haga clic y mantenga presionado el botón **Mostrar**.

     El número de intentos de introducción de la contraseña es limitado. De forma predeterminada, el número máximo de intentos de introducción de la contraseña 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 introduce incorrectamente la contraseña el número especificado de veces, la cuenta de usuario quedará bloqueada durante una hora. Puede desbloquear la cuenta de usuario cambiando solo la contraseña.
   - Si es necesario, cambie el botón de alternar a **Desactivado** 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 la 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 **Funciones**, puede asignar dispositivos 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

Puede editar solo los grupos internos.

Para editar un grupo de usuario:

1. En el menú principal, vaya a **USUARIOS Y FUNCIONES → USUARIOS**.
2. Haga clic en el nombre del grupo de usuarios que desea editar.
3. En la ventana de configuración del grupo que se abre, 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.

Adición de cuentas de usuario a un grupo interno

Solo puede añadir cuentas de usuarios internos a un grupo interno.

Para añadir cuentas de usuario a un grupo interno:

1. En el menú principal, vaya a **USUARIOS Y FUNCIONES** → **USUARIOS**.
2. Seleccione las casillas junto a las cuentas de usuario que desea añadir a un grupo.
3. Haga clic en el botón **Asignar grupo**.
4. En la ventana que se abre **Asignar grupo**, seleccione el grupo al que desea añadir cuentas de usuario.
5. Haga clic en el botón **Asignar**.

Las cuentas de usuario se añaden al grupo.

Designación del usuario como propietario del dispositivo

Para obtener información sobre cómo asignar un usuario como propietario de un dispositivo móvil, consulte la Ayuda de Kaspersky Security para dispositivos móviles.

Para asignar un usuario como propietario del dispositivo:

1. En el menú principal, vaya a **USUARIOS Y FUNCIONES** → **USUARIOS**.
2. Haga clic en el nombre de la cuenta de usuario que desea asignar como propietario del dispositivo.
3. En la ventana de configuración de usuario que se abre, seleccione la pestaña **Dispositivos**.
4. Haga clic en **Añadir**.
5. En la lista de dispositivos, seleccione el dispositivo que desea asignar al usuario.
6. Haga clic en **Aceptar**.

El dispositivo seleccionado se añade a la lista de dispositivos asignados al usuario.

Puede realizar la misma operación en **DISPOSITIVOS** → **DISPOSITIVOS ADMINISTRADOS**, haciendo clic en el nombre del dispositivo que desea asignar y después haciendo clic en el enlace **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 FUNCIONES** → **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 **Correcto**.

Se elimina el usuario o el grupo de seguridad.

Creación de funciones de usuario

Para crear una función de usuario:

1. En el menú principal, vaya a **USUARIOS Y FUNCIONES** → **Funciones**.
2. Haga clic en **Añadir**.
3. En la ventana **Nombre de la nueva función** que se abre, introduzca el nombre de la nueva función.
4. Haga clic en **Correcto** para aplicar los cambios.
5. En la ventana de propiedades de la función que se abre, cambie la configuración de la función:
   - En la pestaña **Control de aplicaciones**, modifique el nombre de la función.
     No puede editar el nombre de una función predefinida.
   - En la pestaña **Configuración**, modifique la cobertura de la función y directivas y los perfiles asociados con la función.
   - En la pestaña **Derechos de acceso**, modifique los derechos para el acceso a aplicaciones de Kaspersky.
6. Haga clic en **Guardar** para guardar los cambios.

La nueva función aparece en la lista de funciones del usuario.

Editar una función de usuario

Para editar una función de usuario:

1. En el menú principal, vaya a **USUARIOS Y FUNCIONES** → **Funciones**.
2. Haga clic en el nombre de la función que desea editar.
3. En la ventana de propiedades de la función que se abre, cambie la configuración de la función:
   - En la pestaña **Control de aplicaciones**, modifique el nombre de la función.
     No puede editar el nombre de una función predefinida.
   - En la pestaña **Configuración**, modifique la cobertura de la función y directivas y los perfiles asociados con la función.
   - En la pestaña **Derechos de acceso**, modifique los derechos para el acceso a aplicaciones de Kaspersky.
4. Haga clic en **Guardar** para guardar los cambios.

La nueva función aparece en la lista de funciones de usuario.

Editar la cobertura de una función de usuario

Una *cobertura de la función de usuario* es una combinación de usuarios y grupos de administración. La configuración asociada con una función de usuario se aplica solo a los dispositivos que pertenecen a usuarios que tienen esta función y solo si estos dispositivos pertenecen a grupos asociados con esta función, incluidos los grupos secundarios.

Para añadir usuarios, grupos de seguridad y grupos de administración a la cobertura de una función del usuario, puede utilizar cualquiera de los siguientes métodos:

Método 1:

1. En el menú principal, vaya a **USUARIOS Y FUNCIONES** → **USUARIOS**.
2. Seleccione las casillas de verificación junto a los usuarios y grupos de seguridad que desee añadir a la cobertura de la función de usuario.
3. Haga clic en el botón **Asignar función**.
   Se inicia el Asistente de asignación de funciones. Avance a través del Asistente utilizando el botón **Siguiente**.
4. En la página del Asistente **Seleccionar función**, seleccione la función de usuario que quiere asignar.
5. En la página del Asistente **Definir cobertura**, seleccione el grupo de administración que desea añadir a la cobertura de la función de usuario.
6. Haga clic en el botón **Asignar función** para cerrar el Asistente.

Los usuarios o grupos de seguridad seleccionados y el grupo de administración seleccionado se añaden al ámbito de la función de usuario.

Método 2:

1. En el menú principal, vaya a **USUARIOS Y FUNCIONES** → **Funciones**.
2. Haga clic en el nombre de la función para la que desea definir la cobertura.
3. En la ventana de propiedades de la función que se abre, seleccione la pestaña **Configuración**.
4. En la sección **Cobertura de la función**, haga clic en **Añadir**.
   Se inicia el Asistente de asignación de funciones. Avance a través del Asistente utilizando el botón **Siguiente**.
5. En la página del Asistente **Definir cobertura**, seleccione el grupo de administración que desea añadir a la cobertura de la función de usuario.
6. En la página del Asistente **Seleccionar usuarios**, seleccione el grupo de seguridad y usuarios que desea añadir a la cobertura de la función de usuario.
7. Haga clic en el botón **Asignar función** para cerrar el Asistente.
8. Haga clic en el botón **Cerrar** (✕) para cerrar la ventana de propiedades de la función.

Los usuarios o grupos de seguridad seleccionados y el grupo de administración seleccionado se añaden al ámbito de la función de usuario.

Eliminar una función de usuario

Para eliminar una función de usuario:

1. En el menú principal, vaya a **USUARIOS Y FUNCIONES** → **Funciones**.
2. Seleccione las casillas de verificación junto al nombre de la función que quiere eliminar.
3. Haga clic en **Eliminar**.
4. En la ventana que se abre, haga clic en **Correcto**.

Se elimina la función del usuario.

Asociación de perfiles de directivas con funciones

Puede asociar funciones de usuario con perfiles de directiva. En este caso, la regla de activación para este perfil de directiva se basa en la función: el perfil de directiva se activa para un usuario que tiene la función especificada.

Por ejemplo, la directiva obstruye cualquier software de navegación GPS en todos los dispositivos en un grupo de administración. El software de navegación GPS solo hace falta en un dispositivo del grupo de administración de usuarios: el perteneciente al mensajero. En este caso, puede asignar una función de "Mensajero" a su propietario y luego crear un perfil de directiva que permita que el software de navegación GPS se ejecute solo en los dispositivos cuyos propietarios tienen asignada la función de "Mensajero". Todas las demás configuraciones de directivas se conservan. Solo el usuario con la función "Mensajero" podrá ejecutar el software de navegación GPS. Más adelante, si a otro trabajador se le asigna la función de "Mensajero", el nuevo trabajador también puede ejecutar el software de navegación en el dispositivo de su organización. La ejecución del software de navegación GPS aún estará prohibida en otros dispositivos en el mismo grupo de administración.

Asociar una función con un perfil de directiva:

1. En el menú principal, vaya a **USUARIOS Y FUNCIONES** → **Funciones**.
2. Haga clic en el nombre de la función que desea asociar con un perfil de directiva.
   La ventana de propiedades de la función se abre con la pestaña **Control de aplicaciones** seleccionada.
3. Seleccione la pestaña **Configuración** y desplácese hacia abajo a la sección **Directivas y perfiles**.
4. Haga clic en **Editar**.
5. Asociar la función con:
   - **Un perfil de directiva existente**: Haga clic en el icono de flecha (›) al lado del nombre de la directiva requerida, y luego seleccione la casilla que está al lado del perfil con la cual desea asociar la función.
   - **Nuevo perfil de directiva**:
     a. Seleccione la casilla junto a la directiva para la que desee crear un perfil.

b. Haga clic en **Nuevo perfil de directiva**.

c. Seleccione la casilla de verificación junto a la directiva para la que desea crear un perfil.

d. Haga clic en el botón **Guardar**.

e. Seleccione la casilla de verificación junto al nuevo perfil.

6. Haga clic en **Asignar a función**.

El perfil está asociado con la función y aparece en las propiedades de la función. El perfil se aplica automáticamente a cualquier dispositivo cuyo propietario tenga asignada la función.

Administración de revisiones de objetos

Esta sección contiene información sobre la administración de la revisión de objetos. Kaspersky Security Center Linux le permite rastrear la modificación de objetos. Cada vez que guarda cambios realizados en un objeto, se crea una *revisión*. Cada revisión tiene un número.

Los objetos de aplicación que admiten administración de la revisión incluyen:

- Servidores de administración
- Directivas
- Tareas
- Grupos de administración
- Cuentas de usuario
- Paquetes de instalación

Puede realizar las acciones siguientes en revisiones de objetos:

- Compare una revisión seleccionada con la actual
- Comparar revisiones seleccionadas
- Compare un objeto con una revisión seleccionada de otro objeto del mismo tipo
- Vea una revisión seleccionada
- Deshaga cambios realizados en un objeto a una revisión seleccionada
- Guardar revisiones como un archivo .txt

En la ventana de propiedades de cualquier objeto que admita administración de la revisión, la sección **Historial de revisiones** muestra una lista de revisiones de objetos con los siguientes datos:

- Número de revisión del objeto
- Fecha y hora de modificación del objeto
- Nombre del usuario que modificó el objeto
- Acción que se ejecutó sobre el objeto
- Descripción de la revisión relacionada con el cambio realizado a la configuración de objeto

  De forma predeterminada, la descripción de la revisión de objeto está en blanco. Para agregar una descripción a una revisión, seleccione la revisión relevante y haga clic en el botón **Descripción**. En la ventana **Descripción de la revisión del objeto**, añada texto para la descripción de la revisión.

Sobre las revisiones de objetos

Puede realizar las acciones siguientes en revisiones de objetos:

- Compare una revisión seleccionada con la actual
- Comparar revisiones seleccionadas
- Compare un objeto con una revisión seleccionada de otro objeto del mismo tipo
- Vea una revisión seleccionada

- Deshaga cambios realizados en un objeto a una revisión seleccionada
- Guardar revisiones como un archivo .txt

En la ventana de propiedades de cualquier objeto que admita administración de la revisión, la sección **Historial de revisiones** muestra una lista de revisiones de objetos con los siguientes datos:

- Número de revisión del objeto
- Fecha y hora de modificación del objeto
- Nombre del usuario que modificó el objeto
- Acción que se ejecutó sobre el objeto
- Descripción de la revisión relacionada con el cambio realizado a la configuración de objeto

Devolver un objeto a una revisión anterior

Puede revertir los cambios realizados en un objeto, si es necesario. Por ejemplo, es posible que tenga que revertir la configuración de una directiva a su estado en una fecha específica.

Para revertir los cambios realizados en un objeto:

1. En la ventana de propiedades del objeto, abra la pestaña **Historial de revisión**.
2. En la lista de revisiones de objetos, seleccione la revisión en la que quiere revertir los cambios.
3. Haga clic en el botón **Revertir**.
4. Haga clic en **Aceptar** para confirmar la operación.

   El objeto se revierte ahora a la revisión seleccionada. La lista de revisiones de objetos muestra un registro de la acción que se tomó. La descripción de la revisión muestra la información sobre el número de la revisión a la cual revertió 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, incluidos los siguientes:

- Directivas
- Tareas
- Paquetes de instalación
- Servidores de administración virtual
- Usuarios
- Grupos de seguridad
- Grupos de administración

Cuando elimina un objeto, la información sobre él permanece 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**.

Uso de la utilidad klscflag para abrir el puerto 13291

El puerto 13291 del Servidor de administración se usa para recibir conexiones desde las Consolas de administración. En equipos que no usan Windows, este puerto no está abierto de forma predeterminada. Si no desea utilizar la Consola de administración basada en MMC o la utilidad klakaut, puede abrir este puerto mediante la utilidad klscflag. Esta 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 con el siguiente comando:
   ```
   $ sudo systemctl restart kladminserver_srv
   ```

El puerto 13291 queda abierto.

Para comprobar si el puerto 13291 se ha abierto correctamente:

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\";"
```

Este comando devuelve el siguiente resultado:

