kaspersky

Kaspersky Security Center 15 Linux

目录

Kaspersky Security Center Linux 帮助

新闻新功能

- 新闻

程序和硬件要求硬件和软件要求

- 管理服务器要求
- Web Console 要求
- 网络代理要求

启动启动

- 安装
- 快速启动向导
- 保护部署向导

授权许可授权许可和激活

- 激活 Kaspersky Security Center Linux
- 受管理应用程序的授权许可

PC_08部署和配置

- 发现网络设备
- 分发点和/或连接网关的调整
- 替换第三方安全应用程序
- Kaspersky 应用程序。集中部署
- 配置网络保护

- Kaspersky 应用程序。更新数据库和软件模块

Alarm_01监控

- 监控和报告

附加功能附加功能

- 导出事件到 SIEM 系统
- 层级指南（仅限在线帮助）

新闻

Kaspersky Security Center 15 Linux

Kaspersky Security Center 15 Linux 具有多个新功能和改进。

- 域控制器轮询允许您轮询 Microsoft Active Directory 域控制器和 Samba 域控制器。您可以使用管理服务器或分发点来轮询 Microsoft Active Directory。您只能通过基于 Linux 的分发点轮询 Samba 域控制器。当您轮询域控制器时，管理服务器或分发点会检索有关域中包含的设备的域结构、用户账户、安全组和 DNS 名称的信息。
- Kaspersky Security Center Linux 现在支持使用以下 DBMS：
  - PostgreSQL 15.x
  - Postgres Pro 15.x
- 如果您使用 PostgreSQL 或 Postgres Pro 作为 DBMS，则 Kaspersky Security Center Linux 可支持多达 50,000 个受管理设备。
- 从 Kaspersky Security Center Windows迁移到 Kaspersky Security Center Linux。您可以运行向导来迁移 Kaspersky Security Center对象，包括任务、策略和管理组结构。之后，您可以将导入的受管理设备移至 Kaspersky Security Center Linux 的管理之下。
- Kaspersky Security Center Linux 现在支持使用以下卡巴斯基应用程序：
  - Kaspersky Security for Virtualization Light Agent
  - Kaspersky Embedded Systems Security for Windows
  - Kaspersky Embedded Systems Security for Linux
  - Kaspersky Industrial CyberSecurity for Nodes
  - Kaspersky Industrial CyberSecurity for Networks
  - Kaspersky Endpoint Security for Mac
  - Kaspersky Endpoint Agent
  - Kaspersky Security for Virtualization Light Agent
- 远程诊断基于 Windows 和 Linux 的受管理设备。
- 改进的应用程序控制组件。您现在可以根据选定文件夹中的可执行文件列表或卡巴斯基应用程序类别创建应用程序类别。然后，您可以指定在组织中允许还是阻止创建的类别中的应用程序。
- 导出和导入事件分类。您可以将用户定义的事件分类及其设置导出到 KLO 文件，然后将保存的事件分类导入到 Kaspersky Security Center Windows 或Kaspersky Security Center Linux。
- 在威胁报告中，您现在可以通过单击**查看警报**链接来打开威胁发展链。
- Kaspersky Security Center Linux 现在支持集群技术。如果管理组包含集群或服务器阵列，则“**受管理设备**”页面将显示两个选项卡：一个用于单个设备，另一个用于集群和服务器阵列。受管理设备被检测为集群节点

后，集群将被作为单独对象添加到**集群和服务器阵列**选项卡。集群节点与其他受管理设备一起列在**设备**选项卡上。

- Kaspersky Security Center Linux 对某些平台的支持已终止，因为这些平台不再受到其供应商的支持。

Kaspersky Security Center 14.2 Linux

Kaspersky Security Center 14.2 Linux 具有多个新功能和改进。

- 在管理服务器层次结构中，基于 Linux 的管理服务器现在可以充当主服务器，可以管理充当辅助服务器的基于 Linux 或基于 Windows 的服务器。
- Kaspersky Security Center Linux 现在支持卡巴斯基安全网络 (KSN)、KSN 代理服务和卡巴斯基专用安全网络 (KPSN)。
- Kaspersky Security Center Linux 现在支持 Kaspersky Security for Windows 作为受管理应用程序。

  只有通过基于 Windows 的分发点使用操作系统工具，才能在客户端设备上远程安装 Windows 网络代理。
- 基于 Windows 的受管理设备上的数据现在可以加密以降低笔记本电脑或硬盘被盗或丢失时敏感数据和公司数据意外泄露的风险。此功能可通过 Kaspersky Endpoint Security for Windows 实现。
- Kaspersky Security Center Linux 允许您直接在 Kaspersky Security Center Linux 的用户界面中下载和更新卡巴斯基应用程序的分发包和管理 Web 插件。
- 默认情况下，有关安装在基于 Linux 和基于 Windows 的受管理设备上的应用程序的信息会被发送到管理服务器。
- 现在自动验证对卡巴斯基服务器的访问。如果无法使用系统 DNS 访问服务器，应用程序将使用公共 DNS。
- 在主管理服务器、从属管理服务器和网络代理之间传输的敏感数据现在受到 AES 加密算法的保护。
- 虚拟管理服务器上的用户权限可随时独立于主管理服务器进行配置。此外，您可以为主服务器用户分配管理虚拟服务器的权限。
- Kaspersky Security Center Linux 现在支持使用以下 DBMS：
  - PostgreSQL 13.x
  - PostgreSQL 14.x
  - Postgres Pro 13.x（所有版本）
  - Postgres Pro 14.x（所有版本）
- 您可以使用 Kaspersky Security Center Web Console 将策略和任务导出到一个文件，然后将策略和任务导入到 Kaspersky Security Center Windows 或 Kaspersky Security Center Linux。
- “**不使用代理服务器**”选项已从以下任务中删除：
  - *将更新下载至管理服务器存储库*
  - *将更新下载至分发点存储库*

Kaspersky Security Center 14 Linux

Kaspersky Security Center Linux 具有多个新功能和改进：

- 除了“*将更新下载至管理服务器存储库*”任务，现在还可以通过“*将更新下载至分发点存储库*”任务下载卡巴斯基安全应用程序的反病毒数据库。
- 受管理设备上的反病毒数据库和应用程序模块可以通过管理服务器或分发点进行传播和更新。您可以选择最适合您组织的更新方案，以减少管理服务器上的负载并优化公司网络上的数据流量。
- Kaspersky Security Center Linux 仅从卡巴斯基更新服务器下载卡巴斯基安全应用程序请求的更新。这可以减少下载数据的大小。
- 您现在可以使用 差异文件功能下载反病毒数据库和软件模块。diff 文件描述了数据库或软件模块的文件的两个版本之间的差异。使用 diff 文件节省您公司网络内的流量，因为 diff 文件相比数据库和软件模块的完整文件占据更少的空间。
- 添加了“*更新验证*”任务。通过使用此任务，您可以在受管理设备上安装更新之前自动检查下载的更新的可操作性和错误。
- Kaspersky Security Center 现在支持将 Kaspersky Industrial Cybersecurity for Linux Nodes 1.3 作为受管理应用程序。

关于 Kaspersky Security Center Linux

本部分介绍 Kaspersky Security Center Linux 的用途和主要功能和组件、以及如何购买 Kaspersky Security Center Linux。

Kaspersky Security Center Linux（也称为 Kaspersky Security Center）旨在通过使用基于 Linux 的管理服务器来部署和管理对客户端设备的保护。

Kaspersky Security Center Linux 允许您在公司网络中的设备上安装 Kaspersky 安全应用程序，远程运行扫描和更新任务，以及管理受管理应用程序的安全策略。作为管理员，您可以使用详细的控制板，其中提供公司设备状态的快照、详细的报告以及保护策略中的细化设置。

与具有基于 Windows® 管理服务器的 Kaspersky Security Center 相比，Kaspersky Security Center Linux 具有不同的功能集。

Kaspersky Security Center Linux 是一款面向企业网络管理员和各种组织中负责设备保护的员工的应用程序。

使用 Kaspersky Security Center 您可以做以下事情：

- 创建一个管理服务器层级结构来管理组织网络以及远程办公室网络或客户组织网络。
  *客户端组织*是指由服务提供商确保反病毒保护的一种组机构。
- 创建一个管理组层级结构以整体的形式管理一组选定的客户端设备。
- 管理基于 Kaspersky 程序构建的反病毒保护系统。
- 由 Kaspersky 和其他软件供应商执行应用程序的远程安装。
- 将 Kaspersky 应用程序的授权许可密钥集中部署到客户端设备、监控其使用情况，以及续订授权许可。
- 接收有关程序和设备运行的统计信息和报告。
- 接收有关 Kaspersky 程序操作中严重事件的通知。
- 管理存储在 Windows 设备的硬盘驱动器和可移动驱动器上的信息的加密。
- 管理用户对 Windows 设备上的加密数据的访问。
- 创建已连接至组织网络的硬件清查列表。
- 集中管理被安全应用程序移动到隔离区或备份区中的文件，以及安全应用程序已经推迟处理的文件。

您可以通过 Kaspersky（例如，https://www.kaspersky.com.cn）或其合作伙伴公司购买 Kaspersky Security Center Linux。

如果通过 Kaspersky 购买 Kaspersky Security Center Linux，您可以从我们的网站复制应用程序。支付得到处理后，程序激活所需的信息会通过邮件发送给您。

硬件和软件要求

- 管理服务器要求
- Web Console 要求

- 网络代理要求

管理服务器要求

最小硬件条件：

- 运行频率为 1,4 GHz 或更高的 CPU。
- RAM：4 GB。
- 可用磁盘空间：10 GB (/var/opt/kaspersky/klnagent_srv)。

支持以下操作系统：

- Debian GNU/Linux 10.x (Buster) 64 位
- Debian GNU/Linux 11.x (Bullseye) 64 位
- Debian GNU/Linux 12 (Bookworm) 64 位
- Ubuntu Server 18.04 LTS (Bionic Beaver) 64 位
- Ubuntu Server 20.04 LTS (Focal Fossa) 64 位
- Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64 位
- CentOS 7.x 64 位
- CentOS Stream 9 64 位
- Red Hat Enterprise Linux Server 7.x 64 位
- Red Hat Enterprise Linux Server 8.x 64 位
- Red Hat Enterprise Linux Server 9.x 64 位
- SUSE Linux Enterprise Server 12 (所有服务包) 64 位
- SUSE Linux Enterprise Server 15 (所有服务包) 64 位
- Astra Linux 特别版 RUSB.10015-01（操作更新 1.6）64 位
- Astra Linux 特别版 RUSB.10015-01（操作更新 1.7）64 位
- Astra Linux Common Edition（操作更新 2.12）64 位
- ALT SP Server 10 64 位
- ALT Server 10 64 位
- ALT Server 9.2 64 位
- ALT 8 SP Server (LKNV.11100-01) 64 位

- ALT 8 SP Server (LKNV.11100-02) 64 位
- ALT 8 SP Server (LKNV.11100-03) 64 位
- Oracle Linux 7 64 位
- Oracle Linux 8 64 位
- Oracle Linux 9 64 位
- RED OS 7.3 Server 64 位
- RED OS 7.3 Certified Edition 64 位
- ROSA COBALT 7.9 64 位

> 我们建议您使用 EXT4 文件系统及其默认设置。

支持以下虚拟平台：

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0
- VMware Workstation 16 Pro
- VMware Workstation 17 Pro
- Microsoft Hyper-V Server 2012 64 位
- Microsoft Hyper-V Server 2012 R2 64 位
- Microsoft Hyper-V Server 2016 64 位
- Microsoft Hyper-V Server 2019 64 位
- Microsoft Hyper-V Server 2022 64 位
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 17
- Oracle VM VirtualBox 6.x
- Oracle VM VirtualBox 7.x
- 基于内核的虚拟机（管理服务器支持的所有 Linux 操作系统）

支持以下数据库服务器（可以安装在其他设备上）：

- MySQL 5.7 Community 32 位/64 位
- MySQL 8.0 32 位/64 位
- MariaDB 10.1（内部版本 10.1.30 及更高版本）32 位/64 位
- MariaDB 10.3（内部版本 10.3.22 及更高版本）32 位/64 位
- MariaDB 10.4（内部版本 10.4.26 及更高版本）32 位/64 位
- MariaDB 10.5（内部版本 10.5.17 及更高版本）32 位/64 位
- 搭载 InnoDB 存储引擎的 MariaDB Galera Cluster 10.3 32 位/64 位
- PostgreSQL 13.x 64 位
- PostgreSQL 14.x 64 位
- PostgreSQL 15.x 64 位
- Postgres Pro 13.x 64 位（所有版本）
- Postgres Pro 14.x 64 位（所有版本）
- Postgres Pro 15.x 64 位（所有版本）
- Platform V Pangolin 5.4.0 64 位
- Jatoba 4 64-bit

Web Console 要求

Kaspersky Security Center Web Console 服务器

最小硬件条件：

- CPU：4 核，工作频率 2.5 GHz。
- RAM：8 GB。
- 可用磁盘空间：40 GB (/var/opt/kaspersky)。

以下操作系统之一（仅限 64 位版本）：

- Debian GNU/Linux 10.x (Buster)
- Debian GNU/Linux 11.x (Bullseye)
- Debian GNU/Linux 12 (Bookworm)
- Ubuntu Server 18.04 LTS (Bionic Beaver)

- Ubuntu Server 20.04 LTS (Focal Fossa)
- Ubuntu Server 22.04 LTS (Jammy Jellyfish)
- CentOS Stream 9
- Red Hat Enterprise Linux Server 7.x
- Red Hat Enterprise Linux Server 8.x
- Red Hat Enterprise Linux Server 9.x
- SUSE Linux Enterprise Server 12 (所有服务包)
- SUSE Linux Enterprise Server 15 (所有服务包)
- Astra Linux 特别版 RUSB.10015-01（操作更新 1.6）
- Astra Linux 特别版 RUSB.10015-01（操作更新 1.7）
- Astra Linux Common Edition（操作更新 2.12）
- ALT SP Server 10
- 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 7
- Oracle Linux 8
- Oracle Linux 9
- RED OS 7.3 Server
- RED OS 7.3 Certified Edition
- ROSA COBALT 7.9
- 基于内核的虚拟机（Kaspersky Security Center Web Console 服务器支持的所有 Linux 操作系统）

客户端设备

对于客户端，Kaspersky Security Center Web Console 的使用仅需要一个浏览器。

设备的硬件和软件需求和 Kaspersky Security Center Web Console 所使用的浏览器的需求是相同的。

浏览器：

- Google Chrome 100.0.4896.88 或更高版本（正式版本）
- Microsoft Edge 100 或更高版本
- Safari 15 on macOS
- “Yandex” 浏览器 23.5.0.2271 或更高版本
- Mozilla Firefox 扩展支持版本 102.0 或更高版本

网络代理要求

最小硬件条件：

- 运行频率为 1 GHz 或更高的 CPU。64 位操作系统，CPU 最低频率 1.4 GHz。
- RAM：512 MB。
- 可用磁盘空间：1 GB。

基于 Linux 的设备的软件要求：必须安装 Perl 语言解释器 5.10 或更高版本。

支持以下操作系统：

- Microsoft Windows Embedded POSReady 2009 with latest Service Pack 32 位
- Microsoft Windows Embedded 7 Standard with Service Pack 1 32 位/64 位
- Microsoft Windows Embedded 8.1 工业专业版 32 位/64 位
- Microsoft Windows 10 Enterprise 2015 LTSB 32 位 / 64 位
- Microsoft Windows 10 Enterprise 2016 LTSB 32 位 / 64 位
- Microsoft Windows 10 IoT Enterprise 2015 LTSB 32 位 / 64 位
- Microsoft Windows 10 IoT Enterprise 2016 LTSB 32 位 / 64 位
- Microsoft Windows 10 Enterprise 2019 LTSC 32 位/64 位
- Microsoft Windows 10 IoT Enterprise 版 1703 32 位/64 位
- Microsoft Windows 10 IoT Enterprise 版 1709 32 位/64 位
- Microsoft Windows 10 IoT Enterprise 版 1803 32 位/64 位
- Microsoft Windows 10 IoT Enterprise 版 1809 32 位/64 位
- Microsoft Windows 10 20H2 IoT Enterprise 32 位/64 位
- Microsoft Windows 10 21H2 IoT Enterprise 32 位/64 位
- Microsoft Windows 10 IoT Enterprise 32 位/64 位

- Microsoft Windows 10 IoT Enterprise version 1909 32 位/64 位
- Microsoft Windows 10 IoT Enterprise LTSC 2021 32 位/64 位
- Microsoft Windows 10 IoT Enterprise 版 1607 32 位/64 位
- Microsoft Windows 10 Home RS3 (Fall Creators Update, v1709) 32 位/64 位
- Microsoft Windows 10 Pro RS3 (Fall Creators Update, v1709) 32 位/64 位
- Microsoft Windows 10 Pro for Workstations RS3 (Fall Creators Update, v1709) 32 位/64 位
- Microsoft Windows 10 Enterprise RS3 (Fall Creators Update, v1709) 32 位/64 位
- Microsoft Windows 10 Education RS3 (Fall Creators Update, v1709) 32 位/64 位
- Microsoft Windows 10 Home RS4 (April 2018 Update, 17134) 32 位/64 位
- Microsoft Windows 10 Pro RS4 (April 2018 Update, 17134) 32 位/64 位
- Microsoft Windows 10 Pro for Workstations RS4 (April 2018 Update, 17134) 32 位/64 位
- Microsoft Windows 10 Enterprise RS4 (April 2018 Update, 17134) 32 位/64 位
- Microsoft Windows 10 Education RS4 (April 2018 Update, 17134) 32 位/64 位
- Microsoft Windows 10 Home RS5（2018 年 10 月）32 位/64 位
- Microsoft Windows 10 Pro RS5（2018 年 10 月）32 位/64 位
- Microsoft Windows 10 Pro for Workstations RS5（2018 年 10 月）32 位/64 位
- Microsoft Windows 10 Enterprise RS5（2018 年 10 月）32 位/64 位
- Microsoft Windows 10 Education RS5（2018 年 10 月）32 位/64 位
- Microsoft Windows 10 Home 19H1 32 位/64 位
- Microsoft Windows 10 Pro 19H1 32 位/64 位
- Microsoft Windows 10 Pro for Workstations 19H1 32 位/64 位
- Microsoft Windows 10 Enterprise 19H1 32 位/64 位
- Microsoft Windows 10 Education 19H1 32 位/64 位
- Microsoft Windows 10 家庭版 19H2 32 位/64 位
- Microsoft Windows 10 专业版 19H2 32 位/64 位
- Microsoft Windows 10 专业工作站版 19H2 32 位/64 位
- Microsoft Windows 10 企业版 19H2 32 位/64 位
- Microsoft Windows 10 教育版 19H2 32 位/64 位