```
+--- (PARAMS_T)
+---KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN = (BOOL_T)true
```

El valor `true` significa que el puerto está abierto. De lo contrario, se muestra el valor `false`.

Actualización de bases de datos Kaspersky y aplicaciones

Esta sección describe los pasos que debe seguir para actualizar regularmente lo siguiente:

- Bases de datos y módulos de software de Kaspersky
- Aplicaciones instaladas de Kaspersky, incluidos los componentes de Kaspersky Security Center y las aplicaciones de seguridad

Escenario: actualización periódica de las bases de datos y aplicaciones de Kaspersky

Esta sección proporciona un escenario para la actualización regular de las bases de datos, módulos de software y aplicaciones de Kaspersky. Una vez completado el escenario de configuración de la protección de red, debe mantener la fiabilidad del sistema de protección para garantizar que los Servidores de administración y los dispositivos administrados estén protegidos contra diversas amenazas, entre ellas virus, ataques de red y ataques de phishing.

La protección de la red se mantiene actualizada mediante actualizaciones periódicas de lo siguiente:

- Bases de datos y módulos de software de Kaspersky
- Aplicaciones instaladas de Kaspersky, incluidos los componentes de Kaspersky Security Center y las aplicaciones de seguridad

Cuando complete este escenario, puede estar seguro de lo siguiente:

- Su red está protegida por el software más reciente de Kaspersky, incluidos los componentes de Kaspersky Security Center Linux y las aplicaciones de seguridad.
- Las bases de datos antivirus y otras bases de datos de Kaspersky críticas para la seguridad de la red estarán siempre actualizadas.

Requisitos previos

Los dispositivos administrados deben tener conexión con el Servidor de administración. Si no tienen conexión, considere actualizar las bases de datos y los módulos de software de Kaspersky de forma manual o directamente desde los servidores de actualización de Kaspersky.

El Servidor de administración debe tener una conexión a Internet.

Antes de comenzar, asegúrese de haber hecho lo siguiente:

1. Desplegado las aplicaciones de seguridad de Kaspersky en los dispositivos administrados según el escenario de implementación de aplicaciones de Kaspersky a través de Kaspersky Security Center 14 Web Console.
2. Creado y configurado todas las directivas, perfiles de directivas y tareas requeridas de acuerdo con el escenario de configuración de la protección de red.
3. Asignado una cantidad apropiada de puntos de distribución de acuerdo con la cantidad de dispositivos administrados y la topología de la red.

La actualización de bases de datos y aplicaciones de Kaspersky sucede en etapas:

1 **Elección de un esquema de actualización**

Hay varios esquemas que puede usar para instalar actualizaciones para los componentes de Kaspersky Security Center y las aplicaciones de seguridad. Elija el esquema o varios esquemas que cumplan con los requisitos de su red.

2. **Creación de 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 es necesaria para descargar actualizaciones de los servidores de actualización de Kaspersky al repositorio del Servidor de administración, así como para actualizar las bases de datos y módulos de software de Kaspersky para Kaspersky Security Center. Una vez que se descarguen las actualizaciones, se pueden propagar a los dispositivos administrados.

   Si su red tiene puntos de distribución asignados, las actualizaciones se descargan automáticamente desde el repositorio del Servidor de administración a los repositorios de los puntos de distribución. En este caso, los dispositivos administrados incluidos en la cobertura de un punto de distribución descargan las actualizaciones desde el repositorio del punto de distribución en lugar del repositorio del Servidor de administración.

   Instrucciones: Crear la tarea para descargar actualizaciones en el repositorio del Servidor de administración

3. **Creación de la tarea para descargar actualizaciones a los repositorios de los puntos de distribución (opcional)**

   De forma predeterminada, las actualizaciones se descargan a los puntos de distribución desde el Servidor de administración. Puede configurar Kaspersky Security Center para descargar las actualizaciones a los puntos de distribución directamente desde los servidores de actualización de Kaspersky. La descarga a los repositorios de puntos de distribución es preferible 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.

   Cuando su red ha asignado puntos de distribución y se crea la tarea *Descargar actualizaciones en los repositorios de puntos de distribución*, los puntos de distribución descargan actualizaciones de los servidores de actualización 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 puntos de distribución**

   Cuando su red tenga puntos de distribución asignados, asegúrese de que la opción **Desplegar actualizaciones** esté habilitada en las propiedades de todos los puntos de distribución requeridos. Cuando esta opción está deshabilitada para un punto de distribución, los dispositivos incluidos en la cobertura del punto de distribución se actualizan desde el repositorio del Servidor de administración.

5. **Optimización del proceso de actualización mediante el uso de archivos diff (opcional)**

   Puede optimizar el tráfico entre el Servidor de administración y los dispositivos administrados utilizando archivos diff. Cuando esta función está habilitada, el Servidor de administración o un punto de distribución descarga archivos diferenciales en lugar de archivos completos de bases de datos o módulos de software de Kaspersky. Un archivo diff describe las diferencias entre dos versiones de un archivo de una base de datos o un módulo de software. Por lo tanto, un archivo diff ocupa menos espacio que un archivo completo. Esto reduce el tráfico entre el Servidor de administración o los puntos de distribución y los dispositivos administrados. Para usar esta función, active la opción **Descargar archivos de comparación** en las propiedades de la tarea Descargar actualizaciones en el repositorio del Servidor de administración y/o la tarea Descargar actualizaciones en los repositorios de puntos de distribución.

   Instrucciones: Uso de archivos diff para actualizar las bases de datos y módulos de software de Kaspersky

6. **Configuración de instalación automática de actualizaciones para las aplicaciones de seguridad**

   Cree las tareas de actualización para las aplicaciones administradas para proporcionar actualizaciones oportunas a los módulos de software y las bases de datos de Kaspersky, incluidas las bases de datos antivirus. Para garantizar actualizaciones oportunas, le recomendamos que seleccione la opción **Cuando se descarguen nuevas actualizaciones en el repositorio** al configurar la programación de tareas.

   Si su red incluye dispositivos solo IPv6 y quiere actualizar regularmente las aplicaciones de seguridad instaladas en dichos dispositivos, asegúrese de que el Servidor de administración versión 13.2 y el Agente de red 13.2 estén instalados en los dispositivos administrados.

   Si una actualización requiere revisar y aceptar los términos del Contrato de licencia de usuario final, primero debe aceptar los términos. Después de eso, la actualización se puede propagar a los dispositivos administrados.

Resultados

Una vez completado el escenario, Kaspersky Security Center Linux queda configurado para actualizar las bases de datos de Kaspersky después de que las actualizaciones se descargan en el repositorio del Servidor de administración. Después, puede proceder a monitorear el estado de la red.

Acerca de la actualización de las bases de datos, módulos de software y aplicaciones de Kaspersky

Para asegurarse de que la protección de sus Servidores de administración y dispositivos administrados esté actualizada, debe proporcionar actualizaciones oportunas de las siguientes:

- Bases de datos y módulos de software de Kaspersky

  Antes de descargar las bases de datos y los módulos de software de Kaspersky, Kaspersky Security Center comprueba si se puede acceder a los servidores de Kaspersky. Si no es posible acceder a los servidores mediante el DNS del sistema, la aplicación utiliza el DNS público. Esto es necesario para asegurarse de que las bases de datos antivirus estén actualizadas y se mantenga el nivel de seguridad para los dispositivos administrados.

- Aplicaciones instaladas de Kaspersky, incluidos los componentes de Kaspersky Security Center y las aplicaciones de seguridad

  Kaspersky Security Center no puede actualizar las aplicaciones de Kaspersky automáticamente. Para actualizar las aplicaciones, descargue las últimas versiones de las aplicaciones desde el sitio web de Kaspersky e instálelas manualmente:

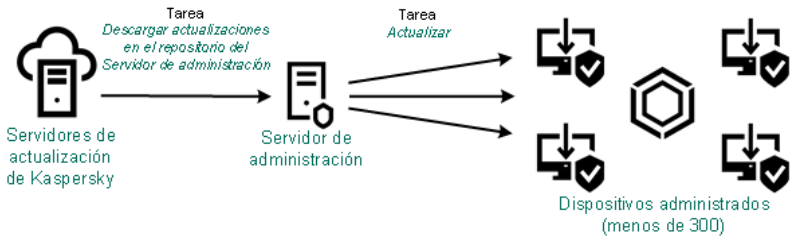
- Servidor de administración de Kaspersky Security Center, Kaspersky Security Center 14 Web Console
- Agente de red, Kaspersky Endpoint Security para Linux, complemento web de administración

Dependiendo de la configuración de su red, puede utilizar los siguientes esquemas de descarga y distribución de las actualizaciones necesarias para los dispositivos administrados:

- Mediante el uso de una sola tarea: *Descargar actualizaciones en el repositorio del Servidor de administración*
- Mediante el uso de dos tareas:
  - La tarea *Descargar actualizaciones en el repositorio del Servidor de administración*
  - La tarea *Descargar actualizaciones en los repositorios de puntos de distribución*
- Manualmente a través de una carpeta local, una carpeta compartida o un servidor FTP
- Directamente desde los servidores de actualización de Kaspersky a Kaspersky Endpoint Security for Linux en los dispositivos administrados
- A través de una carpeta local o de red si el Servidor de administración no tiene conexión a Internet

Uso de la tarea Descargar actualizaciones en el repositorio del Servidor de administración

En este esquema, Kaspersky Security Center descarga actualizaciones a través de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*. En redes pequeñas que contienen menos de 300 dispositivos administrados en un solo segmento de red o menos de 10 dispositivos administrados en cada segmento de red, las actualizaciones se distribuyen a los dispositivos administrados directamente desde el repositorio del Servidor de administración (ver la siguiente figura).



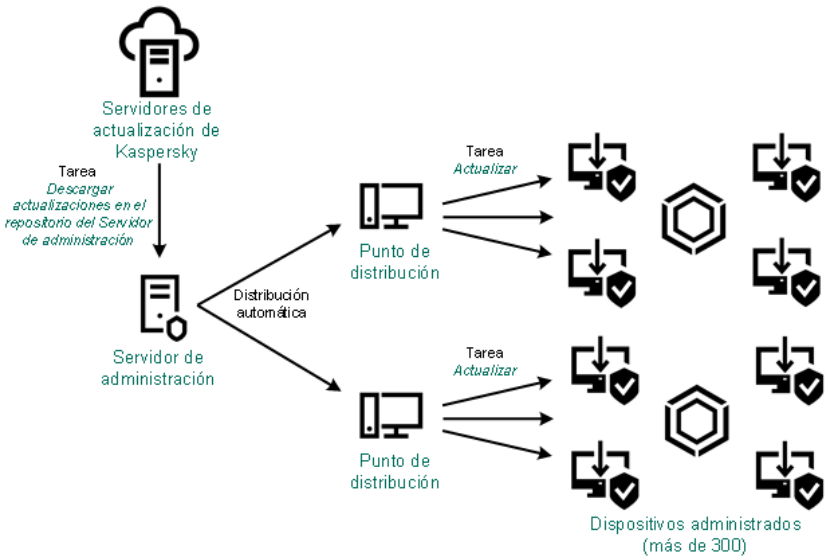
Actualización utilizando la tarea Descargar actualizaciones en el repositorio del Servidor de administración sin puntos de distribución

Como fuente de actualizaciones, no solo puede usar los servidores de actualización de Kaspersky, sino también una carpeta local o de red.

De forma predeterminada, el Servidor de administración se comunica con los servidores de actualización de Kaspersky y descarga las actualizaciones utilizando el protocolo HTTPS. Puede configurar Servidor de administración para que utilice el protocolo HTTP en lugar del HTTPS.

Si su red contiene 300 o más dispositivos administrados en un solo segmento de red o si su red consta de varios segmentos de red con más de 9 dispositivos administrados en cada segmento de red, le recomendamos que utilice puntos de distribución para propagar las actualizaciones a los dispositivos administrados (ver la siguiente figura). Los puntos de distribución reducen la carga en el Servidor de administración y optimizan el tráfico entre el Servidor de administración y los dispositivos administrados. Puede calcular el número y la configuración de los puntos de distribución necesarios para su red.

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 la cobertura de un punto de distribución descargan las actualizaciones desde el repositorio del punto de distribución en lugar del repositorio del Servidor de administración.



Actualización utilizando la tarea Descargar actualizaciones en el repositorio del Servidor de administración con puntos de distribución

Cuando se completa la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*, las actualizaciones de las bases de datos de Kaspersky y los módulos de software para Kaspersky Endpoint Security for Linux se descargan en el repositorio del Servidor de administración. Estas actualizaciones se instalan a través de la Tarea de actualización de Kaspersky Endpoint Security for Linux.

La tarea del Servidor de administración Descargar actualizaciones en el repositorio no está disponible en los Servidores de administración virtuales. El repositorio del Servidor de administración virtual muestra las actualizaciones descargadas en el Servidor de administración principal.

Puede configurar las actualizaciones para verificar su operatividad y errores en un conjunto de dispositivos de prueba. Si la verificación es exitosa, las actualizaciones se distribuyen a otros dispositivos administrados.

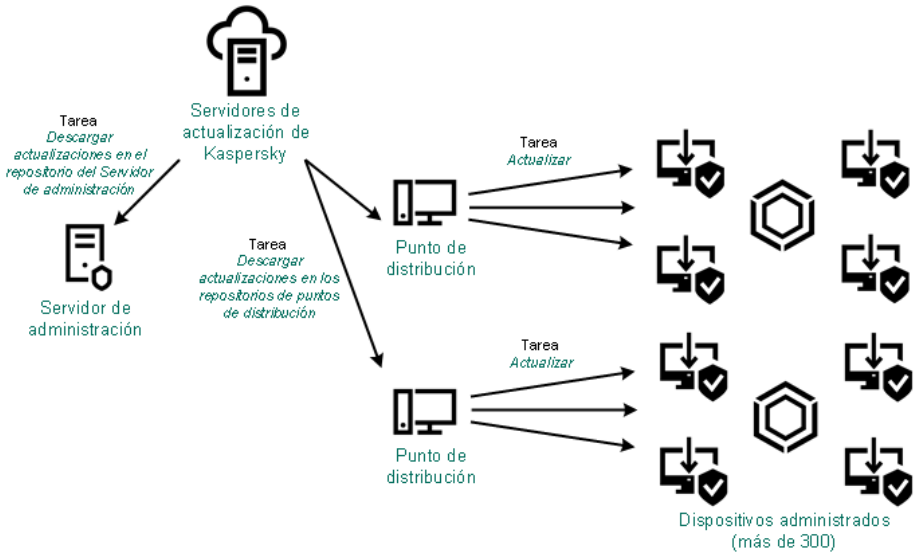
Cada aplicación de Kaspersky solicita actualizaciones requeridas del Servidor de administración. El Servidor de administración añade estas solicitudes y descarga solo aquellas actualizaciones que son solicitadas por cualquier aplicación. Esto garantiza que las mismas actualizaciones no se descarguen varias veces y que las actualizaciones innecesarias no se descarguen en absoluto. 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 actualización de Kaspersky automáticamente para garantizar la descarga de versiones relevantes de las bases de datos de Kaspersky y los módulos de software:

- Id. y versión de la aplicación
- Id. de instalación de aplicaciones
- Id. de clave activa
- Id. de ejecución de la tarea *Descargar actualizaciones al repositorio del Servidor de administración*

Ninguna información transmitida contiene datos personales u otros datos confidenciales. AO Kaspersky Lab protege la información de acuerdo con los requisitos establecidos por la ley.

Usando dos tareas: la tarea Descargar actualizaciones en el repositorio del Servidor de administración y la tarea Descargar actualizaciones en los repositorios de puntos de distribución

Puede descargar actualizaciones a los repositorios de puntos de distribución directamente desde los servidores de actualizaciones de Kaspersky en lugar del repositorio del Servidor de administración y después distribuir las actualizaciones a los dispositivos administrados (consulte la siguiente figura). La descarga a los repositorios de puntos de distribución es preferible 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.



Actualización utilizando la tarea Descargar actualizaciones en el repositorio del Servidor de administración y la tarea Descargar actualizaciones en los repositorios de puntos de distribución

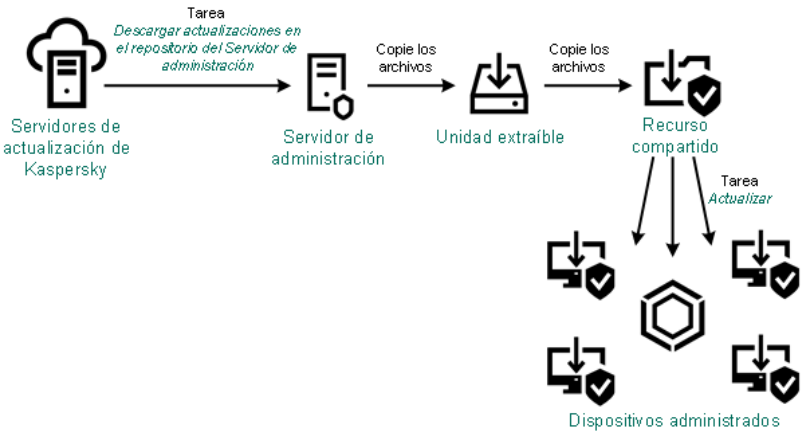
De forma predeterminada, el Servidor de administración y los puntos de distribución se comunican con los servidores de actualización de Kaspersky y descargan las actualizaciones utilizando el protocolo HTTPS. Puede configurar el Servidor de administración y/o los puntos de distribución para utilizar el protocolo HTTP en lugar de HTTPS.

Para implementar este esquema, cree la tarea *Descargar actualizaciones en los repositorios de puntos de distribución* además de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*. Después de esto, los puntos de distribución descargarán actualizaciones desde servidores de actualizaciones de Kaspersky y no desde el repositorio del Servidor de administración.

La tarea *Descargar actualizaciones en el repositorio del Servidor de administración* también es necesaria para este esquema, ya que esta tarea se utiliza para descargar las bases de datos y los módulos de software de Kaspersky para Kaspersky Security Center.

Manualmente a través de una carpeta local, una carpeta compartida o un servidor FTP

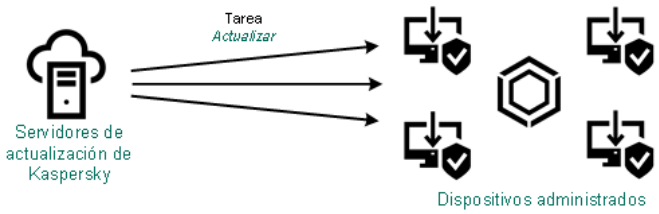
Si los dispositivos cliente no tienen una conexión con el Servidor de administración, puede usar una carpeta local o un recurso compartido como fuente para actualizar las bases de datos, módulos de software y aplicaciones de Kaspersky. En este esquema, debe copiar las actualizaciones requeridas desde el repositorio del Servidor de administración a una unidad extraíble, luego copiar las actualizaciones a la carpeta local o al recurso compartido especificado como origen de actualizaciones en la configuración de Kaspersky Endpoint Security for Linux (ver la siguiente figura).



Actualización a través de una carpeta local, una carpeta compartida o un servidor FTP

Directamente desde los servidores de actualización de Kaspersky a Kaspersky Endpoint Security for Linux en los dispositivos administrados

En los dispositivos administrados, puede configurar Kaspersky Endpoint Security for Linux para recibir actualizaciones directamente desde los servidores de actualización de Kaspersky (ver la siguiente figura).



Actualizar aplicaciones de seguridad directamente desde los servidores de actualización de Kaspersky

En este esquema, la aplicación de seguridad no utiliza el repositorio proporcionado por Kaspersky Security Center. Para recibir actualizaciones directamente de los servidores de actualización de Kaspersky, especifique los servidores de actualización de Kaspersky como origen de actualizaciones en la aplicación de seguridad. Para obtener una descripción completa de la configuración, consulte la documentación de Kaspersky Endpoint Security for Linux.

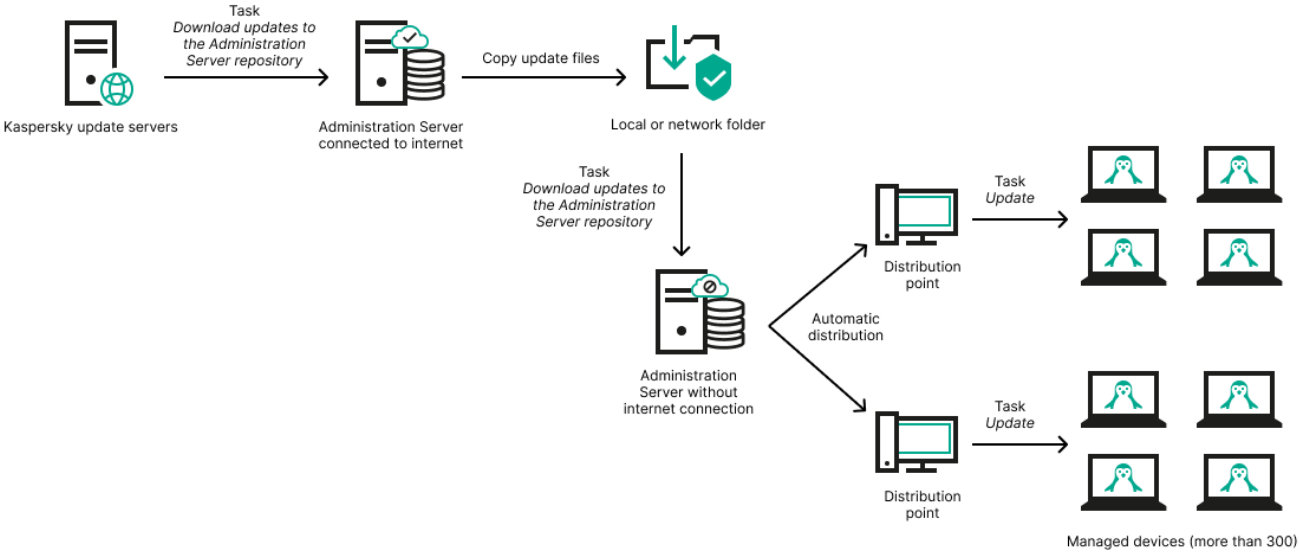
A través de una carpeta local o de red si el Servidor de administración no tiene conexión a Internet

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 actualizaciones utilizando el esquema antiguo**.



Actualizar a través de una carpeta local o de red si el Servidor de administración no tiene conexión a Internet

- Utilidad Kaspersky Update

  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 actualizaciones utilizando el esquema antiguo*.

Crear la Descarga de actualizaciones para la tarea del repositorio del Servidor de administración.

Expandir todo | Contraer todo

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 verificarlas antes de distribuirlas, configure la opción **Ejecutar verificación de actualizaciones** en la configuración de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*.

Para crear la tarea Descargar actualizaciones en el repositorio del Servidor de administración:

1. Vaya a **DISPOSITIVOS → TAREAS**.
2. Haga clic en **Añadir**.

   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. Especifique el nombre para la tarea que está creando. El nombre de la tarea no puede contener más de 100 caracteres y no puede incluir ningún carácter especial (como "*<>?\:|).
5. En la página **Finalizar la creación de tareas**, 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 especificada en el portapapeles. No puede cambiar la ruta a una carpeta específica para una tarea de grupo.

   - **Copiar las actualizaciones descargadas en carpetas adicionales**

     Una vez que el Servidor de administración recibe actualizaciones, las copia en las carpetas especificadas. Utilice esta opción si desea administrar de manera manual la distribución de actualizaciones en su red.

     Por ejemplo, puede querer usar esta opción en la siguiente situación: la red de su organización consta de varias subredes independientes y los dispositivos de cada una de las subredes no tienen acceso a otras subredes. Sin embargo, los dispositivos en todas las subredes tienen acceso a un recurso compartido de red común. En este caso, configura el Servidor de administración en una de las subredes para descargar actualizaciones de los servidores de actualización de Kaspersky, active esta opción y luego especifique este recurso compartido de red. En las actualizaciones descargadas de las tareas del repositorio para otros Servidores de administración, especifique el mismo recurso compartido de red que el origen de actualización.

     Esta opción está desactivada de forma predeterminada.

   - **Descargar archivos de comparación**

     Esta opción habilita la función de descarga de archivos diff.

     Esta opción está desactivada de forma predeterminada.

   - **Descargar actualizaciones utilizando el esquema anterior**

     A partir de la versión 14, Kaspersky Security Center descarga las actualizaciones de bases de datos y los módulos de software utilizando el nuevo esquema. Para que la aplicación descargue actualizaciones utilizando el nuevo esquema, el origen de actualización debe contener los archivos de actualización cuyos metadatos sean compatibles con el nuevo esquema. Si el origen de actualización contiene archivos de actualización cuyos metadatos son compatibles solo con el esquema anterior, active la **Descargar actualizaciones utilizando el esquema anterior** opción. De lo contrario, la tarea de descarga de la actualización no funcionará.

Por ejemplo, debe activar esta opción cuando se especifica una carpeta local o de red como fuente de actualización y los archivos de actualización en esta carpeta fueron descargados por una de las siguientes aplicaciones:

- Utilidad Kaspersky Update

  Esta utilidad descarga actualizaciones utilizando el esquema antiguo.

- Kaspersky Security Center 13.2 o una versión anterior

  Por ejemplo, su Servidor de administración 1 no tiene conexión a Internet. En este caso, puede descargar actualizaciones utilizando un Servidor de administración 2 que tenga conexión a Internet y luego colocar las actualizaciones en una carpeta local o de red para usarlas como fuente de actualización para el Servidor de administración 1. Si el Servidor de administración 2 tiene la versión 13.2 o anterior, active la **Descargar actualizaciones utilizando el esquema anterior** opción en la tarea para el Servidor de administración 1.

Esta opción está desactivada de forma predeterminada.

- **Ejecutar verificación de actualizaciones**

  El Servidor de administración descarga las actualizaciones desde el 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 **Cuando se descargan nuevas actualizaciones en el repositorio** empezada). La tarea de descargar actualizaciones al repositorio se termina solo después de completar la tarea *Verificación de actualizaciones*.

  Esta opción está desactivada de forma predeterminada.

9. En la ventana de propiedades de la tarea, en la pestaña **Programación**, cree una programación para el inicio de la tarea. Si es necesario, especifique la siguiente configuración:

- **Inicio programado**

  Seleccione la programación según la cual se ejecuta la tarea y configure la programación seleccionada.

  - **Manualmente** (seleccionado de manera predeterminada)

    La tarea no se ejecuta automáticamente. Solo lo puede iniciar de forma manual.

    Esta opción está activada de forma predeterminada.

  - **Cada N minutos**

    La tarea se ejecuta regularmente, con el intervalo especificado en minutos, a partir de la hora especificada en el día en que se crea la tarea.

    De forma predeterminada, la tarea se ejecuta cada 30 minutos, a partir de la hora actuales del sistema.

  - **Cada N horas**

    La tarea se ejecuta regularmente, con el intervalo especificado en horas, a partir de la fecha y hora especificadas.

    De forma predeterminada, la tarea se ejecuta cada seis horas, a partir de la fecha y hora actuales del sistema.

  - **Cada N días**

    La tarea se ejecuta regularmente, con el intervalo especificado en días. Además, puede especificar una fecha y hora de la primera tarea ejecutada. Estas opciones adicionales estarán disponibles si son compatibles con la aplicación para la que crea la tarea.

    De forma predeterminada, la tarea se ejecuta cada día, a partir de la fecha y hora actuales del sistema.

  - **Cada N semanas**

    La tarea se ejecuta regularmente, con el intervalo especificado en semanas, en el día especificado de la semana y en el tiempo especificado.

    De forma predeterminada, la tarea se ejecuta todos los lunes a la hora actual del sistema.

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

La tarea se ejecuta regularmente, con el intervalo especificado en días. Este programa no admite el cumplimiento del horario de verano (DST). Esto significa que cuando los relojes saltan una hora hacia adelante o hacia atrás al comienzo o al final del horario de verano, la hora de inicio de la tarea actual no cambia.

No recomendamos que utilice este horario. Es necesario para la compatibilidad con versiones anteriores de Kaspersky Security Center Linux.

De forma predeterminada, la tarea se ejecuta cada día a la hora actual del sistema.

- **Semanalmente**

  La tarea se ejecuta cada semana en el día especificado y a la hora especificada.

- **Por días de la semana**

  La tarea se ejecuta regularmente, en el día de la semana especificado y a la hora especificada.

  De forma predeterminada, la tarea se ejecuta todos los viernes a las 18:00:00 h.

- **Mensualmente**

  La tarea se ejecuta regularmente, en el día del mes especificado y a la hora especificada.

  En los meses que faltan el día especificado, la tarea se ejecuta el último día.

  De forma predeterminada, la tarea se ejecuta el primer día de cada mes, a la hora actual del sistema.

- **Cada mes, en días concretos de las semanas seleccionadas**

  La tarea se ejecuta regularmente, en el día de cada mes especificado y a la hora especificada.

  De forma predeterminada, no se seleccionan días del mes; la hora de inicio predeterminada es las 18:00:00 h.

- **Al completar otra tarea**

  La tarea actual se inicia después de que se complete otra tarea. Puede seleccionar cómo debe completarse la tarea anterior (satisfactoriamente o con errores) para activar el inicio de la tarea actual.

- Ajustes adicionales de la tarea:

  - **Ejecutar tareas no realizadas**

    Esta opción determina el comportamiento de una tarea si un dispositivo cliente no está visible en la red cuando la tarea vaya a comenzar.

    Si esta opción está activada, el sistema intentará iniciar la tarea la próxima vez que la aplicación Kaspersky se ejecute en un dispositivo cliente. Si la programación de la tarea es **Manualmente**, **Una vez** o **Inmediatamente**, la tarea se inicia inmediatamente después de que el dispositivo se haga visible en la red o inmediatamente después de que el dispositivo se incluya en la cobertura de la tarea.

    Si esta opción está desactivada, solo se ejecutarán en dispositivos cliente las tareas programadas; para **Manualmente**, **Una vez** e **Inmediatamente**, las tareas solo se ejecutarán en aquellos dispositivos cliente que estén visibles en la red. Por ejemplo, es posible que desee desactivar esta opción para una tarea que consuma recursos que desee ejecutar solo fuera del horario comercial.

    Esta opción está activada de forma predeterminada.

  - **Usar el retraso aleatorio automáticamente para el inicio de tareas**

    Si esta opción está activada, la tarea se inicia aleatoriamente en los dispositivos cliente, dentro del intervalo de tiempo especificado, es decir, se trata de un *inicio distribuido de tarea*. El inicio distribuido de tareas ayuda a evitar que los dispositivos cliente hagan una elevada cantidad de peticiones simultáneas al Servidor de administración cuando se inicia una tarea programada.

    La hora de inicio distribuido se calcula automáticamente cuando se crea una tarea según el número de dispositivos cliente a los que se la asigna. Más tarde, la tarea se inicia siempre a la hora de inicio calculada. Sin embargo, cuando la configuración de la tarea se edita o la tarea se inicia de forma manual, el valor calculado de la hora de inicio de la tarea cambia.

    Si esta opción está desactivada, la tarea se inicia en los dispositivos cliente de acuerdo con la programación.

  - **Usar el retraso aleatorio para el inicio de tareas con un intervalo de (min)**

Si esta opción está activada, la tarea se inicia en los dispositivos cliente aleatoriamente dentro del intervalo de tiempo especificado. El inicio distribuido de tareas ayuda a evitar que los dispositivos cliente hagan una elevada cantidad de peticiones simultáneas al Servidor de administración cuando se inicia una tarea programada.

Si esta opción está desactivada, la tarea se inicia en los dispositivos cliente de acuerdo con la programación.

Esta opción está desactivada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

- **Detener la tarea si se ha estado ejecutando durante más de (min)**

  Una vez que el periodo de tiempo especificado expira, la tarea se detiene automáticamente, ya esté completa o no.

  Active esta opción si desea interrumpir (o detener) las tareas que tardan mucho en ejecutarse.

  Esta opción está desactivada de forma predeterminada. El tiempo de ejecución de la tarea predeterminado es de 120 minutos.

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

    La tarea se crea y se configura.

Cuando un Servidor de administración realiza la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*, las actualizaciones de las bases de datos y módulos de software se descargan del origen de actualizaciones y se almacenan en la carpeta compartida de un Servidor de administración. Si crea esta tarea para un grupo de administración, solo se aplicará a los Agentes de red incluidos en el grupo de administración especificado.

Las actualizaciones se distribuyen en los dispositivos cliente y en los Servidores de administración secundarios desde la carpeta compartida del Servidor de administración.

Visualización de actualizaciones descargadas

Cuando un Servidor de administración realiza la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*, las actualizaciones de las bases de datos y módulos de software se descargan del origen de actualizaciones y se almacenan en la carpeta compartida de un Servidor de administración. Puede ver las actualizaciones descargadas en la sección **ACTUALIZACIONES DE MÓDULOS DE SOFTWARE Y BASES DE DATOS DE KASPERSKY**.

Para ver la lista de actualizaciones descargadas,

En el menú principal, vaya a **OPERACIONES → APLICACIONES DE KASPERSKY → ACTUALIZACIONES DE MÓDULOS DE SOFTWARE Y BASES DE DATOS DE KASPERSKY**.

Aparece una lista de actualizaciones disponibles.

Verificación de las actualizaciones descargadas

Antes de instalar actualizaciones en los dispositivos administrados, primero puede verificar si las actualizaciones son operativas y los errores a través de la tarea de *Verificación de actualizaciones*. La tarea *Verificación de actualizaciones* se realiza automáticamente como parte de 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 de *verificación de actualizaciones*. Si la tarea termina correctamente, las actualizaciones se copiarán del repositorio temporal a la carpeta compartida del Servidor de administración. Se distribuirán a todos los dispositivos cliente que tengan como origen de actualizaciones ese mismo Servidor de administración.

Si, como resultado de la tarea *Verificación de actualizaciones*, se muestra que las actualizaciones ubicadas en el repositorio temporal son incorrectas o si la tarea *Verificación de actualizaciones* se ha completado con errores, las actualizaciones de este tipo no se copiarán a la carpeta compartida. El Servidor de administración guardará el conjunto de actualizaciones anterior. Además, las tareas que tienen el tipo de programación **Cuando se descargan nuevas actualizaciones en el repositorio** no se inician. Si el análisis de las nuevas actualizaciones se realiza con éxito, dichas operaciones se realizarán en el siguiente inicio de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*.

Se considerará que un conjunto de actualizaciones es incorrecto si se cumple una de las siguientes condiciones en al menos un dispositivo de prueba:

- Se produjo un error en la tarea de actualización.
- El estado de protección en tiempo real de la aplicación de seguridad ha cambiado después de aplicarse las actualizaciones.
- Se ha detectado un objeto infectado mientras se ejecutaba la tarea de análisis a petición.
- Se ha producido un error en el tiempo de ejecución de una aplicación Kaspersky.

Si ninguna de las condiciones indicadas es verdadera para ningún dispositivo de prueba, se considerará que el conjunto de actualizaciones es válido y que la tarea *Verificación de actualizaciones* ha finalizado correctamente.

Antes de empezar a crear la tarea *Verificación de actualizaciones*, realice los requisitos previos:

1. Cree un grupo de administración con varios dispositivos de prueba. Necesitará este grupo para verificar las actualizaciones.

   Recomendamos utilizar los dispositivos con la protección más fiable y con la configuración de aplicaciones más común en la red. Este enfoque aumenta la calidad y la probabilidad de detección de virus durante los análisis y reduce al mínimo el riesgo de falsos positivos. Si se detectan virus en los dispositivos cliente, se considerará que la tarea *Verificación de actualizaciones* no se ha realizado correctamente.

2. Cree las tareas de actualización y análisis de virus para una aplicación compatible con Kaspersky Security Center, por ejemplo, Kaspersky Endpoint Security for Linux. Al crear las tareas de actualización y análisis de virus, especifique el grupo de administración con los dispositivos de prueba.

   La tare *Actualizar verificación* ejecuta secuencialmente las tareas de actualización y análisis de virus en los dispositivos de prueba para verificar que todas las actualizaciones sean válidas. Además, al crear la tarea *Actualizar verificación* debe especificar las tareas de actualización y análisis de virus.

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 que se abre, seleccione la pestaña **Configuración de la aplicación** y después active la opción **Ejecutar verificación de actualizaciones**.
4. Si la tarea *Verificar actualizaciones* existe, haga clic en el botón **Elija una tarea**. En la ventana que se abre, seleccione la tarea *Verificar actualizaciones* en el grupo de administración con dispositivos de prueba.
5. Si no creó la tarea *Verificar actualizaciones* anteriormente, haga lo siguiente:

   a. Haga clic en el botón **Nueva tarea**.

   b. En el Asistente para añadir tareas que se abre, especifique el nombre de la tarea si desea cambiar el nombre predeterminado.

   c. Seleccione el grupo de administración con dispositivos de prueba que creó anteriormente.