- Microsoft Windows 10 Home 20H1（2020 年 5 月更新）32 位/64 位
- Microsoft Windows 10 Pro 20H1（2020 年 5 月更新）32 位/64 位
- Microsoft Windows 10 Enterprise 20H1（2020 年 5 月更新）32 位/64 位
- Microsoft Windows 10 Education 20H1（2020 年 5 月更新）32 位/64 位
- Microsoft Windows 10 Home 20H2（2020 年 10 月更新）32 位/64 位
- Microsoft Windows 10 Pro 20H2（2020 年 10 月更新）32 位/64 位
- Microsoft Windows 10 Enterprise 20H2（2020 年 10 月更新）32 位/64 位
- Microsoft Windows 10 Education 20H2（2020 年 10 月更新）32 位/64 位
- Microsoft Windows 10 Home 21H1（2021 年 5 月更新）32 位/64 位
- Microsoft Windows 10 Pro 21H1（2021 年 5 月更新）32 位/64 位
- Microsoft Windows 10 Enterprise 21H1（2021 年 5 月更新）32 位/64 位
- Microsoft Windows 10 Education 21H1（2021 年 5 月更新）32 位/64 位
- Microsoft Windows 10 Home 21H2（2021 年 10 月更新）32 位/64 位
- Microsoft Windows 10 Pro 21H2（2021 年 10 月更新）32 位/64 位
- Microsoft Windows 10 Enterprise 21H2（2021 年 10 月更新）32 位/64 位
- Microsoft Windows 10 Education 21H2（2021 年 10 月更新）32 位/64 位
- Microsoft Windows 10 Home 22H2（2023 年 10 月更新）32 位/64 位
- Microsoft Windows 10 Pro 22H2（2023 年 10 月更新）32 位/64 位
- Microsoft Windows 10 Enterprise 22H2（2023 年 10 月更新）32 位/64 位
- Microsoft Windows 10 Education 22H2（2023 年 10 月更新）32 位/64 位
- Microsoft Windows 11 Home 64 位
- Microsoft Windows 11 Pro 64 位
- Microsoft Windows 11 Enterprise 64 位
- Microsoft Windows 11 Education 64 位
- Microsoft Windows 11 22H2
- Microsoft Windows 8.1 专业版 32 位/64 位
- Microsoft Windows 8.1 企业版 32 位/64 位
- Microsoft Windows 8 专业版 32 位/64 位

- Microsoft Windows 8 企业版 32 位/64 位
- Microsoft Windows 7 专业版 Service Pack 1 和更高版本 32 位/64 位
- Microsoft Windows 7 企业版/旗舰版 Service Pack 1 和更高版本 32 位/64 位
- Microsoft Windows 7 Home Basic/Premium Service Pack 1 及更高版本 32 位/64 位
- Microsoft Windows XP Professional with Service Pack 2 32 位/64 位（仅受网络代理版本 10.5.1781 支持）
- Microsoft Windows XP Professional Service Pack 3 及更高版本 32 位（受网络代理版本 14.0.0.20023 支持）
- 适用于嵌入式系统的 Microsoft Windows XP Professional Service Pack 3 32 位（受网络代理版本 14.0.0.20023 支持）
- Windows MultiPoint Server 2011 Standard/Premium 64 位
- Windows Server 2008 基础版 Service Pack 2 32 位/64 位
- Windows Server 2008 Service Pack 2（所有版本）32 位/64 位
- Windows Server 2008 R2 Datacenter Service Pack 1 及更高版本 64 位
- Windows Server 2008 R2 Enterprise Service Pack 1 及更高版本 64 位
- Windows Server 2008 R2 Foundation Service Pack 1 及更高版本 64 位
- Windows Server 2008 R2 核心模式 Service Pack 1 及更高版本 64 位
- Windows Server 2008 R2 Standard Service Pack 1 及更高版本 64 位
- Windows Server 2008 R2 Service Pack 1（所有版本）64 位
- Windows Server 2012 Server Core 64 位
- Windows Server 2012 Datacenter 64 位
- Windows Server 2012 Essentials 64 位
- Windows Server 2012 Foundation 64 位
- Windows Server 2012 Standard 64 位
- Windows Server 2012 R2 Server Core 64 位
- Windows Server 2012 R2 Datacenter 64 位
- Windows Server 2012 R2 Essentials 64 位
- Windows Server 2012 R2 Foundation 64 位
- Windows Server 2012 R2 Standard 64 位
- Windows Server 2016 Datacenter (LTSB) 64 位
- Windows Server 2016 Standard (LTSB) 64 位

- Windows Server 2016 Server Core (安装选项) (LTSB) 64 位
- Windows Server 2019 Standard 64 位
- Windows Server 2019 Datacenter 64 位
- Windows Server 2019 Core 64 位
- Windows Server 2022 Standard 64 位
- Windows Server 2022 Datacenter 64 位
- Windows Server 2022 Core 64 位
- Debian GNU/Linux 10.x (Buster) 32 位/64 位
- Debian GNU/Linux 11.x (Bullseye) 32 位/64 位
- Debian GNU / Linux 12 (Bookworm) 32 位/64 位
- Ubuntu Server 18.04 LTS (Bionic Beaver) 32 位/64 位
- Ubuntu Server 20.04 LTS (Focal Fossa) 32 位/64 位
- Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64 位
- CentOS 7.x 64 位
- CentOS Stream 9 64 位
- Red Hat Enterprise Linux Server 6.x 32 位/64 位
- Red Hat Enterprise Linux Server 7.x 64 位
- Red Hat Enterprise Linux Server 8.x 64 位
- Red Hat Enterprise Linux Server 9.x 64 位
- SUSE Linux Enterprise Server 12 (所有服务包) 64 位
- SUSE Linux Enterprise Server 15 (所有服务包) 64 位
- SUSE Linux Enterprise Desktop 15 (Service Pack 3) ARM 64 位
- openSUSE 15 64 位
- EulerOS 2.0 SP8 ARM
- Astra Linux 特别版 RUSB.10015-01（操作更新 1.6）64 位
- Astra Linux 特别版 RUSB.10015-01（操作更新 1.7）64 位
- Astra Linux Common Edition（操作更新 2.12）64 位
- Astra Linux 特别版 RUSB.10152-02（操作更新4.7）ARM 64 位

- ALT SP Server 10 64 位
- ALT SP Workstation 10 64 位
- ALT Server 10 64 位
- ALT Server 9.2 64 位
- ALT Workstation 9.2 32 位/64 位
- ALT Workstation 10 32 位/64 位
- ALT 8 SP Server (LKNV.11100-01) 64 位
- ALT 8 SP Server (LKNV.11100-02) 64 位
- ALT 8 SP Server (LKNV.11100-03) 64 位
- ALT 8 SP Workstation (LKNV.11100-01) 32 位/64 位
- ALT 8 SP Workstation (LKNV.11100-02) 32 位/64 位
- ALT 8 SP Workstation (LKNV.11100-03) 32 位/64 位
- Mageia 4 32 位
- Oracle Linux 7 64 位
- Oracle Linux 8 64 位
- Oracle Linux 9 64 位
- Linux Mint 20.x 64 位
- AlterOS 7.5 及更高版本 64 位
- GosLinux IC6 64 位
- RED OS 7.3 Server 64 位
- RED OS 7.3 Certified Edition 64 位
- ROSA COBALT 7.9 64 位
- ROSA CHROME 12 64 位
- macOS Big Sur (11.x)
- macOS Monterey (12.x)
- macOS Ventura (13.x)
- macOS Sonoma (14.x)
  对于网络代理，还支持 Apple Silicon (M1) 架构以及 Intel。

支持以下虚拟平台：

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0
- VMware Workstation 16 Pro
- VMware Workstation 17 Pro
- Microsoft Hyper-V Server 2012 64 位
- Microsoft Hyper-V Server 2012 R2 64 位
- Microsoft Hyper-V Server 2016 64 位
- Microsoft Hyper-V Server 2019 64 位
- Microsoft Hyper-V Server 2022 64 位
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 17
- Oracle VM VirtualBox 6.x
- Oracle VM VirtualBox 7.x
- 基于内核的虚拟机（网络代理支持的所有 Linux 操作系统）

在运行 Windows 10 RS4 或 RS5 版本的设备上，Kaspersky Security Center 可能无法在启用了大小写敏感的文件夹中检测到一些漏洞。

在运行 Windows 7、Windows Server 2008 或 Windows MultiPoint Server 2011 的设备上安装网络代理之前，请确保您已经安装了 Windows 7 安全更新 (KB3063858)。

在 Microsoft Windows XP，网络代理可能错误执行一些操作。

您只能在 Microsoft Windows XP 中安装或更新 Network Agent for Windows XP。受支持的 Microsoft Windows XP 版本及其相应的网络代理版本列在受支持操作系统列表中。您可以从此页面下载适用于 Microsoft Windows XP 的网络代理所需版本。

我们建议您安装与 Kaspersky Security Center Linux 相同版本的 Linux 网络代理。

适用于 macOS 的网络代理与适用于此操作系统的卡巴斯基安全应用程序一起提供。

Compatible Kaspersky applications and solutions

Kaspersky Security Center Linux supports centralized deployment and management of the following Kaspersky applications:

- Kaspersky Endpoint Security for Windows 12.0 or later (supports file servers)
- Kaspersky Endpoint Security for Linux 11.2 or later (supports file servers)
- Kaspersky Endpoint Security for Linux Elbrus Edition 10 or later
- Kaspersky Endpoint Security for Linux ARM Edition 11.2 or later
- Kaspersky Endpoint Security for Mac 11.3 or later
- Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 or later
- Kaspersky Industrial CyberSecurity for Nodes 3.2 or later
- Kaspersky Industrial CyberSecurity for Networks 3.2 or later
- Kaspersky Endpoint Agent 3.15 or later
- Kaspersky Embedded Systems Security for Windows 3.2 or later
- Kaspersky Embedded Systems Security for Linux 3.3 or later
- Kaspersky Security for Virtualization Light Agent 5.2 or later

Refer to the Product Support Lifecycle webpage for the versions of the applications.

Known issues

Kaspersky Security Center Linux supports management of Kaspersky Endpoint Security for Windows with the following limitations:

- The Adaptive Anomaly Control component is not supported. Kaspersky Security Center Linux does not support Adaptive Anomaly Control rules.
- Kaspersky Sandbox components are not supported.
- The 无缝更新 functionality is not available.

Single Sign-On (SSO) is not supported for Kaspersky Industrial CyberSecurity for Networks.

不支持的操作系统和平台

- 不支持的操作系统和平台。管理服务器
- 不支持的操作系统和平台。Kaspersky Security Center Web Console 服务器
- 不支持的操作系统和平台。网络代理

不支持的操作系统和平台。管理服务器

管理服务器与以下操作系统不兼容：

- Debian GNU/Linux 7.x（最高 7.8）32 位/64 位
- Debian GNU/Linux 8.x (Jessie) 32 位/64 位
- Debian GNU/Linux 9.x (Stretch) 32 位/64 位
- Ubuntu Server 14.04 LTS (Trusty Tahr) 32 位/64 位
- Ubuntu Server 16.04 LTS (Xenial Xerus) 32 位/64 位
- Ubuntu Server 18.04 LTS (Bionic Beaver) 32 位
- Ubuntu Server 20.04.04 LTS (Focal Fossa) ARM 64 位
- Ubuntu Server 20.04 LTS (Focal Fossa) 32 位
- Ubuntu Desktop 14.04 LTS (Trusty Tahr) 32 位/64 位
- Ubuntu Desktop 16.04 LTS (Xenial Xerus) 32 位/64 位
- Ubuntu Desktop 18.04 LTS (Bionic Beaver) 32 位/64 位
- Ubuntu Desktop 20.04 LTS (Focal Fossa) 32 位/64 位
- CentOS 6.x (至 6.6) 64 位
- CentOS 7.x ARM 64 位
- CentOS 8.x 64 位
- Red Hat Enterprise Linux Server 6.x 32 位/64 位
- SUSE Linux Enterprise Desktop 12 (所有服务包) 64 位
- SUSE Linux Enterprise Desktop 15 (所有服务包) 64 位
- SUSE Linux Enterprise Desktop 15 (Service Pack 3) ARM 64 位
- openSUSE 15 64 位
- EulerOS 2.0 SP8 ARM
- Pardus OS 19.1 64 位

- Astra Linux Special Edition 1.5 64 位
- Astra Linux 特别版 RUSB.10152-02（操作更新4.7）ARM 64 位
- ALT Workstation 9.2 32 位/64 位
- ALT Workstation 10 32 位/64 位
- ALT 8 SP Workstation (LKNV.11100-01) 32 位/64 位
- ALT 8 SP Workstation (LKNV.11100-02) 32 位/64 位
- ALT 8 SP Workstation (LKNV.11100-03) 32 位/64 位
- Mageia 4 32 位
- Linux Mint 19.x 32 位
- Linux Mint 20.x 64 位
- AlterOS 7.5 及更高版本 64 位
- RED OS 7.3 64 位
- GosLinux IC6 64 位
- ROSA Enterprise Linux Server 7.3 64 位
- ROSA Enterprise Linux Desktop 7.3 64 位
- ROSA COBALT Workstation 7.3 64 位
- ROSA COBALT Server 7.3 64 位
- ROSA CHROME 12 64 位
- Lotos（Linux 核心版本 4.19.50，DE：MATE）64 位

数据库服务器：

- PostgreSQL Pangolin 64 位
- Microsoft SQL Server 2005 Express 32 位
- Microsoft SQL Server 2005（所有版本）32 位/64 位
- Microsoft SQL Server 2008 Express 32 位
- Microsoft SQL Server 2008（所有版本）32 位/64 位
- Microsoft SQL Server 2008 R2（所有版本）64 位
- Microsoft SQL Server 2008 R2 Service Pack 2（所有版本）64 位
- Microsoft SQL Server 2012（所有版本）32 位/64 位

- MySQL 5.0 32 位/64 位
- MySQL Enterprise 5.0 32 位/64 位
- MySQL Standard Edition 5.5 32 位/64 位
- MySQL Enterprise Edition 5.5 32 位/64 位
- MySQL Standard Edition 5.6 32 位/64 位
- MySQL Enterprise Edition 5.6 32 位/64 位
- MySQL Standard Edition 5.7 32 位/64 位
- MySQL Enterprise Edition 5.7 32 位/64 位
- MySQL 5.6 Community 32 位/64 位
- MariaDB Galera Cluster 10.4 32 位/64 位

不支持以下虚拟化平台：

- VMware vSphere 4.1
- VMware vSphere 5.0
- VMware vSphere 5.1
- VMware vSphere 5.5
- VMware vSphere 6
- VMware vSphere 6.5
- VMware Workstation 9.x
- VMware Workstation 10.x
- VMware Workstation 11.x
- VMware Workstation 12.x Pro
- VMware Workstation Pro 14
- VMware Workstation Pro 15
- Microsoft Hyper-V Server 2008 64 位
- Microsoft Hyper-V Server 2008 R2 64 位
- Microsoft Hyper-V Server 2008 R2 Service Pack 1 及更高版本 64 位
- Microsoft Virtual PC 2007 (6.0.156.0) 32 位/64 位
- Citrix XenServer 5.6

- Citrix XenServer 6.0
- Citrix XenServer 6.1
- Citrix XenServer 6.2
- Citrix XenServer 6.5
- Citrix XenServer 7
- Parallels Desktop 7
- Parallels Desktop 11
- Parallels Desktop 14
- Parallels Desktop 16
- Oracle VM VirtualBox 4.0.4-70112
- Oracle VM VirtualBox 5.x

不支持的操作系统和平台。Kaspersky Security Center Web Console 服务器

Kaspersky Security Center Web Console Server 与以下操作系统不兼容：

- Debian GNU/Linux 7.x（最高 7.8）32 位/64 位
- Debian GNU/Linux 8.x (Jessie) 32 位/64 位
- Debian GNU/Linux 9.x (Stretch) 32 位/64 位
- Ubuntu Server 14.04 LTS (Trusty Tahr) 32 位/64 位
- Ubuntu Server 16.04 LTS (Xenial Xerus) 32 位/64 位
- Ubuntu Server 20.04.04 LTS (Focal Fossa) ARM 64 位
- Ubuntu Desktop 14.04 LTS (Trusty Tahr) 32 位/64 位
- Ubuntu Desktop 16.04 LTS (Xenial Xerus) 32 位/64 位
- Ubuntu Desktop 18.04 LTS (Bionic Beaver) 32 位/64 位
- Ubuntu Desktop 20.04 LTS (Focal Fossa) 32 位/64 位
- CentOS 6.x (至 6.6) 64 位
- CentOS 7.x ARM 64 位
- CentOS 7.x 64 位

- CentOS 8.x 64 位
- Red Hat Enterprise Linux Server 6.x 32 位/64 位
- SUSE Linux Enterprise Desktop 12 (所有服务包) 64 位
- SUSE Linux Enterprise Desktop 15 (所有服务包) 64 位
- SUSE Linux Enterprise Desktop 15 (Service Pack 3) ARM 64 位
- openSUSE 15 64 位
- EulerOS 2.0 SP8 ARM
- Pardus OS 19.1 64 位
- Astra Linux Special Edition 1.5 64 位
- Astra Linux 特别版 RUSB.10152-02（操作更新4.7）ARM 64 位
- ALT Workstation 9.2 32 位/64 位
- ALT Workstation 10 32 位/64 位
- ALT 8 SP Workstation (LKNV.11100-01) 32 位/64 位
- ALT 8 SP Workstation (LKNV.11100-02) 32 位/64 位
- ALT 8 SP Workstation (LKNV.11100-03) 32 位/64 位
- Mageia 4 32 位
- Linux Mint 19.x 32 位
- Linux Mint 20.x 64 位
- AlterOS 7.5 及更高版本 64 位
- RED OS 7.3 64 位
- GosLinux IC6 64 位
- ROSA Enterprise Linux Server 7.3 64 位
- ROSA Enterprise Linux Desktop 7.3 64 位
- ROSA COBALT Workstation 7.3 64 位
- ROSA COBALT Server 7.3 64 位
- ROSA CHROME 12 64 位
- Lotos (Linux 核心版本 4.19.50, DE: MATE) 64 位