   d. Primero, seleccione la tarea de actualización de una aplicación requerida compatible con Kaspersky Security Center y luego seleccione la tarea de análisis de virus.

   Después de eso, aparecerán las siguientes opciones. Recomendamos dejarlos activados:

   - **Reiniciar dispositivo después de actualizar las bases de datos**

     Después de actualizar las bases de datos antivirus en un dispositivo, recomendamos reiniciar el dispositivo.

     La opción está activada de forma predeterminada.

   - **Comprobar el estado de la protección en tiempo real tras la actualización de las bases de datos y el reinicio del dispositivo**

     Si esta opción está activada, la tarea *Verificación de actualizaciones* comprueba si las actualizaciones descargadas en el repositorio del Servidor de administración son válidas y si el nivel de protección ha disminuido después de la actualización de la base de datos antivirus y el reinicio del dispositivo.

     Esta opción está activada de forma predeterminada.

   e. Especifique una cuenta desde la cual se ejecutará la tare *Verificación de actualizaciones*. Puede usar su cuenta y dejar activada la opción **Cuenta predeterminada**. Como alternativa, puede especificar que la tarea se ejecute con otra cuenta que tenga los derechos de acceso necesarios. Para ello, seleccione la opción **Especificar cuenta** y luego ingrese las credenciales de esa cuenta.

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*, que comenzará desde la verificación de actualización.

Creación de la tarea para descargar actualizaciones a los repositorios de los puntos de distribución

Expandir todo | Contraer todo

Puede crear la tarea *Descargar actualizaciones en los repositorios de puntos de distribución* para un grupo de administración. Esta tarea se ejecutará para puntos de distribución incluidos en el grupo de administración especificado.

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 es necesaria para descargar actualizaciones de los servidores de actualización de Kaspersky a los repositorios de los puntos de distribución. La lista de actualizaciones incluye:

- Actualizaciones de bases de datos y módulos de software para aplicaciones de seguridad de Kaspersky
- Actualizaciones a los componentes de Kaspersky Security Center
- Actualizaciones a las aplicaciones de seguridad de Kaspersky

Una vez que se descarguen las actualizaciones, se pueden propagar a los dispositivos administrados.

*Para crear la tarea **Descargar actualizaciones en los repositorios de puntos de distribución,** para un grupo de administración seleccionado:*

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

   Se inicia el Asistente para añadir tareas. Siga los pasos del Asistente.
3. Para la aplicación Kaspersky Security Center, seleccione **Descargar actualizaciones en los repositorios de puntos de distribución** en el campo **Tipo de tarea**.
4. Especifique el nombre para la tarea que está creando. El nombre de la tarea no puede contener más de 100 caracteres y no puede incluir ningún carácter especial (como "*<>?\:|).
5. Pulse el botón de opción para especificar el grupo de administración, la selección de dispositivos o los dispositivos a los que se aplica la tarea.
6. En el paso **Finalizar la creación de tareas** paso, si desea modificar la configuración predeterminada de la tarea, active la opción **Abrir los detalles de la tarea cuando se complete la creación**. Si no activa esta opción, la tarea se creará con las configuraciones predeterminadas. Puede modificar la configuración predeterminada más tarde, en cualquier momento.
7. Haga clic en el botón **Crear**.

   La tarea se crea y se muestra en la lista de tareas.
8. Haga clic en el nombre de la tarea creada para abrir la ventana de propiedades de la tarea.
9. En la ficha **Configuración de la aplicación** de la ventana de propiedades de la tarea, especifique la siguiente configuración:

   - Orígenes de actualizaciones

     Los recursos siguientes pueden utilizarse como origen de actualizaciones para el punto de distribución:

     - Servidores de actualización de Kaspersky

       Servidores HTTP(S) de Kaspersky desde los que las aplicaciones Kaspersky descargan las actualizaciones para las bases de datos y los módulos de la aplicación.

       Esta opción está seleccionada de forma predeterminada.
     - Servidor de administración principal

       Este recurso se aplica a las tareas creadas para un Servidor de administración secundario o virtual.
     - Carpeta local o de red

       Una carpeta local o de red que contiene las últimas actualizaciones. Una carpeta de red puede ser un servidor FTP o HTTP o un recurso compartido SMB. Si una carpeta de red requiere autenticación, solo se admite el protocolo SMB. Cuando se selecciona una carpeta local, debe especificar una carpeta en un dispositivo que tenga el Servidor de administración instalado.

       > Un servidor FTP o HTTP o una carpeta de red utilizada por un origen de actualizaciones debe contener una estructura de carpetas (con actualizaciones) que coincida con la estructura creada al usar los servidores de actualización de Kaspersky.

     Si activa la opción **No usar servidor proxy** para los orígenes de actualización Servidores de actualización de Kaspersky o Carpeta local o de red, un punto de distribución no usa un servidor proxy para descargar actualizaciones, incluso si ha activado la opción **Usar servidor proxy** la configuración de la directiva del Agente de red para el punto de distribución.

   - Carpeta para almacenar actualizaciones

     La ruta a la carpeta especificada para almacenar las actualizaciones guardadas. Puede copiar la ruta de la carpeta especificada en el portapapeles. No puede cambiar la ruta a una carpeta específica para una tarea de grupo.

   - Descargar archivos de comparación

     Esta opción habilita la función de descarga de archivos diff.

     Esta opción está desactivada de forma predeterminada.

- **Descargar actualizaciones utilizando el esquema anterior**

  A partir de la versión 14, Kaspersky Security Center descarga las actualizaciones de bases de datos y los módulos de software utilizando el nuevo esquema. Para que la aplicación descargue actualizaciones utilizando el nuevo esquema, el origen de actualización debe contener los archivos de actualización cuyos metadatos sean compatibles con el nuevo esquema. Si el origen de actualización contiene archivos de actualización cuyos metadatos son compatibles solo con el esquema anterior, active la **Descargar actualizaciones utilizando el esquema anterior** opción. De lo contrario, la tarea de descarga de la actualización no funcionará.

  Por ejemplo, debe activar esta opción cuando se especifica una carpeta local o de red como fuente de actualización y los archivos de actualización en esta carpeta fueron descargados por una de las siguientes aplicaciones:

  - Utilidad Kaspersky Update

    Esta utilidad descarga actualizaciones utilizando el esquema antiguo.

  - Kaspersky Security Center 13.2 o una versión anterior

    Por ejemplo, un punto de distribución está configurado para tomar las actualizaciones de una carpeta local o de red. En este caso, puede descargar actualizaciones utilizando un Servidor de administración que tenga conexión a Internet y luego colocar las actualizaciones en la carpeta local en el punto de distribución. Si el Servidor de administración tiene la versión 13.2 o anterior, active la opción **Descargar actualizaciones utilizando el esquema anterior** en la tarea *Descargar actualizaciones a los repositorios de los puntos de distribución*.

  Esta opción está desactivada de forma predeterminada.

10. Crear una planificación para el inicio de la tarea. Si es necesario, especifique la siguiente configuración:

- **Inicio programado**:

  Seleccione la programación según la cual se ejecuta la tarea y configure la programación seleccionada.

  - **Manualmente** (seleccionado de manera predeterminada)

    La tarea no se ejecuta automáticamente. Solo lo puede iniciar de forma manual.

    Esta opción está activada de forma predeterminada.

  - **Cada N minutos**

    La tarea se ejecuta regularmente, con el intervalo especificado en minutos, a partir de la hora especificada en el día en que se crea la tarea.

    De forma predeterminada, la tarea se ejecuta cada 30 minutos, a partir de la hora actuales del sistema.

  - **Cada N horas**

    La tarea se ejecuta regularmente, con el intervalo especificado en horas, a partir de la fecha y hora especificadas.

    De forma predeterminada, la tarea se ejecuta cada seis horas, a partir de la fecha y hora actuales del sistema.

  - **Cada N días**

    La tarea se ejecuta regularmente, con el intervalo especificado en días. Además, puede especificar una fecha y hora de la primera tarea ejecutada. Estas opciones adicionales estarán disponibles si son compatibles con la aplicación para la que crea la tarea.

    De forma predeterminada, la tarea se ejecuta cada día, a partir de la fecha y hora actuales del sistema.

  - **Cada N semanas**

    La tarea se ejecuta regularmente, con el intervalo especificado en semanas, en el día especificado de la semana y en el tiempo especificado.

    De forma predeterminada, la tarea se ejecuta todos los lunes a la hora actual del sistema.

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

    La tarea se ejecuta regularmente, con el intervalo especificado en días. Este programa no admite el cumplimiento del horario de verano (DST). Esto significa que cuando los relojes saltan una hora hacia adelante o hacia atrás al comienzo o al final del horario de verano, la hora de inicio de la tarea actual no cambia.

    No recomendamos que utilice este horario. Es necesario para la compatibilidad con versiones anteriores de Kaspersky Security Center Linux.

De forma predeterminada, la tarea se ejecuta cada día a la hora actual del sistema.

- **Semanalmente**

  La tarea se ejecuta cada semana en el día especificado y a la hora especificada.

- **Por días de la semana**

  La tarea se ejecuta regularmente, en el día de la semana especificado y a la hora especificada.

  De forma predeterminada, la tarea se ejecuta todos los viernes a las 18:00:00 h.

- **Mensualmente**

  La tarea se ejecuta regularmente, en el día del mes especificado y a la hora especificada.

  En los meses que faltan el día especificado, la tarea se ejecuta el último día.

  De forma predeterminada, la tarea se ejecuta el primer día de cada mes, a la hora actual del sistema.

- **Cada mes, en días concretos de las semanas seleccionadas**

  La tarea se ejecuta regularmente, en el día de cada mes especificado y a la hora especificada.

  De forma predeterminada, no se seleccionan días del mes; la hora de inicio predeterminada es las 18:00:00 h.

- **Al detectar un foco de virus**

  La tarea se ejecuta después de que se produzca un evento de *Brote de virus*. Seleccione los tipos de aplicaciones que supervisarán los brotes de virus. Los siguientes tipos de aplicación están disponibles:

  - Antivirus para estaciones de trabajo y servidores de archivos
  - Antivirus para la protección del perímetro
  - Antivirus para sistemas de correo

  De forma predeterminada, están seleccionados todos los tipos de aplicación.

  Es posible que desee ejecutar diferentes tareas según el tipo de aplicación antivirus que informe sobre un brote de virus. En este caso, elimine la selección de los tipos de aplicaciones que no necesita.

- **Al completar otra tarea**

  La tarea actual se inicia después de que se complete otra tarea. Puede seleccionar cómo debe completarse la tarea anterior (satisfactoriamente o con errores) para activar el inicio de la tarea actual.

- **Ejecutar tareas no realizadas**

  Esta opción determina el comportamiento de una tarea si un dispositivo cliente no está visible en la red cuando la tarea vaya a comenzar.

  Si esta opción está activada, el sistema intentará iniciar la tarea la próxima vez que la aplicación Kaspersky se ejecute en un dispositivo cliente. Si la programación de la tarea es **Manualmente**, **Una vez** o **Inmediatamente**, la tarea se inicia inmediatamente después de que el dispositivo se haga visible en la red o inmediatamente después de que el dispositivo se incluya en la cobertura de la tarea.

  Si esta opción está desactivada, solo se ejecutarán en dispositivos cliente las tareas programadas; para **Manualmente**, **Una vez** e **Inmediatamente**, las tareas solo se ejecutarán en aquellos dispositivos cliente que estén visibles en la red. Por ejemplo, es posible que desee desactivar esta opción para una tarea que consuma recursos que desee ejecutar solo fuera del horario comercial.

  Esta opción está activada de forma predeterminada.

- **Usar el retraso aleatorio automáticamente para el inicio de tareas**

  Si esta opción está activada, la tarea se inicia aleatoriamente en los dispositivos cliente, dentro del intervalo de tiempo especificado, es decir, se trata de un *inicio distribuido de tarea*. El inicio distribuido de tareas ayuda a evitar que los dispositivos cliente hagan una elevada cantidad de peticiones simultáneas al Servidor de administración cuando se inicia una tarea programada.

  La hora de inicio distribuido se calcula automáticamente cuando se crea una tarea según el número de dispositivos cliente a los que se la asigna. Más tarde, la tarea se inicia siempre a la hora de inicio calculada. Sin embargo, cuando la configuración de la tarea se edita o la tarea se inicia de forma manual, el valor calculado de la hora de inicio de la tarea cambia.

Si esta opción está desactivada, la tarea se inicia en los dispositivos cliente de acuerdo con la programación.

- **Usar el retraso aleatorio para el inicio de tareas con un intervalo de (min)**

  Si esta opción está activada, la tarea se inicia en los dispositivos cliente aleatoriamente dentro del intervalo de tiempo especificado. El inicio distribuido de tareas ayuda a evitar que los dispositivos cliente hagan una elevada cantidad de peticiones simultáneas al Servidor de administración cuando se inicia una tarea programada.

  Si esta opción está desactivada, la tarea se inicia en los dispositivos cliente de acuerdo con la programación.

  Esta opción está desactivada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

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

La tarea se crea y se configura.

Además de la configuración que especifique durante la creación de la tarea, puede cambiar otras propiedades de una tarea creada.

Cuando se realiza la tarea *Descargar actualizaciones en los repositorios de puntos de distribución*, las actualizaciones para bases de datos y módulos del software se descargan desde el origen de actualizaciones y se almacenan en la carpeta compartida. Las actualizaciones descargadas solo se utilizarán por puntos de distribución que se incluyen en el grupo de administración especificado y que no tienen una tarea de descarga de actualización explícitamente definida para ellos.

Adición de fuentes de actualizaciones para la tarea Descargar actualizaciones al repositorio del Servidor de administración

Al crear o usar la tarea para descargar actualizaciones al repositorio del Servidor de administración, puede elegir las siguientes fuentes de actualizaciones:

- Servidores de actualización 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 poner los archivos descargados en la carpeta necesaria.

Puede especificar solo una ruta a una carpeta local o de red. La carpeta local solo puede estar en el Servidor de administración. La carpeta de red solo puede estar en un servidor FTP o HTTP.

Si añade 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 **Especificar cuenta para el acceso a la carpeta compartida del origen de actualizaciones (si la hay)** e ingrese las credenciales de cuenta requeridas para el acceso.

Para añadir los orígenes 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 **Añadir**.
6. En la lista de orígenes de actualización, añada los orígenes necesarios. Si marca la casilla **Carpeta local o de red**, especifique una ruta a la carpeta.
7. Haga clic en **Aceptar** y, a continuación, cierre la ventana de propiedades del origen de actualizaciones.
8. En la ventana de orígenes de actualizaciones haga clic en **Aceptar**.
9. Haga clic en el botón **Guardar** en la ventana de la 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 bases de datos y 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 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. **Activar la función en el Servidor de administración**

   Habilite la función en la configuración de una tarea *Descargar de actualizaciones en el repositorio del Servidor de administración*.

2. **Activar 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, active la función en la configuración de la directiva del Agente de red para un punto de distribución que reciba actualizaciones del servidor de administración.

   A continuación, active 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 esté activada con éxito, puede medir el tráfico interno antes y después de realizar el escenario.

Descargar actualizaciones por puntos de distribución

Expandir todo | Contraer todo

Kaspersky Security Center Linux permite que los puntos de distribución reciban actualizaciones del Servidor de administración, de los servidores de Kaspersky o de una carpeta local o en red.

Para configurar la descarga de actualizaciones para un punto de distribución:

1. En la ventana principal de la aplicación, haga clic en el icono de **Configuración** () junto al nombre del Servidor de administración requerido.
   Se abre la ventana Propiedades del Servidor de administración.
2. En la pestaña **Control de aplicaciones**, seleccione 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 una fuente de actualización para el punto de distribución:

   - **Fuente de actualizaciones**

     Seleccione una fuente de actualizaciones para el punto de distribución:

- Para permitir al punto de distribución recibir actualizaciones del Servidor de administración, seleccione **Descargar del Servidor de administración**.
- Para permitir que el punto de distribución reciba actualizaciones mediante una tarea, seleccione **Utilizar la tarea de descarga de actualizaciones** y, a continuación, especifique una tarea *Descargar actualizaciones a los repositorios de los puntos de distribución*:
  - Si dicha tarea ya existe en el dispositivo, selecciónela en la lista.
  - Si aún no existe tal tarea en el dispositivo, haga clic en el enlace **Crear una tarea** para crear una tarea. Se inicia el Asistente para añadir tareas. Siga las instrucciones del Asistente.

- **Descargar archivos de comparación**

  Esta opción habilita la función de descarga de archivos diff.

  Esta opción está activada de forma predeterminada.

El punto de distribución recibirá actualizaciones del origen especificado.

Actualización de las bases de datos y módulos de software de Kaspersky en dispositivos desconectados

Actualizar las bases de datos y los módulos de software de Kaspersky en dispositivos administrados es una tarea importante para mantener la protección de los dispositivos contra virus y otras amenazas. Los administradores generalmente configuran actualizaciones regulares mediante el uso del repositorio del Servidor de administración.

Cuando necesite actualizar 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 este caso, debe enviar los archivos de las actualizaciones necesarias mediante un dispositivo de almacenamiento masivo, como una unidad flash o un disco duro externo.

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 desconectado, 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 mediante 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 módulos de software de Kaspersky en dispositivos desconectados

1. Conecte la unidad extraíble al dispositivo donde está instalado el Servidor de administración.
2. Copie los archivos de las actualizaciones en 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. Para este propósito, utilice la opción **Copiar las actualizaciones descargadas en carpetas adicionales** 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 desconectados (configure Kaspersky Endpoint Security for Linux) para recibir actualizaciones de una carpeta local o un recurso compartido, como un servidor FTP o una carpeta compartida.
4. Copie los archivos de actualización de la unidad extraíble a la carpeta local o al recurso compartido que desee usar como origen de actualizaciones.
5. En el dispositivo desconectado que requiere una instalación de actualización, inicie la tarea de actualización de Kaspersky Endpoint Security for Linux.

Después de completar la tarea de actualización, las bases de datos de Kaspersky y los módulos de software están actualizados en el dispositivo.

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:

- Configura la cobertura de las directivas

  Existe otra forma de aplicar ajustes pertinentes en dispositivos: mediante el uso de *perfiles de directiva*.

- Configura la cobertura de las tareas de grupo

  Existe un enfoque para definir la cobertura de las tareas de grupo que no se basan en una jerarquía de los grupos de administración: el uso de tareas para selecciones de dispositivos y tareas para dispositivos específicos.

- Configura los derechos de acceso a dispositivos, Servidores de administración virtuales y Servidores de administración secundarios

- Asigna puntos de distribución

Al construir la estructura de los grupos de administración, debe tener en cuenta la topología de la red de la organización para la asignación óptima de puntos de distribución. La distribución óptima de los puntos de distribución le permite ahorrar tráfico de la red de la organización.

Según el organigrama y la topología de red de la organización, se pueden aplicar las siguientes configuraciones estándares a la estructura de grupos de administración:

- Oficina única

- Varias oficinas remotas pequeñas

Los dispositivos que funcionan como puntos de distribución se deben proteger, incluida la protección física, contra cualquier acceso no autorizado.

Configuración estándar de puntos de distribución: oficina única

En una configuración de "oficina única" estándar, todos los dispositivos están dentro de la red de la organización. La red de la organización puede consistir en unas partes independientes (redes o segmentos de red) vinculadas por canales estrechos.

Los métodos siguientes de crear la estructura de grupos de administración son posibles:

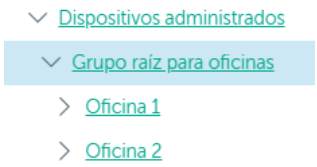
- Crear la estructura de grupos de administración tomando en consideración la topología de red. La estructura de grupos de administración puede no reflejar la topología de red con precisión absoluta. Una coincidencia entre las partes independientes de la red y ciertos grupos de administración sería suficiente. Puede usar la asignación automática de puntos de distribución o asignarlos manualmente.

- La creación de la estructura de grupos de administración, sin tomar la topología de red en cuenta. En este caso, debe desactivar 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 de raíz 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 la misma cobertura que abarca a todos los dispositivos en la red de la organización. En este caso, cada Agente de red se conectará con el punto de distribución que tenga la ruta más corta. La ruta a un punto de distribución se puede rastrear con la herramienta tracert.

Configuración estándar de los puntos de distribución: varias oficinas remotas pequeñas

Esta configuración estándar sirve para varias pequeñas oficinas remotas, que se pueden comunicar con la oficina central mediante Internet. Cada oficina remota está ubicada detrás de la NAT, es decir, la conexión de una oficina remota a otra no es posible porque las oficinas están aisladas la una de la otra.

La configuración se debe reflejar en la estructura de los grupos de administración: se debe crear un grupo de administración independiente para cada oficina remota (grupos **Oficina 1** y **Oficina 2** en la imagen a continuación).



Las oficinas remotas se incluyen en la estructura del grupo de administración

Se deben asignar uno o varios puntos de distribución a cada grupo de administración que corresponda a una oficina. Los puntos de distribución deben ser dispositivos en la oficina remota que tienen una cantidad suficiente de espacio libre en disco. Los dispositivos desplegados en el grupo **Oficina 1**, por ejemplo, accederán a los puntos de distribución asignados al grupo de administración de **Oficina 1**.

Si algunos usuarios se mueven entre oficinas físicamente con sus equipos portátiles, debe seleccionar dos o más dispositivos (además de los puntos de distribución existentes) en cada oficina remota y asignarlos para que funcionen como puntos de distribución para un grupo de administración de alto nivel (**Grupo raíz para oficinas** en la imagen anterior).

Ejemplo: Un equipo portátil se despliega en el grupo de administración de la **Oficina 1** y luego se mueve físicamente a la oficina que corresponde al grupo de administración de la **Oficina 2**. Después de que se mueve el equipo portátil, el Agente de red intenta acceder a los puntos de distribución asignados al grupo de la **Oficina 1**, pero esos puntos de distribución no están disponibles. Entonces, el Agente de red empieza a intentar acceder a los puntos de distribución que se han asignado al **Grupo raíz para oficinas**. Como las oficinas remotas están aisladas la una de la otra, los intentos de acceder a los puntos de distribución asignados al grupo de administración del **Grupo raíz para oficinas** solo tendrán éxito cuando el Agente de red intente acceder a los puntos de distribución en el grupo de la **Oficina 2**. Es decir, el equipo portátil permanecerá en el grupo de administración que corresponde a la oficina inicial, pero el equipo portátil usará el punto de distribución de la oficina donde físicamente se ubica en este momento.

Cálculo del número y la configuración de los puntos de distribución

Cuantos más dispositivos cliente contenga una red, más puntos de distribución requerirá. Le recomendamos que no desactive la asignación automática de puntos de distribución. Cuando la asignación automática de puntos de distribución está activada, el Servidor de administración asigna puntos de distribución si el número de dispositivos cliente es elevado 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 asignados 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 la red	Número de puntos de distribución
Menos de 300	0 (no asigne puntos de distribución)
Más de 300	Aceptable: (N/10,000 + 1), recomendado: (N/5000 + 2), donde N es el número de dispositivos conectados a una red

Número de puntos de distribución asignados 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 la red	Número de puntos de distribución
Menos de 10	0 (no asigne 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 una 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 asigne puntos de distribución como se muestra en las siguientes tablas para evitar una carga excesiva en los canales de comunicación y el Servidor de administración:

Número de estaciones de trabajo que funcionan 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 el segmento de la red	Número de puntos de distribución
Menos de 300	0 (no asigne puntos de distribución)
Más de 300	(N/300 + 1), donde N es el número de dispositivos en red, pero debe haber al menos tres puntos de distribución

Número de estaciones de trabajo que funcionan 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 la red	Número de puntos de distribución
Menos de 10	0 (no asigne puntos de distribución)
10-30	1
31-300	2
Más de 300	(N/300 + 1), donde N es el número de dispositivos en red, pero debe haber al menos tres puntos de distribución

Si un punto de distribución se apaga (o no está disponible por algún otro motivo), los dispositivos administrados en su cobertura pueden acceder al Servidor de administración para obtener actualizaciones.

Asignar puntos de distribución automáticamente

Recomendamos que asigne puntos de distribución automáticamente. En este caso, Kaspersky Security Center Linux seleccionará por sí mismo a qué dispositivos se les deben asignar puntos de distribución.

Para asignar puntos de distribución automáticamente:

1. En la ventana principal de la aplicación, haga clic en el icono de **Configuración** () junto al nombre del Servidor de administración requerido.
   Se abre la ventana Propiedades del Servidor de administración.
2. En la pestaña **Control de aplicaciones**, seleccione la sección **Puntos de distribución**.
3. Seleccione la opción **Asignar automáticamente puntos de distribución**.

   Si la asignación automática de dispositivos para que actúen como puntos de distribución está activada, no se pueden 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 puntos de distribución automáticamente.

Asignar puntos de distribución manualmente

Expandir todo | Contraer todo

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 a qué dispositivos se les deben asignar puntos de distribución. Sin embargo, si tiene que optar por no asignar automáticamente puntos de distribución por cualquier motivo (por ejemplo, si desea usar servidores asignados exclusivamente), puede asignar puntos de distribución manualmente después de calcular su número y configuración.

Los dispositivos que funcionan como puntos de distribución se deben proteger, incluida la protección física, contra cualquier acceso no autorizado.

Para designar manualmente un dispositivo para actuar como punto de distribución:

1. En la ventana principal de la aplicación, haga clic en el icono de **Configuración** () junto al nombre del Servidor de administración requerido.
   Se abre la ventana Propiedades del Servidor de administración.
2. En la pestaña **Control de aplicaciones**, seleccione 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 desea convertir en punto de distribución.
   Al seleccionar un dispositivo, recuerde las características de operación de puntos de distribución y el conjunto de requisitos para el dispositivo que actúa como punto de distribución.
6. Seleccione el grupo de administración que desee incluir en la cobertura del punto de distribución seleccionado.
7. Haga clic en el botón **Aceptar**.
   El punto de distribución que ha añadido se mostrará en la lista de puntos de distribución, en la sección **Puntos de distribución**.
8. Seleccione el punto de distribución recién añadido en la lista para abrir su ventana de propiedades.
9. Configure el punto de distribución perfil en la ventana de propiedades:
   - La sección **General** contiene los parámetros que regulan la interacción del punto de distribución con los dispositivos cliente.
     - **Número de puerto SSL**

       El número del puerto SSL para la conexión cifrada entre los dispositivos cliente y el punto de distribución usando SSL.
       De forma predeterminada, se utiliza el puerto 13000.

     - **Usar multidifusión**

Si se selecciona esta opción, se utilizará la multidifusión IP para la distribución automática de paquetes de instalación en dispositivos cliente dentro del grupo.

La multidifusión IP disminuye el tiempo requerido para instalar una aplicación desde un paquete de instalación hacia un grupo de dispositivos cliente, pero aumenta el tiempo de instalación cuando instala una aplicación en un único dispositivo cliente.

- **Dirección IP de multidifusión**

  La dirección IP que se utilizará para la multidifusión. Puede definir una dirección IP en el rango de 224.0.0.0 – 239.255.255.255

  De manera predeterminada, Kaspersky Security Center Linux asigna automáticamente una dirección IP de multidifusión única dentro del rango dado.

- **Número de puerto de multidifusión IP**

  Número del puerto para multidifusión IP.

  De forma predeterminada el número de puerto es el 15001. Si el dispositivo que tiene el Servidor de administración instalado está configurado como punto de distribución, de forma predeterminada se utiliza el puerto 13001 para la conexión SSL.

- **Implementar actualizaciones**

  Las actualizaciones se distribuyen a los dispositivos administrados desde los siguientes orígenes:

  - Este punto de distribución, si esta opción está activada.
  - Otros puntos de distribución, Servidor de administración o servidores de actualización de Kaspersky, si esta opción está desactivada.

  Si usa puntos de distribución para implementar actualizaciones, puede ahorrar tráfico dado que se reduce la cantidad de descargas. Además, puede aliviar la carga en el Servidor de administración y reubicarla entre los puntos de distribución. Puede calcular el número de puntos de distribución de su red para optimizar el tráfico y la carga.

  Si desactiva esta opción, puede aumentar el número de descargas de actualizaciones y la carga en el Servidor de administración. Esta opción está activada de forma predeterminada.

- **Desplegar paquetes de instalación**

  Los paquetes de instalación se distribuyen a los dispositivos administrados desde las siguientes fuentes:

  - Este punto de distribución, si esta opción está activada.
  - Otros puntos de distribución, Servidor de administración o servidores de actualización de Kaspersky, si esta opción está desactivada.

  Si usa puntos de distribución para implementar paquetes de instalación, puede ahorrar tráfico dado que se reduce la cantidad de descargas. Además, puede aliviar la carga en el Servidor de administración y reubicarla entre los puntos de distribución. Puede calcular el número de puntos de distribución de su red para optimizar el tráfico y la carga.

  Si desactiva esta opción, puede aumentar la cantidad de descargas de paquetes de instalación y la carga en el Servidor de administración. Esta opción está activada de forma 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 una fuente de actualizaciones para el punto de distribución:

  - **Fuente de actualizaciones**

    Seleccione una fuente de actualizaciones para el punto de distribución:

    - Para permitir al punto de distribución recibir actualizaciones del Servidor de administración, seleccione **Descargar del Servidor de administración**.
    - Para permitir que el punto de distribución reciba actualizaciones mediante una tarea, seleccione **Utilizar la tarea de descarga de actualizaciones** y, a continuación, especifique una tarea *Descargar actualizaciones a los repositorios de los puntos de distribución*:
      - Si dicha tarea ya existe en el dispositivo, selecciónela en la lista.
      - Si aún no existe tal tarea en el dispositivo, haga clic en el enlace **Crear una tarea** para crear una tarea. Se inicia el Asistente para añadir tareas. Siga las instrucciones del Asistente.

- **Descargar archivos de comparación**

  Esta opción habilita la función de descarga de archivos diff.

  Esta opción está activada de forma predeterminada.

- Configure el sondeo de rangos de IP en el punto de distribución.

  - **Rangos IP**

    Puede activar la detección de dispositivos para los rangos IPv4 y las redes IPv6.

    Si activa la opción **Activar rango de sondeo**, puede añadir rangos analizados y establecer la programación para ellos. Puede añadir rangos de IP a la lista de intervalos analizados.

    Si activa la opción **Activar el sondeo con la tecnología Zeroconf**, el punto de distribución automáticamente sondea la red IPv6 mediante el uso de las redes de configuración cero (también denominadas *Zeroconf*). En este caso, los rangos de IP especificados se ignoran, porque el punto de distribución sondea toda la red.

- En la sección **Avanzado**, especifique la carpeta que debe utilizar el punto de distribución para almacenar datos distribuidos.

  - **Usar carpeta predeterminada**

    Si selecciona esta opción, la aplicación usará la carpeta de instalación de Agente de red en el punto de distribución.

  - **Usar carpeta especificada**

    Si se selecciona esta opción, se podrá especificar la ruta de la carpeta en el campo siguiente. Puede ser una carpeta local en el punto de distribución, o bien un directorio remoto en cualquier dispositivo de la red corporativa.

    La cuenta de usuario utilizada en el punto de distribución para ejecutar el Agente de red debe tener acceso de lectura y escritura a la carpeta especificada.

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

    Los dispositivos seleccionados se comportan como puntos de distribución.

Modificación de la lista de puntos de distribución para un grupo de administración

Puede ver la lista de puntos de distribución asignados para un grupo de administración específico y modificar la lista añadiendo o eliminando puntos de distribución.

Para ver y modificar la lista de puntos de distribución para un grupo de administración:

1. Vaya a **DISPOSITIVOS** → **Grupos**.
2. En la estructura del grupo de administración, seleccione el grupo de administración para el que desea ver los puntos de distribución asignados.
3. Haga clic en la pestaña **PUNTOS DE DISTRIBUCIÓN**.
4. Añada nuevos puntos de distribución para el grupo de administración utilizando el botón **Asignar** o elimine los puntos de distribución asignados utilizando el botón **Desasignar**.

Según sus modificaciones, los nuevos puntos de distribución se añaden a la lista o los puntos de distribución existentes se eliminan 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 los dispositivos gestionados por Agente de red. Por ejemplo, se debe activar 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 activa el servidor push. Si tiene varios puntos de distribución asignados para el mismo grupo de administración, puede activar 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.

Se recomienda utilizar puntos de distribución como servidores push para asegurarse de que haya una conectividad continua entre un dispositivo administrado y el Servidor de administración. Se necesita conectividad continua para algunas operaciones, como ejecutar y detener tareas locales, recibir estadísticas para una aplicación administrada o crear un túnel. Si utiliza un punto de distribución como servidor push, no es necesario utilizar la opción **No desconectar del Servidor de administración** en dispositivos administrados o enviar paquetes al puerto UDP del Agente de red.

Un servidor push soporta la carga de hasta 50 000 conexiones simultáneas.

Para habilitar el servidor push en un punto de distribución:

1. Haga clic en el icono de **Configuración** ( ) junto al nombre del Servidor de administración requerido.
   Se abre la ventana Propiedades del Servidor de administración.
2. En la pestaña **Control de aplicaciones**, seleccione 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 **Control de aplicaciones**, active 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.

Administrar aplicaciones de terceros en dispositivos cliente

Esta sección describe las funciones de Kaspersky Security Center Linux relacionadas con la administración de aplicaciones de terceros que se ejecutan en dispositivos cliente.

Escenario: administración de aplicaciones

Puede administrar el inicio de aplicaciones en dispositivos de usuario. Puede permitir o bloquear aplicaciones para que se ejecuten en dispositivos administrados. Esta funcionalidad se ejecuta mediante el componente Control de aplicaciones.

El componente Control de aplicaciones está disponible para Kaspersky Endpoint Security 11.2 para Linux y versiones posteriores.

Requisitos previos

- Kaspersky Security Center Linux se ha implementado en su organización.
- La directiva Kaspersky Endpoint Security for Linux queda creada y activada.

Etapas

El escenario de uso de Control de aplicaciones procede en etapas:

1. **Formar y ver la lista de archivos ejecutables en dispositivos cliente**

   Esta etapa le ayuda a descubrir qué archivos ejecutables se encuentran en los dispositivos administrados. Examine la lista de los archivos ejecutables y compárela con las listas de archivos ejecutables permitidos y prohibidos. Las restricciones sobre el uso de archivos ejecutables pueden estar relacionadas con las directivas de seguridad de la información de su organización. Puede omitir esta etapa si sabe exactamente los archivos ejecutables están instalados en los dispositivos administrados.

   Instrucciones: Obtener y ver una lista de archivos ejecutables almacenada en dispositivos cliente

2. **Crear categorías de aplicaciones para las aplicaciones utilizadas en su organización**

   Analizar las listas de archivos ejecutables almacenados en los dispositivos administrados. Basándose en el análisis, crear categorías de aplicaciones. Se recomienda crear una categoría de «Aplicaciones de trabajo» que cubra el conjunto estándar de aplicaciones que se utilizan en su organización. Si diferentes grupos de usuarios usan diferentes conjuntos de aplicaciones en su trabajo, se puede crear una categoría de aplicación separada para cada grupo de usuarios.

   Instrucciones: Crear categoría de aplicaciones con contenido agregado manualmente

3. **Configurar el Control de aplicaciones en la directiva de Kaspersky Endpoint Security for Linux**

   Configure el componente Control de aplicaciones en la directiva de Kaspersky Endpoint Security for Linux utilizando las categorías de aplicaciones que creó en la etapa anterior.

4. **Verificación de la configuración de Control de aplicaciones**

   Asegúrese de haber hecho lo siguiente:

   - Creado categorías de aplicaciones.

- Configurado Control de aplicaciones mediante las categorías de aplicaciones.

Resultados

Cuando se completa el escenario, se controla el inicio de aplicaciones en dispositivos administrados. Los usuarios solo pueden iniciar las aplicaciones que estén permitidas en su organización y no aquellas que estén prohibidas.

Para obtener información detallada sobre Control de aplicaciones, consulte la Ayuda en línea de Kaspersky Endpoint Security para Linux.

Acerca del Control de aplicaciones

El componente Control de aplicaciones supervisa los intentos de los usuarios de iniciar aplicaciones y regula el inicio de las aplicaciones mediante el uso de reglas.

El componente Control de aplicaciones está disponible para Kaspersky Endpoint Security 11.2 para Linux y versiones posteriores.

El inicio de las aplicaciones cuya configuración no coincide con ninguna de las reglas de Control de aplicaciones está regulado por el modo operativo seleccionado del componente:

- *Lista de rechazados*. Este modo se utiliza si desea permitir el inicio de todas las aplicaciones, excepto las aplicaciones especificadas en las reglas de bloqueo. Este modo está seleccionado de forma predeterminada.
- *Lista de admitidos*. El modo se utiliza si desea bloquear el inicio de todas las aplicaciones, excepto las aplicaciones especificadas en las reglas de permiso.

Las Reglas de control de aplicaciones se implementan las mediante categorías de aplicaciones. Crea categorías de aplicaciones que definen criterios específicos. En Kaspersky Security Center Linux, solo puede crear categorías con contenido agregado manualmente. Defina condiciones, por ejemplo, metadatos de archivo, código hash de archivo, certificado de archivo, categoría KL y ruta de archivo, para incluir archivos ejecutables en la categoría.

Para obtener información detallada sobre Control de aplicaciones, consulte la Ayuda en línea de Kaspersky Endpoint Security para Linux.

Obtener y ver una lista de archivos ejecutables almacenados en dispositivos cliente

Puede obtener una lista de archivos ejecutables almacenados en dispositivos administrados. Para inventariar 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 de inventario de archivos ejecutables en dispositivos cliente:

1. Vaya a **DISPOSITIVOS** → **TAREAS**.
   Se muestra la lista de tareas.
2. Haga clic en el botón **Añadir**.
   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 for Linux.
4. Desde la lista desplegable **Tipo de tarea**, seleccione **Inventario**.
5. En la página **Finalizar la creación de tareas**, haga clic en el botón **Finalizar**.

   Una vez que se completa el Asistente de nueva tarea, la tarea **Inventario** queda creada y configurada. Si lo desea, puede cambiar la configuración de la tarea creada. La nueva tarea creada se muestra 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.

Después de realizar la tarea de **Inventario**, se forma la lista de archivos ejecutables almacenados en los dispositivos administrados y puede consultarla.

Durante el inventario, se detectan archivos ejecutables de los siguientes formatos: MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR y HTML.

haga lo siguiente para ver una lista de los archivos ejecutables almacenados en dispositivos cliente:

En la lista desplegable **OPERACIONES** → **APLICACIONES DE TERCEROS**, seleccione **ARCHIVOS EJECUTABLES**.

La página muestra la lista de los archivos ejecutables almacenados en dispositivos cliente.

Crear categoría de aplicación con contenido agregado manualmente

Expandir todo | Contraer todo

Puede especificar un conjunto de criterios como una plantilla de archivos ejecutables cuyo inicio desea permitir o bloquear en su organización. Según los archivos ejecutables correspondientes a los criterios, puede crear una categoría de aplicaciones y usarla en la configuración del componente Control de aplicaciones.

Para crear una categoría de aplicaciones con contenido agregado manualmente, haga lo siguiente:

1. En la lista desplegable **OPERACIONES → APLICACIONES DE TERCEROS**, seleccione **CATEGORÍAS DE APLICACIONES**.

   Se muestra la 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 del Asistente **Seleccione el método de creación de la categoría**, seleccione la opción **Categoría con contenido añadido manualmente. Los datos de los archivos ejecutables se agregan manualmente 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 página **Criterios de condición**, seleccione un tipo de regla para la creación de categoría de la lista:

   - Seleccionar el certificado del repositorio

     Si esta opción está seleccionada, puede especificar los certificados del almacenamiento. Los archivos ejecutables que se han firmado de acuerdo con los certificados especificados se agregarán a la categoría de usuario.

   - Especificar la ruta a la aplicación (se admiten máscaras)

     Si se selecciona esta opción, se puede especificar la ruta a la carpeta del dispositivo cliente que contiene los archivos ejecutables que se agregarán a la categoría de aplicación personalizada.

   - Unidad extraíble

     Si se selecciona esta opción, se puede especificar el tipo de medio (cualquier unidad o disco extraíble) en el que se ejecutará la aplicación. Las aplicaciones que se hayan ejecutado en el tipo selecciona de unidad de disco se agregarán a la categoría de aplicación personalizada.

   - **Hash, metadatos o certificado**:

     - Seleccionar de la lista de archivos ejecutables

       Si esta opción está seleccionada, puede usar la lista de archivos ejecutables en el dispositivo cliente para seleccionar aplicaciones y agregarlas a la categoría.

     - Seleccionar del registro de aplicaciones

       Si se selecciona esta opción, se muestra el registro de la aplicación. Puede seleccionar una aplicación del registro y especificar los siguientes metadatos de archivo:

       - Nombre del archivo.
       - Versión del archivo. Puede especificar el valor preciso de la versión o describir una condición, por ejemplo, «mayor que 5.0».
       - Nombre de la aplicación.
       - Versión de la aplicación. Puede especificar el valor preciso de la versión o describir una condición, por ejemplo, «mayor que 5.0».
       - Proveedor.

     - Especificar manualmente

Si se selecciona esta opción, debe especificar archivo hash, metadatos o certificado como condición para agregar aplicaciones a la categoría de usuario.

Archivo hash

Según la versión de la aplicación de seguridad instalada en los dispositivos en su red, debe seleccionar un algoritmo para que Kaspersky Security Center Linux calcule el valor de hash para archivos en esta categoría. La información sobre los valores de hash calculados se almacena en la base de datos del Servidor de administración. El almacenamiento de valores de hash no aumenta significativamente el tamaño de la base de datos.

SHA-256 es una función hash criptográfica: no se ha encontrado ninguna vulnerabilidad en su algoritmo, y por lo que se la considera como la función criptográfica más fiable hoy en día. Kaspersky Endpoint Security para Linux es compatible con el cálculo de SHA-256.

Seleccione cualquiera de las opciones de cálculo 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 for Linux, marque la casilla **Número de errores**.
- Marque la casilla **Hash MD5** solo si utiliza Kaspersky Endpoint Security para Windows. Kaspersky Endpoint Security para Linux no es compatible con la función hash MD5.

Metadatos

Si se selecciona esta opción, puede especificar metadatos de archivo como nombre de archivo, versión de archivo y proveedor. Los metadatos se enviarán al Servidor de administración. Los archivos ejecutables que contienen los mismos metadatos se agregarán a la categoría de la aplicación.

Certificado

Si esta opción está seleccionada, puede especificar los certificados del almacenamiento. Los archivos ejecutables que se han firmado de acuerdo con los certificados especificados se agregarán a la categoría de usuario.

- Desde la carpeta comprimida

Si esta opción está seleccionada, puede especificar un archivo de una carpeta archivada y luego seleccionar qué condición desea usar para añadir aplicaciones a la categoría de usuario. La carpeta archivada se descomprime y las condiciones que ha seleccionado se aplican a los archivos de la carpeta. Como condición, puede seleccionar uno de los siguientes criterios:

- **Archivo hash**

  Usted selecciona qué función hash (MD5 o SHA-256) desea usar para calcular los valores hash. Las aplicaciones que tienen el mismo valor hash que los archivos de la carpeta archivada se añaden a la categoría aplicación de 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 con los mismos metadatos se agregarán a la categoría de aplicaciones personalizada.

- **Certificado**

  Seleccione qué propiedades del certificado (asunto del certificado, huella digital o emisor) desea utilizar como criterio. Los archivos ejecutables que se han firmado con los certificados que tienen las mismas propiedades se agregarán a la categoría de usuario.

El criterio seleccionado se agrega a la lista de condiciones.

Puede agregar tantos criterios para la categoría de aplicación de creación como necesite.

6. En la página **Exclusiones** del Asistente, haga clic en el botón **Agregar** a fin de agregar un criterio de condición exclusiva para excluir archivos en la categoría que se crea.
7. En la página **Criterios de condición**, seleccione un tipo de regla de la lista del mismo modo que seleccionó un tipo de regla para la creación de la categoría.

Cuando finaliza el Asistente, se crea la categoría de aplicaciones. Se muestra en la lista de categorías de aplicaciones. Puede usar la categoría de aplicaciones creada cuando configura el Control de aplicaciones.

Para obtener información detallada sobre Control de aplicaciones, consulte la Ayuda en línea de Kaspersky Endpoint Security para Linux.

Ver la lista de categorías de aplicaciones

Puede ver la lista de categorías de aplicaciones configuradas y la configuración de cada categoría de aplicaciones.

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 la 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.

Añadir archivos ejecutables relacionados con eventos a la categoría de aplicaciones

Después de configurar Control de aplicaciones en las directivas de Kaspersky Endpoint Security for Linux, en la lista de eventos se mostrarán los eventos siguientes:

- **Inicio de aplicación prohibido** (evento *crítico*). Este evento se muestra si ha configurado el Control de aplicaciones para aplicar reglas.
- **Inicio de la aplicación prohibido en el modo de prueba** (evento de *información*). Este evento se muestra si ha configurado el Control de aplicaciones para probar reglas.
- **Mensaje de bloqueo de inicio de aplicación al administrador** (evento de *advertencia*). Este evento se muestra si ha configurado el Control de aplicaciones para aplicar reglas y un usuario ha solicitado acceso a la aplicación cuyo inicio se ha bloqueado.

Se recomienda crear selecciones de eventos para ver eventos relacionados con la operación de Control de aplicaciones.

Puede agregar archivos ejecutables relacionados con los eventos de Control de aplicaciones a una categoría de aplicaciones existente o a una nueva categoría de aplicaciones. Puede agregar archivos ejecutables solo a una categoría de aplicaciones con contenido agregado manualmente.

Para agregar archivos ejecutables relacionados con 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. Seleccione la selección de eventos para ver eventos relacionados con el Control de aplicaciones e inicie esta selección de eventos.

   Si no ha creado una selección de eventos relacionada con el Control de aplicaciones, puede seleccionar e iniciar una selección predefinida, por ejemplo, **Eventos recientes**.

   Se muestra la lista de eventos.

3. Seleccione los eventos cuyos archivos ejecutables asociados desea agregar a la categoría de aplicaciones y haga clic en el botón **Asignar a categoría**.

   Se inicia el Asistente para crear nueva categoría. Avance por el Asistente utilizando el botón **Siguiente**.

4. En la página del Asistente, especifique la configuración relevante:

   - En la sección **Acción en el archivo ejecutable relacionado con el evento**, seleccione una de las siguientes opciones:

     - **Añadir a una nueva categoría de aplicaciones**

       Seleccione esta opción si desea crear una nueva categoría de aplicación basada en archivos ejecutables relacionados con eventos.

       Esta opción está seleccionada de forma predeterminada.

       Si ha seleccionado esta opción, especifique un nuevo nombre de categoría.

     - **Añadir a una categoría de aplicaciones existente**

       Seleccione esta opción si quiere agregar eventos relacionados con archivos ejecutables a una categoría de aplicaciones existente.

       Esta opción no está seleccionada de forma predeterminada.

       Si ha seleccionado esta opción, seleccione la categoría de aplicación con contenido agregado manualmente al que desea agregar archivos ejecutables.

   - En la sección **Tipo de regla**, seleccione una de las siguientes opciones:

     - **Reglas para añadir inclusiones**
     - **Reglas para añadir 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. Se pueden firmar varios archivos con el mismo certificado. Por ejemplo, se pueden firmar diferentes versiones de la misma aplicación con el mismo certificado o se pueden firmar varias aplicaciones diferentes del mismo proveedor con el mismo certificado. Cuando selecciona un certificado, varias versiones de una aplicación o varias aplicaciones del mismo proveedor pueden terminar en la categoría.

    Cada archivo tiene su propia función hash SHA-256 exclusiva. Cuando selecciona una función hash SHA-256, solo el archivo correspondiente, por ejemplo, la versión de la aplicación que se ha definido, termina en la categoría.

    Seleccione esta opción si quiere agregar a las reglas de la categoría los detalles del certificado de un archivo ejecutable (o la función hash SHA-256 para archivos sin certificado).

    Esta opción está seleccionada de forma predeterminada.

  - **Detalles del certificado (se omitirán los archivos sin certificado)**

    Los archivos pueden estar firmados con un certificado. Se pueden firmar varios archivos con el mismo certificado. Por ejemplo, se pueden firmar diferentes versiones de la misma aplicación con el mismo certificado o se pueden firmar varias aplicaciones diferentes del mismo proveedor con el mismo certificado. Cuando selecciona un certificado, varias versiones de una aplicación o varias aplicaciones del mismo proveedor pueden terminar en la categoría.

    Seleccione esta opción si quiere agregar los detalles del certificado de un archivo ejecutable a las reglas de la categoría. Si el archivo ejecutable no tiene certificados, este archivo se omitirá. No se agregará ninguna información sobre este archivo a la categoría.

  - **Solo SHA-256 (se omitirán los archivos sin hash)**

    Cada archivo tiene su propia función hash SHA-256 exclusiva. Cuando selecciona una función hash SHA-256, solo el archivo correspondiente, por ejemplo, la versión de la aplicación que se ha definido, termina en la categoría.

    Seleccione esta opción si solo quiere 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 exclusiva. Cuando selecciona una función hash MD5, solo el archivo correspondiente, por ejemplo, la versión de la aplicación que se ha definido, termina en la categoría.

5. Haga clic en **Aceptar**.

Cuando finalice el Asistente, los archivos ejecutables relacionados con los eventos de Control de aplicaciones se añaden a la categoría de aplicaciones existente o a una nueva categoría de aplicaciones. Puede ver la configuración de la categoría de aplicaciones que ha modificado o creado.

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 capacidades le brindan una descripción general de su infraestructura, estados de protección y estadísticas.

Después del despliegue de Kaspersky Security Center Linux o durante su operación, puede configurar las funciones de supervisión e informes para que se adapten mejor a sus necesidades.

Escenario: seguimiento e informes

Esta sección proporciona un escenario para configurar la función Supervisión e informes en Kaspersky Security Center Linux.

Requisitos previos

Después de desplegar Kaspersky Security Center Linux en la red de una organización, puede comenzar a supervisarlo y generar informes sobre su funcionamiento.

El seguimiento y la elaboración de informes en la red de una organización se realizan en etapas:

1. **Configuración del cambio de estado de los dispositivos**

   Obtenga información sobre la configuración de los estados del dispositivo según las condiciones específicas. Al cambiar estas configuraciones, puede cambiar la cantidad de eventos con niveles de importancia *Crítica* o *Advertencia*. Al configurar la conmutación de estados de dispositivo, asegúrese de lo siguiente:

   - Las nuevas configuraciones no entran en conflicto con las directivas de seguridad de la información de su organización.
   - Usted tiene la capacidad de reaccionar a eventos de seguridad importantes en la red de su organización de manera oportuna.

2. **Configuración de notificaciones sobre eventos en dispositivos cliente**

   Instrucciones:

   Configure la notificación (por correo electrónico, SMS o ejecutando un archivo ejecutable) de eventos en dispositivos cliente

3. **Realizar acciones recomendadas para notificaciones críticas y de advertencia**

   Instrucciones:

   Acciones recomendadas a realizar para la red de su organización

4. **Revisión del estado de seguridad de la red de su organización**

   Instrucciones:

   - Revisión del widget Estado de la protección
   - Generación y revisión del Informe del estado de la protección
   - Generación y revisión del Informe de errores

5. **Ubicación de dispositivos cliente que no están protegidos**

   Instrucciones:

   - Revisión del widget Nuevos dispositivos
   - Generación y revisión del Informe del despliegue de la protección

6. **Comprobación de protección de dispositivos cliente**

   Instrucciones:

   - Generación y revisión de los informes desde las categorías Estado de la protección y Estadísticas de amenazas
   - Inicio y revisión de la selección de eventos Crítico

7. **La evaluación y la limitación del evento se cargan 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 en el Servidor de administración, evalúe y limite el número máximo de eventos que se pueden almacenar en la base de datos.

   Instrucciones:

   - Limitar el número máximo de eventos

8. **Consultar la información de la licencia**

   Instrucciones:

   - Adición del widget Uso de claves de licencia al panel y revisión
   - Generación y revisión del Informe de uso de claves de licencia

Resultados

Al completar el escenario, estará informado sobre la protección de la red de su organización y, por lo tanto, podrá planificar acciones para una mayor protección.

Acerca de los tipos de supervisión e informes

La información sobre eventos de seguridad en la red de una organización se almacena en la base de datos del Servidor de administración. En función de los eventos, Kaspersky Security Center 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 de control le permite supervisar las tendencias de seguridad en la red de su organización al proporcionarle una visualización gráfica de la información

Informes

La característica de los informes le permiten obtener información numérica detallada sobre la seguridad de la red de su organización, guardar esta información en un archivo, enviarla por correo electrónico e imprimirla.

Selecciones de eventos

Las selecciones de eventos proporcionan una vista en pantalla de los conjuntos de eventos con nombre que se seleccionan desde la base de datos del Servidor de administración. Estos conjuntos de eventos se agrupan según las siguientes categorías:

- Por nivel de importancia: **Eventos críticos**, **Fallos operativos**, **Advertencias** y **Eventos de información**
- Por tiempo: **Eventos recientes**
- Por tipo: **Solicitudes de los usuarios** 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 sobre eventos y le ayudan a acelerar sus respuestas a estos eventos al realizar acciones recomendadas o acciones que usted considera apropiadas.

Panel de control y widgets

Esta sección contiene información sobre el panel y los widgets que este proporciona. La sección incluye instrucciones sobre cómo administrar y configurar los widgets.

Uso del tablero

El panel de control le permite supervisar las tendencias de seguridad en la red de su organización al proporcionarle una visualización gráfica de la información

El panel está disponible en Kaspersky Security Center 14 Web Console, en la sección **SUPERVISIÓN E INFORMES**, al hacer clic en **PANEL**.

El panel proporciona widgets que se pueden personalizar. Puede elegir una gran cantidad de widgets diferentes, presentados como gráficos circulares o en forma de anillo, tablas, gráficos, gráficos de barras y listas. La información mostrada en los widgets se actualiza automáticamente; el periodo de actualización es de uno a dos minutos. El intervalo entre actualizaciones varía para widgets diferentes. Puede actualizar los datos en 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 la protección**
- **Despliegue**
- **Actualización**
- **Estadísticas de amenazas**
- **Otro**

Algunos widgets tienen información de texto con enlaces. Puede consultar la información detallada haciendo clic en un enlace.

Al configurar el panel, puede añadir widgets que necesite, esconder widgets que no necesite, cambiar el tamaño o el aspecto de widgets, mover widgets y cambiar su configuración.

Añadir widgets al panel de control

Para añadir widgets al panel de control:

1. En el menú principal, vaya a **SUPERVISIÓN E INFORMES → PANEL**.
2. Haga clic en el botón **Añadir o restaurar un widget web**.
3. En la lista de widgets disponibles, seleccione los artefactos que desea añadir al panel.

   Los widgets están agrupados por la categoría. Para ver la lista de widgets incluidos en una categoría, haga clic en el icono de flecha (>) junto al nombre de la categoría.
4. Haga clic en el botón **Añadir**.

Los widgets seleccionados se añaden al final del panel de control.

Ahora puede editar la representación y los parámetros de los artefactos añadidos.

Ocultar un widget desde el panel de control

Ocultar un widget mostrado desde el panel de control:

1. En el menú principal, vaya a **SUPERVISIÓN E INFORMES → PANEL**.
2. Haga clic en el icono de la **Configuración** (⚙) al lado del widget que desea ocultar.
3. Seleccionar **Ocultar el widget web**.
4. En la ventana **Advertencia** que se abre, haga clic en **Aceptar**.

El widget seleccionado se oculta. Más tarde, puede añadir este widget al panel de control nuevamente.

Mover un widget en el tablero

Mover un widget en el panel de control:

1. En el menú principal, vaya a **SUPERVISIÓN E INFORMES → PANEL**.
2. Haga clic en el icono de la **Configuración** (⚙) al lado del widget que desea mover.
3. Seleccionar **Mover**.
4. Haga clic en la localización a la que quiera mover el widget. Solo puede seleccionar otro widget.

Se intercambian los lugares de los widgets seleccionados.

Cambio del tamaño o aspecto del widget

Para los widgets que muestran un gráfico, puede cambiar su representación: un gráfico de barras o un gráfico de líneas. Para algunos widgets, puede cambiar su tamaño: compacto, medio o máximo.

Para cambiar la representación del widget:

1. En el menú principal, vaya a **SUPERVISIÓN E INFORMES → PANEL**.
2. Haga clic en el icono de la **Configuración** (⚙) al lado del widget que desea editar.
3. Realice una de las siguientes acciones:
   - Para mostrar el widget como un gráfico de barras, seleccione el **Tipo de gráfico: barras**.
   - Para mostrar el widget como un gráfico de líneas, seleccione el **Tipo de gráfico: líneas**.
   - Para cambiar el área ocupada por el widget, seleccione uno de los valores:
     - **Compacto**

- **Compacto (solo barra)**
- **Medio (gráfico de anillos)**
- **Medio (gráfico de barras)**
- **Máximo**

Se cambia la representación del widget seleccionado.

Cambiar configuración del widget

Cambiar configuración de un widget:

1. En el menú principal, vaya a **SUPERVISIÓN E INFORMES → PANEL**.
2. Haga clic en el icono de la **Configuración** (⚙) al lado del widget que desea cambiar.
3. Seleccionar **Mostrar configuración**.
4. En la ventana de configuración del widget que se abre, cambie la configuración del widget según sea necesario.
5. Haga clic en **Guardar** para guardar los cambios.

Se modifican los ajustes del widget seleccionado.

El conjunto de ajustes depende del widget específico. A continuación, se presentan algunos de los ajustes comunes:

- **Cobertura del widget web** (conjunto de objetos de los que muestra la información el widget): por ejemplo, un grupo de administración o de selección de dispositivos.
- **Elija una tarea** (la tarea de la que muestra la información 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.
- **Asignar estado Crítico si se especifica lo siguiente** y **Asignar estado Advertencia si se especifica lo siguiente** (las reglas que determinan el color de las luces del semáforo).

Acerca del modo Solo panel

Puede configurar el modo Solo panel para los empleados que no administran la red pero que desean ver las estadísticas de protección de la red en Kaspersky Security Center (por ejemplo, un alto directivo). Cuando un usuario tiene este modo activado, solo se le muestra un panel con un conjunto predefinido de widgets. Así, puede monitorear las estadísticas especificadas en los widgets, por ejemplo, el estado de protección de todos los dispositivos administrados, la cantidad de amenazas recién detectadas o la lista de las amenazas más frecuentes en la red.

Cuando un usuario trabaja en el modo Solo panel, se aplican las siguientes restricciones:

- El menú principal no se muestra al usuario, para que no pueda cambiar la configuración de protección de la red.
- El usuario no puede realizar ninguna acción con los widgets, por ejemplo, añadirlos u ocultarlos. Por lo tanto, debe colocar y configurar todos los widgets necesarios para el usuario en el panel, por ejemplo, establecer la regla de conteo de objetos o especificar el intervalo de tiempo.

No puede asignarse a sí mismo el modo de Solo panel. Si desea trabajar en este modo, comuníquese con un administrador del sistema, un proveedor de servicios administrados (MSP) o un usuario que tenga el derecho **Modificar ACL de objetos** el área funcional **Características generales: Permisos de usuario**.

Configuración del modo Solo panel

Antes de comenzar el Modo Solo panel, asegúrese de que se cumplan los siguientes requisitos previos:

- Tiene el derecho **Modificar ACL de objetos** en el área funcional **Funciones generales: Permisos de usuario**. Si no tiene este derecho, no verá la pestaña para configurar el modo.