不支持的操作系统和平台。网络代理

不支持以下操作系统：

- Microsoft Windows Embedded POSReady 7 32 位/64 位
- Microsoft Windows Embedded 8 标准版 32 位/64 位
- Microsoft Windows Embedded 8 Industry Pro 32 位/64 位
- Microsoft Windows Embedded 8 Industry Enterprise 32 位 / 64 位
- Microsoft Windows Embedded 8.1 工业企业版 32 位/64 位
- Microsoft Windows Embedded 8.1 工业更新版 32 位/64 位
- Microsoft Windows 10 Home (Threshold 1, 1507) 32 位/64 位
- Microsoft Windows 10 Pro (Threshold 1, 1507) 32 位/64 位
- Microsoft Windows 10 Enterprise (Threshold 1, 1507) 32 位/64 位
- Microsoft Windows 10 Education (Threshold 1, 1507) 32 位/64 位
- Microsoft Windows 10 Mobile (Threshold 1, 1507) 32 位
- Microsoft Windows 10 Mobile Enterprise (Threshold 1, 1507) 32 位
- Microsoft Windows 10 Home Threshold 2（2015 年 11 月更新，1511）32 位/64 位
- Microsoft Windows 10 Pro Threshold 2（2015 年 11 月更新，1511）32 位/64 位
- Microsoft Windows 10 Enterprise Threshold 2（2015 年 11 月更新，1511）32 位/64 位
- Microsoft Windows 10 Education Threshold 2（2015 年 11 月更新，1511）32 位/64 位
- Microsoft Windows 10 Mobile Threshold 2（2015 年 11 月更新，1511）32 位
- Microsoft Windows 10 Mobile Enterprise Threshold 2（2015 年 11 月更新，1511）32 位
- Microsoft Windows 10 Home RS1 (Anniversary Update, 1607) 32 位/64 位
- Microsoft Windows 10 Pro RS1 (Anniversary Update, 1607) 32 位/64 位
- Microsoft Windows 10 Enterprise RS1 (Anniversary Update, 1607) 32 位/64 位
- Microsoft Windows 10 Education RS1 (Anniversary Update, 1607) 32 位/64 位
- Microsoft Windows 10 Mobile RS1 (Anniversary Update, 1607) 32 位
- Microsoft Windows 10 Mobile Enterprise RS1 (Anniversary Update, 1607) 32 位
- Microsoft Windows 10 Home RS2 (Creators Update, 1703) 32 位/64 位

- Microsoft Windows 10 Pro RS2 (Creators Update, 1703) 32 位/64 位
- Microsoft Windows 10 Enterprise RS2 (Creators Update, 1703) 32 位/64 位
- Microsoft Windows 10 Education RS2 (Creators Update, 1703) 32 位/64 位
- Microsoft Windows 10 Mobile RS2 (Creators Update, 1703) 32 位
- Microsoft Windows 10 Mobile Enterprise RS2 (Creators Update, 1703) 32 位
- Microsoft Windows 10 Mobile RS3 32 位
- Microsoft Windows 10 Mobile Enterprise RS3 32 位
- Microsoft Windows 10 Mobile RS4 32 位
- Microsoft Windows 10 Mobile Enterprise RS4 32 位
- Microsoft Windows 10 Mobile RS5 32 位
- Microsoft Windows 10 Mobile Enterprise RS5 32 位
- Microsoft Windows 8 (Core) 32 位/64 位
- Microsoft Windows 7 专业版 32 位/64 位
- Microsoft Windows 7 企业版/旗舰版 32 位/64 位
- Microsoft Windows 7 Home Basic/Premium 32 位/64 位
- Microsoft Windows Vista Business with Service Pack 1 32 位/64 位
- Microsoft Windows Vista Enterprise with Service Pack 1 32 位/64 位
- Microsoft Windows Vista Ultimate with Service Pack 1 32 位/64 位
- Microsoft Windows Vista Business with Service Pack 2 及更高版本 32 位/64 位
- Microsoft Windows Vista Enterprise with Service Pack 2 及更高版本 32 位/64 位
- Microsoft Windows Vista Ultimate with Service Pack 2 及更高版本 32 位/64 位
- Microsoft Windows XP Professional with Service Pack 2 32 位/64 位
- Microsoft Windows XP Home Service Pack 3 及更高版本 32 位
- Windows Essential Business Server 2008 Standard 64 位
- Windows Essential Business Server 2008 Premium 64 位
- Windows Small Business Server 2003 Standard with Service Pack 1 32 位
- Windows Small Business Server 2003 Premium with Service Pack 1 32 位
- Windows Small Business Server 2003 R2 Standard 32 位

- Windows Small Business Server 2003 R2 Premium 32 位
- Windows Small Business Server 2008 Standard 64 位
- Windows Small Business Server 2008 Premium 64 位
- Windows Small Business Server 2011 Standard 64 位
- Windows Small Business Server 2011 Premium Add-on 64 位
- Windows Small Business Server 2011 Essentials 64 位
- Windows Home Server 2011 64 位
- Windows MultiPoint Server 2010 Standard 64 位
- Windows MultiPoint Server 2010 Premium 64 位
- Windows MultiPoint Server 2012 Standard/Premium 64 位
- Microsoft Windows 2000 Server 32 位
- Windows Server 2003 Enterprise with Service Pack 2 32 位/64 位
- Windows Server 2003 Standard with Service Pack 2 32 位/64 位
- Windows Server 2003 R2 Enterprise with Service Pack 2 32 位/64 位
- Windows Server 2003 R2 Standard with Service Pack 2 32 位/64 位
- Windows Server 2008 Datacenter Service Pack 1 32 位/64 位
- Windows Server 2008 Enterprise with Service Pack 1 32 位/64 位
- Windows Server 2008 Service Pack 1 Server Core 32 位/64 位
- Windows Server 2008 Standard with Service Pack 1 32 位/64 位
- Windows Server 2008 Standard 32 位/64 位
- Windows Server 2008 Enterprise 32 位/64 位
- Windows Server 2008 Datacenter 32 位/64 位
- Windows Server 2008 R2 Server Core 64 位
- Windows Server 2008 R2 Datacenter 64 位
- Windows Server 2008 R2 Enterprise 64 位
- Windows Server 2008 R2 Foundation 64 位
- Windows Server 2008 R2 Standard 64 位
- Windows Server 2016 Nano（安装选项）(CBB)

- Windows Storage Server 2008 32 位/64 位
- Windows Storage Server 2008 Service Pack 2 64 位
- Windows Storage Server 2008 R2 64 位
- Windows Storage Server 2012 64 位
- Windows Storage Server 2012 R2 64 位
- Windows Storage Server 2016 64 位
- Windows Storage Server 2019 64 位
- Debian GNU/Linux 9.x (Stretch) 32 位/64 位
- Debian GNU/Linux 7.x（最高 7.8）32 位/64 位
- Debian GNU/Linux 8.x (Jessie) 32 位/64 位
- Ubuntu Server 14.04 LTS (Trusty Tahr) 32 位/64 位
- Ubuntu Server 16.04 LTS (Xenial Xerus) 32 位/64 位
- Ubuntu Server 20.04.04 LTS (Focal Fossa) ARM 64 位
- Ubuntu Desktop 14.04 LTS (Trusty Tahr) 32 位/64 位
- Ubuntu Desktop 16.04 LTS (Xenial Xerus) 32 位/64 位
- Ubuntu Desktop 18.04 LTS (Bionic Beaver) 32 位/64 位
- Ubuntu Desktop 20.04 LTS (Focal Fossa) 32 位/64 位
- CentOS 6.x (至 6.6) 64 位
- CentOS 7.x ARM 64 位
- CentOS 8.x 64 位
- SUSE Linux Enterprise Desktop 12（所有服务包）64 位
- SUSE Linux Enterprise Desktop 15 (所有服务包) 64 位
- Astra Linux Special Edition 1.5 64 位
- Astra Linux 特别版 RUSB.10265-01（操作更新 8.1）Elbrus
- Astra Linux 特别版 RUSB.10015-16（操作更新 8.1）Elbrus
- Pardus OS 19.1 64 位
- Linux Mint 19.x 32 位
- Lotos (Linux 核心版本 4.19.50, DE: MATE) 64 位

- ROSA Enterprise Linux Server 7.3 64 位
- ROSA Enterprise Linux Desktop 7.3 64 位
- ROSA COBALT Workstation 7.3 64 位
- ROSA COBALT Server 7.3 64 位

不支持以下虚拟化平台：

- VMware vSphere 4.1
- VMware vSphere 5.0
- VMware vSphere 5.1
- VMware vSphere 5.5
- VMware vSphere 6
- VMware vSphere 6.5
- VMware Workstation 9.x
- VMware Workstation 10.x
- VMware Workstation 11.x
- VMware Workstation 12.x Pro
- VMware Workstation Pro 14
- VMware Workstation Pro 15
- Microsoft Hyper-V Server 2008 64 位
- Microsoft Hyper-V Server 2008 R2 64 位
- Microsoft Hyper-V Server 2008 R2 Service Pack 1 及更高版本 64 位
- Citrix XenServer 6.0
- Citrix XenServer 6.1
- Citrix XenServer 6.2
- Citrix XenServer 6.5
- Citrix XenServer 7

分发包

您可以通过 Kaspersky 的在线商店（例如，https://www.kaspersky.com.cn）或其合作伙伴公司购买应用程序。

如果您在在线商店购买 Kaspersky Security Center Linux，则可以从该商店的网站复制程序。支付后，程序激活所需的信息会通过邮件发送给您。

About compatibility of Administration Server and Kaspersky Security Center Web Console

We recommend that you use the latest version of both Kaspersky Security Center Linux Administration Server and Kaspersky Security Center Web Console. Otherwise, the functionality of Kaspersky Security Center Linux may be limited.

You can install and upgrade Kaspersky Security Center Linux Administration Server and Kaspersky Security Center Web Console independently. In this case you should ensure that the version of the installed Kaspersky Security Center Web Console is compatible with the version of the Administration Server to which you connect:

- Web Console included in Kaspersky Security Center Linux 15 supports Kaspersky Security Center Linux Administration Server of the following versions: 15 and 14.2.
- Administration Server included in Kaspersky Security Center Linux 15 supports Kaspersky Security Center Web Console of the following versions: 15 and 14.2.

Comparison of Kaspersky Security Center: Windows-based vs. Linux-based

Kaspersky provides Kaspersky Security Center as an on-premises solution for two platforms—Windows and Linux. In the Windows-based solution, you install Administration Server on a Windows device, and the Linux-based solution has the Administration Server version that is designed to be installed on a Linux device. This Online Help contains information about Kaspersky Security Center Linux. For detailed information about the Windows-based solution, refer to the Kaspersky Security Center Windows Online Help.

The table below lets you compare the main features of Kaspersky Security Center as a Windows-based solution and as a Linux-based solution.

Feature comparison of Kaspersky Security Center working as a Windows-based solution and Linux-based solution

Feature or property	Kaspersky Security Center 14.2 Windows	Kaspersky Security Center 15 Linux
Administration Server location	On-premises	On-premises
Database management system (DBMS) location	On-premises	On-premises
Operating system to install Administration Server on	Windows	Linux
Administration console type	On-premises and web-based	Web-based
Operating system to install the web-based administration console on	Windows or Linux	Linux
Hierarchy of Administration Servers	✓	✓
Administration group hierarchy	✓	✓

Network polling	✓	✓ (by IP ranges and domain controllers, Samba 4 Active Directory, Microsoft Active Directory)
Maximum number of managed devices	100,000	50,000 (with PostgreSQL and Postgres Pro)
Protection of Windows, macOS, and Linux-managed devices	✓	✓
Protection of mobile devices	✓	–
Protection of virtual machines	✓	✓
Protection of public cloud infrastructure	✓	–
Device-centric security management	✓	✓
User-centric security management	✓	✓
Application policies	✓	✓
Tasks for Kaspersky applications	✓	✓
Kaspersky Security Network	✓	✓
KSN Proxy	✓	✓
Kaspersky Private Security Network	✓	✓
Centralized deployment of license keys for Kaspersky applications	✓	✓
Updating anti-virus databases automatically	✓	✓
Support for virtual Administration Servers	✓	✓
Installing third-party software updates and fixing third-party software vulnerabilities	✓	– (by using a remote installation task only)
Notifications about events that occurred on managed devices	✓	✓
Creating and managing user accounts	✓	✓
Sign-in to the console by using domain authentication	✓	✓ (Single Sign-on is currently not supported)
Integration with SIEM systems	✓	✓ (by using Syslog only)
Monitoring the policies and tasks status	✓	✓
Deployment of the Kaspersky Security Center failover cluster	✓	✓
Installing Administration Server on a Windows Server failover cluster	✓	–
Using SNMP to send Administration Server statistics to third-party applications	✓	–
Remote diagnostics of client devices	✓	✓
Remote connection to the desktop of a client device	✓	–

Managing object revisions	✓	–
Updating Kaspersky applications automatically	✓	–
Deployment of operating systems on client devices	✓	–
Web Server for publishing installation packages and other files	✓	–
Viewing and working with alerts detected by Kaspersky Endpoint Detection and Response Optimum	✓	✓
Using Administration Server as WSUS server	✓	–
Integration with Kaspersky Managed Detection and Response	✓	–
Support for Adaptive Anomaly Control	✓	–
Support of clusters and server arrays in administration groups	✓ (in MMC-based Administration Console only)	✓
Managing third-party licenses	✓	–

About Kaspersky Security Center Cloud Console

Using Kaspersky Security Center as an on-premises application means that you install Kaspersky Security Center, including Administration Server, on a local device and manage the network security system through the Microsoft Management Console-based Administration Console or Kaspersky Security Center Web Console.

However, you can use Kaspersky Security Center as a cloud service instead. In this case Kaspersky Security Center is installed and maintained for you by Kaspersky experts in the cloud environment, and Kaspersky gives you access to the Administration Server as a service. You manage the network security system through the cloud-based Administration Console named Kaspersky Security Center Cloud Console. This console has an interface similar to the interface of Kaspersky Security Center Web Console.

The interface and documentation of Kaspersky Security Center Cloud Console are available in the following languages:

- English
- French
- German
- Italian
- Japanese
- Portuguese (Brazil)
- Russian

- Simplified Chinese
- Spanish
- Spanish (LATAM)
- Traditional Chinese

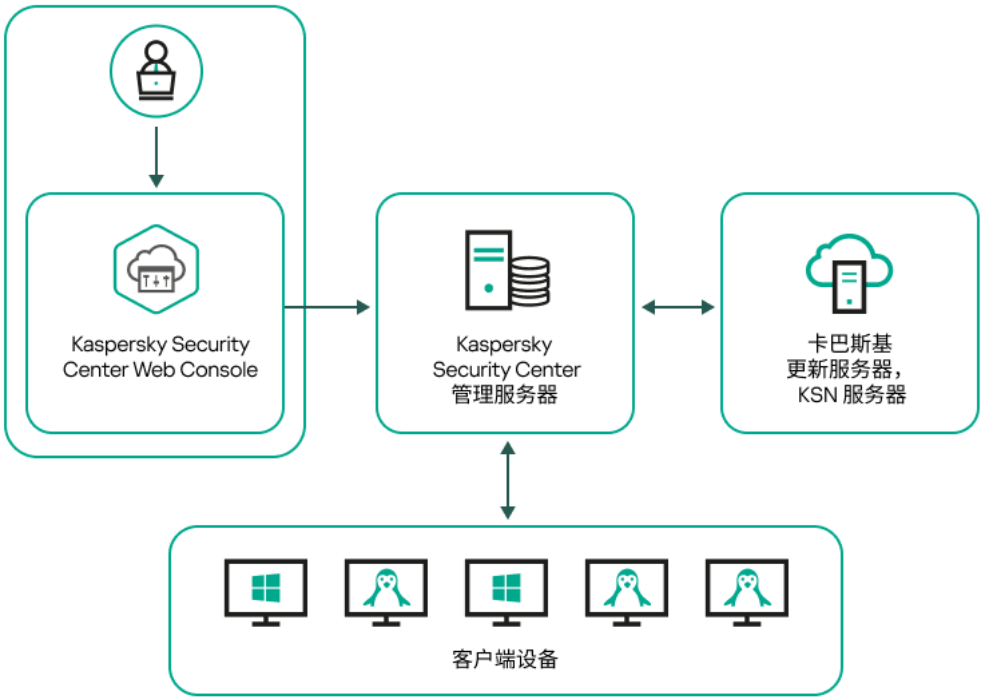
More information about Kaspersky Security Center Cloud Console and its features is available in the Kaspersky Security Center Cloud Console documentation and in the Kaspersky Endpoint Security for Business documentation.

架构和基本概念

本部分解释与 Kaspersky Security Center Linux 有关的架构和基本概念。

架构

该部分提供了对 Kaspersky Security Center 组件和其交互的描述。



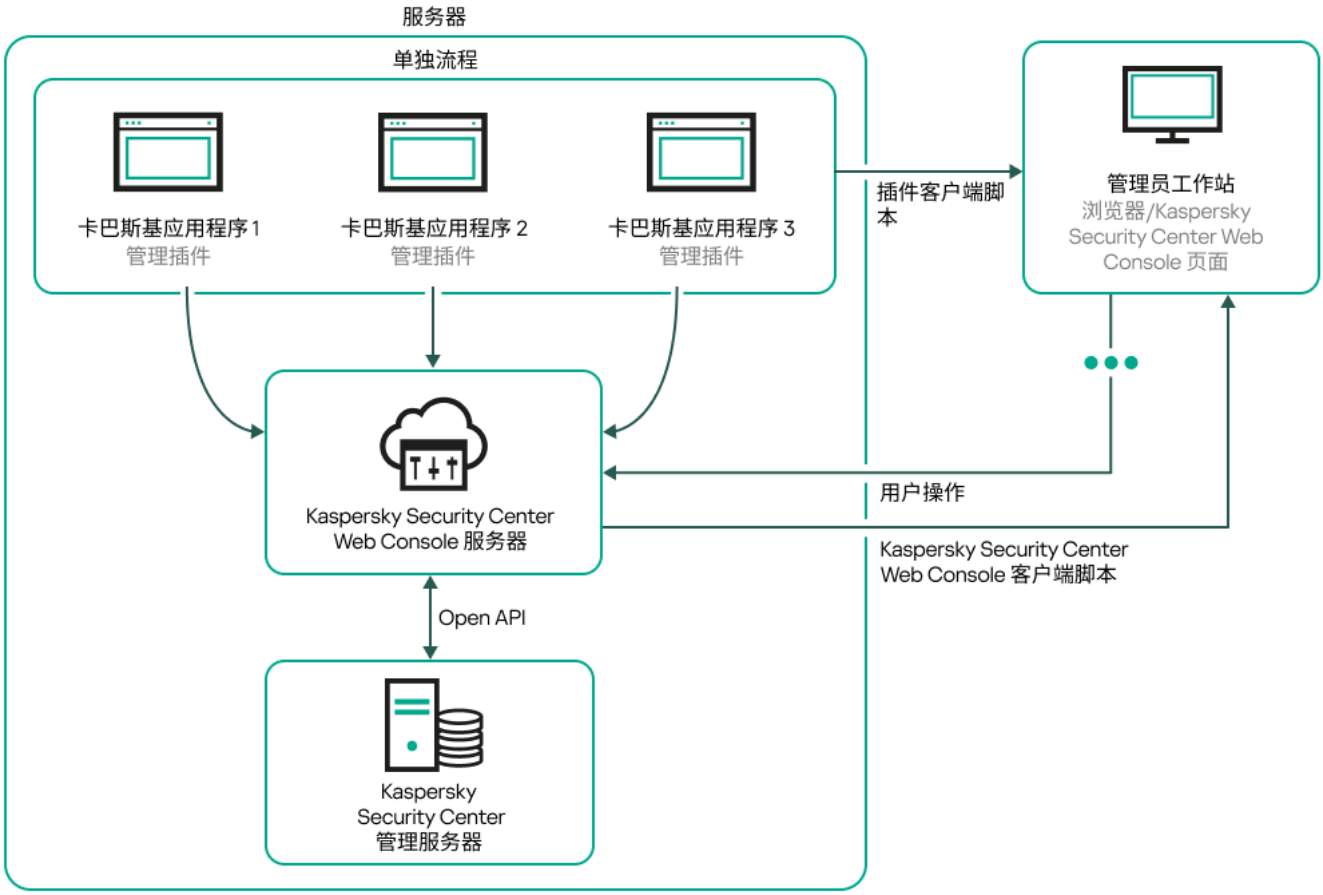
Kaspersky Security Center Linux 架构

Kaspersky Security Center Linux 包括以下主要组件：

- **Kaspersky Security Center Web Console**。提供 Web 界面以创建和维护由 Kaspersky Security Center 管理的客户端组织网络的保护系统。
- **Kaspersky Security Center 管理服务器**（也称为"*服务器*"）。集中管理组织网络中所安装应用程序的信息存储，并包含如何管理这些应用程序的信息。
- **Kaspersky 更新服务器**。Kaspersky 程序可以从 Kaspersky 的 HTTP(S) 服务器下载数据库和应用程序模块更新。
- **KSN 服务器**。包含 Kaspersky 数据库的服务器，该数据库中包含持续更新的文件、网络资源和软件信誉信息。卡巴斯基安全网络确保在遇到新型威胁时 Kaspersky 程序能够做出更快速的响应，提高某些保护组件的性能并降低误报的可能性。
- **客户端设备**。受 Kaspersky Security Center Linux 保护的客户公司设备。每台需要保护的设备都必须安装一个 Kaspersky 安全应用程序。

Kaspersky Security Center Linux 管理服务器部署图表和 Kaspersky Security Center Web Console

下图显示 Kaspersky Security Center Linux 管理服务器部署图表和 Kaspersky Security Center Web Console。



Kaspersky Security Center Linux 管理服务器部署图表和 Kaspersky Security Center Web Console

安装到受保护设备上的 Kaspersky 应用程序管理插件（每个应用程序一个插件）与 Kaspersky Security Center Web Console 服务器一起部署。

作为管理员，您通过使用工作站浏览器来访问 Kaspersky Security Center Web Console。

当您在 Kaspersky Security Center Web Console 执行特定操作时，Kaspersky Security Center Web Console 服务器通过 OpenAPI 与 Kaspersky Security Center Linux 管理服务器交互。Kaspersky Security Center Web Console 服务器从 Kaspersky Security Center Linux 管理服务器请求所需信息并在 Kaspersky Security Center Web Console 显示您的操作结果。

Kaspersky Security Center Linux 使用的端口

下表显示了在管理服务器和客户端设备上必须开放的默认端口。如果需要，可以更改这些默认端口号。

Kaspersky Security Center Linux 管理服务器使用的端口

端口号	打开端口的进程名称	协议	端口目的	范围
8060	klcsweb	TCP	传输发布的安装包到客户端设备	发布安装包。 您可以在管理服务器属性窗口的“**Web 服务器**”区域中更改默认端口号。
8061	klcsweb	TCP (TLS)	传输发布的安装包到客户端设备	发布安装包。 您可以在管理服务器属性窗口的“**Web 服务器**”区域中更改默认端口号。

13000	klserver	TCP (TLS)	从网络代理和从属管理服务器接收连接；也用于在从属管理服务器上从主管理服务器接收连接（例如，如果从属管理服务器在 DMZ 中）	管理客户端设备和从属管理服务器。 在安装 Kaspersky Security Center Linux 期间配置连接端口时，可以更改用于接收网络代理连接的默认端口号；您可以在创建管理服务器层级时更改用于接收从属管理服务器连接的默认端口号。
13000	klserver	UDP	接收从网络代理关闭的设备的信息	管理客户端设备。 您可以在网络代理策略设置中更改默认端口号。
13299	klserver	TCP (TLS)	接收从 Kaspersky Security Center Web Console 到管理服务器的连接；接收通过 OpenAPI 到管理服务器的连接	Kaspersky Security Center Web Console，OpenAPI。 您可以在管理服务器属性窗口（“**常规**”区域的“**连接端口**”子区域中）或在创建管理服务器层级时更改默认端口号。
14000	klserver	TCP	接收从网络代理的连接	管理客户端设备。 您可以在安装 Kaspersky Security Center Linux 期间配置连接端口时更改默认端口号，或在手动连接客户端设备到管理服务器时进行更改。
13111（仅当设备上运行 KSN 代理服务时）	ksnproxy	TCP	接收从受管理设备到 KSN 代理服务器的请求	KSN 代理服务器。 您可以在管理服务器属性窗口中更改默认端口号。
15111（仅当设备上运行 KSN 代理服务时）	ksnproxy	UDP	接收从受管理设备到 KSN 代理服务器的请求	KSN 代理服务器。 您可以在管理服务器属性窗口中更改默认端口号。
17000	klactprx	TCP (TLS)	接收受管理设备的应用程序激活连接	用于受管理设备的激活代理服务器。 您可以在管理服务器属性窗口（“**常规**”区域的“**附加端口**”子区域中）中更改默认端口号。
19170	klserver	HTTPS (TLS)	使用 klsctunnel 实用程序建立与受管理设备的隧道连接	使用 Kaspersky Security Center Web Console 远程连接到受管理设备。 您可以使用 klscflag 实用程序更改默认端口号。

如果您在不同设备上安装管理服务器和数据库，则必须使数据库所在设备的必要端口可用（例如，端口 3306 用于 MariaDB）。请参阅 DBMS 文档以获取相关信息。

下表显示了 Kaspersky Security Center Web Console 服务器上必须开放的端口。它可以是安装了管理服务器的同一设备，也可以是其他设备。

Kaspersky Security Center Web Console 服务器使用的端口

端口号	打开端口的进程名称	协议	端口目的	范围

8080	Node.js：服务器端 JavaScript	TCP (TLS)	接收从浏览器到 Kaspersky Security Center Web Console 的连接	Kaspersky Security Center Web Console。 您可以在安装 Kaspersky Security Center Web Console 时更改默认端口号。在 Linux ALT 操作系统上安装 Kaspersky Security Center Web Console 时，必须指定除 8080 以外的端口号，因为端口 8080 被操作系统使用。

下表显示了安装网络代理的受管理设备上必须开放的端口。

网络代理使用的端口

端口号	打开端口的进程名称	协议	端口目的	范围
15000	klnagent	UDP	从管理服务器或者分发点到网络代理的管理信号	管理客户端设备。 您可以在网络代理策略设置中更改默认端口号。
15000	klnagent	UDP 广播	获取有关同一广播域内其他网络代理的数据（然后将数据发送到管理服务器）	传送更新和安装包。
15001	klnagent	UDP	接收来自分发点的多播请求（如果正在使用）	从分发点接收更新和安装包。 您可以在分发点属性窗口中更改默认端口号。

请注意，klnagent 进程也可以从端点操作系统的动态端口范围请求空闲端口。这些端口是由操作系统自动分配给 klnagent 进程的，所以 klnagent 进程可以使用一些已经被其他软件使用的端口。如果 klnagent 进程影响软件操作，请更改此软件中的端口设置，或更改操作系统中的默认动态端口范围以排除受影响的软件使用的端口。

另请注意，有关 Kaspersky Security Center Linux与第三方软件的兼容性的建议仅供参考，可能不适用于新版本的第三方软件。所描述的端口配置建议基于技术支持人员的经验和我们的最佳实践。

下表显示了安装了网络代理用作分发点的受管理设备上必须开放的端口。除了网络代理使用的端口，还必须在分发点设备上开放列出的端口（请参见上表）。

用作分发点的网络代理使用的端口

端口号	打开端口的进程名称	协议	端口目的	范围
13000	klnagent	TCP (TLS)	从网络代理和连接网关接收连接	管理客户端设备、传送更新和安装包。 您可以在分发点属性中更改默认端口号。
13111（仅当设备上运行 KSN 代理服务时）	ksnproxy	TCP	接收从受管理设备到 KSN 代理服务器的请求	KSN 代理服务器。 您可以在分发点属性中更改默认端口号。
15111（仅当设备上运行 KSN 代理服务时）	ksnproxy	UDP	接收从受管理设备到 KSN 代理服务器的请求	KSN 代理服务器。 您可以在分发点属性中更改默认端口号。

Ports used by Kaspersky Security Center Web Console

The table below lists the ports that must be open on the device where Kaspersky Security Center Web Console Server (also referred to as Kaspersky Security Center Web Console) is installed.

Port number	Service name	Protocol	Port purpose	Scop
2001	KSCWebConsolePlugin	HTTPS	API port that is used by the management plug-in processes to receive requests from the KSCWebConsoleManagementService	Running node process manage plug-ins
1329, 2003	KSCWebConsoleManagementService	HTTPS	API ports that are used to receive requests from the KSCWebConsoleManagementService running on the same device	Updatin Kaspers Security Center Console compon
2005	KSCWebConsole	HTTPS	API port that is used to receive requests from the KSCWebConsoleManagementService service running on the same device	Running node process Kaspers Security Center Console
8200	–	HTTP	API port that is used to generate certificates by means of HashiCorp Vault (for more details, see the HashiCorp Vault website)	Installing Kaspers Security Center Console updatin Kaspers Security Center Console compon
4150, 4151, 4152	KSCWebConsoleMessageQueue	HTTPS	API ports of the Message Broker that are used for communication between processes of both Kaspersky Security Center Web Console and management plug-ins	Interact betwee Kaspers Security Center Console manage plug-ins

基本概念

本部分解释与 Kaspersky Security Center Linux 有关的基本概念。

管理服务器

使用 Kaspersky Security Center 组件可远程管理客户端设备上安装的 Kaspersky 应用程序。

安装了管理服务器组件的设备将被称作*管理服务器*（也称作*服务器*）。管理服务器必须被保护，包括物理保护，以防范非授权的访问。

管理服务器作为服务安装在设备上，且拥有以下属性集：

- 名称为“Kaspersky Security Center 管理服务器”
- 设置为在操作系统启动时自动启动
- 具有“**LocalSystem**”账户或在安装管理服务器过程中选择的用户账户

管理服务器执行以下功能：

- 存储管理组结构
- 存储有关客户端设备配置的信息
- 应用程序分发包的存储结构
- 将应用程序远程安装至客户端设备和远程卸载应用程序
- 更新 Kaspersky 应用程序的应用程序数据库和软件模块
- 管理客户端设备上的策略和任务
- 存储有关客户端设备上已发生事件的信息
- 生成有关 Kaspersky 应用程序操作的报告
- 向客户端设备部署授权许可密钥并存储授权许可密钥信息
- 转发有关任务进度的通知（例如在客户端设备上检测到病毒）

在应用程序界面中命名管理服务器

在 Kaspersky Security Center Web Console 的界面中，管理服务器可以具有以下名称：

- 管理服务器设备的名称，例如：“*设备名称*”或“管理服务器：*设备名称*”。
- 管理服务器设备的 IP 地址，例如：“*IP 地址*”或“管理服务器：*IP 地址*”。
- 从属管理服务器和虚拟管理服务器具有自定义名称，这些名称是您在将虚拟或从属管理服务器连接到主管理服务器时指定的。
- 如果您使用 Linux 设备上安装的 Kaspersky Security Center Web Console，则该应用程序将显示您在响应文件中指定的受信任管理服务器的名称。

您可以使用 Kaspersky Security Center Web Console 连接到管理服务器。

管理服务器层级

管理服务器可以排列在层级中。在该层次结构的不同嵌套级别上，每个管理服务器都可以拥有多个从属管理服务器（称为*从属服务器*）。从属服务器的嵌套级别不受限制。这样，主管理服务器的管理组将会包括所有从属管理服务器的客户端设备。因而，网络的隔离和独立区段可以通过不同的管理服务器进行管理，而后者又通过主服务器进行管理。

在层次结构中，基于 Linux 的管理服务器既可以作为主服务器也可以作为辅助服务器。基于 Linux 的主服务器可以管理基于 Linux 和基于 Windows 的辅助服务器。基于 Windows 的主服务器可以管理基于 Linux 的辅助服务器。

*虚拟管理服务器*是从属管理服务器的一个特例。

您可以使用管理服务器的层次结构执行以下操作：

- 降低管理服务器的负载（与整个网络中安装的单个管理服务器相比）。
- 减少 Intranet 流量并简化远程办公室的工作。您不必在主管理服务器和所有网络设备（例如，它们可能位于不同地区）之间建立连接。只需在每个网络节点中安装从属管理服务器，在从属服务器的各个管理组中分发设备，以及通过快速通信通道在从属服务器和主服务器之间建立连接。
- 在反病毒安全管理员之间分配责任。用于集中管理和监控企业网络中的反病毒安全状态的所有功能仍然可用。
- 服务提供商使用 Kaspersky Security Center。服务提供商只需安装 Kaspersky Security Center 和 Kaspersky Security Center Web Console。为了管理大量的多个组织的更多客户端设备，服务提供商可以向管理服务器层级中添加从属管理服务器（包括虚拟服务器）。

管理组层次结构中包括的每台设备都只能连接到一个管理服务器。您必须独立监控设备到管理服务器的连接。使用这些功能可以根据网络属性在不同服务器的管理组中搜索设备。

虚拟管理服务器

虚拟管理服务器（下文也称作*虚拟服务器*）是 Kaspersky Security Center Linux 的一个组件，用于管理客户端阻止网络的反病毒保护系统。

虚拟管理服务器是从属管理服务器的特例，与物理管理服务器相比，具有以下限制：

- 只能在主管理服务器上创建虚拟管理服务器。
- 虚拟管理服务器在其操作中使用主管理服务器数据库。虚拟管理服务器不支持数据备份和还原任务以及更新扫描和下载任务。
- 虚拟服务器不支持从属管理服务器（包括虚拟服务器）的创建。

此外，虚拟管理服务器具有以下限制：

- 在虚拟管理服务器属性窗口中，区域的数量是有限的。
- 要在虚拟管理服务器管理的客户端设备上远程安装 Kaspersky 应用程序，您必须确保已在其中一台客户端设备上安装网络代理，以确保与虚拟管理服务器通信。在第一次连接到虚拟管理服务器时，该设备会被自动分配为分发点，并充当客户端设备与虚拟管理服务器的连接网关。
- 虚拟服务器只能通过分发点进行网络轮询。

- 若要重启发生故障的虚拟服务器，Kaspersky Security Center Linux 需要重启主管理服务器和所有虚拟管理服务器。
- 在虚拟服务器上创建的用户无法在管理服务器上被分配角色。

虚拟管理服务器的管理员在该特定虚拟服务器上具有所有权限。

Web 服务器

Kaspersky Security Center *Web Server*（以下简称"*Web 服务器*"），是 Kaspersky Security Center 的一个组件，与管理服务器一同安装。Web 服务器用于通过网络传输独立安装包和共享文件夹的文件。

当您创建独立安装包时，它会自动发布在 Web 服务器上。已创建的独立安装包列表中会显示用于下载独立包的链接。必要时，您可以取消发布独立包或在 Web 服务器上重新发布。

共享文件夹专用于存储通过管理服务器所管理的所有设备用户的信息。如果用户无法直接访问共享文件夹，他/她可以通过 web 服务器的方式获取共享文件夹的信息。

要通过 web 服务器为用户提供共享文件夹的信息，管理员需要在共享文件夹中创建一个名为"public"的子文件夹并将相关信息复制至此。

信息传输链接的句法按以下格式：

`https://<Web 服务器名称>:<HTTPS 端口>/public/<对象>`

其中：

- `<Web 服务器名称>`为 Kaspersky Security Center Web Server 的名称。
- `<HTTPS 端口>`为由管理员定义的 Web 服务器的 HTTPS 端口。HTTPS 端口可以在管理服务器属性窗口的"**Web 服务器**"区域设置。默认端口号是 8061。
- `<对象>`是用户可以访问的子文件夹或文件。

管理员可以通过任意方式如电子邮件等将新链接发送给用户。

通过单击链接，用户可将所需信息下载至本地设备。

网络代理

管理服务器和设备之间的交互由 Kaspersky Security Center Linux 的*网络代理*组件执行。网络代理必须安装在所有使用 Kaspersky Security Center Linux 来管理 Kaspersky 应用程序的设备上。