- El usuario tiene el derecho de Lectura en el área funcional **Funciones generales**: **Funcionalidad básica**.

Si hay una jerarquía de Servidores de administración en su red, para configurar el modo Solo panel, vaya al servidor donde la cuenta de usuario está disponible en la sección **USUARIOS Y FUNCIONES → USUARIOS**. Puede ser un servidor primario o un servidor secundario físico. No es posible ajustar el modo en un servidor virtual.

Para configurar el modo Solo panel:

1. En el menú principal, vaya a **USUARIOS Y FUNCIONES → USUARIOS**.
2. Haga clic en el nombre de la cuenta de usuario cuyo panel con widgets desea ajustar.
3. En la ventana de configuración que se abre, seleccione la pestaña **Panel**.

   En la pestaña que se abre, se muestra el mismo Panel para usted que para el usuario.
4. Si está activada la opción **Mostrar la consola en modo de solo panel**, pulse el botón de alternancia para desactivarla.

   Cuando esta opción está activada, tampoco puede cambiar el panel. Después de desactivar la opción, puede administrar los widgets.
5. Configure la apariencia del panel. El conjunto de widgets preparados en la pestaña **Panel** está disponible para el usuario de la cuenta personalizable. Él o ella no puede cambiar ninguna configuración o tamaño de los widgets, ni añadir o eliminar widgets del panel. Por lo tanto, ajústelos para el usuario, para que pueda ver las estadísticas de protección de la red. Para tal efecto, en la pestaña **Panel** puede realizar las mismas acciones con los widgets que en la sección **SUPERVISIÓN E INFORMES → PANEL**:
   - Añadir nuevos widgets al panel de control.
   - Ocultar widgets que el usuario no necesita.
   - Mover widgets para ponerlos en un orden específico.
   - Cambiar el tamaño o la apariencia de los widgets.
   - Cambiar la configuración de los widgets.
6. Pulse el botón de alternancia para activar la opción **Mostrar la consola en modo de solo panel**.

   Después de eso, solo el panel está disponible para el usuario. Él o ella puede monitorear las estadísticas, pero no puede cambiar la configuración de protección de la red ni la apariencia del panel. Como se muestra el mismo panel para usted que para el usuario, tampoco usted puede cambiar el panel.

   Si mantiene la opción desactivada, se muestra el menú principal para el usuario, de modo que pueda realizar varias acciones en Kaspersky Security Center, entre ellas cambiar la configuración de seguridad y los widgets.
7. Haga clic en el botón **Guardar** cuando termine de configurar el modo Solo panel. Solo después de que lo haga, el panel preparado se mostrará al usuario.
8. Si el usuario desea ver las estadísticas de las aplicaciones compatibles de Kaspersky y necesita derechos de acceso para hacerlo, configure los derechos del usuario Después de eso, los datos de las aplicaciones de Kaspersky se muestran al usuario en los widgets de estas aplicaciones.

Ahora el usuario puede iniciar sesión en Kaspersky Security Center con la cuenta personalizada y monitorear las estadísticas de protección de la red en el modo Solo panel.

Informes

Esta sección describe cómo usar 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 característica de los informes le permiten obtener información numérica detallada sobre la seguridad de la red de su organización, guardar esta información en un archivo, enviarla por correo electrónico e imprimirla.

Los informes están disponibles en Kaspersky Security Center 14 Web Console, en la sección **SUPERVISIÓN E INFORMES**, al hacer clic en **INFORMES**.

De forma predeterminada, los informes incluyen información de los últimos 30 días.

Kaspersky Security Center Linux tiene un conjunto predeterminado de informes de las siguientes categorías:

- **Estado de la protección**
- **Despliegue**
- **Actualización**
- **Estadísticas de amenazas**
- **Otro**

Puede crear plantillas de informe personalizadas, modificar plantillas de informe y eliminarlas.

Puede crear informes que se basan en plantillas existentes, exportar informes a archivos y crear tareas para la entrega del informe.

Crear una plantilla de informes

Para crear una plantilla de informes:

1. En el menú principal, vaya a **SUPERVISIÓN E INFORMES → INFORMES**.
2. Haga clic en **Añadir**.

   Se ejecutará el Asistente de nueva plantilla de informe. Avance a través del Asistente utilizando el botón **Siguiente**.
3. En la primera página del Asistente, introduzca el nombre del informe y seleccione el tipo de informe.
4. En la página del Asistente **Cobertura**, seleccione el conjunto de dispositivos cliente (grupo de administración, selección de dispositivos, dispositivos seleccionados o todos los dispositivos de red) cuyos datos se mostrarán en informes que se basen en esta plantilla de informe.
5. En la página del Asistente **Período del informe**, especifique el periodo del informe. Los valores disponibles son los siguientes:

   - Entre las dos fechas especificadas
   - Desde la fecha especificada hasta la fecha de creación del informe
   - Desde la fecha de creación del informe menos el número especificado de días hasta la fecha de creación del informe

   Esta página puede no aparecer para algunos informes.
6. Haga clic **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 informes y ejecutar un informe basado esto.

     Se guarda la plantilla del informe. Se genera el informe.
   - Haga clic en el botón **Guardar** para guardar la nueva plantilla de informe.

     Se guarda la plantilla del informe.

Se puede utilizar esta nueva plantilla para generar y visualizar informes.

Ver y editar las propiedades de la plantilla de informe

Expandir todo | Contraer todo

Puede ver y editar las propiedades básicas de una plantilla de informe, por ejemplo, el nombre de la plantilla de informe o los campos que se muestran en el informe.

Para ver y editar las propiedades de una plantilla de informe:

1. En el menú principal, vaya a **SUPERVISIÓN E INFORMES → INFORMES**.
2. Seleccione la casilla de verificación junto a la plantilla de informe cuyas propiedades quiere ver y modificar.

   Como una alternativa, primero puede generar el informe y después hacer clic en el botón **Editar**.
3. Haga clic en el botón **Abrir propiedades de plantillas de informes**.

   Se abre la ventana **Editar informe <Nombre del informe>** con la pestaña **Control de aplicaciones** seleccionada.
4. Editar las propiedades de la plantilla del informe:

   - Pestaña **Control de aplicaciones**:

     - Nombre de la plantilla de informe
     - Número máximo de entradas que mostrar

       Si esta opción está activada, el número de entradas que se muestran en la tabla con datos detallados del informe no excede el valor especificado.

       Las entradas de informe se ordenan primero de acuerdo con las reglas especificadas en la sección **Campos → Campos detallados** de las propiedades de la plantilla de informe y luego solo se conserva la primera de las entradas resultantes. El encabezado de la tabla con datos detallados del informe muestra el número de entradas que se muestra y el número total de entradas disponibles que coinciden con otras configuraciones de la plantilla de informes.

Si esta opción está desactivada, la tabla con datos detallados del informe muestra todas las entradas disponibles. No le recomendamos que utilice esta opción. La limitación del número de entradas de informe visualizadas reduce la carga en el sistema de administración de bases de datos (DBMS) y reduce el tiempo requerido para generar y exportar el informe. Algunos de los informes contienen demasiadas entradas. Si este es el caso, puede resultarle difícil leerlos y analizarlos todos. Además, su dispositivo puede quedarse sin memoria mientras genera un informe de este tipo, y, por consiguiente, no podrá ver el informe.

Esta opción está activada de forma predeterminada. El valor predeterminado es 1000.

- **Grupo**

  Haga clic en el botón **Configuración** para cambiar el conjunto de dispositivos cliente para los que se crea el informe. Para algunos tipos de informes, el botón puede no estar disponible. La configuración real 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 periodo del informe. Para algunos tipos de informes, el botón puede no estar disponible. Los valores disponibles son los siguientes:

  - Entre las dos fechas especificadas
  - Desde la fecha especificada hasta la fecha de creación del informe
  - Desde la fecha de creación del informe menos el número especificado de días hasta la fecha de creación del informe

- Incluir datos de los Servidores de administración secundarios y virtuales

  Si esta opción está activada, el informe incluye la información de los Servidores de administración secundarios y virtuales que están subordinados al Servidor de administración para el cual se crea la plantilla de informe.

  Desactive esta opción si desea ver solo los datos del Servidor de administración actual.

  Esta opción está activada de forma predeterminada.

- Hasta el nivel de anidamiento

  El informe incluye datos de los Servidores de administración secundarios y virtuales que se encuentran bajo el Servidor de administración actual en un nivel de anidamiento menor o igual al valor especificado.

  El valor predeterminado es 1. Es posible que desee cambiar este valor si tiene que recuperar información de los Servidores de administración secundarios ubicados en los niveles más bajos del árbol.

- Intervalo de espera de datos (min)

  Antes de generar el informe, el Servidor de administración para el que se crea la plantilla de informe espera los datos de los Servidores de administración secundarios durante la cantidad de minutos especificada. Si no se reciben datos de un Servidor de administración secundario al final de este periodo, el informe se ejecuta de todos modos. En lugar de los datos reales, el informe muestra los datos tomados del caché (si la opción **Copiar en caché datos de los Servidores de administración secundarios** está activada) o, por el contrario, **N/A** (no disponible).

  El valor predeterminado es 5 (minutos).

- Copiar en caché datos de los Servidores de administración secundarios

  Los Servidores de administración secundarios transfieren regularmente datos al Servidor de administración para el que se crea la plantilla del informe. Allí, los datos transferidos se almacenan en el caché.

  Si el Servidor de administración actual no puede recibir datos de un Servidor de administración secundario mientras genera el informe, se muestran los datos tomados de la caché en él. También se muestra la fecha en que se transfirieron los datos al caché.

  Habilitar esta opción le permite ver la información de los Servidores de administración secundarios, incluso si no se pueden recuperar los datos actualizados. Sin embargo, los datos mostrados pueden ser obsoletos.

  Esta opción está desactivada de forma predeterminada.

- Frecuencia de actualización de la caché (h)

  Los Servidores de administración secundarios transfieren a intervalos regulares datos al Servidor de administración para el que se crea la plantilla del informe. Puede especificar este periodo en horas. Si especifica 0 horas, los datos se transfieren solo cuando se termina de generar el informe.

  El valor predeterminado es 0.

- Transferir información detallada desde los Servidores de administración secundarios

En el informe generado, la tabla con datos detallados del informe incluye datos de los Servidores de administración secundarios del Servidor de administración para los cuales se crea la plantilla del informe.

Habilitar esta opción ralentiza la generación de informes y aumenta el tráfico entre los Servidores de administración. Sin embargo, puede ver todos los datos en un informe.

En lugar de activar esta opción, es posible que desee analizar datos de informes detallados para detectar un Servidor de administración secundario defectuoso y luego generar el mismo informe solo para ese Servidor de administración defectuoso.

Esta opción está desactivada de forma predeterminada.

- Pestaña **Campos**

  Seleccione los campos que se mostrarán en el informe y utilice el botón **Subir** y el botón **Bajar** para cambiar el pedido de estos campos. Use el botón **Añadir** o **Editar** para especificar si la información en el informe debe ser ordenada y filtrada por cada uno de los campos.

  En la sección **Filtros de los campos de detalles**, también puede hacer clic en el botón **Convertir filtros** para comenzar a usar el formato de filtrado extendido. Este formato le permite combinar las condiciones de filtrado especificadas en varios campos, utilizando la operación lógica OR. Después de hacer clic en el botón, a la derecha se abre el panel **Convertir filtros**. Haga clic en el botón **Convertir filtros** para confirmar la revocación. Ahora puede definir un filtro convertido con condiciones de la sección **Campos detallados** que se aplican mediante la operación lógica OR.

  La conversión de un informe al formato que admite condiciones de filtrado complejas hará que el informe sea incompatible con las versiones anteriores de Kaspersky Security Center (11 y anteriores). Además, el informe convertido no contendrá ningún dato de los Servidores de administración secundarios que ejecuten versiones incompatibles.

5. Haga clic en **Guardar** para guardar los cambios.
6. Haga clic en el botón de **Cerrar** (✕) para cerrar la ventana **Edición del 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. Seleccione la casilla de verificación junto al informe que desea exportar a un archivo.
3. Haga clic en el botón **Exportar informe**.
4. En la ventana que se abre, cambie el nombre del archivo del informe en el campo **Nombre**. De forma predeterminada, el nombre de archivo coincide con el nombre de la plantilla de informe seleccionada.
5. Seleccione el tipo de archivo del 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 **Exportar informe**.

   El informe en el formato seleccionado se descargará a su dispositivo, a la carpeta predeterminada de su dispositivo, o se abrirá una ventana estándar **Guardar como** en su navegador para permitirle guardar el archivo donde desee.

El informe se guarda al archivo.

Generación y visualización de un informe

Para crear y visualizar un informe:

1. En el menú principal, vaya a **SUPERVISIÓN E INFORMES → INFORMES**.
2. Haga clic en el nombre de la planilla de informe que desea usar para crear un informe.

Se genera y se muestra un informe utilizando la plantilla seleccionada.

El informe muestra los siguientes datos:

- En la pestaña **Resumen**:

- El nombre y tipo de informe, una descripción breve del mismo y el periodo cubierto, así como información sobre el grupo de dispositivos para el que se generará el informe.
- Gráfico que muestra los datos más representativos del informe.
- Tabla consolidada con indicadores de informe calculados.

- Sobre la pestaña **Detalles** se muestra una tabla con los datos detallados del informe.

Crear una tarea de entrega de informes

Puede crear una tarea que entregará informes seleccionados.

Para crear una tarea de entrega de informes:

1. Vaya a **SUPERVISIÓN E INFORMES → INFORMES**.
2. [Opcional] Seleccione la casilla junto a la plantilla de informe para la que desea crear una tarea de generación de informe.
3. Haga clic en el botón **Nueva tarea de entrega de informes**.
4. Se inicia el Asistente para crear nueva tarea. Avance a través del Asistente utilizando el botón **Siguiente**.
5. En la primera página del Asistente, introduzca el nombre de la tarea. El nombre predeterminado es **Entregar informes (<N>)**, donde <N> es el número de la secuencia de la tarea.
6. En la página de configuración de tareas del Asistente, especifique la siguiente configuración:
   a. Plantillas de informes a ser entregados por la tarea. Si los seleccionó en el paso 2, omita este paso.
   b. El formato del informe: 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. Si los informes se enviarán por correo electrónico, junto con la configuración de las notificaciones de 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 otras configuraciones de tarea después de crear la tarea, en la página **Finalizar la creación de tareas** del Asistente, active 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 crea la tarea de entrega de informes. Si activó la opción **Abrir los detalles de la tarea cuando se complete la creación**, se abre la ventana de configuración de tareas.

Eliminación de las plantillas del informe

Eliminar una o varias plantillas de informe:

1. En el menú principal, vaya a **SUPERVISIÓN E INFORMES → INFORMES**.
2. Seleccione la casilla de verificación al lado de las plantillas de informe 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 informe seleccionadas. Si estas plantillas de informes se incluyeron en las tareas de entrega de informes, también se eliminan de las tareas.

Eventos y selecciones de eventos

Esta sección proporciona información sobre eventos y selecciones de eventos, sobre los tipos de eventos que ocurren en los componentes de Kaspersky Security Center Linux y sobre cómo administrar el bloqueo de eventos frecuentes.

Utilización de selecciones de eventos

Las selecciones de eventos proporcionan una vista en pantalla de los conjuntos de eventos con nombre que se seleccionan desde la base de datos del Servidor de administración. Estos conjuntos de eventos se agrupan según las siguientes categorías:

- Por nivel de importancia: **Eventos críticos**, **Fallos operativos**, **Advertencias** y **Eventos de información**
- Por tiempo: **Eventos recientes**
- Por tipo: **Solicitudes de los usuarios** 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.

Las 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 forma predeterminada, las selecciones de eventos incluyen información de los últimos 7 días.

Kaspersky Security Center Linux tiene un conjunto predeterminado de las selecciones (predefinidas) del evento:

- Eventos con niveles de importancia diferentes:
  - **Eventos críticos**
  - **Fallos operativos**
  - **Advertencias**
  - **Mensajes de información**
- **Solicitudes de usuario** (eventos de aplicaciones administradas)
- **Eventos recientes** (durante la semana anterior)
- **Eventos de auditoría**.

También puede crear y configurar selecciones adicionales definidas por el usuario. En las selecciones definidas por el usuario, puede filtrar eventos por las propiedades de los dispositivos de los que se originaron (nombres de dispositivos, rangos de IP y grupos de administración), por tipos de evento y niveles de gravedad, por nombre de aplicación y componente, y por intervalo de tiempo. También es posible incluir resultados de tareas en el ámbito de búsqueda. También puede usar un campo de búsqueda simple donde se puede escribir una palabra o varias palabras. Se muestran todos los eventos que contienen cualquiera de las palabras escritas en cualquier lugar de sus atributos (como el nombre del evento, la descripción y el nombre del componente).

Tanto para selecciones predefinidas como definidas por el usuario, puede limitar el número de eventos mostrados o el número de registros para buscar. 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 las 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

Creación de 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 **Añadir**.
3. En la ventana **Nueva selección de eventos** que se abre, especifique la configuración de la nueva selección de eventos. Haga esto en una o varias de las secciones en 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, mantenga seleccionada la casilla **Ir al resultado de la selección**.

6. Haga clic en **Guardar** para confirmar la creación de selección de eventos.

Para ver el resultado de la selección de eventos, mantenga activada la casilla **Ir al resultado de la selección**. De otro modo, la nueva selección de eventos aparece en la lista de selecciones de eventos.

Editar una selección de eventos

Editar una selección de eventos:

1. En el menú principal, vaya a **SUPERVISIÓN E INFORMES → SELECCIONES DE EVENTOS**.
2. Seleccione la casilla de verificación junto a la selección de eventos que quiera editar.
3. Haga clic en el botón **Propiedades**.
   Se abrirá una ventana de configuración de selección de eventos.
4. Editar las propiedades de la selección de eventos.

   > Para selecciones de eventos predefinidas, solo puede editar las propiedades en las siguientes pestañas: **Control de aplicaciones** (excepto el nombre de selección), **Hora** y **Derechos de acceso**.

   Para las selecciones definidas por el usuario, puede editar todas las propiedades.
5. Haga clic en **Guardar** para guardar los cambios.

La selección de eventos editado se muestra en la lista.

Visualización de 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. Seleccione la casilla de verificación al lado de la selección de eventos que quiera iniciar.
3. Realice una de las siguientes acciones:
   - Si desea configurar la clasificación en el resultado de selección de eventos, haga lo siguiente:
     a. Haga clic en el botón **Reconfigurar la clasificación y comenzar**.
     b. En la ventana que se muestra **Reconfigurar la clasificación para la selección de eventos**, especifique la configuración de clasificación.
     c. Haga clic en el nombre de la selección.
   - De lo contrario, si 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 selección de eventos.

Ver detalles de un evento

Para ver detalles de un evento:

1. Iniciar una selección de eventos.
2. Haga clic en la hora del evento requerido.
   Se abre la ventana **Propiedades del evento**.
3. En la ventana mostrada, puede hacer lo siguiente:
   - Consultar la información sobre el evento seleccionado
   - Ir al siguiente evento y al evento anterior en el resultado de selección de eventos
   - Ir al dispositivo en el que ocurrió el evento

- Ir al grupo de administración que incluye el dispositivo en el que ocurrió el evento
- Para un evento relacionado con una tarea, vaya a las propiedades de la tarea

Exportar eventos a un archivo

Exportar eventos a un archivo:

1. Iniciar una selección de eventos.
2. Seleccione la casilla de verificación junto al evento requerido.
3. Haga clic en el botón **Exportar a archivo**.

El evento seleccionado se exporta a un archivo.

Visualización de un historial de objeto desde un evento

Desde un evento de creación o modificación de un objeto que admite la administración de la revisión, puede cambiar al historial de la revisión del objeto.

Para visualizar un historial de objeto desde un evento:

1. Iniciar una selección de eventos.
2. Seleccione la casilla de verificación junto al evento requerido.
3. Haga clic en el botón **Historial de revisión**.

El historial de la revisión del objeto se abre.

Eliminar eventos

Para eliminar uno o varios eventos:

1. Iniciar una selección de eventos.
2. Seleccione las casillas de verificación junto a los eventos requeridos.
3. Haga clic en el botón **Eliminar**.

Los eventos seleccionados se eliminan y no se pueden restaurar.

Eliminación de selecciones de eventos

Puede eliminar solo las 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. Seleccione las casillas de verificación junto a las selecciones de eventos que desea 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 aplicaciones de Kaspersky instaladas en dispositivos administrados. La información sobre eventos se guarda en la base de datos del Servidor de administración. Es posible que deba almacenar algunos eventos durante un período de tiempo más largo o más corto que el especificado por los valores predeterminados. Puede cambiar la configuración predeterminada del término de almacenamiento para un evento.

Si no está interesado en almacenar algunos eventos en la base de datos del Servidor de administración, puede desactivar la configuración adecuada en la directiva del Servidor de administración y la directiva de 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. Sin embargo, un término de almacenamiento más largo para un evento le permite realizar tareas de supervisión e informes durante un período de tiempo más largo.

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 término de almacenamiento de los eventos del Agente de red o de una aplicación Kaspersky administrada, haga clic en el nombre de la directiva correspondiente.

     Se abre la ventana de propiedades de la directiva.
   - Para configurar los eventos del Servidor de administración, en la parte superior de la pantalla, haga clic en el icono 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 de **Fallo operativo**, **Advertencia** o **Información**.
5. En la lista de tipos de evento en el panel derecho, haga clic en el enlace del evento cuyo término de almacenamiento desea cambiar.

   En la sección **Registro de eventos** de la ventana que se abre, la opción **Almacenar en la base de datos del Servidor de administración durante (días)** está activada.
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, desactive la opción **Almacenar en la base de datos del Servidor de administración durante (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 puede redefinir el valor del término de almacenamiento para un evento.
8. Haga clic en **Aceptar**.

   Se cierra la ventana de propiedades de la directiva.

A partir de ahora, cuando el Servidor de administración reciba y almacene los eventos del tipo seleccionado, estos tendrán el plazo de almacenamiento modificado. El Servidor de administración no cambia el plazo de almacenamiento de los eventos recibidos anteriormente.

Tipos de evento

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 ocurren en las aplicaciones de Kaspersky no se enumeran en esta sección.

Estructura de datos de descripción de tipo de evento

Para cada tipo de evento, se proporcionan su nombre para mostrar, el identificador (Id.), el código alfabético, la descripción y el plazo de almacenamiento predeterminado.

- **Nombre de visualización del tipo de evento**. Este texto se muestra en Kaspersky Security Center Linux cuando configura los eventos y cuando ocurren.
- **ID del tipo de evento**. Este código numérico se usa cuando procesa eventos utilizando herramientas de terceros para el análisis de eventos.
- **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**. Este texto contiene las situaciones en las que ocurre un evento y lo que puede hacer en tal caso.
- **Plazo de almacenamiento predeterminado**. Este es el número de días durante los cuales el evento se almacena en la base de datos del Servidor de administración y se muestra en la lista de eventos en el Servidor de administración. Transcurrido este periodo, se elimina el evento. Si el valor del

plazo de almacenamiento de eventos es 0, dichos eventos se detectan pero no se muestran en la lista de eventos en el 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

Esta sección contiene información sobre los eventos relacionados con el Servidor de administración.

Eventos críticos del Servidor de administración

La siguiente tabla muestra los eventos del Servidor de administración de Kaspersky Security Center Linux que tienen el nivel de importancia **Crítico**.

Eventos críticos del Servidor de administración

Nombre de visualización del tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo de almacenamiento predeterminado
Se ha superado el límite de licencias	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Una vez al día, Kaspersky Security Center Linux comprueba si se ha excedido alguna restricción de licencia. Los eventos de este tipo ocurren cuando el Servidor de administración detecta que las aplicaciones de Kaspersky instaladas en dispositivos cliente exceden algunos límites de licencia y si el número de unidades de licencia utilizadas actualmente y cubiertas por una sola licencia supera el 110 % del número total de unidades cubiertas por la licencia. Incluso cuando se produce este evento, los dispositivos cliente están protegidos. Puede responder al evento de las siguientes formas: • Mire la lista de dispositivos administrados. Elimine dispositivos que no están en uso. • Proporcione una licencia para más dispositivos (añada un código de activación o un archivo clave válidos al Servidor de administración). Kaspersky Security Center Linux determina las reglas para generar eventos cuando se excede una restricción de licencia.	180 días
Se ha perdido la conexión con el dispositivo	4111	KLSRV_HOST_OUT_CONTROL	Los eventos de este tipo ocurren si un dispositivo administrado es visible en la red pero no se ha conectado al Servidor de administración durante un cierto periodo de tiempo. Averigüe lo que impide el buen funcionamiento del Agente de red en el dispositivo. Las causas posibles incluyen problemas de red y la eliminación de Agente de red del dispositivo.	180 días
El estado del dispositivo es Crítico	4113	KLSRV_HOST_STATUS_CRITICAL	Los eventos de este tipo ocurren cuando se le asigna el estado *Crítico* a un dispositivo administrado. Puede configurar las condiciones en las cuales el estado del dispositivo se cambia a *Crítico*.	180 días
El archivo clave se ha añadido a la lista de rechazados	4124	KLSRV_LICENSE_BLACKLISTED	Los eventos de este tipo ocurren cuando Kaspersky ha añadido a la lista de rechazados el código de activación o el archivo clave que usa en la lista de prohibidos. Póngase en contacto con el Servicio de soporte técnico para obtener más detalles.	180 días
La licencia caduca pronto	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Ocurren eventos de este tipo cuando se acerca la fecha de caducidad de la licencia comercial.	180 días

			Una vez al día, Kaspersky Security Center comprueba si se acerca la fecha de caducidad de la licencia. Los eventos de este tipo se publican 30 días, 15 días, 5 días y 1 día antes de la fecha de caducidad de la licencia. Este número de días no se puede cambiar. Si el Servidor de administración se apaga el día especificado antes de la fecha de caducidad de la licencia, el evento no se publicará hasta el día siguiente. Cuando caduca la licencia comercial, Kaspersky Security Center Linux presta solo la funcionalidad básica. Puede responder al evento de las siguientes formas: • Asegúrese de añadir una clave de licencia de reserva al Servidor de administración. • Si usa una suscripción, asegúrese de renovarla. Una suscripción ilimitada se renueva automáticamente si se ha pagado previamente al proveedor de servicios en el plazo de vencimiento.	
El certificado ha caducado	4132	KLSRV_CERTIFICATE_EXPIRED	Los eventos de este tipo ocurren cuando caduca el certificado del Servidor de administración para la Administración de dispositivos móviles. Debe actualizar el certificado caducado. Puede configurar actualizaciones automáticas de certificados seleccionando la casilla de verificación **Reemitir el certificado automáticamente siempre que sea posible** en la configuración de emisión del certificado.	180 días

Servidor de administración eventos de fallos operativos

La siguiente tabla muestra los eventos del Servidor de administración de Kaspersky Security Center Linux que tienen el nivel de importancia **Fallo operativo**.

Servidor de administración eventos de fallos operativos

Nombre de visualización del tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo de almacenamiento predeterminado
Error en tiempo de ejecución	4125	KLSRV_RUNTIME_ERROR	Los eventos de este tipo ocurren debido a problemas desconocidos. La mayoría de las veces, se trata de 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
Se ha superado el límite de instalaciones para uno de los grupos de aplicaciones con licencia	4126	KLSRV_INVLICPROD_EXCEDED	El Servidor de administración genera eventos de este tipo de manera periódica (cada 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 las siguientes formas: • Mire la lista de dispositivos administrados. Elimine la aplicación de terceros de los dispositivos en los cuales la aplicación no está en uso. • Utilice una licencia de terceros para más dispositivos.	180 días

			Puede administrar claves de licencia de terceros utilizando la funcionalidad de grupos de aplicaciones con licencia. Un grupo de aplicaciones con licencia incluye las aplicaciones de terceros que cumplen los criterios establecidos por usted.	
Error al copiar las actualizaciones en la carpeta especificada	4123	KLSRV_UPD_REPL_FAIL	Los eventos de este tipo ocurren cuando las actualizaciones de software se copian a (una) carpeta(s) compartida(s) adicional(es). Puede responder al evento de las siguientes formas: • Compruebe si la cuenta de usuario 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.	180 días
No queda espacio libre en el 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. Liberar espacio en disco en el dispositivo.	180 días
La carpeta compartida no está disponible	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	Los eventos de este tipo ocurren si la carpeta compartida del Servidor de administración no está disponible. Puede responder al evento de las siguientes formas: • Compruebe si el Servidor de administración (donde se encuentra la carpeta compartida) está encendido y disponible. • Compruebe si se cambió/cambiaron un nombre de usuario y / o una contraseña de la carpeta. • Compruebe la conexión de red.	180 días
La base de datos de información 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 no está disponible. Puede responder al evento de las siguientes formas: • Compruebe si está disponible el servidor remoto que instala SQL Server. • 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, un servidor remoto que tiene instalado SQL Server podría no estar disponible debido al mantenimiento preventivo.	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 seguir guardando en la base de datos.	180 días

A continuación se describen las causas de este evento, según el DBMS que utiliza, y las respuestas adecuadas al evento:

- Usted utiliza el DBMS de SQL Server Express Edition:
  - En la documentación de SQL Server Express, revise el límite del tamaño de la base de datos de la versión que utiliza. Probablemente, la base de datos de su Servidor de administración ha superado el límite del tamaño de la base de datos.
  - Limite el número de eventos para almacenar en la base de datos del Servidor de administración.