网络代理作为服务安装在设备上，且具有以下属性集：

- 名称为"Kaspersky Security Center 网络代理"
- 设置为在操作系统启动时自动启动
- 使用 LocalSystem 账户

安装了网络代理的设备被称为*受管理设备*或*设备*。您可以从以下来源之一安装网络代理：

- 管理服务器存储中的安装包（您必须安装了管理服务器）
- Kaspersky Web 服务器上的安装包

安装管理服务器时，网络代理的服务器版本会与管理服务器一起自动安装。尽管如此，若要像管理任何其他受管理设备一样管理管理服务器设备，请安装 Network Agent for Linux 在管理服务器设备上。在这种情况下，Network Agent for Linux 的安装和运行独立于网络代理的服务器版本，后者是与管理服务器一起安装的。

网络代理启动的进程的名称如下：

- klnagent64.service（对于 64 位操作系统）
- klnagent.service（对于 32 位操作系统）

网络代理同步管理服务器的受管理设备。我们建议您设置同步间隔（也叫*心跳*）为每 10,000 台受管理设备 15 分钟。

管理组

管理组（以下简称*组*）是受管理设备的逻辑集合，根据某一特征组合在一起以便作为 Kaspersky Security Center Linux 的一个单元来统一管理。

管理组内的所有受管理设备都被配置以做如下事情：

- 使用共同的应用程序设置（您可以在组策略中指定）。
- 通过以指定设置创建组任务，对所有应用程序使用通用的操作模式。组任务的例子包括创建和安装公用安装包、更新程序数据库和模块、按需扫描设备和启用实时保护。

受管理设备只能属于一个管理组。

您可以创建管理服务器和组的层级。单个层次结构级别可以包括从属和虚拟管理服务器、组和受管理设备。您可以从一个组移动设备到其他组，而不做物理移动。例如，如果企业员工的职位从会计变更为开发者，您可以将该员工的计算机从会计管理组移动到开发者管理组。然后，该计算机将自动接收开发者的应用程序设置。

受管理设备

*受管理设备*是运行 Linux 且安装了网络代理的计算机。您可以通过设备上安装的应用程序的任务和策略来管理此类设备。您也可以从受管理设备接收报告。

您可以让受管理设备作为分发点和连接网关来运行。

设备仅可以被一个管理服务器管理。一个管理服务器可以管理最多 20,000 台设备。

未分配的设备

*未分配的设备*是网络中未被包含在任何管理组中的设备。您可以在未分配设备上运行一些操作，例如，移动它们到管理组或在其上安装应用程序。

当在您的网络中发现新设备时，该设备转到"未分配的设备"管理组。您可以配置规则以便设备在被发现后被自动移动到其他管理组。

管理员工作站

安装了 Kaspersky Security Center Web Console 服务器的设备称为*管理员工作站*。管理员可以使用这些设备来远程集中管理客户端设备上安装的 Kaspersky 应用程序。

管理员工作站的数量不受限制。在任何管理员工作站中，都可以同时管理网络中多个管理服务器的管理组。您可以将管理员的工作站连接至层次结构任何级别的（物理或虚拟）管理服务器。

您可以将管理员的工作站作为客户端设备包括在管理组中。

在任何管理服务器的管理组中，同一台设备可以充当管理服务器客户端、管理服务器或管理员工作站。

管理 Web 插件

特殊组件 — *管理 Web 插件* — 通过 Kaspersky Security Center Web Console 对 Kaspersky 软件进行远程管理。在下文中，管理 Web 插件也称为*管理插件*。管理插件是 Kaspersky Security Center Web Console 与特定 Kaspersky 应用程序之间的接口。使用管理插件，您可以配置应用程序任务和策略。

您可以从卡巴斯基技术支持网页下载管理 Web 插件。

管理插件提供以下：

- 创建和编辑应用程序任务和设置的界面
- 用于创建和编辑策略和策略配置文件以便远程集中配置 Kaspersky 应用程序和设备的界面
- 应用程序事件传输
- Kaspersky Security Center Web Console 显示应用程序的操作数据和事件，以及从客户端设备转发的统计信息

策略

*策略*是应用于一个管理组和其子组的 Kaspersky 应用程序设置集。您可以在管理组的设备上安装多个 Kaspersky 应用程序。Kaspersky Security Center 为管理组中的每个 Kaspersky 应用程序提供一个策略。策略具有以下状态之一：

策略的状态

状态	描述
活动	应用于设备的当前策略。对于每个管理组中的 Kaspersky 应用程序，只能有一个策略处于活动状态。设备对 Kaspersky 应用程序应用活动策略的设置值。
非活动	当前未应用于设备的策略。

漫游	如果选择该选项，策略将在设备离开企业网络时变为活动状态。

策略根据以下规则发挥作用：

- 您可以为单个应用程序配置拥有不同值的多个策略。
- 对于当前应用程序，只能有一个策略处于活动状态。
- 策略可以有子策略。

通常，您可以将策略用作对紧急情况（如病毒攻击）的准备。例如，如果存在通过闪存驱动器进行的攻击，您可以激活相应策略来阻止访问闪存驱动器。在这种情况下，当前的活动策略将自动变为非活动状态。

为了防止维护多个策略，例如，在不同的场合下只是更改几个设置时，可以使用策略配置文件。

*策略配置文件*是策略设置值的命名子集，用于替换策略的设置值。策略配置文件影响受管理设备上有效设置的形成。*有效设置*是当前应用于设备的一组策略设置、策略配置文件设置和本地应用程序设置。

策略配置文件根据以下规则发挥作用：

- 当出现特定的激活情况时，策略配置文件生效。
- 策略配置文件包含的设置值与策略设置不同。
- 激活策略配置文件会更改受管理设备的有效设置。
- 一个策略可以包含最多 100 个策略配置文件。

策略配置文件

有时候有必要为不同的管理组创建单一策略的若干实例；您也可能想要集中修改这些策略的设置。这些实例实例可能仅有一两处设置不同。例如，企业中所有的会计工作在相同策略下 — 但是高级会计被允许使用闪存驱动器，而初级会计不被允许。此种情况下，仅通过管理组层级应用策略到设备可能不方便。

要帮助您避免创建单一策略的多个实例，Kaspersky Security Center Linux 允许您创建*策略配置文件*。策略配置文件用于在单一管理组中的设备在不同策略设置下运行时。

策略配置文件是策略设置的命名子集。该子集随带策略在大设备上分发，在特别条件*配置文件激活条件*下将其补充。配置文件仅包含与"基本"策略不同的设置，并在受管理设备上活动。配置文件的激活将修改在设备上最初活动的"基本"策略的设置。修改的设置将使用已在配置文件中指定的值。

任务

Kaspersky Security Center Linux 通过创建和运行*任务*来管理设备上安装的 Kaspersky 应用程序。安装、启用和停用程序、扫描文件、更新数据库和软件模块以及程序的其他操作均需要任务。

特定应用程序的任务仅在安装了该应用程序的管理插件时可以被创建。

任务可以在管理服务器和设备上执行。

以下任务在管理服务器上执行：

- 自动分发报告
- 将更新下载至管理服务器存储库
- 备份管理服务器数据
- 数据库维护
- 基于参考设备的操作系统镜像创建安装包

以下类型的任务在设备上执行：

- *本地任务* — 在特定设备上执行的任务。

  本地任务可以由管理员使用 Kaspersky Security Center Web Console 修改，或者由远程设备用户修改（例如，通过安全应用程序界面）。如果本地任务同时被管理员和受管理设备用户修改，管理员的修改将生效，因为其具有更高优先级。

- *组任务* — 在特定组的所有设备上执行的任务。

  除非在任务属性中指定了其他项，组任务也影响所选组的所有子组。组任务还影响（可选）已连接到部署在该组或其任意子组中的从属和虚拟管理服务器的设备。

- *全局任务* — 在一组设备上执行的任务，与设备是否包含在某个组中无关。

您可以为每个应用程序创建不管多少个组任务、全局任务或本地任务。

您可以更改任务设置、查看任务进度、复制、导出、导入和删除任务。

仅当为其创建任务的应用程序在运行时，才能在设备上启动任务。

任务结果保存在 Syslog 事件日志和 Kaspersky Security Center Linux 事件日志中，既集中在管理服务器上，又位于每个设备上。

不在任务设置中包括私人数据。例如，避免指定域管理员密码。

任务范围

*任务范围*是执行任务的设备集合。范围的类型包括以下：

- 对于*本地任务*，范围是设备本身。
- 对于*管理服务器任务*，范围是管理服务器。
- 对于*组任务*，范围是包含在组中的设备列表。

当创建*全局任务*时，您可以使用以下方法指定范围：

- 手动指定特定设备。

您可以使用 IP 地址（或 IP 范围）或 DNS 名称作为设备地址。

- 从包含有要添加的设备地址的 .txt 文件来导入设备列表（每一个计算机地址必须单独一行）。

  如果通过文件导入设备列表或手动创建设备列表，且如果设备是以名称定义，则列表可以只包含其信息已被输入到管理服务器数据库中的设备。而且，信息必须在设备被连接或设备发现中输入。

- 指定设备分类。

  后续，任务范围随着包含在分类中的设备集的更改而更改。设备分类可以基于设备属性（包含安装在设备上的软件）创建，也可以基于分配到设备的标签来创建。设备分类是指定任务范围的最灵活的方法。

  设备分类的任务总是按管理服务器计划运行。这些任务无法运行在缺少管理服务器连接的设备上。使用其他方法指定范围的任务直接运行在设备上，且因此不取决于到管理服务器的设备连接。

  设备分类的任务不会按设备本地时间运行；相反，它们将按照管理服务器本地时间运行。使用其他方法指定范围的任务以设备本地时间运行。

本地应用程序设置与策略的关系

您可以使用策略为组中的所有设备设置完全相同的应用程序设置值。

使用本地应用程序设置可以为组中的各个设备重新定义策略指定的设置值。您只能设置策略允许修改的设置的值，即解锁设置的值。

应用程序在客户端设备上使用的设置的值由策略中该设置的锁定位置（🔒）确定：

- 如果设置修改被锁定，则在所有客户端设备中使用策略中定义的相同值。
- 如果设置修改被“解锁”，则应用程序使用每台客户端设备上的本地设置值，而不是策略中指定的值。然后，您可以在本地应用程序设置中更改设置。

这意味着在客户端设备上运行任务时，应用程序以两种不同的方式使用所定义的设置：

- 如果没有锁定设置以避免策略更改，则通过任务设置和本地应用程序设置使用。
- 如果锁定设置以避免更改，则通过组策略使用。

在首先根据策略设置应用策略之后，才会更改本地应用程序设置。

分发点

分发点（先前称为“更新代理”）是指安装了网络代理的设备，用于分发更新、远程安装应用程序和检索联网设备信息。分发点可执行以下功能：

- 将从管理服务器接收到的更新和安装包分发到组中的客户端设备（包括使用 UDP 通过多播进行分发）。更新可以从管理服务器接收，或者从 Kaspersky 更新服务器获取。如果是后者，必须为分发点创建更新任务。

  分发点加速更新发布并释放管理服务器资源。

- 使用 UDP 通过多点传送分发策略和组任务。
- 用作管理组中的设备与管理服务器的连接网关。

如果组中的受管理设备与管理服务器之间的直接连接无法建立，则分发点可用作此组的管理服务器连接网关。在这种情况下，受管理设备将连接到连接网关，连接网关又连接到管理服务器。

用作连接网关的分发点的可用性不会阻止受管理设备与管理服务器之间的直接连接。如果连接网关不可用，但在技术上可与管理服务器进行直接连接，则受管理设备将直接连接到管理服务器。

- 轮询网络以检测新设备并更新现有设备的信息。分发点应用与管理服务器相同的设备发现方法。
- 执行卡巴斯基和其他软件供应商的应用程序的远程安装，包括在没有网络代理的客户端设备上安装。

  此功能允许将网络代理的安装包远程传输到位于管理服务器无直接访问权限的网络上的客户端设备。
- 作为代理服务器加入卡巴斯基安全网络 (KSN)。

  您可以在分发点端启用 KSN 代理服务器以使设备作为 KSN 代理服务器。此种情况下，KSN 代理服务在设备上运行。

文件通过 HTTP 或者 HTTPS 从管理服务器传输到分发点。使用 HTTP 或 HTTPS 促成更高性能，相比通过流量的 SOAP。

安装有网络代理的设备可以被手动（通过管理员）或自动（通过管理服务器）分配分发点。指定管理组的分发点的完整列表显示在关于分发点列表的报告中。

分发点的范围是管理员将其分配到其中的管理组，以及其所有嵌套级别的子组。如果已在管理组的层次结构中分配几个分发点，则受管理设备上的网络代理会连接到层次结构中最近的分发点。

如果分发点被管理服务器自动分配，它通过广播域分配，而不是通过管理组。此情况发生在所有广播域已知时。网络代理在相同的子网与其它网络代理交换信息并发送给管理服务器它的其它网络代理的信息。管理服务器可以用此信息通过广播域分组网络代理。在管理组中超过 70% 的网络代理被轮询后，广播域对管理服务器已知。管理服务器每两小时轮询一次广播域。分发点通过广播域分配后，就无法通过管理组重新分配。

如果管理员手动分配分发点，则可以将它们分配给管理组或网络位置。

带有活动连接配置文件的网络代理不参与广播域检测。

Kaspersky Security Center Linux 为每个网络代理分配一个不同于其他所有地址的唯一 IP 多播地址。这允许您避免由于 IP 重叠引起的网络过载。应用程序先前版本分配的 IP 多点传送地址将不被更改。

当两个或更多分发点分配在单独的网络区域或单独的管理组，其中一个会变成活动分发点，其余的变成备用分发点。活动分发点直接从管理服务器下载更新和安装包，备用分发点只从活动分发点接收更新。此种情况下，文件从管理服务器下载一次，然后在分发点之间发布。如果因为任何原因活动分发点不可用，其中一个备用分发点将变成活动的。管理服务器自动分配分发点做为备用。

分发点状态（*活动*/*备用*）通过 klnagchk 报告中的复选框进行显示。

一个分发点需要至少 4 GB 的可用磁盘空间。如果分发点的磁盘剩余空间少于 2 GB，Kaspersky Security Center Linux 将创建一个重要级别为“*警告*”的安全问题。安全问题将被发布在设备属性中，在**安全问题**区域。

在分配为分发点的设备上运行远程安装任务需要另外的可用磁盘空间。剩余磁盘空间卷必须超过安装包的总大小。

在分配为分发点的设备上运行任何更新（补丁）任务和漏洞修复任务需要另外的可用磁盘空间。剩余磁盘空间卷必须是至少两倍的要安装补丁的总大小。

作为分发点的设备必须被保护，包括物理保护，以防范非授权的访问。

Connection gateway

A *connection gateway* is a Network Agent acting in a special mode. A connection gateway accepts connections from other Network Agents and tunnels them to the Administration Server through its own connection with the Server. Unlike an ordinary Network Agent, a connection gateway waits for connections from the Administration Server rather than establishes connections to the Administration Server.

A connection gateway can receive connections from up to 10,000 devices.

You have two options for using connection gateways:

- We recommend that you install a connection gateway in a demilitarized zone (DMZ). For other Network Agents installed on out-of-office devices, you need to specially configure a connection to Administration Server through the connection gateway.

  A connection gateway does not in any way modify or process data that is transmitted from Network Agents to Administration Server. Moreover, it does not write this data into any buffer and therefore cannot accept data from a Network Agent and later forward it to Administration Server. If Network Agent attempts to connect to Administration Server through the connection gateway, but the connection gateway cannot connect to Administration Server, Network Agent perceives this as if Administration Server is inaccessible. All data remains on Network Agent (not on the connection gateway).

  A connection gateway cannot connect to Administration Server through another connection gateway. It means that Network Agent cannot simultaneously be a connection gateway and use a connection gateway to connect to Administration Server.

  All connection gateways are included in the list of distribution points in the Administration Server properties.

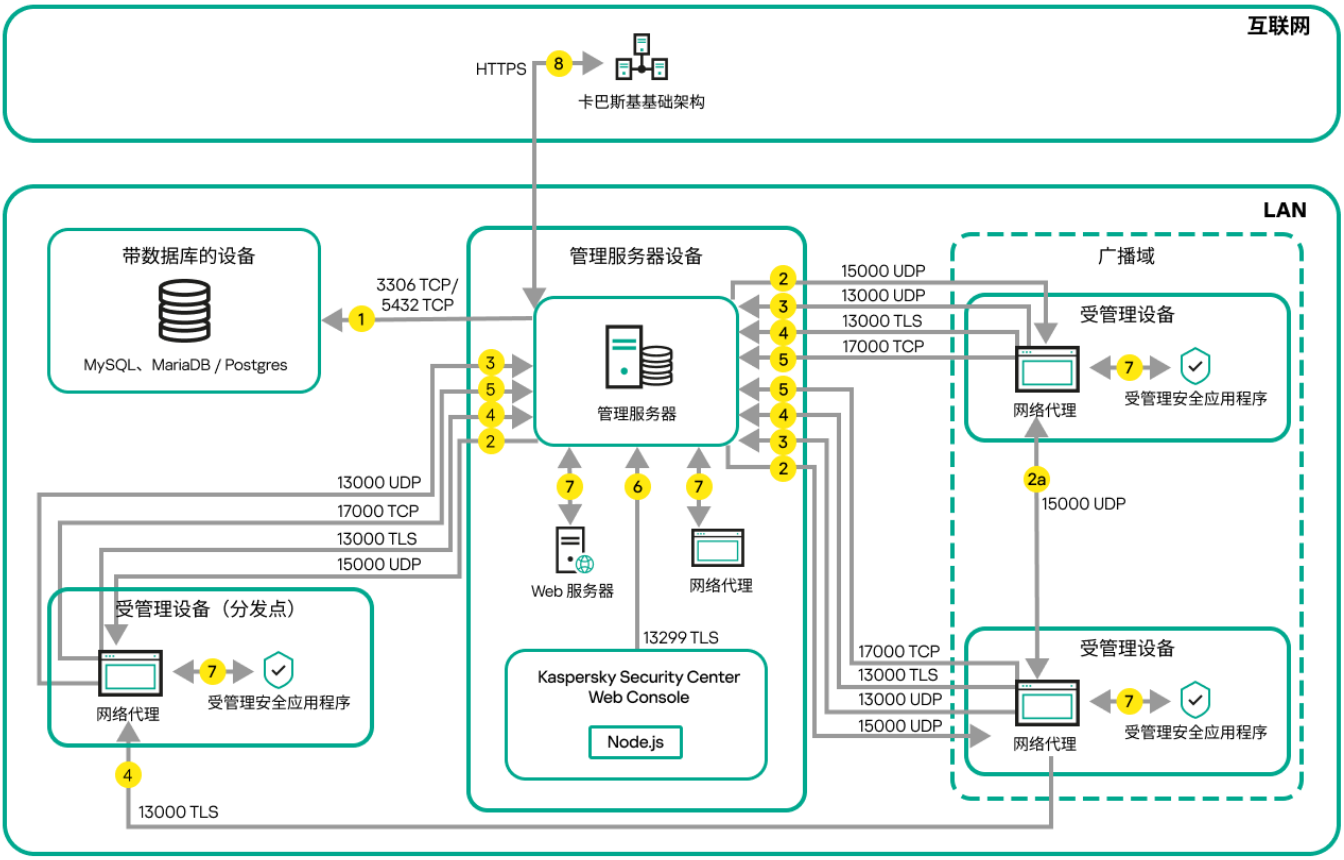
- You can also use connection gateways within the network. For example, automatically assigned distribution points also become connection gateways in their own scope. However, within an internal network, connection gateways do not provide considerable benefit. They reduce the number of network connections received by Administration Server, but do not reduce the volume of incoming data. Even without connection gateways, all devices could still connect to Administration Server.

数据流量和端口使用的 schema

该部分提供了 Kaspersky Security Center Linux 组件、受管理安全应用程序和不同配置下的外部服务器之间的数据流量 schema。该 schema 使用在本地设备上必须可用的端口号提供。

LAN 中的管理服务器和受管理设备

下图显示 Kaspersky Security Center 仅在局域网 (LAN) 中被部署时的数据流量。



局域网 (LAN) 中的管理服务器和受管理设备

该图片显示了受管理设备连接到管理服务器的不同方式：直接或通过分发点。分发点降低发布更新时管理服务器的负载并优化网络流量。然而，分发点仅在受管理设备数量足够大时被需要。如果受管理设备数量较小，所有受管理设备可以从管理服务器直接接收更新。

箭头表示流量的开始：每个箭头从发起连接的设备指向"回答"请求的设备。端口号和用于数据传输的协议名称被提供。每个箭头都有数字标签，对应的数据流量详情是：

1. 管理服务器发送数据到数据库。如果您在不同设备上安装管理服务器和数据库，您必须使数据库所在设备的必要端口可用（例如，端口 3306 用于 MySQL Server 和 MariaDB Server，端口 5432 用于 PostgreSQL Server 或者 Postgres Pro Server）。请参阅 DBMS 文档以获取相关信息。

2. 来自管理服务器的通信请求被传输到所有非移动受管理设备，通过 UDP 端口 15000。

   网络代理在一个广播域内相互发送请求。然后将数据发送到管理服务器，并用于定义广播域的限制和分发点的自动分配（如果启用了此选项）。

   如果管理服务器无法直接访问受管理设备，则不会直接发送从管理服务器到这些设备的通信请求。

   2a.非移动受管理设备上的网络代理交换同一广播域内其他网络代理的数据（数据然后被发送到管理服务器）。

3. 受管理设备关闭的信息通过 UDP 端口 13000 被从网络代理传输到管理服务器。

4. 管理服务器通过 SSL 端口 13000 从网络代理和从属管理服务器接收连接。

   如果您使用 Kaspersky Security Center 的早期版本，您网络中的管理服务器可以通过非 SSL 端口 14000 从网络代理接收连接。Kaspersky Security Center 也支持通过端口 14000 连接网络代理，但推荐使用 SSL 端口 13000。

5. 受管理设备（除了移动设备）通过 TCP 端口 17000 请求激活。如果设备自己拥有互联网连接，则不必要；此种情况下，设备直接通过互联网发送数据到 Kaspersky 服务器。

6. Kaspersky Security Center Web Console 服务器通过 TLS 端口 13299 发送数据到管理服务器，该管理服务器可能被安装到相同或不同设备。

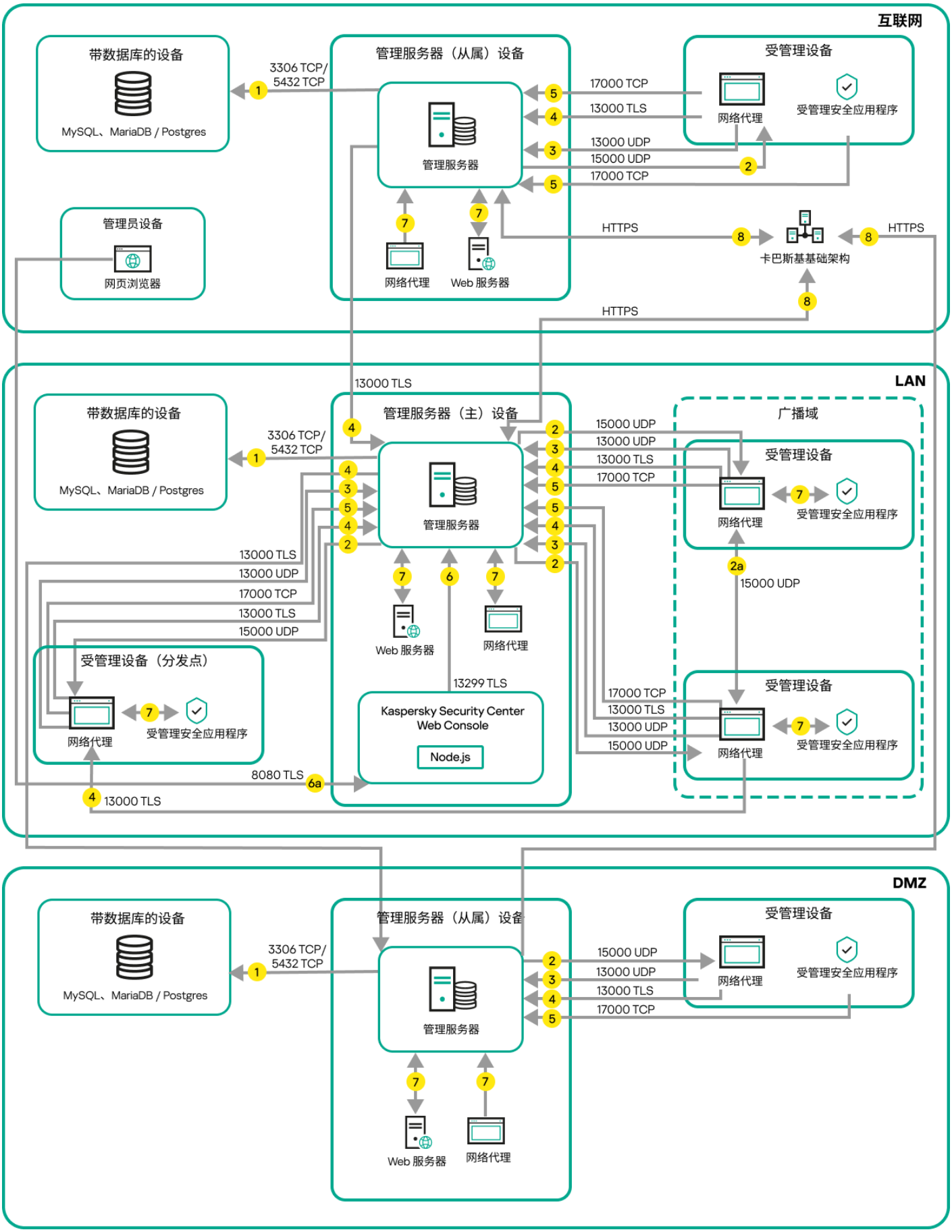
7. 单一设备上的应用程序交换本地流量（在管理服务器上或受管理设备上）。不需要打开任何外部端口。

8. 从管理服务器到 Kaspersky 服务器的数据（例如 KSN 数据或授权许可信息）和从 Kaspersky 服务器到管理服务器的数据（例如应用程序更新和反病毒数据库更新）使用 HTTPS 协议传输。

   如果您不想让您的管理服务器拥有互联网连接，您必须手动管理该数据。

局域网中的主管理服务器和两个从属管理服务器

下图显示管理服务器层级：主管理服务器位于局域网 (LAN)。一个从属管理服务器位于 DMZ；另一个从属管理服务器位于互联网。



管理服务器层级：主管理服务器和两个从属管理服务器

箭头表示流量的开始：每个箭头从发起连接的设备指向"回答"请求的设备。端口号和用于数据传输的协议名称被提供。每个箭头都有数字标签，对应的数据流量详情是：

1. 管理服务器发送数据到数据库。如果您在不同设备上安装管理服务器和数据库，您必须使数据库所在设备的必要端口可用（例如，端口 3306 用于 MySQL Server 和 MariaDB Server，端口 5432 用于 PostgreSQL Server 或者 Postgres Pro Server）。请参阅 DBMS 文档以获取相关信息。

2. 来自管理服务器的通信请求被传输到所有非移动受管理设备，通过 UDP 端口 15000。

   网络代理在一个广播域内相互发送请求。然后将数据发送到管理服务器，并用于定义广播域的限制和分发点的自动分配（如果启用了此选项）。

   如果管理服务器无法直接访问受管理设备，则不会直接发送从管理服务器到这些设备的通信请求。

3. 受管理设备关闭的信息通过 UDP 端口 13000 被从网络代理传输到管理服务器。

4. 管理服务器通过 SSL 端口 13000 从网络代理和从属管理服务器接收连接。

   如果您使用 Kaspersky Security Center 的早期版本，您网络中的管理服务器可以通过非 SSL 端口 14000 从网络代理接收连接。Kaspersky Security Center Linux 也支持通过端口 14000 连接网络代理，但推荐使用 SSL 端口 13000。

5. 受管理设备（除了移动设备）通过 TCP 端口 17000 请求激活。如果设备自己拥有互联网连接，则不必要；此种情况下，设备直接通过互联网发送数据到 Kaspersky 服务器。

6. Kaspersky Security Center Web Console 服务器通过 TLS 端口 13299 发送数据到管理服务器，该管理服务器可能被安装到相同或不同设备。

   6a.来自 Web 浏览器（安装在管理员的其他设备）的数据通过 TLS 端口 8080 传输到 Kaspersky Security Center Web Console 服务器。Kaspersky Security Center Web Console 可以安装到管理服务器或其他设备。

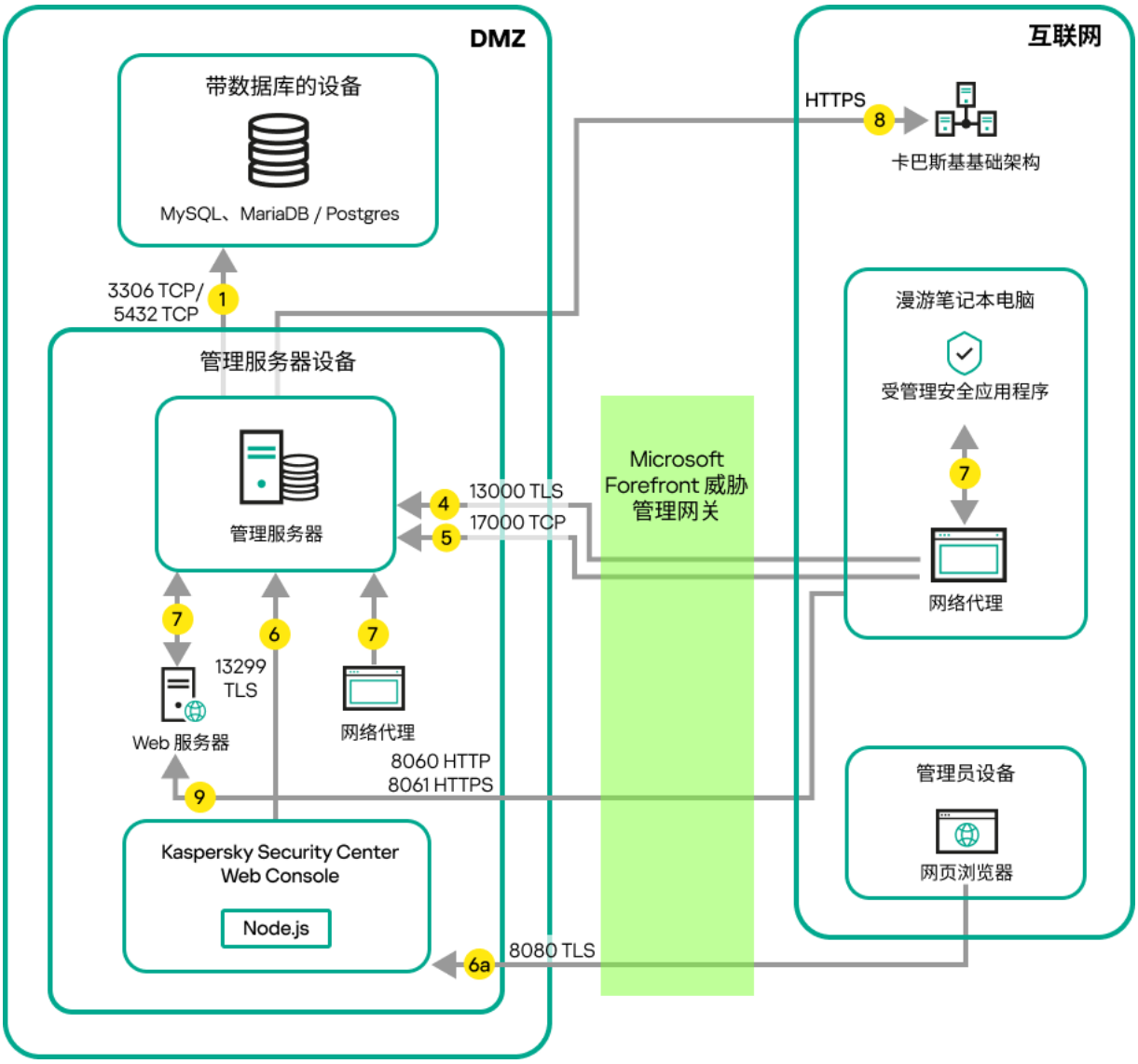
7. 单一设备上的应用程序交换本地流量（在管理服务器上或受管理设备上）。不需要打开任何外部端口。

8. 从管理服务器到 Kaspersky 服务器的数据（例如 KSN 数据或授权许可信息）和从 Kaspersky 服务器到管理服务器的数据（例如应用程序更新和反病毒数据库更新）使用 HTTPS 协议传输。

   如果您不想让您的管理服务器拥有互联网连接，您必须手动管理该数据。

管理服务器位于 LAN、受管理设备位于互联网、防火墙使用中

下图显示管理服务器处于局域网 (LAN) 中且受管理设备在互联网中时的数据流量。在此图中，您选择的企业防火墙正在使用中。请参考应用程序的文档了解详情。



管理服务器位于局域网；受管理设备通过公司防火墙连接到管理服务器

如果您不想让移动设备直接连接到管理服务器，且不想在 DMZ 中分配连接网关，则该部署方案被推荐。

箭头表示流量的开始：每个箭头从发起连接的设备指向"回答"请求的设备。端口号和用于数据传输的协议名称被提供。每个箭头都有数字标签，对应的数据流量详情是：

1. 管理服务器发送数据到数据库。如果您在不同设备上安装管理服务器和数据库，您必须使数据库所在设备的必要端口可用（例如，端口 3306 用于 MySQL Server 和 MariaDB Server，端口 5432 用于 PostgreSQL Server 或者 Postgres Pro Server）。请参阅 DBMS 文档以获取相关信息。

2. 来自管理服务器的通信请求被传输到所有非移动受管理设备，通过 UDP 端口 15000。

   网络代理在一个广播域内相互发送请求。然后将数据发送到管理服务器，并用于定义广播域的限制和分发点的自动分配（如果启用了此选项）。

   如果管理服务器无法直接访问受管理设备，则不会直接发送从管理服务器到这些设备的通信请求。

3. 受管理设备关闭的信息通过 UDP 端口 13000 被从网络代理传输到管理服务器。

4. 管理服务器通过 SSL 端口 13000 从网络代理和从属管理服务器接收连接。

   如果您使用 Kaspersky Security Center 的早期版本，您网络中的管理服务器可以通过非 SSL 端口 14000 从网络代理接收连接。Kaspersky Security Center Linux 也支持通过端口 14000 连接网络代理，但推荐使用 SSL 端口 13000。

5. 受管理设备（除了移动设备）通过 TCP 端口 17000 请求激活。如果设备自己拥有互联网连接，则不必要；此种情况下，设备直接通过互联网发送数据到 Kaspersky 服务器。

6. Kaspersky Security Center Web Console 服务器通过 TLS 端口 13299 发送数据到管理服务器，该管理服务器可能被安装到相同或不同设备。

   6a.来自 Web 浏览器（安装在管理员的其他设备）的数据通过 TLS 端口 8080 传输到 Kaspersky Security Center Web Console 服务器。Kaspersky Security Center Web Console 可以安装到管理服务器或其他设备。

7. 单一设备上的应用程序交换本地流量（在管理服务器上或受管理设备上）。不需要打开任何外部端口。

8. 从管理服务器到 Kaspersky 服务器的数据（例如 KSN 数据或授权许可信息）和从 Kaspersky 服务器到管理服务器的数据（例如应用程序更新和反病毒数据库更新）使用 HTTPS 协议传输。