  - En la base de datos del Servidor de administración hay 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 del Control de aplicaciones en la base de datos del Servidor de administración.
- Usted utiliza un DBMS distinto de 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.

Consulte la información sobre la selección de DBMS.

Eventos de advertencia del Servidor de administración

La siguiente tabla muestra los eventos del Servidor de administración de Kaspersky Security Center Linux que tienen el nivel de importancia **Advertencia**.

Eventos de advertencia del Servidor de administración

Nombre de visualización del tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo de almacenamiento predeterminado
Se ha superado el límite de licencias	4098	KLSRV_EV_LICENSE_CHECK_100_110	Una vez al día, Kaspersky Security Center Linux comprueba si se ha excedido alguna restricción de licencia. Los eventos de este tipo ocurren cuando el Servidor de administración detecta que las aplicaciones de Kaspersky instaladas en los dispositivos cliente exceden algunos límites de licencia y si el número de unidades de licencia utilizadas actualmente y cubiertas por una sola licencia constituye del 100 % al 110 % del número total de unidades cubiertas por la licencia. Incluso cuando se produce este evento, los dispositivos cliente están protegidos. Puede responder al evento de las siguientes formas: • Mire la lista de dispositivos administrados. Elimine dispositivos que no están en uso.	90 días

			• Proporcione una licencia para más dispositivos (añada un código de activación o un archivo clave válidos al Servidor de administración). Kaspersky Security Center Linux determina las reglas para generar eventos cuando se excede una restricción de licencia.	
El dispositivo ha permanecido inactivo en la red durante mucho tiempo	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	Los eventos de este tipo ocurren cuando un dispositivo administrado muestra inactividad durante algún tiempo. La mayoría de las veces, esto sucede cuando se da de baja un dispositivo administrado. Puede responder al evento de las siguientes formas: • Elimine manualmente el dispositivo de la lista de dispositivos administrados. Especifique el intervalo de tiempo después del cual se crea el evento **El dispositivo ha permanecido inactivo en la red durante mucho tiempo** mediante Kaspersky Security Center 14 Web Console. • Especifique el intervalo de tiempo después del cual el dispositivo se eliminará automáticamente del grupo mediante Kaspersky Security Center 14 Web Console.	90 días
Conflicto de nombres de dispositivo	4102	KLSRV_EVENT_HOSTS_CONFLICT	Los eventos de este tipo ocurren cuando el Servidor de administración considera que dos o más dispositivos administrados distintos son un solo dispositivo. La mayoría de las veces, esto sucede cuando se ha utilizado un disco duro clonado para el despliegue de software en los dispositivos administrados y sin haber cambiado el Agente de red al modo de clonación de discos específico en un dispositivo de referencia. Para evitar este problema, cambie el Agente de red al modo de clonación de discos en un dispositivo de referencia antes de clonar el disco duro de este dispositivo.	90 días
El estado del dispositivo es Advertencia	4114	KLSRV_HOST_STATUS_WARNING	Los eventos de este tipo ocurren cuando se le asigna el estado de *Advertencia* a un dispositivo administrado. Puede configurar las condiciones en las cuales el estado del dispositivo se cambia a *Advertencia*.	90 días
Pronto se superará el límite de instalaciones de uno de los grupos de aplicaciones con licencia	4127	KLSRV_INVLICPROD_FILLED	Los eventos de este tipo ocurren cuando la cantidad de instalaciones de aplicaciones de terceros incluidas en un grupo de aplicaciones con licencia alcanza el 90 % del valor máximo permitido que se especifica en las propiedades de la clave de licencia. Puede responder al evento de las siguientes formas: • Si la aplicación de terceros no está en uso en algunos de los dispositivos administrados, elimínela de estos dispositivos. • Si cree que la cantidad de instalaciones de la aplicación de terceros excederá pronto el máximo permitido, le recomendamos que adquiera con anticipación una licencia de terceros	90 días

			para una mayor cantidad de dispositivos. Puede administrar claves de licencia de terceros utilizando la funcionalidad de grupos de aplicaciones con licencia.	
Se ha solicitado el certificado	4133	KLSRV_CERTIFICATE_REQUESTED	Los eventos de este tipo ocurren cuando no se puede volver a emitir automáticamente un certificado para Administración de dispositivos móviles. A continuación se mencionan las probables causas del evento y las respuestas adecuadas a este: • Se ha iniciado la nueva emisión automática de un certificado para el que la opción **Reemitir el certificado automáticamente siempre que sea posible** está desactivada. Esto puede deberse a un error ocurrido durante la creación del certificado. Es posible que se deba volver a emitir el certificado de forma manual. • Si utiliza una integración con una infraestructura de clave pública, la causa podría ser la falta del 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
El certificado se ha eliminado	4134	KLSRV_CERTIFICATE_REMOVED	Los eventos de este tipo ocurren cuando un administrador elimina algún tipo de certificado (General, Correo, VPN) para Administración de dispositivos móviles. Después de eliminar un certificado, los dispositivos móviles que estén conectados a través de este certificado no podrán conectarse al Servidor de administración. Este evento puede resultar útil a la hora de investigar errores asociados con la administración de dispositivos móviles.	90 días
El certificado de APNs ha caducado	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Los eventos de este tipo ocurren cuando caduca un certificado de APNs. Debe renovar el certificado de APNs manualmente e instalarlo en un servidor de MDM para iOS.	No almacenado
El certificado de APNs caducará pronto	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	Los eventos de este tipo ocurren cuando quedan menos de 14 días para que caduque el certificado de APNs. Cuando el certificado de APNs caduca, debe renovarlo manualmente e instalarlo en un servidor de MDM para iOS. Le recomendamos que programe la renovación del certificado de APNs antes de la fecha de caducidad.	No almacenado
No se ha podido enviar el mensaje FCM al dispositivo móvil	4138	KLSRV_GCM_DEVICE_ERROR	Los eventos de este tipo ocurren cuando Administración de dispositivos móviles está configurada para usar Google Firebase Cloud Messaging (FCM) para conectarse a dispositivos móviles administrados con sistema operativo Android y cuando el servidor de FCM no puede manejar algunas de las solicitudes que recibe del Servidor de administración. Significa que algunos de los dispositivos móviles administrados no recibirán una notificación push.	90 días

			Lea el código HTTP en los detalles de la descripción del evento y actúe en consecuencia. Para obtener más información sobre los códigos HTTP que se reciben del servidor de FCM y los errores relacionados, consulte la documentación del servicio Google Firebase (consulte el capítulo "Códigos de respuesta de errores de mensajes descendentes").	
Se produjo un error de HTTP al enviar el mensaje FCM al servidor FCM	4139	KLSRV_GCM_HTTP_ERROR	Los eventos de este tipo ocurren cuando Administración de dispositivos móviles está configurada para usar Google Firebase Cloud Messaging (FCM) para conectar dispositivos móviles administrados con sistema operativo Android y cuando el servidor de FCM devuelve un código HTTP distinto de 200 (OK) a la solicitud del Servidor de administración. A continuación se mencionan las probables causas del evento y las respuestas adecuadas a este: • Problemas en el lado del servidor de FCM. Lea el código HTTP en los detalles de la descripción del evento y actúe en consecuencia. Para obtener más información sobre los códigos HTTP que se reciben del servidor de FCM y los errores relacionados, consulte la documentación del servicio Google Firebase (consulte el capítulo "Códigos de respuesta de errores de mensajes descendentes"). • Problemas del servidor proxy (si usa un servidor proxy). Lea el código HTTP en los detalles del evento y actúe en consecuencia.	90 días
No se ha podido enviar el mensaje FCM al servidor FCM	4140	KLSRV_GCM_GENERAL_ERROR	Los eventos de este tipo ocurren debido a errores inesperados en el Servidor de administración cuando se trabaja con el protocolo HTTP de Google Firebase Cloud Messaging. Lea los detalles en la descripción del evento y actúe en consecuencia. Si no puede encontrar la solución para un problema por su cuenta, le recomendamos que se comunique con el Servicio de soporte técnico de Kaspersky.	90 días
Poco espacio libre en el disco duro	4105	KLSRV_NO_SPACE_ON_VOLUMES	Los eventos de este tipo ocurren cuando el disco duro del dispositivo donde está instalado el Servidor de administración casi se queda sin espacio libre. Liberar espacio en disco en el dispositivo.	90 días
Poco espacio libre en la base de datos del Servidor de administración	4106	KLSRV_NO_SPACE_IN_DATABASE	Los eventos de este tipo ocurren si el espacio en la base de datos del Servidor de administración es demasiado reducido. Si no soluciona la situación, la base de datos del Servidor de administración pronto alcanzará su capacidad y el Servidor de administración no funcionará. A continuación se describen las causas de este evento, según el DBMS que utiliza, y las respuestas adecuadas al evento. Usted utiliza el DBMS de SQL Server Express Edition: • En la documentación de SQL Server Express, revise el límite del tamaño de la base de datos de la versión que utiliza. Probablemente la base de datos de su Servidor de administración esté	90 días

			por alcanzar el límite del tamaño de la base de datos. • Limite el número de eventos para almacenar en la base de datos del Servidor de administración. • En la base de datos del Servidor de administración hay 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 del Control de aplicaciones en la base de datos del Servidor de administración. Usted utiliza un DBMS distinto de 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. Consulte la información sobre la selección de DBMS.	
Se ha interrumpido la conexión con el Servidor de administración secundario	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	Los eventos de este tipo ocurren cuando se interrumpe una conexión con el Servidor de administración secundario. Lea el Registro de eventos de Kaspersky del dispositivo donde está 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	Los eventos de este tipo ocurren cuando se interrumpe una conexión con el Servidor de administración principal. Lea el Registro de eventos de Kaspersky del dispositivo donde está instalado el Servidor de administración principal y responda en consecuencia.	90 días
Se han registrado las nuevas actualizaciones para los módulos del software Kaspersky	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	Los eventos de este tipo ocurren cuando el Servidor de administración registra actualizaciones nuevas para el software de Kaspersky instalado en los dispositivos administrados que usted debe aprobar para su instalación. Apruebe o rechace las actualizaciones mediante Kaspersky Security Center Web Console.	90 días
Se ha superado el límite del número de eventos en la base de datos, se ha iniciado la eliminación de eventos	4145	KLSRV_EVP_DB_TRUNCATING	Los eventos de este tipo ocurren cuando ha comenzado la eliminación de eventos antiguos de la base de datos del Servidor de administración después de que se alcanzó la capacidad de la base de datos del Servidor de administración. Puede responder al evento de las siguientes formas: • Cambie el número de eventos almacenados 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.	No almacenado
Se ha superado el límite del	4146	KLSRV_EVP_DB_TRUNCATED	Los eventos de este tipo ocurren cuando se han eliminado los eventos antiguos de la	No almacenado

número de eventos en la base de datos, los eventos se han eliminado	base de datos del Servidor de administración después de que se alcanzó la capacidad de la base de datos del Servidor de administración. Puede responder al evento de las siguientes formas: • Cambie el número máximo permitido de eventos que se almacenarán 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.

Eventos informativos del Servidor de administración

La siguiente tabla muestra los eventos del Servidor de administración de Kaspersky Security Center Linux que tienen el nivel de importancia **Información**.

Eventos informativos del Servidor de administración

Nombre de visualización del 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 ha detectado un nuevo dispositivo	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 días
El dispositivo se ha agregado automáticamente al grupo	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 días
El dispositivo se ha eliminado del grupo: inactivo en la red durante mucho tiempo	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 días
Pronto se superará el límite de instalaciones de uno de los grupos de aplicaciones con licencia (ya se ha usado más del 95 %)	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 han copiado correctamente en la carpeta especificada	4122	KLSRV_UPD_REPL_OK	30 días
La conexión con el Servidor de administración secundario está establecida	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 días
La conexión con el Servidor de administración principal está establecida	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 días
Las bases de datos se han actualizado	4144	KLSRV_UPD_BASES_UPDATED	30 días
Auditoría: Se ha establecido la conexión con el Servidor de administración	4147	KLAUD_EV_SERVERCONNECT	30 días
Auditoría: Se ha modificado el objeto	4148	KLAUD_EV_OBJECTMODIFY	30 días
Auditoría: El estado del objeto ha cambiado	4150	KLAUD_EV_TASK_STATE_CHANGED	30 días
Comprobar: Parámetros de grupo modificados	4149	KLAUD_EV_ADMGROUP_CHANGED	30 días
Auditoría: Se ha finalizado la conexión al Servidor de administración	4151	KLAUD_EV_SERVERDISCONNECT	30 días
Auditoría: Se han modificado las propiedades del objeto	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 días
Auditoría: Se han modificado los permisos de usuario	4153	KLAUD_EV_OBJECTACLMODIFIED	30 días

Eventos del Agente de red

Esta sección contiene información sobre los eventos relacionados con el Agente de red.

Eventos de advertencia del Agente de red

La siguiente tabla muestra los eventos del Agente de red de Kaspersky Security Center Linux que tienen el nivel de gravedad **Advertencia**.

Eventos de advertencia del Agente de red

Nombre de visualización del tipo de evento	Id. del tipo de evento	Tipo de evento	Plazo de almacenamiento predeterminado
Se ha producido un incidente	549	GNRL_EV_APP_INCIDENT_OCCURED	30 días

Eventos informativos de advertencia del Agente de red

La siguiente tabla muestra los eventos del Agente de red de Kaspersky Security Center Linux que tienen el nivel de gravedad **Información**.

Eventos informativos de advertencia del Agente de red

Nombre de visualización del tipo de evento	Id. del tipo de evento	Tipo de evento	Plazo de almacenamiento predeterminado
La aplicación se ha instalado	7703	KLNAG_EV_INV_APP_INSTALLED	30 días
La aplicación se ha desinstalado	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 días
La aplicación supervisada se ha instalado	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 días
La aplicación supervisada se ha desinstalado	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 días
Se ha agregado un nuevo dispositivo	7708	KLNAG_EV_DEVICE_ARRIVAL	30 días
El dispositivo se ha eliminado	7709	KLNAG_EV_DEVICE_REMOVE	30 días
Se ha detectado un nuevo dispositivo	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 días
El dispositivo se ha autorizado	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 días

Bloqueo de eventos frecuentes

En esta sección se proporciona información sobre cómo administrar el bloqueo de eventos frecuentes y sobre cómo eliminar el bloqueo de eventos frecuentes.

Acerca del bloqueo de eventos frecuentes

Una aplicación administrada, por ejemplo, Kaspersky Endpoint Security for Linux, instalada en uno o varios dispositivos administrados, puede enviar muchos eventos del mismo tipo al Servidor de administración. La recepción de eventos frecuentes puede sobrecargar la base de datos del Servidor de administración y sobrescribir otros eventos. El Servidor de administración comienza a bloquear los eventos más frecuentes cuando el total de eventos recibidos excede el límite especificado para la base de datos.

El Servidor de administración bloquea la recepción automática de eventos frecuentes. No puede bloquear los eventos frecuentes usted, mismo ni elegir qué eventos bloquear.

Si desea saber si un evento está bloqueado, puede ver la lista de notificaciones o comprobar si 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 desea impedir que se sobrescriba la base de datos, puede continuar bloqueando la recepción de este tipo de eventos.
- Si desea, por ejemplo, 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 todos modos.
- Si desea seguir recibiendo los eventos frecuentes hasta que se los vuelva a bloquear, puede eliminar el bloqueo de eventos frecuentes.

Gestión del bloqueo de eventos frecuentes

El Servidor de administración bloquea la recepción de eventos frecuentes, pero usted puede desbloquearla y continuar recibiendo eventos frecuentes. También puede bloquear la recepción de eventos frecuentes que desbloqueó antes.

Para gestionar el bloqueo de eventos frecuentes:

1. En la ventana principal de la aplicación, haga clic en el icono de **Configuración** ( ) junto al nombre del Servidor de administración requerido.
   Se abre la ventana Propiedades del Servidor de administración.
2. En la pestaña **Control de aplicaciones**, seleccione la sección **Bloqueo de eventos frecuentes**.
3. En sección **Bloqueo de eventos frecuentes**:

- Si desea desbloquear la recepción de eventos frecuentes:

  a. Seleccione los eventos frecuentes que desea desbloquear y haga clic en el botón **Excluir**.

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

- Si desea bloquear eventos frecuentes, haga lo siguiente:

  a. Seleccione los eventos frecuentes que desea bloquear y haga clic en el botón **Bloquear**.

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

El Servidor de administración recibe los eventos frecuentes desbloqueados y no recibe los bloqueados.

Eliminación del bloqueo de eventos frecuentes

Puede eliminar el bloqueo de los eventos frecuentes y comenzar a recibirlos hasta que el Servidor de administración los vuelva a bloquear.

Para eliminar el bloqueo de eventos frecuentes, haga lo siguiente:

1. En la ventana principal de la aplicación, haga clic en el icono de **Configuración** ( ) junto al nombre del Servidor de administración requerido.
   Se abre la ventana Propiedades del Servidor de administración.
2. En la pestaña **Control de aplicaciones**, seleccione la sección **Bloqueo de eventos frecuentes**.
3. En la sección **Bloqueo de eventos frecuentes**, seleccione la fila del evento frecuente cuyo bloqueo desea eliminar.
4. Haga clic en el botón **Quitar del bloqueo**.

El evento frecuente se elimina de la lista de eventos frecuentes. El Servidor de administración recibirá eventos de este tipo.

Procesamiento y almacenamiento 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. Cada evento se atribuye a un determinado tipo y nivel de gravedad (*Evento crítico*, *Fallo operativo*, *Advertencia* o *Información*). Según las condiciones en que tengan lugar los eventos, la aplicación puede asignar diferentes niveles de gravedad a eventos del mismo tipo.

Puede ver los tipos y niveles de gravedad asignados a eventos en la sección **Configuración de eventos** de la ventana de propiedades del Servidor de administración. Asimismo, en la sección **Configuración de eventos**, puede configurar el procesamiento de cada evento por parte del Servidor de administración:

- 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 que se utiliza para notificar un evento al administrador (por ejemplo, por mensaje de correo electrónico o de texto).

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 especifica el número máximo de eventos, la aplicación calcula una cantidad aproximada de espacio de almacenamiento requerido para el número especificado. Puede usar 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 45 millones de eventos.

Si el número de eventos en la base de datos llega al valor máximo especificado por el administrador, la aplicación elimina los eventos más antiguos sobrescribiéndolos con los nuevos. Cuando el Servidor de administración elimina eventos antiguos, no puede guardar eventos nuevos 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 luego se guardan en la base de datos una vez que se completa la operación de eliminación.

Notificaciones y estados del dispositivo

Esta sección contiene información sobre cómo ver notificaciones, configurar la entrega de notificaciones, usar los estados de los dispositivos y habilitar el cambio de estado de los dispositivos.

Uso de notificaciones

Las notificaciones le alertan sobre eventos y le ayudan a acelerar sus respuestas a estos eventos al realizar acciones recomendadas o acciones que usted considera 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. La respuesta debe ser la más apropiada 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 actualizaciones de bases de datos antivirus que se han descargado)
   - **Prevención de exploits**
   - **Servidor de administración** (esto incluye eventos que conciernen únicamente al Servidor de administración)
   - **Enlaces 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:

- Icono relacionado con el tema de la notificación: despliegue (), protección (), actualizaciones (), Administrador de dispositivos (), prevención de exploits (), Servidor de administración ().
- Nivel de importancia de la notificación. Se muestran notificaciones de los siguientes niveles de importancia: **Notificaciones críticas** (), **Notificaciones de advertencia** (), **Notificaciones informativas**. Las notificaciones de la lista se agrupan por niveles de importancia.
- **Notificación**. Esto contiene una descripción de la notificación.
- **Acción**. Esto contiene un enlace a una acción rápida que le recomendamos que realice. Por ejemplo, al hacer clic en este enlace, 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*.
- **Estado registrado**. 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 icono 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, la pestaña **Todas las notificaciones** se selecciona y las notificaciones son agrupadas 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.
   - Icono que indica el tema de la notificación: despliegue (), protección (), actualizaciones (), administración de dispositivos (), prevención de exploits () y Servidor de administración ().
   - Descripción de la notificación.
   - Icono del **Banderín**. El icono de **banderín** está en gris si a las notificaciones se les ha asignado el estado *No revisado*. Cuando selecciona el icono de **banderín** gris y asigna el estado *Revisado* a una notificación, el icono cambia al color blanco.
   - Enlace a la acción recomendada. Cuando realiza la acción recomendada después de hacer clic en el enlace, la notificación recibe el estado de *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 de *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 de verificación **Mostrar filtro** para administrar el filtro.

Ver notificaciones en pantalla en el widget:

1. En la sección **PANEL**, seleccione **Añadir o restaurar un widget web**.
2. En la ventana que se abre, haga clic en la categoría **Otro**, 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 de *Advertencia*. O puede añadir otro widget: **Notificaciones por nivel de importancia seleccionado**, con una *Advertencia* de nivel de importancia.

   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:

- Icono relacionado con el tema de la notificación: despliegue (), protección (), actualizaciones (), Administrador de dispositivos (), prevención de exploits (), Servidor de administración ().
- Descripción de la notificación con un enlace a la acción recomendada. Cuando realiza una acción recomendada después de hacer clic en el enlace, la notificación recibe el estado de *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 enlace, 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 asigna un estado a cada dispositivo administrado. El estado particular depende de si se cumplen 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*
- *Correcto* o *Correcto/Visible*

La tabla a continuación enumera las condiciones predeterminadas que se deben cumplir para asignar el estado *Crítico* o *Advertencia* a un dispositivo, con todos los valores posibles.

Condiciones para asignar 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 una aplicación de seguridad no está instalada.	• El botón está activado. • El botón está desactivado.
Demasiados virus detectados	Una tarea de detección de virus (por ejemplo, la tarea de análisis antivirus) ha detectado 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 es distinto del establecido por el administrador	El dispositivo es visible en la red, pero el nivel de la protección en tiempo real se diferencia del nivel configurado (en la condición) por el administrador para el estado del dispositivo.	• Detenido. • En pausa. • En ejecución.
No se ha realizado ningún análisis antivirus desde hace mucho tiempo	El dispositivo es visible en la red y una aplicación de seguridad está instalada en el dispositivo, pero la tarea de análisis antivirus no se ha ejecutado durante el intervalo de tiempo especificado. La condición se aplica solo a los dispositivos que se agregaron a la base de datos del Servidor de administración hace siete días o antes.	Más de 1 día.
Las bases de datos están desactualizadas	El dispositivo es visible en la red y una aplicación de seguridad está instalada en el dispositivo, pero las bases de datos antivirus no se han actualizado en este dispositivo durante el intervalo de tiempo especificado. La condición se aplica solo a los dispositivos que se agregaron a la base de datos del Servidor de administración hace un día o antes.	Más de 1 día.
No conectado durante mucho tiempo	El Agente de red está instalado en el dispositivo, pero el dispositivo no se ha conectado a un Servidor de administración durante el intervalo de tiempo especificado porque el dispositivo se desactivó.	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 requiere reiniciar	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 el inventario del software realizado a través del Agente de red ha detectado aplicaciones incompatibles instaladas en el dispositivo.	• El botón está desactivado. • El botón está activado.

La licencia comercial ha caducado	El dispositivo es visible en la red, pero la licencia ha caducado.	• El botón está desactivado. • El botón está activado.
la licencia caduca pronto	El dispositivo es visible en la red, pero la licencia caduca en el dispositivo en menos días que el número especificado de días.	Más de 0 días.
Incidentes sin procesar detectados	Se han detectado algunos incidentes no procesados en el dispositivo. Los incidentes se pueden crear automáticamente, mediante las aplicaciones administradas por Kaspersky que están instaladas en el dispositivo cliente, o el administrador las puede crear de forma manual.	• El botón está desactivado. • El botón está activado.
Estado del dispositivo definido por la aplicación	El estado del dispositivo se define por la aplicación administrada.	• El botón está desactivado. • El botón está activado.
El dispositivo no tiene espacio disponible en el disco	El espacio libre en disco en el dispositivo es menor que el valor especificado o el dispositivo no se pudo sincronizar con el Servidor de administración. El estado *Crítico* o *Advertencia* pasa al estado *Correcto* cuando el dispositivo se sincroniza correctamente con el Servidor de administración y el espacio libre en el dispositivo es mayor o igual al valor especificado.	Más de 0 MB.
Se ha perdido la conexión con el dispositivo	Durante la detección de dispositivos, el dispositivo se reconoció como visible en la red, pero más de tres intentos de sincronizar con el Servidor de administración fallaron.	• El botón está desactivado. • El botón está activado.
La protección está desactivada	El dispositivo es visible en la red, pero la aplicación de seguridad en el dispositivo se ha desactivado durante más tiempo que el intervalo de tiempo especificado.	Más de 0 minutos.
La aplicación de seguridad no se está ejecutando	El dispositivo es visible en la red y hay una aplicación de seguridad instalada en el dispositivo pero no se está ejecutando.	• El botón está desactivado. • El botón está activado.

Kaspersky Security Center Linux le permite configurar el cambio automático del estado de un dispositivo en un grupo de administración cuando las condiciones especificadas se cumplen. Cuando las condiciones especificadas se cumplen, se asigna al dispositivo cliente uno de los estados siguientes: *Crítico* o *Advertencia*. Cuando no se cumplen las condiciones especificadas, al dispositivo cliente se le asigna el estado *Correcto*.

Distintos estados pueden corresponder a distintos valores de una condición. Por ejemplo, de manera predeterminada, si 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 fuera **Más de 7 días**, se le asignaría 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 la condición) se tiene en cuenta el indicador de visibilidad. Por ejemplo, si a un dispositivo administrado se le ha asignado el estado *Crítico* porque se cumplió la condición Las bases de datos están desactualizadas, y luego se configuró el indicador de visibilidad para el dispositivo, entonces al dispositivo se le asigna el estado *Correcto*.

Configuración del cambio de estado de los dispositivos

Puede cambiar las condiciones para asignar el estado *Crítico* o *Advertencia* a un dispositivo.

Para activar el cambio del estado del dispositivo a Crítico:

1. En el menú principal, vaya a **DISPOSITIVOS → JERARQUÍA DE GRUPOS**.
2. En la lista de grupos que se abre, haga clic en el enlace con el nombre de un grupo para el que desea cambiar los estados de los dispositivos.
3. En la ventana de 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 **Se establece en Crítico si se especifican**, active la condición para cambiar un dispositivo al estado *Crítico*.

   Solo puede cambiar la configuración que no esté bloqueada en la directiva primaria.

6. Seleccione el botón de selección junto a la condición en la lista.
7. En la esquina superior izquierda de la lista, haga clic en el botón **Editar**.
8. Configure el valor requerido para la condición seleccionada.
   Los valores no pueden configurarse para cada condición.
9. Haga clic en **Aceptar**.

Cuando se cumplen las condiciones especificadas, al dispositivo administrado se le asigna el estado *Crítico*.

Para activar el cambio del estado del dispositivo a Advertencia:

1. En el menú principal, vaya a **DISPOSITIVOS → JERARQUÍA DE GRUPOS**.
2. En la lista de grupos que se abre, haga clic en el enlace con el nombre de un grupo para el que desea cambiar los estados de los dispositivos.
3. En la ventana de 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 **Se establece en Advertencia si se especifican**, active la condición para cambiar un dispositivo al estado *Advertencia*.

   Solo puede cambiar la configuración que no esté bloqueada en la directiva primaria.

6. Seleccione el botón de selección junto a la condición en la lista.
7. En la esquina superior izquierda de la lista, haga clic en el botón **Editar**.
8. Configure el valor requerido para la condición seleccionada.
   Los valores no pueden configurarse para cada condición.
9. Haga clic en **Aceptar**.

Cuando se cumplen las condiciones especificadas, al dispositivo administrado se le asigna el estado *Advertencia*.

Configurar entrega de notificaciones

Expandir todo | Contraer todo

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 icono de la **Configuración** ( ) al lado del nombre del Servidor de administración requerido.
   La ventana de propiedades del Servidor de administración se abre con la pestaña **Control de aplicaciones** 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** le permite configurar la notificación de eventos por correo electrónico.

En el campo **Servidores SMTP**, especifique las direcciones del servidor de correo, separándolos con punto y coma. Puede usar los siguientes valores:

- Dirección IPv4 o IPv6
- Nombre DNS del servidor SMTP

En el campo **Puerto del servidor SMTP**, especifique el número de un puerto de comunicación del servidor SMTP. El número de puerto predeterminado es el 25.

Si activa la opción **Buscar registros 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 activa la opción **Buscar registros MX por DNS** y no activa 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 para 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 desactivar el cifrado de mensajes de correo electrónico.

- **Utilizar 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 con el 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 activar la comunicación mediante cualquier versión de TLS o solo a través de TLS 1.2 o versiones posteriores. Además, puede especificar un certificado para la autenticación del cliente en el servidor SMTP.

Puede especificar certificados para una conexión TLS al hacer clic en el enlace **Especificar certificados**:

- Busque un archivo de certificado para el servidor SMTP:

Puede recibir un archivo con la lista de certificados de una autoridad de certificación confiable y cargar el archivo en el 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 certificado para el cliente:

Puede utilizar un certificado que haya recibido de cualquier fuente, por ejemplo, de cualquier autoridad de certificación confiable. Debe especificar el certificado y su clave privada mediante uno de los siguientes tipos de certificado:

- Certificado X-509:

Debe especificar un archivo con el certificado y un archivo con la clave privada. Ambos archivos no dependen el uno del otro y, por ende, no importa el orden en el que se carguen. Cuando se carguen ambos archivos, deberá especificar la contraseña para decodificar la clave privada. La contraseña puede tener un valor vacío si la clave privada no está codificada.

- Contenedor pkcs12:

Debe cargar un solo archivo que contenga el certificado y su clave privada. Cuando se cargue el archivo, deberá especificar la contraseña para decodificar la clave privada. La contraseña puede tener un valor vacío si la clave privada no está codificada.

Al hacer clic en el botón **Enviar mensaje de prueba**, puede verificar si ha configurado las notificaciones correctamente: la aplicación envía una notificación de prueba al destinatario que ha especificado.

En el campo **Destinatarios (direcciones de correo electrónico)**, especifique las direcciones de correo electrónico a las cuales 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 **Correo electrónico del remitente: si este valor no está definido, se usará la dirección del destinatario. Advertencia: Le recomendamos que no utilice una dirección de correo electrónico ficticia**, especifique 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 el texto estándar con información sobre el evento que la aplicación envía cuando un evento ocurre. 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 símbolo porcentual (%), lo tiene que escribir dos veces seguidas para permitir el envío del mensaje. Por ejemplo, "La carga de la CPU es del 100%%".

Al hacer clic en el enlace **Configurar límite numérico de notificaciones**, puede especificar el número máximo de notificaciones que la aplicación puede enviar durante el intervalo de tiempo especificado.

- **SMS**

La pestaña **SMS** le permite configurar la transmisión de notificaciones por SMS de varios eventos a un teléfono celular. Los mensajes SMS se envían a través de una puerta de enlace de correo electrónico.

En el campo **Servidores SMTP**, especifique las direcciones del servidor de correo, separándolos con punto y coma. Puede usar los siguientes valores:

- Dirección IPv4 o IPv6
- Nombre DNS del servidor SMTP

En el campo **Puerto del servidor SMTP**, especifique el número de un puerto de comunicación del servidor SMTP. El número de puerto predeterminado es el 25.

Si la opción **Utilizar autenticación ESMTP** está activada, 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 desactivar el cifrado de mensajes de correo electrónico.

- **Utilizar 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 con el 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 activar la comunicación mediante cualquier versión de TLS o solo a través de TLS 1.2 o versiones posteriores. Además, puede especificar un certificado para la autenticación del cliente en el servidor SMTP.

Puede especificar un archivo de certificado del 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 en el 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 **Destinatarios (direcciones de correo electrónico)**, especifique las direcciones de correo electrónico a las cuales la aplicación enviará notificaciones. Puede especificar varias direcciones en este campo, separándolas con punto y coma. Las notificaciones se transmitirán 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 este valor no está definido, se usará la dirección del destinatario. Advertencia: No recomendamos usar una dirección de correo electrónico ficticia**, especifique 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 **Números de teléfono de destinatarios de mensajes SMS**, especifique los números de teléfono celular de los destinatarios de la notificación 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 incluye parámetros sustitutos, como el nombre del evento, el nombre del dispositivo y el nombre del dominio.

Si el texto de la notificación contiene un símbolo porcentual (%), lo tiene que escribir dos veces seguidas para permitir el envío del mensaje. Por ejemplo, "La carga de la CPU es del 100%%".

Haga clic en **Enviar mensaje de prueba** para verificar si ha configurado las notificaciones correctamente: la aplicación envía una notificación de prueba al destinatario que ha especificado.

Haga clic en el enlace **Configurar 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 lanzar

  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**, especifique la carpeta y el nombre del archivo que se ejecutará. Antes de especificar el archivo, prepare el archivo y especifique los marcadores que definen los detalles del evento que se enviarán 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 enlace **Configurar límite numérico de notificaciones**, puede 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.

Comprobación de notificaciones

Para comprobar si se han enviado las notificaciones del evento, la aplicación utiliza la notificación de la detección de virus de prueba EICAR en los dispositivos cliente.

Para comprobar el envío de notificaciones de eventos:

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. A continuación, vuelva a activar la protección en tiempo real del sistema de archivos.
2. Ejecute una tarea de análisis para los dispositivos cliente en un grupo de administración o para dispositivos específicos, incluido uno que tenga el virus EICAR.

   Si la tarea de análisis se ha configurado correctamente, se detectará el virus de prueba. Si las notificaciones se han configurado correctamente, recibirá una notificación sobre la detección de 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, la mayoría de fabricantes de aplicaciones de seguridad identifican este archivo como un virus. Puede descargar el virus de prueba desde el sitio web oficial de EICAR.

Notificaciones de eventos mostradas mediante archivos ejecutables

Mediante la ejecución de un archivo ejecutable, Kaspersky Security Center Linux puede informar al administrador sobre los eventos que ocurran en los dispositivos cliente. El archivo ejecutable debe contener otro archivo ejecutable con los marcadores de posición del evento que se transferirá al administrador.

Marcadores de posición para describir un evento

Marcador de posición	Descripción del marcador de posición
%SEVERITY%	Nivel de importancia del evento
%COMPUTER%	Nombre del dispositivo en el que ocurrió el evento
%DOMAIN%	Dominio
%EVENT%	Evento
%DESCR%	Descripción de eventos
%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 conexión

Ejemplo:

Las notificaciones de eventos se envían por medio de un archivo ejecutable (como script1.bat), dentro del cual se inicia otro archivo ejecutable (como script2.bat) con el marcador de posición %COMPUTER%. Cuando ocurre un evento, el archivo script1.bat se abre en el dispositivo del administrador, que a su vez abre el archivo script2.bat con el marcador de posición %COMPUTER%. El administrador recibe el nombre del dispositivo en el que ha ocurrido el evento.

Avisos de Kaspersky

Esta sección describe cómo usar, configurar y desactivar los anuncios de Kaspersky.

Acerca de los anuncios de Kaspersky

La sección Anuncios de Kaspersky (**SUPERVISIÓN E INFORMES → Anuncios de Kaspersky**) le mantiene informado al brindarle información relacionada con su versión de Kaspersky Security Center y las aplicaciones administradas que están instaladas en los dispositivos administrados. Kaspersky Security Center actualiza periódicamente la información de la sección, eliminando anuncios desactualizados y añadiendo nueva información.

Kaspersky Security Center muestra solo los anuncios de Kaspersky relacionados con el Servidor de administración conectado y las aplicaciones de Kaspersky instaladas en los dispositivos administrados de este Servidor de administración. Los anuncios se muestran individualmente para cualquier tipo de Servidor de administración: principal, secundario o virtual.

El Servidor de administración debe tener una conexión a Internet para recibir anuncios de Kaspersky.

Los anuncios están destinados a mantener las aplicaciones de Kaspersky instaladas en su red actualizadas y completamente funcionales. Los anuncios pueden incluir información sobre actualizaciones críticas para las aplicaciones de Kaspersky, correcciones para las vulnerabilidades encontradas y formas de solucionar otros problemas en las aplicaciones de Kaspersky. De forma predeterminada, los anuncios de Kaspersky están activados. Si no desea recibir los anuncios, puede desactivar esta función.

Para mostrarle la información que corresponde a la configuración de la protección de su red, Kaspersky Security Center envía datos a los servidores en la nube de Kaspersky y recibe solo aquellos anuncios relacionados 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 cuando instala el Servidor de administración de Kaspersky Security Center.

La información nueva se divide en las siguientes categorías según su importancia:

1. Información crítica
2. Novedades importantes
3. Advertencia
4. Información

Cuando aparece información nueva en la sección Anuncios de Kaspersky, Kaspersky Security Center 14 Web Console muestra una etiqueta de notificación que corresponde al nivel de importancia del anuncio. Puede hacer clic en la etiqueta para ver este anuncio en la sección Anuncios de Kaspersky.

Puede especificar la configuración de Anuncios de Kaspersky, incluidas las categorías de anuncios que desea ver y dónde mostrar la etiqueta de notificación. Si no desea recibir anuncios, puede desactivar esta función.

Especificación de la configuración de anuncios de Kaspersky

En la sección Anuncios de Kaspersky, puede especificar la configuración de los anuncios de Kaspersky, incluidas las categorías de los 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** → **ANUNCIOS DE KASPERSKY**.
2. Haga clic en el enlace **Configuración**.
   Se abre la ventana de configuración de Anuncios de Kaspersky.
3. Especifique los siguientes parámetros:
   - 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 notificaciones. La etiqueta se puede mostrar en todas las secciones de la consola o en la sección **SUPERVISIÓN E INFORMES** y sus subsecciones.
4. Haga clic en el botón **Aceptar**.
   La configuración de Anuncios de Kaspersky está establecida.

Desactivación de anuncios de Kaspersky

La sección Anuncios de Kaspersky (**SUPERVISIÓN E INFORMES** → **Anuncios de Kaspersky**) le mantiene informado al brindarle información relacionada con su versión de Kaspersky Security Center y las aplicaciones administradas que están instaladas en los dispositivos administrados. Si no desea recibir anuncios de Kaspersky, puede desactivar esta función.

Para desactivar los anuncios de Kaspersky

1. En la ventana principal de la aplicación, haga clic en el icono de **Configuración** ( ) junto al nombre del Servidor de administración requerido.
   Se abre la ventana Propiedades del Servidor de administración.
2. En la pestaña **Control de aplicaciones**, seleccione la sección **Anuncios de Kaspersky**.
3. Ponga el conmutador en la posición **Los anuncios relacionados con la seguridad están desactivados**.
4. Haga clic en el botón **Guardar**.
   Los anuncios de Kaspersky quedan desactivados.

Exportación de eventos a sistemas SIEM

Esta sección describe cómo configurar la exportación de eventos a los sistemas SIEM.

Configuración de la exportación de eventos a sistemas SIEM

Kaspersky Security Center Linux permite configurar la exportación de eventos a sistemas SIEM mediante uno de los siguientes métodos: 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 Linux. Cuando completa este escenario, el Servidor de administración envía automáticamente eventos al sistema SIEM.

Requisitos previos

Antes de iniciar la exportación de la configuración de eventos en Kaspersky Security Center Linux:

- Obtenga más información sobre los métodos de exportación de eventos.
- Asegúrese de contar con los valores de la configuración del sistema.

> Puede realizar los pasos de este escenario en cualquier orden.

El proceso de exportación de eventos al sistema SIEM consta de las siguientes etapas:

- **Configurar el sistema SIEM para recibir eventos de Kaspersky Security Center Linux**

  Instrucciones prácticas: Configurar la exportación de eventos en un sistema SIEM

- **Seleccionar eventos que desea exportar al sistema SIEM**

  Marque los eventos que desea exportar al sistema SIEM Primero, marque los eventos generales que ocurren en todas las aplicaciones administradas de Kaspersky. A continuación, pude marcar los eventos para aplicaciones Kaspersky administradas específicas.

- **Configuración de la exportación de eventos al sistema SIEM**

  Puede exportar eventos usando uno de los siguientes métodos:

  - Utilizando los protocolos TCP/IP, UDP o TLS sobre TCP.
  - Usando la exportación de eventos directamente desde la base de datos de Kaspersky Security Center (Se proporciona un conjunto de vistas públicas en la base de datos de Kaspersky Security Center; puede encontrar la descripción de estas vistas públicas en el documento klakdb.chm).

Resultados

Después de configurar la exportación de eventos al sistema SIEM, puede ver los resultados de la exportación si seleccionó los eventos que desea exportar.

Antes de empezar

Expandir todo | Contraer todo

Al configurar la exportación automática de eventos en Kaspersky Security Center Linux, debe especificar ciertos parámetros de la configuración del sistema SIEM. Se recomienda que compruebe esta configuración 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 siguientes ajustes:

- **Dirección del servidor del sistema SIEM**

  La dirección IP del servidor en el que está instalado el sistema SIEM actualmente en uso. Compruebe este valor en su 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 receptor de su sistema SIEM.

- **Protocolo**

  Protocolo usado para transferir mensajes desde Kaspersky Security Center Linux a su sistema SIEM. Especifica este valor en la configuración de Kaspersky Security Center Linux y en la configuración del receptor 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 aplicaciones de Kaspersky instaladas en dispositivos administrados. La información sobre eventos se guarda en la base de datos del Servidor de administración. Puede exportar esta información a sistemas SIEM externos. La exportación de la información de eventos a sistemas SIEM externos permite a los administradores de sistemas SIEM responder lo antes posible a eventos del sistema de seguridad que ocurren en dispositivos administrados o grupos de dispositivos.

Eventos por tipo

En Kaspersky Security Center Linux existen los siguientes tipos de eventos:

- Eventos generales. Estos eventos ocurren en todas las aplicaciones de Kaspersky administradas. Por ejemplo, FBrote de virus es un evento general. Los eventos generales tienen una sintaxis y semántica definidas estrictamente. Los eventos generales se utilizan, por ejemplo, en informes y paneles.
- Eventos específicos de 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. Según las condiciones en que se produzca, un evento se puede asignar varios niveles de importancia. Existen cuatro niveles de importancia de eventos:

- Un *evento crítico* es un evento que indica que se ha producido un problema crítico que puede llevar a la pérdida de datos, un funcionamiento defectuoso o un error crítico.
- Un *fallo operativo* es un evento que indica que se ha producido un grave problema, un error o un funcionamiento defectuoso que ocurrió durante el funcionamiento de la aplicación o al realizar un procedimiento.
- Una *advertencia* es un evento que no es necesariamente grave, pero también indica un problema posible en el futuro. La mayor parte de los eventos se designan como advertencias si la aplicación se puede restaurar sin la pérdida de datos o capacidades funcionales después de que tales eventos ocurran.
- Un evento *de información* es un evento que se produce para informar sobre la finalización correcta de una operación, el correcto funcionamiento de la aplicación o la finalización de un procedimiento.

Cada evento tiene un plazo de almacenamiento definido, durante el cual puede verlo o modificarlo 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 definido es el cero. Solo los eventos que se almacenarán en la base de datos del Servidor de administración durante al menos un día se pueden exportar a sistemas externos.

Sobre exportación de eventos

Puede utilizar la exportación de eventos en sistemas centralizados que tratan con problemas de seguridad a un nivel organizativo y técnico, proporcionan servicios de supervisión de la seguridad y unifican la información de soluciones diferentes. Estos son sistemas de SIEM, que proporcionan análisis en tiempo real de alertas de seguridad y eventos generados por el hardware de la red y las aplicaciones o Centros operativos de seguridad (SOCs).

Estos sistemas reciben datos desde muchas fuentes, redes incluidas, seguridad, servidores, bases de datos y aplicaciones. Los sistemas SIEM también proporcionan funcionalidad para consolidar datos supervisados a fin de ayudarle a evitar omitir eventos críticos. Además, los sistemas realizan análisis automatizados de eventos correlacionados y alertas a fin de notificar a los administradores sobre problemas de seguridad inmediatos. La generación de alertas se puede implementar a través de un panel o se puede enviar a través de canales de terceros, como el correo electrónico.

El proceso de exportar eventos desde Kaspersky Security Center Linux a sistemas SIEM externos involucra a dos partes: la que envía el evento, Kaspersky Security Center Linux, y un destinatario del evento, un sistema SIEM. Para exportar eventos correctamente, debe configurar estos parámetros en su sistema de SIEM y en la Consola de administración de Kaspersky Security Center Linux. No importa qué componente configura primero. Puede configurar la transmisión de eventos desde Kaspersky Security Center Linux y, a continuación, configurar la recepción de eventos por parte del sistema SIEM o viceversa.

Formato Syslog de exportación de eventos

Puede enviar eventos en formato Syslog a cualquier sistema SIEM. Usando el formato Syslog, puede transmitir cualquier evento que ocurra en el Servidor de administración y 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 el sistema SIEM

El sistema SIEM debe recibir y analizar correctamente los eventos recibidos desde Kaspersky Security Center Linux. Con estos objetivos, debe configurar correctamente el sistema SIEM. La configuración depende del sistema SIEM específico utilizado. No obstante, hay varios pasos generales en la configuración de todos los sistemas SIEM, por ejemplo, configurando el receptor y el analizador.

Acerca de la configuración de la exportación de eventos en un sistema SIEM

Expandir todo | Contraer todo

El proceso de exportar eventos desde Kaspersky Security Center Linux a sistemas SIEM externos involucra a dos partes: un remitente del evento, Kaspersky Security Center Linux y un destinatario del evento, el sistema SIEM. Debe configurar la exportación de eventos en su sistema SIEM y en Kaspersky Security Center Linux.

La configuración que especifica en el sistema SIEM dependerá del sistema que usted esté usando. Generalmente, para todos los sistemas SIEM debe configurar un receptor y, opcionalmente, un analizador sintáctico del mensaje para analizar los eventos recibidos.

Configuración del receptor

Para poder recibir los eventos enviados por Kaspersky Security Center Linux, debe configurar el receptor en su sistema SIEM. En general, la configuración siguiente se debe especificar en el sistema SIEM:

- **Protocolo de exportación**

  Un protocolo de transferencia de mensajes, ya sea UDP, TCP o TLS sobre TCP. Este protocolo debe ser el mismo que el protocolo que especificó en Kaspersky Security Center Linux.

- **Puerto**

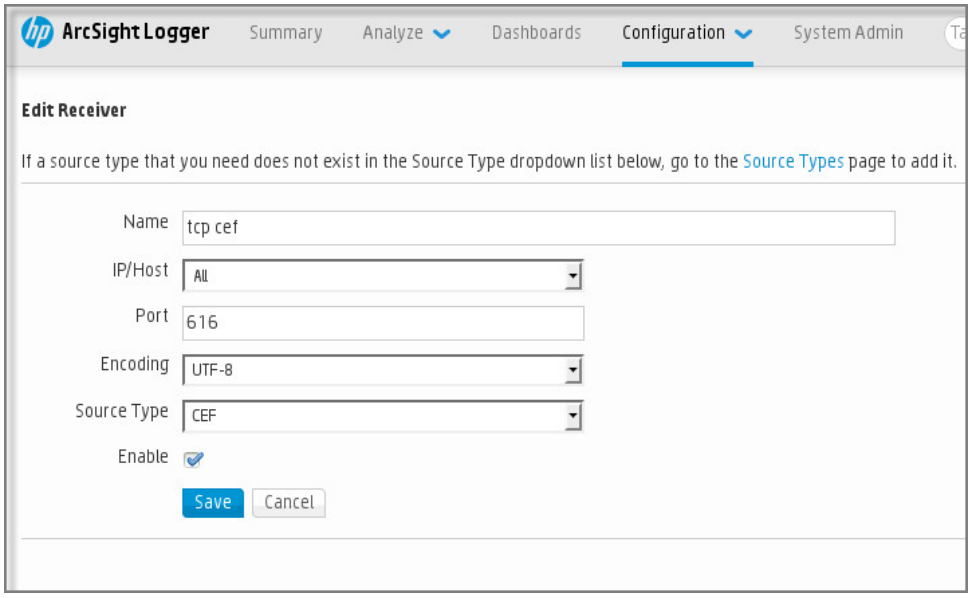
  Número de puerto para conectar con Kaspersky Security Center Linux. Este puerto debe ser el mismo que el puerto que especifica en Kaspersky Security Center Linux durante la configuración con un sistema SIEM.

- **Formato de datos**

  Especifique el formato Syslog.

Según el sistema SIEM que utilice, es posible que deba especificar la configuración del receptor adicional.

La cifra siguiente muestra la pantalla de instalación del receptor en ArcSight.



Instalación del receptor en ArcSight

Analizador sintáctico del mensaje

Los eventos de Exportar se transfieren a sistemas SIEM como mensajes. Estos mensajes se deben analizar correctamente de modo que la información sobre los eventos se pueda utilizar por el sistema SIEM. Los analizadores sintácticos de los mensajes son una parte del sistema SIEM; se utilizan para dividir los contenidos del mensaje en los campos relevantes, como ID del evento, gravedad, descripción, parámetros, etc. Esto permite al sistema SIEM procesar eventos recibidos de Kaspersky Security Center Linux para 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.

Marcado de eventos para exportar a sistemas SIEM en formato Syslog

Esta sección describe cómo marcar eventos para su posterior exportación a sistemas SIEM en formato Syslog.

Acerca del marcado de eventos para exportar al sistema SIEM en formato Syslog

Después de activar la exportación automática de eventos, debe seleccionar qué eventos se exportarán al sistema SIEM externo.

Puede configurar la exportación de eventos en formato Syslog a un sistema externo según una de las condiciones siguientes:

- Marcado de eventos generales. Si marca los eventos para exportar en una directiva, en la configuración de un evento, o en la configuración del Servidor de administración, el sistema SIEM recibirá los eventos marcados que se produjeron en todas las aplicaciones administradas por la directiva específica. Si los eventos exportados se seleccionaran en la directiva, no podrá redefinirlos para una aplicación particular administrada por esta directiva.
- Marcado de eventos para una aplicación administrada. Si marca eventos para exportar para una aplicación administrada instalada en un dispositivo administrado, el sistema SIEM solo recibirá los eventos que hayan ocurrido en esta aplicación.

Marcar eventos de una aplicación de Kaspersky para exportar 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 aplicaciones. En este caso, los eventos marcados se exportan desde todos los dispositivos incluidos en la cobertura de la directiva.

Para marcar eventos que desea exportar para una aplicación administrada específica:

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 directivas.
3. Vaya a la sección **Configuración de eventos**.
4. Seleccione las casillas junto a los eventos que desea 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 eventos**, que se abre al hacer clic en el enlace del evento.

6. Una marca de verificación (✓) aparece en la columna **Syslog** del evento o los eventos que haya marcado para 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 para la exportación de un dispositivo administrado, haga lo siguiente:

1. En el menú principal, vaya a **DISPOSITIVOS → DISPOSITIVOS ADMINISTRADOS**.
   Se muestra la lista de dispositivos administrados.
2. Haga clic en el enlace con el nombre del dispositivo requerido en la lista de dispositivos administrados.
   Se muestra la ventana de propiedades del dispositivo seleccionado.
3. Vaya a la sección **Aplicaciones**.
4. Haga clic en el enlace con el nombre de la aplicación pertinente en la lista de aplicaciones.
5. Vaya a la sección **Configuración de eventos**.
6. Seleccione las casillas de verificación junto a los eventos que desea exportar a SIEM.
7. Haga clic en el botón **Marcar para exportar al sistema SIEM mediante Syslog**.

   Además, puede marcar un evento para exportarlo a un sistema SIEM en la sección **Registro de eventos**, que se abre al hacer clic en el enlace del evento.

8. Una marca de verificación (✓) aparece en la columna **Syslog** del evento o los eventos que haya marcado para exportar al sistema SIEM.

A partir de ahora, el Servidor de administración envía los eventos marcados al sistema SIEM si la exportación al sistema SIEM está configurada.

Marcar eventos generales para exportar en formato Syslog

Puede utilizar el formato Syslog para marcar eventos generales que el Servidor de administración exportará a sistemas SIEM.

Para marcar eventos generales para exportar a un sistema SIEM:

1. Realice una de las siguientes acciones:
   - Haga clic en el icono de **Configuración** ( ) junto al nombre del Servidor de administración requerido.
   - En el menú principal, vaya a **DISPOSITIVOS** → **DIRECTIVAS Y PERFILES** y, luego, haga clic en el enlace de una directiva.
2. En la ventana que se abre, diríjase a la pestaña **Configuración de eventos**.
3. Haga clic en **Marcar para exportar al sistema SIEM mediante Syslog**.

   Además, puede marcar un evento para exportarlo al sistema SIEM en la sección **Registro de eventos**, que se abre al hacer clic en el enlace del evento.

4. Una marca de verificación ( ) aparece en la columna **Syslog** del evento o los eventos que haya marcado para exportar al sistema SIEM.

A partir de ahora, el Servidor de administración envía los eventos marcados al sistema SIEM si la exportación al sistema SIEM está configurada.

Acerca de la exportación de eventos mediante el formato Syslog

Puede utilizar el formato Syslog para exportar a sistemas SIEM los eventos que se producen en el Servidor de administración y otras aplicaciones de Kaspersky instaladas en dispositivos administrados.

Syslog es un estándar para el protocolo de registro de mensajes. Permite la separación del software que genera mensajes, el sistema que los almacena y el software que los notifica y los analiza. Cada mensaje se etiqueta mediante un código, indicando el tipo del software que genera el mensaje y se le asigna un nivel de gravedad.

El formato Syslog se define por los documentos Request for Comments (RFC) publicados por el Internet Engineering Task Force (estándares de Internet). Para exportar los eventos desde Kaspersky Security Center Linux a sistemas externos se utiliza el estándar RFC 5424 .

En Kaspersky Security Center Linux, puede usar el protocolo Syslog para configurar la exportación de los eventos a sistemas externos.

El proceso de exportación consiste en dos pasos:

1. La activación de la exportación de evento automática. En este paso, Kaspersky Security Center Linux se configura para enviar eventos al sistema SIEM. Kaspersky Security Center Linux empieza a enviar eventos inmediatamente después de que usted activa la exportación automática.
2. La selección de los eventos que exportar al sistema externo. En este paso, usted selecciona qué evento exportar al sistema SIEM.

Configuración de Kaspersky Security Center Linux para la exportación de eventos a un sistema SIEM

Expandir todo | Contraer todo

Para exportar eventos al sistema SIEM, debe configurar el proceso de exportación en Kaspersky Security Center Linux.

Para configurar la exportación a sistemas 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**, seleccione la sección **SIEM**.
4. Haga clic en el enlace **Configuración**.

   Se abre la sección **Exportar configuración**.

5. Ajuste la configuración en la sección **Exportar configuración**:
   - Dirección del servidor del sistema SIEM

     La dirección IP del servidor en el que está instalado el sistema SIEM actualmente en uso. Compruebe este valor en su 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 receptor de su sistema SIEM.

- Protocolo

  Seleccione el protocolo para transferir mensajes al sistema SIEM. Puede seleccionar el protocolo TCP/IP, UDP o TLS sobre TCP.

  Puede ajustar la configuración de TLS si selecciona TLS sobre el protocolo TCP:

  - **Autenticación del servidor**

    En el campo **Autenticación del servidor**, puede seleccionar los valores **Certificados de confianza** o **Huellas digitales SHA**:

    - **Certificados de confianza**. Puede recibir un archivo con la lista de certificados de una autoridad de certificados (CA) de confianza y cargar el archivo en Kaspersky Security Center Linux. Kaspersky Security Center Linux verifica si el certificado del servidor del sistema SIEM también está firmado por una CA de confianza o no.

      Para agregar un certificado de confianza, haga clic en el botón **Busque archivo de certificados de CA** y, a continuación, cargue el certificado.

    - **Huellas digitales SHA**. Puede especificar huellas digitales SHA-1 de certificados del sistema SIEM en Kaspersky Security Center. Para agregar una huella digital SHA-1, introdúzcala en el campo **Huellas digitales** y, a continuación, haga clic en el botón **Añadir**.

    Al usar el ajuste **Añadir autenticación del cliente**, puede generar un certificado para autenticar Kaspersky Security Center. Por lo tanto, utilizará un certificado autofirmado emitido por Kaspersky Security Center. En este caso, puede usar un certificado de confianza y una huella digital SHA para autenticar el servidor del sistema SIEM.

  - **Añadir Nombre del sujeto/Nombre alternativo del sujeto**

    El nombre del sujeto es un nombre de dominio para el que se recibe el certificado. Kaspersky Security Center Linux no puede conectarse al servidor del sistema SIEM si el nombre de dominio del servidor del sistema SIEM no coincide con el nombre del sujeto del certificado del servidor del sistema SIEM. Sin embargo, el servidor del sistema SIEM puede cambiar su nombre de dominio si el nombre ha cambiado en el certificado. En este caso, se pueden especificar los nombres de sujeto en el campo **Añadir Nombre del sujeto/Nombre alternativo del sujeto**. Si alguno de los nombres de sujeto especificados coincide con el nombre de sujeto del certificado del sistema SIEM, Kaspersky Security Center Linux validará el certificado del servidor del sistema SIEM.

  - **Añadir autenticación del cliente**

    Para la autenticación del cliente, puede insertar su certificado o generarlo en Kaspersky Security Center.

    - **Ingresar certificado**. Puede utilizar un certificado que haya recibido de cualquier fuente; por ejemplo, de cualquier CA de confianza. Debe especificar el certificado y su clave privada mediante uno de los siguientes tipos de certificado:

      - **PEM certificado X.509**. Cargue un archivo con un certificado en el campo **Archivo con certificado** y un archivo con una clave privada en el campo **Archivo con clave**. Ninguno de estos archivos dependen el uno del otro y, por tanto, no importa el orden en el que se carguen. Cuando se carguen ambos archivos, especifique la contraseña para descodificar la clave privada en el campo **Verificación de certificado o contraseña**. La contraseña puede tener un valor vacío si la clave privada no está codificada.

      - **PKCS12 certificado X.509**. Cargue un único archivo que contenga un certificado y su clave privada en el campo **Archivo con certificado**. Cuando se cargue el archivo, especifique la contraseña para descodificar la clave privada en el campo **Verificación de certificado o contraseña**. La contraseña puede tener un valor vacío si la clave privada no está codificada.

    - **Generar clave**. Puede generar un certificado autofirmado en Kaspersky Security Center. Como resultado, Kaspersky Security Center Linux almacena el certificado autofirmado generado y puede pasar la parte pública del certificado o huella digital SHA1 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 enlace **Establezca la fecha de inicio de la exportación**.

   b. En la sección que se abre, especifique la fecha de inicio en el campo **Fecha para iniciar la exportación**.

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

7. Cambie la opción a la posición **Exportación automática de eventos a la base de datos del sistema SIEM ACTIVADA**.

8. Haga clic en el botón **Guardar**.

La exportación al sistema SIEM queda configurada. Desde este momento, si configuró la recepción de eventos en un sistema SIEM, el Servidor de administración exportará los eventos marcados a un sistema SIEM. Si establece la fecha de inicio de la exportación, el Servidor de administración también exportará los eventos que haya marcado y que estén almacenados en la base de datos del Servidor de administración desde la fecha especificada.

Exportar 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 Linux. Puede consultar las vistas públicas directamente y recuperar los datos del evento o crear sus propias vistas sobre la base de las vistas públicas existentes y dirigirse a ellas para conseguir los datos que necesita.

Vistas públicas

Para su comodidad, se proporciona un conjunto de vistas públicas 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 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 el nombre de la base de datos.

Creación de una consulta SQL usando la herramienta klsql2

Esta sección describe cómo descargar y usar la utilidad klsql2, y cómo crear una consulta SQL usando esta utilidad. Cuando crea una consulta 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 aborda las vistas públicas de Kaspersky Security Center Linux directamente.

Para descargar y usar la utilidad klsql2:

1. Descargar la utilidad klsql2 desde el sitio web de Kaspersky.
2. Copie y extraiga el archivo klsql2.zip descargado en cualquier carpeta en el dispositivo con el Servidor de administración del 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 desee y 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 siguiente comando para ejecutar la consulta SQL desde el archivo src.sql y guarde los resultados en el archivo result.xml:
   ```
   klsql2 -i src.sql -o result.xml
   ```
6. Abra el archivo result.xml recién creado para ver los resultados de la consulta.

Puede modificar el archivo src.sql y crear cualquier consulta en las vistas públicas. A continuación, desde la línea de comandos, ejecute su pregunta y guarde los resultados en un archivo.

Ejemplo de una consulta SQL en 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 los eventos que ocurrieron en dispositivos durante los últimos siete días, y muestra los eventos solicitados cuando ocurren; los eventos más recientes se muestran primero.

Ejemplo:

```
SELECT
e.nId, /* identificador de eventos */
e.tmRiseTime, /* hora, cuando se produjo el evento */
e.strEventType, /* nombre interno del tipo de evento */
e.wstrEventTypeDisplayName, /* nombre del evento mostrado */
e.wstrDescription, /* descripción del evento mostrada */
e.wstrGroupName, /* nombre del grupo, donde se encuentra el dispositivo */
```

```
    h.wstrDisplayName, /* nombre del dispositivo mostrado, 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 /* IP-address del dispositivo, donde 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
```

La 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 SQL Server, MySQL o MariaDB, debe conocer el nombre de la base de datos a fin de conectarse desde su editor de scripts de SQL.

Ver el nombre de la base de datos de Kaspersky Security Center Linux:

1. Haga clic en el icono de **Configuración** ( ) junto al nombre del Servidor de administración requerido.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Control de aplicaciones**, seleccione la sección **Detalles de la base de datos actual**.

El nombre de la base de datos se especifica en el campo **Nombre de la base de datos**. Use el nombre de la base de datos para dirigirse a la base de datos en sus consultas SQL.

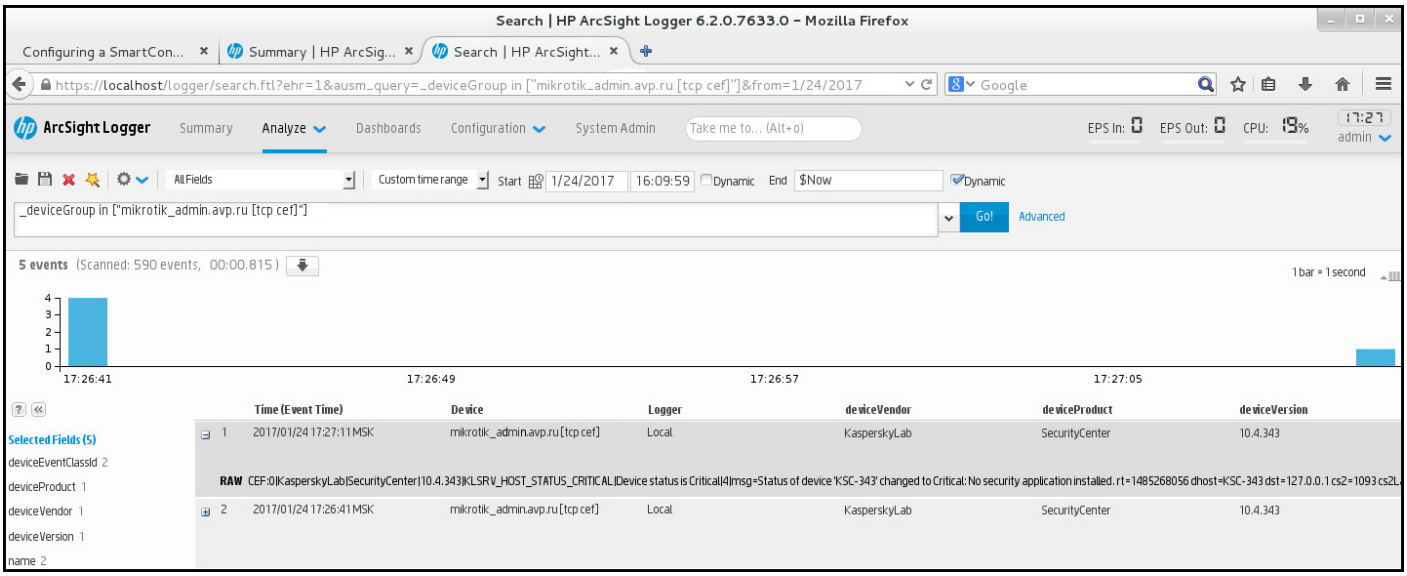
Visualización de resultados de exportación

Puede controlar la finalización correcta del procedimiento de exportación del evento. Para hacerlo, compruebe si los mensajes con eventos de exportación se reciben por su sistema SIEM.

Si su sistema SIEM recibe y analiza correctamente los eventos enviados desde Kaspersky Security Center Linux, esto significa que la configuración en ambos lados se ha realizado bien. De lo contrario, compruebe que la configuración que especificó en Kaspersky Security Center Linux corresponda a la configuración de su sistema SIEM.

La figura a continuación muestra los eventos exportados a ArcSight. Por ejemplo, el primer evento es un evento crítico del Servidor de administración: "*El estado del dispositivo es crítico*".

La representación de eventos de exportación en el sistema SIEM varía según el sistema SIEM que use.



Ejemplo de eventos

Selecciones de dispositivos

Las *selecciones de dispositivos* son una herramienta para filtrar dispositivos de acuerdo con condiciones específicas. Puede usar las selecciones de dispositivos para administrar varios dispositivos: por ejemplo, para ver un informe sobre estos dispositivos únicamente o para mover todos estos dispositivos a otro grupo.

Kaspersky Security Center proporciona una amplia gama de *selecciones predefinidas* (por ejemplo, **Dispositivos con el estado Crítico**, **La protección está desactivada**, **Se han detectado amenazas activas**). Las selecciones predefinidas no se pueden eliminar. También puede crear y configurar selecciones adicionales *definidas por el usuario*.

En las selecciones definidas por el usuario, puede establecer la cobertura de la búsqueda y seleccionar todos los dispositivos, dispositivos administrados o dispositivos no asignados. Los parámetros de búsqueda se especifican en las condiciones. En la selección de dispositivos puede crear varias condiciones con diferentes parámetros de búsqueda. Por ejemplo, puede crear dos condiciones y especificar diferentes rangos de IP en cada una de ellas. Si se especifican varias condiciones, una selección muestra los dispositivos que cumplen alguna de las condiciones. Por el contrario, los parámetros de búsqueda dentro de una condición están superpuestos. Si tanto el rango de IP como el nombre de una aplicación instalada se especifican en una condición, solo se mostrarán aquellos dispositivos donde la aplicación esté instalada y la dirección de IP pertenezca al rango especificado.

Para ver la selección de dispositivos:

1. En el menú principal, vaya a la sección **DISPOSITIVOS → SELECCIONES DE DISPOSITIVOS** o **DETECCIÓN Y DESPLIEGUE → SELECCIONES DE DISPOSITIVOS**.
2. En la lista de selección, haga clic en el nombre de la selección relevante.

Se muestra el resultado de selección de dispositivos.

Creación de 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 **Añadir**.
   Se abre la ventana **Configuración de Selección de dispositivos**.
3. Introduzca 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 **Añadir**.
6. En la ventana emergente, especifique las condiciones que se deben cumplir para incluir dispositivos en esta selección y, luego, haga clic en el botón **Aceptar**.
7. Haga clic en el botón **Guardar**.

La selección de dispositivo se crea y se añade a la lista de selecciones de dispositivos.

Configuración de una selección de dispositivos

Expandir todo | Contraer todo

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 pertinente que definió el usuario.
   Se abre la ventana **Configuración de Selección de dispositivos**.
3. En la pestaña **Control de aplicaciones**, especifique las condiciones que se deben cumplir para incluir dispositivos en esta selección.
4. Haga clic en el botón **Guardar**.

La configuración se aplica y se guarda.

A continuación, aparecen descripciones de las condiciones para asignar dispositivos a una selección. Las condiciones se combinan con el operador lógico OR. En la selección estarán los dispositivos que cumplan al menos una de las condiciones enumeradas.

General

En la sección **General**, puede cambiar el nombre de una condición de la selección y especificar si esa condición se debería invertir:

Revertir condición de la selección

Si esta opción está activada, la condición de selección especificada se invertirá. La selección incluirá todos los dispositivos que no cumplen la condición.

Esta opción está desactivada de forma 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 de la ventana de propiedades del dispositivo: en el campo **Descripción** de la sección **General**.

  Para describir texto en el campo **Descripción**, se pueden utilizar los siguientes caracteres:

  - Dentro de una palabra:
    - *****. Sustituye cualquier cadena con cualquier número de caracteres.

      Ejemplo:

      Para describir las palabras como **Servidor** o **Servidores** puedes escribir **Servidor***.

    - **?.** Sustituye cualquier carácter individual.

      Ejemplo:

      Para describir frases como **SUSE Linux Enterprise Server 12** o **SUSE Linux Enterprise Server 15**, puedes ingresar **SUSE Linux Enterprise Server 1?**.

      El asterisco (*****) o signo de interrogación (**?**) no se puede utilizar como el primer carácter de la pregunta.

  - Para encontrar varias palabras:
    - Espacio. Muestra todos los dispositivos cuyas descripciones contienen alguna de las palabras de la lista.

      Ejemplo:

      Para buscar una frase que incluya las palabras **secundario** o **virtual**, en la consulta puede incluir la línea **secundario virtual**.

    - **+**. Cuando se introduce el signo más delante de una palabra, todos los resultados de la búsqueda incluirán esa palabra.

      Ejemplo:

      Para encontrar una frase que contenga tanto **secundario** como **virtual**, introduzca la consulta **+secundario+virtual**.

    - **-**. Cuando se introduce el signo menos delante de una palabra, ningún resultado de la búsqueda incluirá esa palabra.

      Ejemplo:

      Para encontrar una frase que tenga la palabra **secundario**, pero no la palabra **virtual**, introduzca la consulta **+secundario-virtual**.

    - **"<algún texto>"**. El texto escrito entre comillas debe formar parte del texto.

      Ejemplo:

      Para encontrar una frase que contenga la combinación de palabras **Servidor secundario**, introduzca **"Servidor secundario"** en la consulta.

- Rango IP

  Si esta opción está activada, se pueden introducir las direcciones IP inicial y final del rango IP en el que se incluirán los dispositivos pertinentes.

  Esta opción está desactivada de forma predeterminada.

Etiquetas

En la sección **Etiquetas**, puede configurar criterios para incluir dispositivos en una selección según palabras clave (etiquetas) que se añadieron anteriormente a las descripciones de dispositivos administrados:

- Aplicar si coincide al menos una etiqueta especificada

  Si esta opción está activada, los resultados de las búsquedas mostrarán dispositivos cuyas descripciones contengan al menos una de las etiquetas seleccionadas.

  Si esta opción está desactivada, los resultados de la búsqueda solo mostrarán dispositivos con descripciones que contengan todas las etiquetas seleccionadas.

  Esta opción está desactivada de forma predeterminada.

- La etiqueta debe incluirse

  Si se selecciona esta opción, los resultados de búsqueda mostrarán los dispositivos cuyas descripciones contienen la etiqueta seleccionada. Para buscar dispositivos, puede usar el asterisco, que significa cualquier cadena con cualquier número de caracteres.

  Esta opción está seleccionada de forma predeterminada.

- La etiqueta debe excluirse

  Si esta opción se selecciona, los resultados de búsqueda mostrarán los dispositivos cuyas descripciones no contienen la etiqueta seleccionada. Para buscar dispositivos, puede usar el asterisco, que significa cualquier cadena con cualquier número de caracteres.

Actividad de red

En la sección **Actividad de red**, puede especificar los criterios que serán usados para incluir dispositivos en la selección según su actividad de red:

- Este dispositivo es un punto de distribución

  En la lista desplegable, puede establecer un criterio para incluir dispositivos en una selección al realizar búsquedas:
  - **Sí**. La selección incluirá dispositivos que funcionan como puntos de distribución.
  - **No**. Los dispositivos que funcionan como puntos de distribución no se incluirán en la selección.
  - **No se ha seleccionado ningún valor**. No se aplica el criterio.

- No desconectar del Servidor de administración

  En la lista desplegable, puede establecer un criterio para incluir dispositivos en una selección al realizar búsquedas:
  - **Activado**. La selección incluirá dispositivos en los que la casilla de verificación **No desconectar del Servidor de administración** está seleccionada.
  - **Desactivado**. La selección incluirá dispositivos en los que la casilla de verificación **No desconectar del Servidor de administración** no está seleccionada.
  - **No se ha seleccionado ningún valor**. No se aplica el criterio.

- Perfil de conexión cambiado

  En la lista desplegable, puede establecer un criterio para incluir dispositivos en una selección al realizar búsquedas:
  - **Sí**. La selección incluirá dispositivos que se conectaron al Servidor de administración después del cambio del perfil de conexión.
  - **No**. La selección no incluirá dispositivos que se conectaron al Servidor de administración después del cambio del perfil de conexión.
  - **No se ha seleccionado ningún valor**. No se aplica el criterio.

- Última conexión al Servidor de administración

  Puede utilizar esta casilla para establecer un criterio de búsqueda de dispositivos en función de la hora de la última conexión al Servidor de administración.

  Si se activa esta casilla de verificación, en el campo de entrada se puede especificar el intervalo de tiempo (fecha y hora) durante el que se produjo la última conexión entre el Agente de red instalado en el dispositivo cliente y el Servidor de administración. La selección incluirá los dispositivos que se encuentren dentro del intervalo especificado.

No se aplica el criterio si esta casilla está vacía.

De forma predeterminada, esta casilla está en blanco.

- El sondeo de la red ha detectado dispositivos nuevos

  Busca los nuevos dispositivos que se han detectado mediante el sondeo de la red hace pocos días.

  Si esta opción está activada, la selección incluirá solamente los nuevos dispositivos que se hayan detectado mediante la detección de dispositivos durante el número de días especificados en el campo **Periodo de detección (días)**.

  Si esta opción está desactivada, la selección incluye todos los dispositivos que han sido detectados por detección de dispositivos.

  Esta opción está desactivada de forma predeterminada.

- El dispositivo es visible

  En la lista desplegable, puede establecer un criterio para incluir dispositivos en una selección al realizar búsquedas:

  - **Sí**. La aplicación incluye en la selección los dispositivos actualmente visibles en la red.
  - **No**. La aplicación incluye en la selección los dispositivos actualmente invisibles en la red.
  - **No se ha seleccionado ningún valor**. No se aplica el criterio.

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 establecer un criterio para incluir los dispositivos en una selección al realizar búsquedas por el nombre de una aplicación Kaspersky.

  La lista proporciona únicamente los nombres de las aplicaciones con los complementos de administración instalados en la estación de trabajo del administrador.

  No se aplica el criterio si no se selecciona ninguna aplicación.

- Versión de la aplicación

  En el campo de entrada, puede establecer un criterio para incluir los dispositivos en una selección al realizar búsquedas por el número de versión de una aplicación Kaspersky.

  No se aplica el criterio si no indica el número de la versión.

- Nombre de la actualización crítica

  En el campo de entrada, puede establecer un criterio para incluir dispositivos en una selección al realizar búsquedas por el nombre de una aplicación o el número de paquete de una actualización.

  No se aplica el criterio si deja el campo en blanco.

- Última actualización de los módulos

  Puede utilizar esta opción como criterio para realizar búsquedas de dispositivos según la hora de la última actualización de los módulos de las aplicaciones instaladas en esos dispositivos.

  Si se selecciona esta casilla, en los campos de entrada podrá especificar el intervalo de tiempo (fecha y hora) en el que se realizó la última actualización de los módulos de las aplicaciones instaladas en esos dispositivos.

  No se aplica el criterio si esta casilla está vacía.

  De forma predeterminada, esta casilla está en blanco.

- El dispositivo se administra a través de Kaspersky Security Center 14

  En la lista desplegable, puede incluir en la selección los dispositivos administrados mediante Kaspersky Security Center Linux:

  - **Sí**. En la selección los dispositivos administrados mediante Kaspersky Security Center Linux.
  - **No**. La aplicación incluye en la selección dispositivos que no estén administrados por Kaspersky Security Center Linux.

- **No se ha seleccionado ningún valor**. No se aplica el criterio.

- Aplicación de seguridad instalada

  En la lista desplegable, puede incluir en la selección todos los dispositivos con la aplicación de seguridad instalada:
  - **Sí**. La aplicación incluye en la selección todos los dispositivos con la aplicación de seguridad instalada.
  - **No**. La aplicación incluye en la selección todos los dispositivos que no tienen aplicación de seguridad instalada.
  - **No se ha seleccionado ningún valor**. No se aplica el criterio.

Sistema operativo

En la sección **Sistema operativo**, puede especificar los criterios que serán usados para incluir dispositivos en la selección según su tipo del sistema operativo.

- Versión del sistema operativo

  Si se selecciona esta casilla de verificación, puede seleccionar un sistema operativo de la lista. Los dispositivos que tienen el sistema operativo especificado instalado se incluyen en los resultados de la búsqueda.

- Tamaño de bits del sistema operativo

  En la lista desplegable, puede seleccionar la arquitectura de su sistema operativo, que determinará cómo aplicar la regla de migración a su dispositivo (**Desconocido**, **x86**, **AMD64**, or **IA64**). De forma predeterminada, ninguna opción está seleccionada en la lista de modo que no se define la arquitectura del sistema operativo.

- Versión del 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 forma predeterminada, no se especifica ningún valor de la versión.

- Compilación del sistema operativo

  Esta configuración solo se aplica a los sistemas operativos de Windows.

  El número de compilación del sistema operativo. Puede especificar si el sistema operativo seleccionado debe tener un número de compilación igual, anterior o posterior. También puede configurar la búsqueda de todos los números de compilación, excepto el especificado.

- ID de versión del sistema operativo

  Esta configuración solo se aplica a los sistemas operativos de Windows.

  El identificador de la versión (Id.) del sistema operativo. Puede especificar si el sistema operativo seleccionado debe tener un Id. de versión igual, anterior o posterior. También puede configurar la búsqueda de todos los números de 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 desde una aplicación administrada:

- Estado del dispositivo

  Lista desplegable en la que se puede seleccionar uno de los estados del dispositivo: *Aceptar*, *Crítico* o *Advertencia*.

- Descripción del estado del dispositivo

  En este campo se pueden seleccionar las casillas de verificación que se muestran junto a las condiciones que, si se cumplen, asignarán uno de los siguientes estados al dispositivo: *Aceptar*, *Crítico* o *Advertencia*.

- Estado del dispositivo definido por la aplicación

  Lista desplegable en la que se puede seleccionar el estado de protección en tiempo real. Se incluyen en la selección los dispositivos que tengan el estado de protección en tiempo real especificado.

Componentes de protección

En la sección **Componentes de protección**, puede configurar los criterios para incluir dispositivos en una selección según su estado de protección:

- Bases de datos lanzadas

  Si esta opción está seleccionada, se puede hacer una búsqueda de dispositivos cliente por la fecha de lanzamiento de la base de datos antivirus. En los campos de entrada se puede establecer el intervalo de tiempo con el que se realizará la búsqueda.

  Esta opción está desactivada de forma predeterminada.

- Último análisis

  Si esta casilla está activada, se puede hacer una búsqueda de dispositivos cliente por la fecha de último análisis antivirus. En los campos de entrada puede especificar el período de tiempo en el cual se realizó el último análisis antivirus.

  Esta opción está desactivada de forma predeterminada.

- Número total de amenazas detectadas

  Si esta opción está activada, puede buscar dispositivos cliente por número de virus detectados. En los campos de entrada se pueden establecer los valores máximo y mínimo del número de virus encontrados.

  Esta opción está desactivada de forma predeterminada.

Registro de aplicaciones

En la sección **Registro de aplicaciones**, puede configurar los criterios para buscar dispositivos según aplicaciones instaladas en ellos:

- Nombre de la aplicación

  Lista desplegable en la que se puede seleccionar la aplicación. En la selección se incluirán los dispositivos que tengan instalada la aplicación especificada.

- Versión de la aplicación

  Campo de entrada en el que se puede especificar la versión de la aplicación seleccionada.

- Proveedor

  Lista desplegable en la que se puede seleccionar el fabricante de una aplicación instalada en el dispositivo.

- Estado de la aplicación

  Una lista desplegable en la que se puede seleccionar el estado de una aplicación (*Instalada*, *No instalada*). Los dispositivos en los cuales la aplicación especificada está instalada o no instalada, según el estado seleccionado, se incluirán en la selección.

- Buscar por la actualización

Si esta opción está activada, la búsqueda se realizará utilizando los detalles de las actualizaciones para las aplicaciones instaladas en los dispositivos relevantes. Después de seleccionar la casilla de verificación, los campos **Nombre de la aplicación**, **Versión de la aplicación** y **Estado de la aplicación** cambian a **Nombre de actualización**, **Versión de actualización** y **Estado** respectivamente.

Esta opción está desactivada de forma predeterminada.

- Nombre de la aplicación de seguridad incompatible

  Lista desplegable en la que se puede seleccionar aplicaciones de seguridad de terceros. Durante la búsqueda, se incluirán en la selección los dispositivos que tengan instalada la aplicación especificada.

- Etiqueta de la aplicación

  En la lista desplegable se puede seleccionar la etiqueta de la aplicación. Todos los dispositivos que han instalado aplicaciones con la etiqueta seleccionada en la descripción se incluyen en la selección de dispositivos.

- Aplicar a los dispositivos que no tengan etiquetas especificadas

  Si esta opción está activada, el perfil de la directiva incluirá los dispositivos con descripciones que no contengan ninguna de las etiquetas seleccionadas.

  Si esta opción está desactivada, el software no se actualiza.

  Esta opción está desactivada de forma predeterminada.

Registro de hardware

En la sección **Registro de hardware**, puede configurar criterios para incluir dispositivos incluidos en una selección según su hardware instalado:

- Dispositivo

  En la lista desplegable, puede seleccionar el tipo de unidad. Todos los dispositivos con esta unidad se incluyen en los resultados de la búsqueda.

  El campo admite búsqueda de texto completo.

- Proveedor

  En la lista desplegable se puede seleccionar el nombre del fabricante de la unidad. Todos los dispositivos con esta unidad se incluyen en los resultados de la búsqueda.

  El campo admite búsqueda 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 con la descripción especificada en este campo se incluirán en la selección.

  La descripción de un dispositivo en cualquier formato se puede introducir en la ventana de propiedades de ese dispositivo. El campo admite búsqueda de texto completo.

- Proveedor del dispositivo

  Nombre del fabricante del dispositivo. Los dispositivos fabricados por el fabricante especificado en este campo se incluirán en la selección.

  Puede introducir el nombre del fabricante en la ventana de propiedades de un dispositivo.

- Número de serie

  Todas las unidades de hardware con el número de serie especificado en este campo se incluirán en la selección.

- Número de inventario

  El equipo con el número de inventario especificado en este campo se incluirá en la selección.

- Usuario

  Todas las unidades de hardware del usuario especificado en este campo se incluirán en la selección.

- Ubicación

  Ubicación de un dispositivo o una unidad de hardware (por ejemplo, en la sede central o en una filial). Los dispositivos u otros dispositivos desplegados 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 ese dispositivo.

- Frecuencia de la CPU (MHz)

  Intervalo de frecuencia de una CPU. Los dispositivos con las CPU que coincidan con el intervalo de frecuencia especificado en estos campos (valores máximo y mínimo incluidos) se incluirán en la selección.

- Núcleos de CPU virtual

  Intervalo del número de núcleos virtuales en una CPU. Los dispositivos con las CPU que coincidan con el intervalo especificado en estos campos (valores máximo y mínimo incluidos) se incluirán en la selección.

- Volumen del disco duro, en GB

  Intervalo de los valores para el tamaño del disco duro en el dispositivo. Los dispositivos con los discos duros que coincidan con el intervalo especificado en estos campos de entrada (valores máximo y mínimo incluidos) se incluirán en la selección.

- Tamaño de RAM, en MB

  Intervalo de los valores para el tamaño de la RAM de un dispositivo. Los dispositivos con las RAM que coincidan con el intervalo especificado en estos campos de entrada (valores máximo y mínimo incluidos) se incluirán en la selección.

Máquinas virtuales

En la sección **Máquinas virtuales**, puede configurar los criterios para incluir dispositivos en la selección según si estos son máquinas virtuales o parte de la Infraestructura de escritorio virtual (VDI):

- Es una máquina virtual

  En la lista desplegable puede seleccionar las siguientes opciones:

  - **No es importante**.
  - **No**. Buscar dispositivos que no son máquinas virtuales.
  - **Sí**. Buscar dispositivos que son máquinas virtuales.

- Tipo de máquina virtual

  En la lista desplegable se puede seleccionar el fabricante de la máquina virtual.

  Esta lista desplegable está disponible si el valor **Sí** o **No es importante** se selecciona 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 formen parte de la Infraestructura de escritorio virtual.
- **Sí**. Buscar dispositivos que formen parte de una Infraestructura de escritorio virtual (VDI) de Microsoft.

Usuarios

En la sección **Usuarios**, puede configurar los criterios para incluir dispositivos en la selección según las cuentas de usuarios que han iniciado sesión en el sistema operativo.

- Último usuario que inició sesión en el sistema

  Si esta opción está activada, haga clic en el botón **Examinar** para especificar una cuenta de usuario. Los resultados de la búsqueda incluyen los dispositivos en los que un usuario específico ha iniciado sesión por última vez.

- Usuario que inició sesión en el sistema al menos una vez

  Si esta opción está activada, haga clic en el botón **Examinar** para especificar una cuenta de usuario. Los resultados de la búsqueda incluyen los dispositivos en los que el usuario especificado inició sesión en el sistema al menos una vez.

Problemas relacionados con el estado de las aplicaciones administradas

En la sección **Problemas relacionados con el estado de 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 al menos un problema que selecciona existe en un dispositivo, el dispositivo se incluirá en la selección. Cuando selecciona un problema listado para varias aplicaciones, tiene la opción de seleccionar este problema en todas las listas automáticamente.

Descripción del estado del dispositivo

En este campo puede seleccionar las casillas para las descripciones de estados desde la aplicación administrada; al recibir estos estados, los dispositivos se incluirán en la selección. Cuando selecciona un estado listado para varias aplicaciones, tiene la opción de seleccionar este estado en todas las listas automáticamente.

Estados de los componentes en aplicaciones administradas

En la sección **Estados de los componentes en aplicaciones administradas**, puede configurar criterios para incluir dispositivos en una selección según los estados de componentes en aplicaciones administradas:

- Estado de la prevención contra fugas de datos

  Buscar dispositivos por el estado de Prevención de fuga de datos (*No hay datos del dispositivo, Detenido, Iniciando, En pausa, En ejecución, Fallo*).

- Estado de la protección de los servidores de colaboración

  Buscar dispositivos por el estado de la protección de colaboración del servidor (*No hay datos del dispositivo, Detenido, Iniciando, En pausa, En ejecución, Fallo*).

- Estado de la protección antivirus de servidores de correo

  Buscar dispositivos por el estado de protección del servidor de correo (*No hay datos del dispositivo, Detenido, Iniciando, En pausa, En ejecución, Fallo*).

- Estado de sensor de Endpoint

  Buscar dispositivos por el estado del componente del sensor de Endpoint (*No hay datos del dispositivo, Detenido, Iniciando, En pausa, En ejecución, Fallo*).

Componentes de la aplicación

Esta sección contiene la lista de componentes de aquellas aplicaciones que tienen complementos de administración correspondientes instalados en la Consola de administración.

En la sección **Componentes de la aplicación**, puede especificar los criterios para incluir dispositivos en una selección de acuerdo con los estados y números de versión de los componentes que se refieren a la aplicación que seleccione:

- **Estado**

  Buscar dispositivos de acuerdo con el estado del componente enviado por una aplicación al Servidor de administración. Puede seleccionar uno de los siguientes estados: *No se reciben datos del dispositivo*, *Detenido*, *Iniciado*, *Pausado*, *En ejecución*, *Mal funcionamiento* o *No instalado*. Si el componente seleccionado de la aplicación instalada en un dispositivo administrado tiene el estado especificado, el dispositivo se incluye en la selección de dispositivos.

  Estados enviados por solicitudes:

  - *Iniciando:* El componente está actualmente en el proceso de iniciación.
  - *En ejecución:* El componente se activa y funciona correctamente.
  - *En pausa:* El componente se suspende, por ejemplo, después de que el usuario ha hecho una pausa la protección en la aplicación administrada.
  - *Mal funcionamiento:* Un error ha ocurrido durante la operación del componente.
  - *Detenido:* El componente está desactivado y no funciona en este momento.
  - *No instalado:* El usuario no seleccionó el componente para la instalación al configurar la instalación personalizada de la aplicación.

  A diferencia de otros estados, las aplicaciones *no envían datos del estado del dispositivo*. Esta opción muestra que las aplicaciones no tienen información sobre el estado del componente seleccionado. Por ejemplo, esto puede suceder cuando el componente seleccionado no pertenece a ninguna de las aplicaciones instaladas en el dispositivo o cuando el dispositivo está apagado.

- **Versión**

  Buscar dispositivos de acuerdo con el número de versión del componente que seleccione en la lista. Puede escribir un número de versión, por ejemplo `3.4.1.0`, y luego especificar si el componente seleccionado debe tener una versión igual, anterior o posterior. También puede configurar la búsqueda de todas las versiones excepto la especificada.

Guía de referencia de API

Esta guía de referencia de Kaspersky Security Center OpenAPI está diseñada para ayudar en las siguientes tareas:

- Automatización y personalización. Usted puede automatizar las tareas que no desee gestionar de forma manual. Por ejemplo, como administrador, puede utilizar Kaspersky Security Center OpenAPI para crear y ejecutar scripts que faciliten el desarrollo de la estructura de los grupos de administración y la mantengan actualizada.
- Desarrollo a la medida. Usando OpenAPI, puede desarrollar una aplicación cliente.

Puede usar el campo de búsqueda en la parte derecha de la pantalla para encontrar la información que necesita en la guía de referencia de OpenAPI.

GUÍA DE REFERENCIA DE OPENAPI

Muestras de scripts

La guía de referencia de OpenAPI contiene muestras de los scripts de Python que se enumeran en la siguiente tabla. Los ejemplos muestran cómo 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.

Muestra	Propósito de la muestra	Escenario
Log 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/secundaria"	Puede añadir 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.	Obtención de 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.	Generación y visualización de 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.	Inicio de una tarea de forma manual
Registrar puntos de distribución para dispositivos en un grupo	Puede asignar dispositivos administrados como puntos de distribución (antes conocidos como agentes de actualización).	Actualización de bases de datos Kaspersky y aplicaciones
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 tareas, consultar estadísticas de 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.	Supervisión de la ejecución de tareas
Crear y ejecuta una tarea	Puede crear una tarea. Especifique los siguientes parámetros de la tarea en la muestra: • Tipo • 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.	Creación de una tarea
Enumerar claves de licencia	Puede obtener una lista de todas las claves de licencia activas	Visualización de información sobre

	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.	claves de licencias en uso
Crear y buscar un usuario interno	Puede crear una cuenta para un trabajo adicional.	Selección de una 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 usuarios mediante SrvView	Puede usar la clase SrvView para solicitar información detallada al Servidor de administración. Por ejemplo, puede obtener una lista de usuarios utilizando esta muestra.	Administración de 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. Entre esas aplicaciones están Kaspersky Anti Targeted Attack Platform y Kaspersky Security for Virtualization. También puede ser una aplicación cliente personalizada que usted desarrolló a partir de OpenAPI.

Las aplicaciones que interactúan con Kaspersky Security Center a través de OpenAPI se conectan al Servidor de administración. Si ha configurado un lista de direcciones IP permitidas para conectarse al Servidor de administración, agregue las direcciones IP de los dispositivos donde están instaladas las aplicaciones que utilizan Kaspersky Security Center OpenAPI. Para saber si la aplicación que utiliza funciona con OpenAPI, consulte la Ayuda de esta aplicación.

Integración entre Kaspersky Security Center Web Console y otras soluciones de Kaspersky

Esta sección describe cómo configurar el acceso desde Kaspersky Security Center Web Console a otra aplicación de Kaspersky, como Kaspersky Endpoint Detection and Response y Kaspersky Managed Detection and Response.

Configuración del 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 para Kaspersky Anti Targeted Attack Platform (KATA / KEDR Web Console). Si utiliza tanto Kaspersky Security Center 14 Web Console como KATA / KEDR Web Console, puede configurar el acceso a KATA / KEDR Web Console 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**, ingrese la URL de KATA/KEDR Web Console en el campo **URL a KATA/KEDR Web Console**.
4. Haga clic en el botón **Guardar**.

Se añade la lista desplegable de **Administración avanzada** en la parte superior de la ventana principal de la aplicación. Puede utilizar este menú para abrir KATA / KEDR Web Console. Después de hacer clic en **Seguridad cibernética avanzada**, se abre una nueva pestaña en su navegador con el URL que ha especificado.

Establecimiento de 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 conocida como MDR), debe establecer una conexión en segundo plano entre Kaspersky Security Center Web Console y el Servidor de administración. Puede establecer esta conexión solo si su cuenta tiene el derecho Modificar LCA de objetos en el área funcional **Funciones generales: Permisos de usuario**.

Solo puede configurar la interacción 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. Para establecer una conexión en segundo plano, desplace el botón de alternancia a la posición: **Establecer una conexión en segundo plano para la integración ACTIVADO**.

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 una 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. El Servidor de administración cambia automáticamente la contraseña de la cuenta de servicio una vez cada 30 días, por razones de seguridad. No puede eliminar este servicio manualmente. El Servidor de administración elimina esta cuenta automáticamente cuando desactiva una conexión entre servicios. El Servidor de administración crea una cuenta de servicio única para cada Kaspersky Security Center 14 Web Console y Consola de administración y asigna todas las cuentas de servicio al grupo de seguridad con el nombre ServiceNwcGroup. El Servidor de administración crea este grupo de seguridad automáticamente durante el proceso de instalación de Kaspersky Security Center. No puede eliminar este grupo de seguridad manualmente.

Contactar con el Servicio de Soporte Técnico

Esta sección describe cómo obtener soporte técnico y las condiciones en que está disponible.

Cómo obtener soporte técnico

Si no encuentra una solución a su problema en la documentación de Kaspersky Security Center Linux o en alguna de las fuentes de información sobre Kaspersky Security Center Linux, póngase en contacto con el Servicio de soporte técnico. Los especialistas del Servicio de soporte técnico responderán a todas sus preguntas sobre la instalación y el uso de Kaspersky Security Center Linux.

Kaspersky proporciona asistencia técnica a Kaspersky Security Center Linux durante su ciclo de vida (consulte la página del ciclo de vida del soporte del producto). Antes de ponerse en contacto con el Servicio de Soporte Técnico lea las reglas de asistencia .

Puede ponerse en contacto con el Servicio de soporte técnico de una de las siguientes formas:

- Visitando el sitio web del Servicio de soporte técnico
- Mediante una solicitud al Servicio de Soporte Técnico, desde el portal Kaspersky CompanyAccount .

Obtener soporte técnico por teléfono

Puede encontrar información sobre cómo obtener soporte técnico en su provincia e información de contacto para el servicio de Soporte Técnico. Puede encontrar información sobre cómo obtener soporte técnico en su provincia e información de contacto del Servicio de soporte técnico en el sitio web del Servicio al cliente de Kaspersky .

Antes de ponerse en contacto con el Servicio de Soporte Técnico lea las reglas de asistencia .

Servicio de soporte técnico a través de Kaspersky CompanyAccount

Kaspersky CompanyAccount es un portal para las empresas que utilizan las aplicaciones Kaspersky. El portal Kaspersky CompanyAccount está diseñado para facilitar la interacción entre los usuarios y los especialista de Kaspersky mediante solicitudes en línea. Puede usar Kaspersky CompanyAccount para rastrear el estado de sus solicitudes en línea y también almacenar un historial de ellas.

Puede registrar a todos los empleados de su organización en una única cuenta de Kaspersky CompanyAccount. Esta cuenta única le permite administrar de forma centralizada las solicitudes electrónicas que envían los empleados registrados a Kaspersky, además de administrar los privilegios de estos empleados mediante Kaspersky CompanyAccount.

El portal Kaspersky CompanyAccount está disponible en los idiomas siguientes:

- 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 sobre 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.

La página de Kaspersky Security Center en la Base de conocimientos

La *Base de conocimientos* es una sección en el sitio web del Servicio 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. Los artículos en la base de conocimiento también pueden contener noticias del Servicio de soporte técnico.

Discuta sobre las aplicaciones de Kaspersky con la comunidad

Si su pregunta no requiere una respuesta inmediata, puede tratarla con expertos de Kaspersky y otros usuarios en nuestro Foro.

En el Foro puede ver los temas de debate, publicar sus comentarios y crear nuevos temas de debate.

> Se requiere una conexión a Internet para acceder a los recursos del sitio web.

Si no puede encontrar una 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 la tarea *Descargar actualizaciones a los repositorios de los puntos de distribución*, la autenticación de usuario no funciona si selecciona como fuente de actualización una carpeta local o de red protegida con contraseña. Para resolver este problema, primero monte la carpeta protegida con contraseña y luego especifique las credenciales requeridas, por ejemplo, mediante el sistema operativo. Después, 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 especifica la configuración del servidor proxy en 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*, esta opción se ignora y la conexión se establece a través del servidor proxy.
- Si abre Kaspersky Security Center 14 Web Console en diferentes navegadores y descarga el archivo de certificado del Servidor de administración en la ventana de propiedades del Servidor de administración, los archivos descargados tienen nombres diferentes.
- Se produce un error cuando intenta restaurar un objeto desde el repositorio **COPIA DE SEGURIDAD** (**OPERACIONES** → **REPOSITORIOS** → **COPIA DE SEGURIDAD**) o enviar el objeto a Kaspersky.
- La configuración bloqueada en una directiva de nivel superior de Kaspersky Endpoint Security for Linux se hereda, pero no se bloquea en las directivas secundarias.
- 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.
- Puede eliminar una categoría de aplicaciones que haya añadido a la función Control de aplicaciones en la directiva de Kaspersky Endpoint Security for Linux.
- Un dispositivo administrado que tiene más de un adaptador de red envía información al Servidor de administración sobre la dirección MAC del adaptador de red que no se usa 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 funcionará 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 la aplicación), recibidos desde los servidores de actualización de Kaspersky.

Actualización disponible

Conjunto de actualizaciones para los módulos de aplicación de Kaspersky, incluidas las actualizaciones críticas acumuladas durante cierto período de tiempo y los cambios en la arquitectura de la aplicación.

Administración de aplicaciones centralizada

Administración de aplicaciones remota usando los servicios de administración proporcionados en Kaspersky Security Center.

Administración directa de aplicaciones

Administración de aplicaciones a través de una interfaz local.

Administrador de clientes

Empleado de una organización cliente que es responsable de supervisar el estado de la protección antivirus.

Administrador de Kaspersky Security Center

La persona que administra las operaciones de la aplicación a través del sistema de administración centralizada remota de Kaspersky Security Center.

Administrador del proveedor de servicio

Integrante del personal de un proveedor de servicio de protección antivirus. Este administrador realiza trabajos de instalación y mantenimiento de sistemas de protección antivirus basados en productos antivirus de Kaspersky y presta soporte técnico a los clientes.

Agente de autenticación

Interfaz que le permite completar la autenticación para acceder a los discos duros cifrados y cargar el sistema operativo después de que el disco duro de arranque se haya cifrado.

Agente de red

Componente de Kaspersky Security Center que permite la interacción entre el Servidor de administración y las aplicaciones de Kaspersky que se instalan en un nodo de red específico (estación de trabajo o servidor). Este componente es común para todas las aplicaciones de empresa para Microsoft® Windows®. Existen versiones independientes del Agente de red para las aplicaciones Kaspersky desarrolladas para sistemas operativos tipo Unix y macOS.

Aplicación incompatible

Aplicación antivirus de un desarrollador externo o una aplicación Kaspersky que no admite la administración a través de Kaspersky Security Center Linux.

Archivo clave

Un archivo con el formato xxxxxxxx.key que permite utilizar una aplicación Kaspersky según las disposiciones de una licencia comercial o de prueba.

Bases de datos antivirus

Bases de datos que contienen información sobre las amenazas de seguridad informática conocidas por Kaspersky desde el momento en que se lanzan las bases de datos antivirus. Las entradas en las bases de datos antivirus permiten detectar códigos maliciosos en objetos analizados. Las bases de datos antivirus las crean especialistas de Kaspersky y se actualizan cada hora.

Carpeta de copia de seguridad

Carpeta especial para el almacenamiento de copias de datos del Servidor de administración creados mediante la utilidad de copia de seguridad.

Certificado compartido

Certificado diseñado para identificar el dispositivo móvil del usuario.

Certificado del Servidor de administración

El certificado que utiliza el Servidor de administración para los siguientes propósitos:

- Autenticación del Servidor de administración al conectarse a Kaspersky Security Center 14 Web Console
- 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 instala el Servidor de administración y luego se almacena en el Servidor de administración.

Clave activa

Una clave que la aplicación está utilizando actualmente.

Clave de suscripción adicional

Clave que certifica el derecho a usar la aplicación, pero que no se utiliza actualmente.

Cliente del Servidor de administración (dispositivo cliente)

Dispositivo, servidor o estación de trabajo donde el Agente de red está instalado y se ejecutan las aplicaciones administradas por Kaspersky.

Configuración de programa

La configuración de la aplicación que es común a todos los tipos de tareas y rige el funcionamiento general de la aplicación, como la configuración de rendimiento de la aplicación, la configuración de informes y la configuración de la copia de seguridad.

Configuración de tarea

Configuraciones de aplicación que son específicas para cada tipo de tarea.

Consola de administración

Un componente de Kaspersky Security Center basado en Windows (también llamado Consola de administración basada en MMC). Este componente proporciona una interfaz de usuario a los servicios administrativos del Servidor de administración y el Agente de red. La Consola de administración es un análogo de Kaspersky Security Center 14 Web Console.

Copia de seguridad de datos del Servidor de administración

Copia de los datos del Servidor de administración para la copia de seguridad y restauración posterior realizada usando la utilidad de copia de seguridad. La utilidad puede guardar lo siguiente:

- 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 los archivos de instalación para la instalación remota de aplicaciones (contenido de las carpetas: paquetes y actualizaciones sin instalar)
- Certificado del Servidor de administración

Derechos de administrador

Nivel de derechos y privilegios de usuario necesario para la administración de objetos Exchange de una organización Exchange.

Directiva

Una directiva determina la configuración de una aplicación y administra la capacidad de configurar esa aplicación en equipos en un plazo de un grupo de administración. Se debe crear una directiva individual para cada aplicación. Puede crear múltiples directivas para las aplicaciones instaladas en los equipos en cada grupo de administración, pero solo puede aplicarse una directiva a la vez a cada aplicación dentro de un grupo de administración.

Dispositivos administrados

Dispositivos de red corporativos incluidos en un grupo de administración.

Dominio de difusión

Área lógica de una red en que todos los nodos pueden intercambiar datos a través de un canal de difusión en OSI (modelo de referencia básico de interconexión de sistemas abiertos).

Estación de trabajo del administrador

Un dispositivo desde el que se abre Kaspersky Security Center 14 Web Console. Este componente proporciona una interfaz de administración de Kaspersky Security Center.

La estación de trabajo del administrador se utiliza para configurar y administrar el lado del servidor de Kaspersky Security Center. Utilizando la estación de trabajo del administrador, el administrador crea y administra un sistema de protección antivirus centralizado para una LAN corporativa basada en las aplicaciones de Kaspersky.

Estado de la protección

Estado actual de la protección, que define el nivel de seguridad del equipo.

Estado de la protección de la red

Estado de la protección en un momento dado que define la seguridad de los dispositivos de red corporativos. El estado de la protección de la red incluye factores como las aplicaciones de seguridad instaladas, el uso de claves de licencia y la cantidad y los tipos de amenazas detectadas.

Gravedad del evento

Una propiedad de un evento encontrado durante el funcionamiento de una aplicación de Kaspersky. Podemos encontrar los siguientes niveles de gravedad:

- Evento crítico
- Fallo operativo
- Advertencia
- Información

Los eventos del mismo tipo pueden tener diferentes niveles de gravedad, en función de la situación en la que se hayan producido.

Grupo de administración

Conjunto de dispositivos agrupados por función y por las aplicaciones de Kaspersky instaladas. Los dispositivos están agrupados como una sola entidad para facilitar su administración. Un grupo puede incluir otros grupos. Se pueden crear directivas de grupo y tareas de grupo para cada aplicación instalada en el grupo.

Grupo de aplicaciones con licencia

Grupo de aplicaciones creadas según los criterios que estableció un administrador (por ejemplo, el proveedor) para las que se mantienen las estadísticas de instalaciones realizadas en los dispositivos cliente.

Grupo de funciones

Grupo de usuarios de dispositivos móviles de Exchange ActiveSync a quienes se ha concedido derechos de administrador idénticos.

HTTPS

Protocolo de seguridad para la transferencia de datos, que utiliza cifrado, entre un navegador y un servidor web. HTTPS se utiliza para tener acceso a información restringida, como datos corporativos o financieros.

Instalación local

La instalación de una aplicación de seguridad en un dispositivo de una red corporativa que presupone el inicio de instalación manual desde el paquete de distribución de la aplicación de seguridad o el inicio manual de un paquete de instalación publicado previamente descargado en el dispositivo.

Instalación manual

Instalación de una aplicación de seguridad en un dispositivo de una red corporativa desde el paquete de distribución. La instalación manual requiere la participación de un administrador u otro especialista de TI. Por lo general, la instalación manual se lleva a cabo si la instalación remota se completa con un error.

Instalación remota

Instalación de aplicaciones Kaspersky mediante servicios facilitados por Kaspersky Security Center Linux.

JavaScript

Lenguaje de programación que amplía el rendimiento de las páginas web. Las páginas web creadas mediante JavaScript pueden realizar funciones (por ejemplo, cambiar la vista de elementos de la interfaz o abrir ventanas adicionales) sin tener que actualizar la página con nuevos datos del servidor web. Para ver páginas creadas usando JavaScript, active la compatibilidad con JavaScript en la configuración de su navegador.

Kaspersky Private Security Network (KSN privada)

Kaspersky Private Security Network es una solución que ofrece acceso a las bases de datos de reputación de Kaspersky Security Network y otros datos estadísticos a los usuarios de dispositivos con aplicaciones instaladas de Kaspersky acceso a las bases de datos de reputación de Kaspersky Security Network y otros datos estadísticos sin enviar datos desde sus dispositivos a Kaspersky Security Network. Kaspersky Private Security Network está diseñado para clientes corporativos que no pueden participar en Kaspersky Security Network por alguna de las siguientes razones:

- Los dispositivos del usuario no están conectados 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.

Operador de Kaspersky Security Center

Usuario que supervisa el estado y la operación de un sistema de protección administrada con Kaspersky Security Center.

Paquete de instalación

Un conjunto de archivos creados para la instalación remota de una aplicación de Kaspersky mediante el sistema de administración remota de Kaspersky Security Center. El paquete de instalación contiene un intervalo de configuraciones necesarias para instalar la aplicación y ejecutarla inmediatamente después. La configuración corresponde a la configuración predeterminada de las aplicaciones. El paquete de instalación consta de archivos con extensiones .kpd y .kud que se incluyen en el kit de distribución de la aplicación.

Perfil

Conjunto de opciones de configuración de dispositivos móviles Exchange que define su comportamiento cuando están conectados a un servidor Exchange de Microsoft.

Perfil de aprovisionamiento

Conjunto de parámetros de configuración para el funcionamiento de las aplicaciones en dispositivos móviles de iOS. Un perfil de aprovisionamiento contiene información sobre la licencia y está vinculado a una aplicación específica.

Perfil de configuración

Directiva que incluye un conjunto de parámetros y restricciones para un dispositivo móvil con MDM de iOS.

Periodo de vigencia de la licencia

El periodo de licencia es el tiempo durante el que tiene acceso a las funciones de la aplicación y a los derechos para usar servicios adicionales. Los servicios que se pueden utilizar dependerán del tipo de licencia.

Propietario del dispositivo

El propietario del dispositivo es un usuario que el administrador puede comunicarse cuando es necesario efectuar determinadas operaciones con un dispositivo cliente.

Protección antivirus de la red

Conjunto de medidas técnicas y organizativas que disminuyen el riesgo de que entren virus y spam a la red de una organización, y evitan ataques, phishing y otras amenazas contra la red. La seguridad de la red aumenta cuando usa aplicaciones de seguridad y servicios y cuando aplica y se adhiere a la directiva de seguridad de los datos corporativos.

Protección antivirus: proveedor de servicio

Organización que proporciona a una organización cliente servicios de protección antivirus sobre la base de soluciones de Kaspersky.

Puerta de enlace de conexión

Una *puerta de enlace de conexión* es un Agente de red que actúa en un modo especial. Una puerta de enlace de conexión acepta conexiones de otros Agentes de red y las conecta al Servidor de administración a través de su propia conexión con el Servidor. A diferencia de un Agente de red normal, una puerta de enlace de conexión espera las conexiones del Servidor de administración en lugar de establecer conexiones con el Servidor de administración.

Punto de distribución

Equipo que tiene Agente de red instalado y se utiliza para la distribución de actualizaciones, la instalación remota de aplicaciones, la obtención de información sobre equipos en un grupo de administración o dominio de difusión. Los puntos de distribución se han diseñado para reducir la carga del Servidor de administración durante la distribución de actualizaciones y para optimizar el tráfico de red. Los puntos de distribución se pueden asignar de forma automática mediante el Servidor de administración o bien de forma manual por parte del administrador. El punto de distribución se conocía previamente como el agente de actualización.

Repositorio de eventos

Una parte de la base de datos del Servidor de administración dedicada al almacenamiento de información sobre eventos que ocurren en Kaspersky Security Center Linux.

Restauración

Reubicación del objeto original de la Cuarentena o Copia de seguridad a su carpeta original donde el objeto había sido almacenado antes de su puesta en cuarentena, desinfección o eliminación, o en una carpeta definida por un usuario.

Restauración de los datos del Servidor de administración

Restauración de los datos del Servidor de administración a partir de la información guardada en la copia de seguridad mediante la utilidad de copia de seguridad. La utilidad puede restaurar lo siguiente:

- 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 equipos de cliente
- Repositorio de los archivos de instalación para la instalación remota de aplicaciones (contenido de las carpetas: paquetes y actualizaciones sin instalar)
- Certificado del Servidor de administración

Servidor de administración

Componente de Kaspersky Security Center que almacena de forma centralizada la información sobre todas las aplicaciones Kaspersky que estén instaladas en la red de la empresa. También puede utilizarse para administrar estas aplicaciones.

Servidor de administración principal

El Servidor de administración principal es el Servidor de administración que se especificó durante la instalación del Agente de red. El Servidor de administración principal se puede utilizar en la configuración de perfiles de conexión del Agente de red.

Servidor de administración virtual

Componente de Kaspersky Security Center diseñado para la administración del sistema de protección de la red de la organización cliente.

El Servidor de administración virtual es un tipo concreto de Servidor de administración secundario y, en comparación con un Servidor de administración físico, tiene las siguientes restricciones:

- El Servidor de administración virtual solo se puede crear en un Servidor de administración principal.
- Durante su funcionamiento, el Servidor de administración Virtual utiliza la base de datos del Servidor de administración principal. Las tareas de copia de seguridad y restauración de datos, así como las tareas de exploración y descarga de actualizaciones, no son compatibles con un Servidor de administración virtual.
- El Servidor virtual no permite la creación de Servidores de administración secundarios (incluidos los Servidores virtuales).

Servidor web de Kaspersky Security Center

Un componente de Kaspersky Security Center que se instala junto con el Servidor de administración. El Servidor web está diseñado para publicar paquetes de instalación independientes, perfiles de MDM de iOS y archivos de una carpeta compartida a través de una red.

Servidores de actualización de Kaspersky

Servidores HTTP(S) de Kaspersky desde los que las aplicaciones Kaspersky descargan las actualizaciones para las bases de datos y los módulos de la aplicación.

SSL

Protocolo de cifrado de datos usado en Internet y redes locales. El protocolo SSL (capa de conexión segura) se utiliza en aplicaciones web para crear una conexión segura entre un cliente y servidor.

System Health Validator (SHV) de Kaspersky Security Center

Un componente de Kaspersky Security Center diseñado para comprobar la capacidad de funcionamiento del sistema operativo en caso de la operación simultánea de Kaspersky Security Center y de Microsoft NAP.

Tarea

Las funciones realizadas por la aplicación Kaspersky se implementan como tareas, como: protección de archivos en tiempo real, análisis completo del equipo y actualización de las bases de datos.

Tarea de grupo

Tarea definida para un grupo de administración y ejecutada en todos los dispositivos cliente incluidos en ese grupo de administración.

Tarea local

Una tarea definida y ejecutada en un único equipo de cliente.

Tarea para dispositivos específicos

Tarea asignada a un conjunto de dispositivos cliente de grupos de administración arbitrarios y realizados en dichos dispositivos.

Tienda de aplicaciones

Componente de Kaspersky Security Center. La Tienda de aplicaciones se utiliza para instalar aplicaciones en dispositivos Android que pertenecen a los usuarios. La Tienda de aplicaciones le permite publicar los archivos APK de aplicaciones y enlaces a aplicaciones en Google Play.

Usuarios internos

Las cuentas de los usuarios internos se utilizan para trabajar con Servidores de administración virtuales. Kaspersky Security Center otorga los derechos de usuarios reales a los usuarios internos de la aplicación.

Las cuentas de los usuarios internos se crean y utilizan solo en Kaspersky Security Center. No se transfiere ningún dato de los usuarios internos al sistema operativo. Kaspersky Security Center autentifica los usuarios internos.

Zona desmilitarizada (DMZ)

La zona desmilitarizada es un segmento de una red local que contiene servidores que responden a las solicitudes de la Web global. Para garantizar la seguridad de la red local de una organización, el acceso a la LAN desde la zona desmilitarizada se protege mediante un firewall.

Información sobre el código de terceros

La información sobre el código de terceros se encuentra en el archivo legal_notices.txt, en el directorio de instalación de la aplicación.

Avisos de marcas comerciales

Linux es la marca registrada de Linus Torvalds en EE. UU. y otros países.

Micro Focus es una marca comercial o una marca comercial registrada de Micro Focus (IP) Limited o sus subsidiarias en el Reino Unido, Estados Unidos y otros países.

Microsoft, Active Directory, ActiveSync, BitLocker, Excel, Forefront, Internet Explorer, InfoPath, Hyper-V, Microsoft Edge, 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 compañías Microsoft.

Mozilla, Firefox, Thunderbird son marcas registradas de Mozilla Foundation.

Novell es una marca registrada de Novell Enterprises Inc. en Estados Unidos y otros países.

Oracle, Java, JavaScript y TouchDown son marcas registradas de Oracle y/o sus filiales.

Parallels y el logotipo de Parallels son marcas comerciales o marcas comerciales registradas de Parallels International GmbH en Canadá, Estados Unidos u otros lugares.

Chef es una marca comercial o marca comercial registrada de Progress Software Corporation y/o una de sus subsidiarias o filiales en los Estados Unidos y/o en otros países.

Puppet es una marca comercial o 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 comerciales registradas de Red Hat Inc. o sus subsidiarias en los Estados Unidos y otros países.

BlackBerry pertenece a Research In Motion Limited y está registrada en los Estados Unidos y puede estar registrada o pendiente de registro en otros países.

Debian es una marca comercial registrada de Software in the Public Interest, Inc.

Splunk y SPL son marcas comerciales y marcas comerciales registradas de Splunk Inc. en Estados Unidos y otros países.

SUSE es una marca registrada de SUSE LLC en Estados Unidos y otros países.

Symbian es una marca comercial que pertenece a Symbian Foundation Ltd.

OpenAPI es una marca comercial de The Linux Foundation.

VMware, VMware vSphere y VMware Workstation son marcas comerciales registradas o marcas comerciales de VMware, Inc. en Estados Unidos y/o en otras jurisdicciones.

UNIX es una marca registrada en Estados Unidos y otros países, con licencia exclusiva a través de X/Open Company Limited.

Zabbix es una marca registrada de Zabbix SIA.