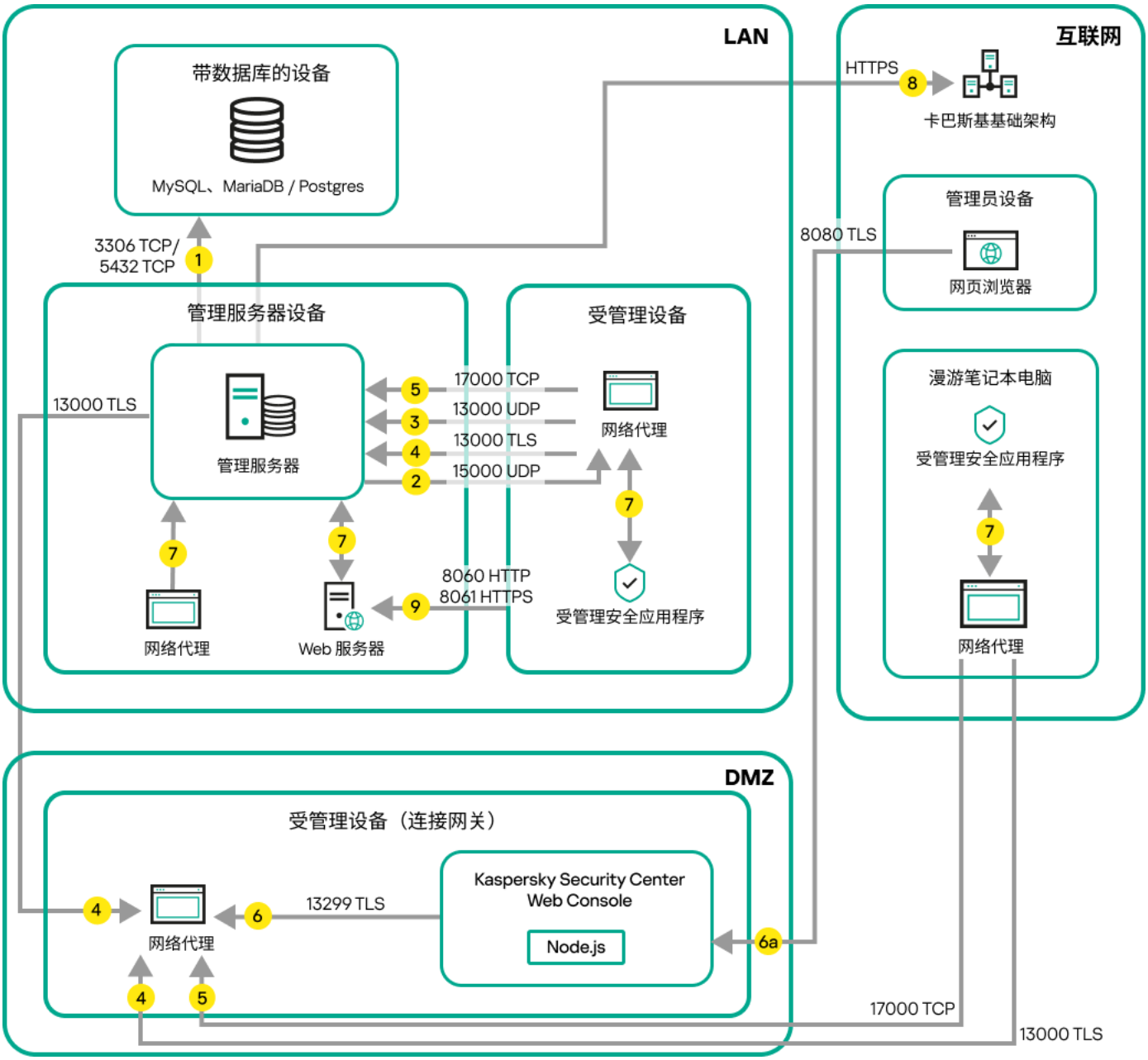
   如果您不想让您的管理服务器拥有互联网连接，您必须手动管理该数据。

9. 来自受管理设备，包括移动设备的包请求被传输到 Web 服务器，该服务器位于管理服务器所在设备。

管理服务器位于 LAN、受管理设备位于互联网、连接网关使用中

下图显示管理服务器处于局域网 (LAN) 中且受管理设备在互联网中时的数据流量。连接网关使用中。

如果您不想让受管理设备直接连接到管理服务器，且不想使用 Microsoft Forefront Threat Management Gateway (TMG) 或企业防火墙，则推荐采用该部署方案。



受管理移动设备通过连接网关连接到管理服务器

在该图中，受管理设备通过 DMZ 中的连接网关连接到管理服务器。未使用 TMG 或企业防火墙。

箭头表示流量的开始：每个箭头从发起连接的设备指向"回答"请求的设备。端口号和用于数据传输的协议名称被提供。每个箭头都有数字标签，对应的数据流量详情是：

1. 管理服务器发送数据到数据库。如果您在不同设备上安装管理服务器和数据库，您必须使数据库所在设备的必要端口可用（例如，端口 3306 用于 MySQL Server 和 MariaDB Server，端口 5432 用于 PostgreSQL Server 或者 Postgres Pro Server）。请参阅 DBMS 文档以获取相关信息。

2. 来自管理服务器的通信请求被传输到所有非移动受管理设备，通过 UDP 端口 15000。

   网络代理在一个广播域内相互发送请求。然后将数据发送到管理服务器，并用于定义广播域的限制和分发点的自动分配（如果启用了此选项）。

   如果管理服务器无法直接访问受管理设备，则不会直接发送从管理服务器到这些设备的通信请求。

3. 受管理设备关闭的信息通过 UDP 端口 13000 被从网络代理传输到管理服务器。

4. 管理服务器通过 SSL 端口 13000 从网络代理和从属管理服务器接收连接。

如果您使用 Kaspersky Security Center 的早期版本，您网络中的管理服务器可以通过非 SSL 端口 14000 从网络代理接收连接。Kaspersky Security Center Linux 也支持通过端口 14000 连接网络代理，但推荐使用 SSL 端口 13000。

5. 受管理设备（除了移动设备）通过 TCP 端口 17000 请求激活。如果设备自己拥有互联网连接，则不必要；此种情况下，设备直接通过互联网发送数据到 Kaspersky 服务器。

6. Kaspersky Security Center Web Console 服务器通过 TLS 端口 13299 发送数据到管理服务器，该管理服务器可能被安装到相同或不同设备。

   6a.来自 Web 浏览器（安装在管理员的其他设备）的数据通过 TLS 端口 8080 传输到 Kaspersky Security Center Web Console 服务器。Kaspersky Security Center Web Console 可以安装到管理服务器或其他设备。

7. 单一设备上的应用程序交换本地流量（在管理服务器上或受管理设备上）。不需要打开任何外部端口。

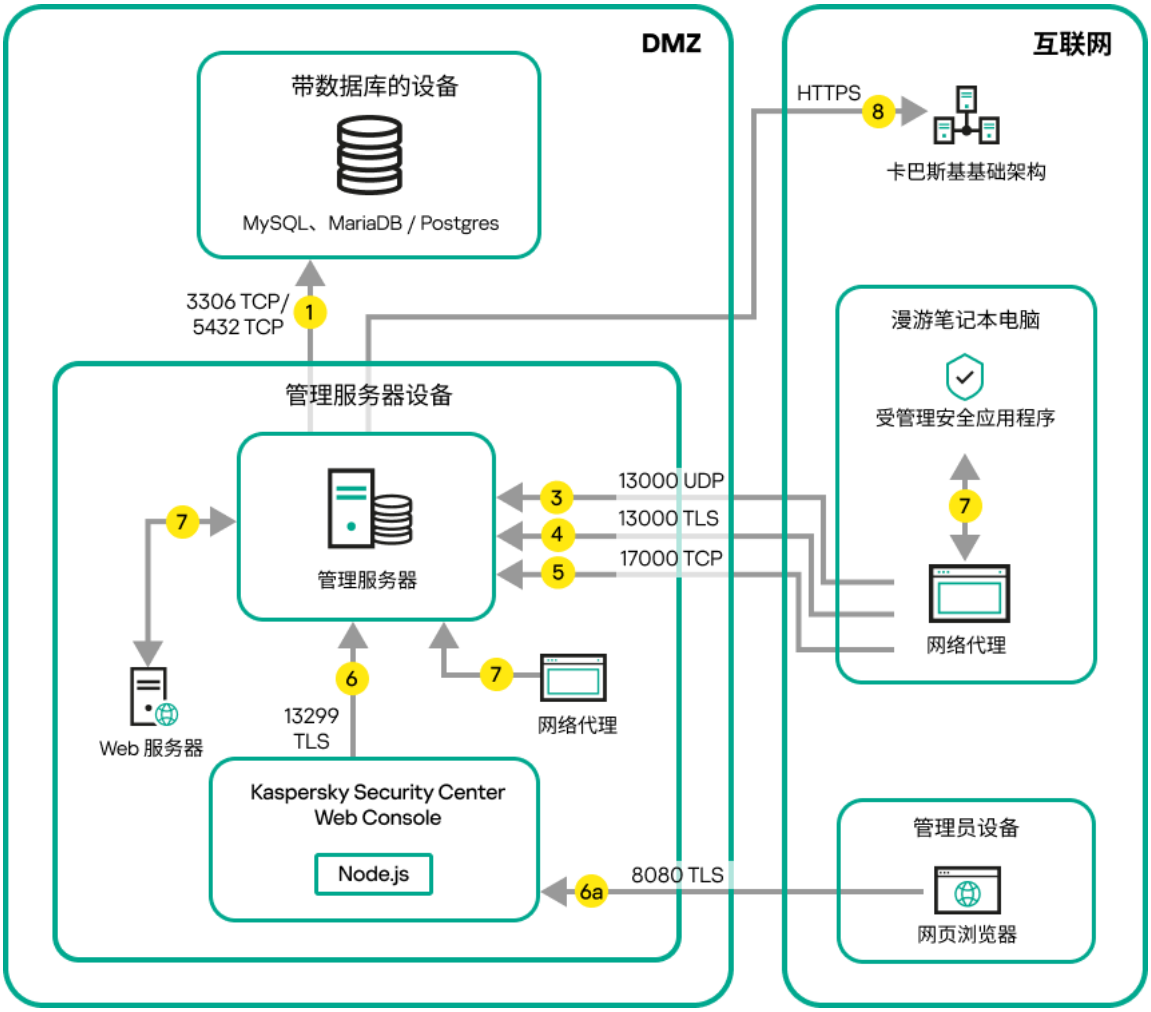
8. 从管理服务器到 Kaspersky 服务器的数据（例如 KSN 数据或授权许可信息）和从 Kaspersky 服务器到管理服务器的数据（例如应用程序更新和反病毒数据库更新）使用 HTTPS 协议传输。

   如果您不想让您的管理服务器拥有互联网连接，您必须手动管理该数据。

9. 来自受管理设备，包括移动设备的包请求被传输到 Web 服务器，该服务器位于管理服务器所在设备。

管理服务器位于 DMZ、受管理设备位于互联网

下图显示管理服务器处于隔离区 (DMZ) 中且受管理设备在互联网中时的数据流量。



管理服务器位于 DMZ、受管理移动设备位于互联网

在该图像中，未使用连接网关：移动设备直接连接到管理服务器。

箭头表示流量的开始：每个箭头从发起连接的设备指向"回答"请求的设备。端口号和用于数据传输的协议名称被提供。每个箭头都有数字标签，对应的数据流量详情是：

1. 管理服务器发送数据到数据库。如果您在不同设备上安装管理服务器和数据库，您必须使数据库所在设备的必要端口可用（例如，端口 3306 用于 MySQL Server 和 MariaDB Server，端口 5432 用于 PostgreSQL Server 或者 Postgres Pro Server）。请参阅 DBMS 文档以获取相关信息。

2. 来自管理服务器的通信请求被传输到所有非移动受管理设备，通过 UDP 端口 15000。

   网络代理在一个广播域内相互发送请求。然后将数据发送到管理服务器，并用于定义广播域的限制和分发点的自动分配（如果启用了此选项）。

   如果管理服务器无法直接访问受管理设备，则不会直接发送从管理服务器到这些设备的通信请求。

3. 受管理设备关闭的信息通过 UDP 端口 13000 被从网络代理传输到管理服务器。

4. 管理服务器通过 SSL 端口 13000 从网络代理和从属管理服务器接收连接。

   如果您使用 Kaspersky Security Center 的早期版本，您网络中的管理服务器可以通过非 SSL 端口 14000 从网络代理接收连接。Kaspersky Security Center Linux 也支持通过端口 14000 连接网络代理，但推荐使用 SSL 端口 13000。

   4a.DMZ 中的连接网关还会通过 SSL 端口 13000 从管理服务器接收连接。由于 DMZ 中的连接网关无法访问管理服务器的端口，因此管理服务器会创建并维护与连接网关的永久信号连接。该信号连接不用于数据传输，仅用于发送网络交互邀请。当连接网关需要连接到服务器时，它将通过此信号连接通知服务器，然后服务器创建数据传输所需的连接。

   漫游设备也通过 SSL 端口 13000 连接到连接网关。

5. 受管理设备（除了移动设备）通过 TCP 端口 17000 请求激活。如果设备自己拥有互联网连接，则不必要；此种情况下，设备直接通过互联网发送数据到 Kaspersky 服务器。

6. Kaspersky Security Center Web Console 服务器通过 TLS 端口 13299 发送数据到管理服务器，该管理服务器可能被安装到相同或不同设备。

   6a.来自 Web 浏览器（安装在管理员的其他设备）的数据通过 TLS 端口 8080 传输到 Kaspersky Security Center Web Console 服务器。Kaspersky Security Center Web Console 可以安装到管理服务器或其他设备。

7. 单一设备上的应用程序交换本地流量（在管理服务器上或受管理设备上）。不需要打开任何外部端口。

8. 从管理服务器到 Kaspersky 服务器的数据（例如 KSN 数据或授权许可信息）和从 Kaspersky 服务器到管理服务器的数据（例如应用程序更新和反病毒数据库更新）使用 HTTPS 协议传输。

   如果您不想让您的管理服务器拥有互联网连接，您必须手动管理该数据。

9. 来自受管理设备的包请求被传输到 Web 服务器，该服务器位于管理服务器所在设备。

Kaspersky Security Center Linux 组件和安全应用程序的交互：更多信息

该部分提供了与 Kaspersky Security Center Linux 组件和受管理安全应用程序交互的方案。方案提供了必须可用的端口号和打开这些端口的进程名称。

交互模式中的惯例

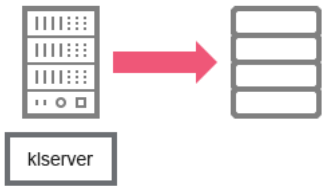
下表提供了方案中使用的转换。

文档约定

图标	含义
	管理服务器
	从属管理服务器
	DBMS
	客户端设备(安装了网络代理和 Kaspersky Endpoint Security 系列应用程序，或 Kaspersky Security Center Linux 可以管理的其他应用程序)
	连接网关
	分发点
	用户设备上的浏览器
	运行在设备和打开端口的进程
	端口和其号码
	TCP 流量(箭头方向显示流量方向)
	TCP 流量(箭头方向显示流量方向)
	DBMS 传输
	DMZ 边界

管理服务器和 DBMS

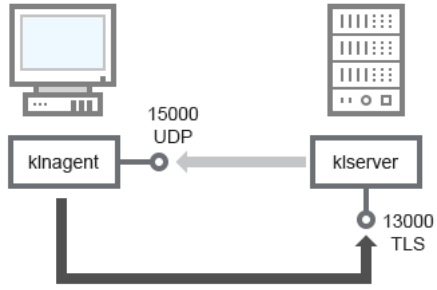
来自管理服务器的数据进入数据库。



如果您在不同设备上安装管理服务器和数据库，则必须使数据库所在设备的必要端口可用（例如，端口 3306 用于 MariaDB）。请参阅 DBMS 文档以获取相关信息。

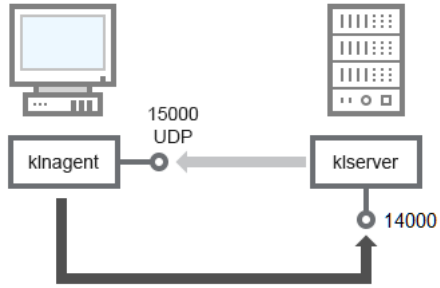
管理服务器和客户端设备：管理安全应用程序

管理服务器通过 TLS 端口 13000 从网络代理接收连接（参见下图）。



管理服务器和客户端设备：管理安全应用程序、通过端口 13000 连接（推荐）

如果您使用 Kaspersky Security Center Linux 的早期版本，您网络中的管理服务器可以通过非 SSL 端口 14000 从网络代理接收连接（参见下图）。Kaspersky Security Center Linux 也支持通过端口 14000 连接网络代理，但推荐使用 SSL 端口 13000。



管理服务器和客户端设备：管理安全应用程序、通过端口 14000 连接（低安全级）

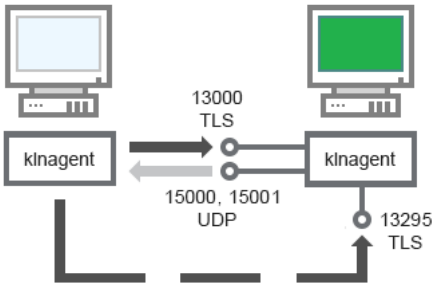
为了澄清方案，参见下图。

管理服务器和客户端设备：管理安全应用程序（流量）

设备	端口号	打开端口的进程名称	协议	端口目的
网络代理	15000	klnagent	UDP	网络代理多点传送
管理服务器	13000	klserver	TCP (TLS)	接收从网络代理的连接
管理服务器	14000	klserver	TCP	接收从网络代理的连接

通过分发点在客户端设备上升级软件

客户端设备通过端口 13000 连接到分发点，如果您将分发点用作推送服务器，则还通过端口 13295 进行连接；分发点通过端口 15000 多播到网络代理（请参见下图）。更新和安装包通过端口 15001 从分发点接收。



通过分发点在客户端设备上升级软件

对于方法描述，参见下表。

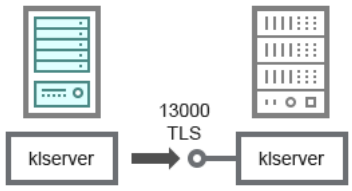
通过分发点升级软件（流量）

设备	端口号	打开端口的进程名称	协议	端口目的
网络代理	15000	klnagent	UDP	网络代理多点传送
网络代理	15001	klnagent	UDP	从分发点接收更新和安装包
分发点	13000	klnagent	TCP (TLS)	接收从网络代理的连接
分发点	13295	klnagent	TCP (TLS)	接收来自客户端设备的连接（服务器推送）

管理服务器层级：主管理服务器和从属管理服务器

方案（参见下图）显示了如何使用端口 13000 确保层级中管理服务器之间的交互。

此后，当管理服务器组合到层级时，您将可以使用连接到主管理服务器的 Kaspersky Security Center Web Console 管理两个管理服务器。因此，主管理服务器端口 13299 的可访问性是仅有的前提。



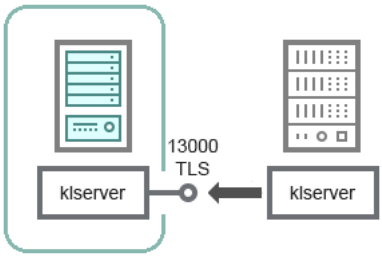
管理服务器层级：主管理服务器和从属管理服务器

对于方法描述，参见下表。

管理服务器层级（流量）

设备	端口号	打开端口的进程名称	协议	端口目的
主管理服务器	13000	klserver	TCP (TLS)	从从属管理服务器接收连接

DMZ 中带有从属管理服务器的管理服务器层级



DMZ 中带有从属管理服务器的管理服务器层级

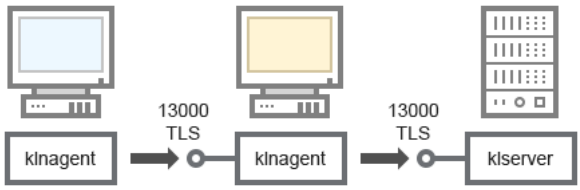
方案显示了管理服务器层级，其中 DMZ 中的从属管理服务器从主管理服务器接收连接（有关方案说明，请参见下表）。当组合两个管理服务器到一个层级，确保端口 13299 在两个管理服务器上都可以访问。Kaspersky Security Center Web Console 通过端口 13291 连接到管理服务器。

此后，当管理服务器组合到层级时，您将可以使用连接到主管理服务器的 Kaspersky Security Center Web Console 管理两个管理服务器。因此，主管理服务器端口 13299 的可访问性是仅有的前提。

DMZ 中带有从属管理服务器的管理服务器层级（流量）

设备	端口号	打开端口的进程名称	协议	端口目的
从属管理服务器	13000	klserver	TCP (TLS)	从主管理服务器接收连接

管理服务器、网段连接网关和客户端设备



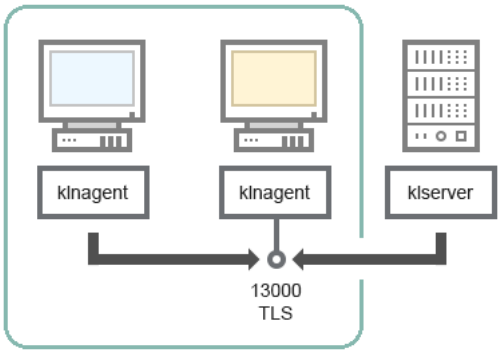
管理服务器、网段连接网关和客户端设备

对于方法描述，参见下表。

管理服务器、网段连接网关和客户端设备（流量）

设备	端口号	打开端口的进程名称	协议	端口目的
管理服务器	13000	klserver	TCP (TLS)	接收从网络代理的连接
网络代理	13000	klnagent	TCP (TLS)	接收从网络代理的连接

管理服务器和 DMZ 中的两台设备：连接网关和客户端设备



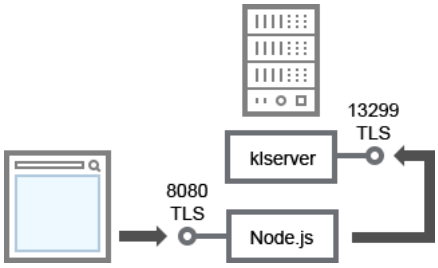
带有连接网关的管理服务器和 DMZ 中的客户端设备

对于方法描述，参见下表。

带有网段连接网关的管理服务器和客户端设备（流量）

设备	端口号	打开端口的进程名称	协议	端口目的
网络代理	13000	klnagent	TCP (TLS)	接收从网络代理的连接

管理服务器和 Kaspersky Security Center Web Console



管理服务器和 Kaspersky Security Center Web Console

对于方法描述，参见下表。

管理服务器和 Kaspersky Security Center Web Console（流量）

设备	端口号	打开端口的进程名称	协议	端口目的
管理服务器	13299	klserver	TCP (TLS)	接收通过 OpenAPI 从 Kaspersky Security Center Web Console 到管理服务器的连接
Kaspersky Security Center Web Console 服务器或管理服务器	8080	Node.js：服务器端 JavaScript	TCP (TLS)	从 Kaspersky Security Center Web Console 接收连接

Kaspersky Security Center Web Console 可以安装到管理服务器或其他设备。

启动

按照此方案，您可以安装 Kaspersky Security Center Linux 管理服务器和 Kaspersky Security Center Web Console，使用快速启动向导执行管理服务器初始化设置，以及使用保护部署向导安装卡巴斯基应用程序到受管理设备。

先决条件

您必须拥有卡巴斯基网络安全解决方案的授权许可密钥（激活码）或 Kaspersky 安全应用程序的授权许可密钥（激活码）。

如果您想先试用 Kaspersky Security Center Linux，则可以在 Kaspersky 网站获得 30 天免费试用。

阶段

主要安装方案分阶段进行：

1. **选择组织保护结构**

   了解更多有关 Kaspersky Security Center Linux 组件的信息。基于网络配置和通信渠道的吞吐量，定义要使用的管理服务器数量以及如何在您的办公室间分发它们（如果您的组织运行分布式网络）。

   定义是否管理服务器层级将被用于您的组织。为此，您必须评估您的情况是否适合用单一管理服务器覆盖所有客户端设备，或者是否有必要创建一个管理服务器层级。您可能必须创建一个对应于您要保护的组织的组织结构的管理服务器层级。

2. **准备使用自定义证书**

   如果组织的公钥基础结构 (PKI) 要求您使用由特定证书颁发机构 (CA) 颁发的自定义证书，请准备这些证书并确保它们满足所有要求。

3. **安装数据库管理系统（DBMS）**

   安装 Kaspersky Security Center Linux 将使用的 DBMS，或者使用现有数据库。

   您可以从支持的 DBMS 中选择一个。对于如何安装所选 DBMS 的信息，请参考其文档。

   如果 Linux 操作系统的发行版不包含受支持的 DBMS，您可以从第三方软件包存储库安装 DBMS。如果禁止从第三方存储库安装发行版，您可以将 DBMS 安装在单独的设备上。

   > 如果您决定安装 PostgreSQL 或 Postgres Pro DBMS，请确保您为超级用户指定了密码。如果未指定密码，管理服务器可能无法连接到数据库。

   如果您安装 MariaDB、PostgreSQL 或 Postgres Pro，请使用建议的设置以确保 DBMS 正常运行。

   > 如果您想在安装后更改DBMS 类型，则必须重新安装 Kaspersky Security Center Linux。数据可以被部分手动传输到另一个数据库。

4. **配置端口**

   确保所有必要的端口都打开以便与您选择的安全结构对应的各组件间进行交互。

   如果您必须提供互联网访问给管理服务器，根据网络配置配置端口并指定连接设置。

5. **安装 Kaspersky Security Center Linux**

选择要用作管理服务器的 Linux 设备，确保该设备满足软件和硬件要求，然后在该设备上安装 Kaspersky Security Center Linux。服务器版本的网络代理将自动与管理服务器一起安装。

6. 安装 Kaspersky Security Center Web Console 和管理 Web 插件

选择要用作管理员工作站的 Linux 设备，确保该设备满足软件和硬件要求，然后在该设备上安装 Kaspersky Security Center Web Console。您可以在安装了管理服务器的同一台设备上或在其他设备上安装 Kaspersky Security Center Web Console。

下载 Kaspersky Endpoint Security for Linux 管理 Web 插件，然后将其安装在安装了 Kaspersky Security Center Web Console 的同一台设备上。

7. 在管理服务器设备上安装 Kaspersky Endpoint Security for Linux 和网络代理

默认情况下，应用程序不将管理服务器设备视为受管理设备。为了保护管理服务器免受病毒和其他威胁的侵害，并像管理任何其他受管理设备一样管理该设备，建议您在管理服务器设备上安装 Kaspersky Endpoint Security for Linux 和 Network Agent for Linux。在这种情况下，Network Agent for Linux 的安装和运行独立于网络代理的服务器版本，后者是与管理服务器一起安装的。

8. 执行初始化设置

当管理服务器安装完成后，在第一次连接到管理服务器时，快速启动向导自动开始。根据现有需求指定管理服务器初始化配置。在初始化配置步骤，向导使用默认设置创建部署保护所需的策略和任务。然而，默认设置可能少于您组织需要的最优设置。您可以编辑策略和任务设置。

9. 发现网络设备

手动发现设备。Kaspersky Security Center Linux 会接收网络中检测到的所有设备的地址和名称。然后您可以使用 Kaspersky Security Center Linux 在检测到的设备上安装卡巴斯基应用程序和其他供应商的软件。Kaspersky Security Center Linux 定期启动设备发现，这意味着如果任何新实例出现在网络，它们将被自动检测。

10. 整理设备到管理组

在一些情况下，最方便的部署保护到网络设备的方式需要您分割整个设备池到管理组，根据组织结构。您可以创建移动规则以在组间分发设备，或者您可以手动分发设备。您可以为管理组分配组任务，定义策略范围并分配分发点。

确保所有受管理设备被正确分配到适当的管理组，且网络中不再有未分配的设备。

11. 分配分发点

分发点被自动分配到管理组，但您也可以在必要时手动分配它们。我们建议您在大规模网络中使用分发点以降低管理服务器负载，以及在具有分布式结构的网络中提供管理服务器通过窄通道访问到设备（或设备组）。

12. 安装网络代理和安全应用程序到网络设备

企业网络的保护部署需要在由管理服务器在设备发现期间检测到的设备上安装网络代理和安全应用程序。

要远程安装应用程序，运行保护部署向导。

安全应用程序保护设备以防病毒和其他威胁程序。网络代理确保设备和管理服务器之间的通信。网络代理设置默认被自动配置。

在您开始安装网络代理和安全应用程序到网络设备之前，确保这些设备是可访问的（开启）。

13. 部署授权许可密钥到客户端设备

部署授权许可密钥到客户端设备以在这些设备上激活受管理安全应用程序。

14. 配置 Kaspersky 应用程序策略

要应用不同应用程序设置到不同设备，您可以使用以设备为中心的安全管理和/或以用户为中心的安全管理。以设备与中心的安全管理可以使用策略和任务实现。您仅可以应用任务到满足特定条件的设备。要设置筛选设备的条件，使用设备分类和标签。

15. 监控网络保护状态

您可以使用控制板的工具来监控您的网络，从 Kaspersky 应用程序生成报告，配置和查看从受管理设备上的应用程序接收的事件分类，以及查看通知列表。

安装

该部分描述了 Kaspersky Security Center Linux 和 Kaspersky Security Center Web Console 的安装。

Configuring the MariaDB x64 server for working with Kaspersky Security Center Linux

Recommended settings for the my.cnf file

For more details about DBMS configuring, refer also to the account configuring procedure. For information about DBMS installation, refer to the DBMS installation procedure.

To configure the my.cnf file:

1. Open the my.cnf file in a text editor.

2. Enter the following lines into the [mysqld] section of the my.cnf file:

```
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
```

   The value of the `innodb_buffer_pool_size` must be no less than 80 percent of the expected KAV database size. Note that the specified memory is allocated at server startup. If the database size is smaller than the specified buffer size, only the required memory is allocated. If you use MariaDB 10.4.3 or older, the actual size of allocated memory is approximately 10 percent greater than the specified buffer size.

   It is recommended to use the parameter value `innodb_flush_log_at_trx_commit=0`, because the values "1" or "2" negatively affect the operating speed of MariaDB.

By default, the optimizer add-ons `join_cache_incremental`, `join_cache_hashed`, `join_cache_bka` are enabled. If these add-ons are not enabled, you must enable them.

To check whether optimizer add-ons are enabled:

1. In the MariaDB client console, execute the command:

```
SELECT @@optimizer_switch;
```

2. Make sure that its output contains the following lines:
   ```
   join_cache_incremental=on
   join_cache_hashed=on
   join_cache_bka=on
   ```
   If these lines are present and have the values `on`, then optimizer add-ons are enabled.

   If these lines are missing or have `off` values, you need to do the following:

   a. Open the my.cnf file in a text editor.

   b. Add the following lines into the my.cnf file:
   ```
   optimizer_switch='join_cache_incremental=on'
   optimizer_switch='join_cache_hashed=on'
   optimizer_switch='join_cache_bka=on'
   ```

The add-ons `join_cache_incremental`, `join_cache_hash`, and `join_cache_bka` are enabled.

配置与 Kaspersky Security Center Linux 配合使用的 PostgreSQL 或 Postgres Pro 服务器

Kaspersky Security Center Linux 支持 PostgreSQL 和 Postgres Pro DBMS。如果您使用这些 DBMS 之一，请考虑配置 DBMS 服务器参数，使 DBMS 与 Kaspersky Security Center Linux 达到最佳工作状态。

配置文件的默认路径是：/etc/postgresql/<VERSION> /main/postgresql.conf

PostgreSQL 和 Postgres Pro 的推荐参数：

- `shared_buffers` =安装 DBMS 的设备的 RAM 值的 25%
  如果 RAM 小于 1 GB，则保留默认值。
- `max_stack_depth` =最大堆栈大小（执行“`ulimit -s`”命令以获取此值（以 KB 为单位）减去 1 MB 安全余量
- `temp_buffers = 24MB`
- `work_mem = 16MB`
- `max_connections = 151`
- `max_parallel_workers_per_gather = 0`
- `maintenance_work_mem = 128 MB`

更新 postgresql.conf 文件以应用更改后重新启动或重新加载服务器。有关详细信息，请参阅 PostgreSQL 文档。

有关如何为 PostgreSQL 和 Postgres Pro 创建和配置账户的详细信息，请参阅以下主题：配置 PostgreSQL 和 Postgres Pro 的使用账户。

有关 PostgreSQL 和 Postgres Pro 服务器参数以及如何指定参数的详细信息，请参阅相应的 DBMS 文档。

场景：验证 PostgreSQL 服务器

我们建议您使用 TLS 证书对 PostgreSQL 服务器进行身份验证。您可以使用来自可信证书颁发机构 (CA) 的证书或自签名证书。请使用来自可信 CA 的证书，因为自签名证书仅提供有限保护。

管理服务器支持 PostgreSQL 的单向和双向 SSL 身份验证。

请按照以下步骤为 PostgreSQL 配置 SSL 身份验证：

1. **为 PostgreSQL 服务器生成证书。**

   运行以下命令：

   ```
   openssl req -new -x509 -days 365 -nodes -text -out psql.crt -keyout psql.key -subj
   "/CN=psql"
   ```

   ```
   chmod og-rwx psql.key
   ```

2. **为管理服务器生成证书。**

   运行以下命令。CN 值应与代表管理服务器连接到 PostgreSQL 的用户名匹配。默认情况下，用户名设置为 postgres。

   ```
   openssl req -new -x509 -days 365 -nodes -text -out postgres.crt -keyout postgres.key -
   subj "/CN=postgres"
   ```

   ```
   chmod og-rwx postgres.key
   ```

3. **配置客户端证书身份验证。**

   修改 pg_hba.conf 如下：

   ```
   hostssl all all 0.0.0.0/0 md5
   ```

   确保 pg_hba.conf 不包含以`host`开头的记录。

4. **指定 PostgreSQL 证书。**

   单向 SSL 身份验证

   修改 postgresql.conf 如下（指定 .crt 和 .key 文件的正确路径）：

   ```
   listen_addresses ='*'
   ssl = on
   ssl_cert_file = 'psql.crt'
   ssl_key_file = 'psql.key'
   ```

   双向 SSL 身份验证

   修改 postgresql.conf 如下（指定 .crt 和 .key 文件的正确路径）：

   ```
   listen_addresses ='*'
   ssl = on
   ssl_ca_file = '<postgres.crt>'
   ssl_cert_file = '<psql.crt>'
   ssl_key_file = '<psql.key>'
   ```

5. **重新启动 PostgreSQL 守护进程。**

   运行以下命令：

   ```
   systemctl restart postgresql-14.service
   ```

6. **指定管理服务器的服务器标志。**

   单向 SSL 身份验证

   导航到 ServerFlags 目录并创建与 KLSRV_POSTGRES_OPT_SSL_CA 服务器标志对应的文件：

   ```
   cd /etc/opt/kaspersky/klnagent_srv/1093/1.0.0.0/ServerFlags/
   mkfile KLSRV_POSTGRES_OPT_SSL_CA
   ```

   在创建的文件中，指定 psql.crt 文件的路径。

   双向 SSL 身份验证

   导航到 ServerFlags 目录并创建与服务器标志对应的文件：

   ```
   cd /etc/opt/kaspersky/klnagent_srv/1093/1.0.0.0/ServerFlags/
   mkfile KLSRV_POSTGRES_OPT_SSL_CA
   mkfile KLSRV_POSTGRES_OPT_SSL_CERT
   mkfile KLSRV_POSTGRES_OPT_SSL_KEY
   ```

   编辑创建的文件如下：

   - KLSRV_POSTGRES_OPT_SSL_CA：指定 psql.crt 文件的路径。
   - KLSRV_POSTGRES_OPT_SSL_CERT：指定 postgres.crt 文件的路径。
   - KLSRV_POSTGRES_OPT_SSL_KEY：指定 postgres.key 文件的路径。

   如果 postgres.key 需要密码，请在 ServerFlags 文件夹中创建 KLSRV_POSTGRES_OPT_TLS_PASPHRASE 文件并在其中指定密码。

7. **重启管理服务器服务。**

场景：验证 MySQL 服务器

我们建议您使用 TLS 证书对 MySQL 服务器进行身份验证。您可以使用来自可信证书颁发机构 (CA) 的证书或自签名证书。请使用来自可信 CA 的证书，因为自签名证书仅提供有限保护。

管理服务器支持 MySQL 的单向和双向 SSL 身份验证。

启用单向 SSL 身份验证

请按照以下步骤为 MySQL 配置单向 SSL 身份验证：

1. 导航到 ServerFlags 目录并创建与 KLSRV_MYSQL_OPT_SSL_CA 服务器标志对应的文件：

   ```
   cd /etc/opt/kaspersky/klnagent_srv/1093/1.0.0.0/ServerFlags/
   mkfile KLSRV_MYSQL_OPT_SSL_CA
   ```

2. 在 KLSRV_MYSQL_OPT_SSL_CA 文件中，指定证书的路径（ca-cert.pem 文件）。

3. 在 my.cnf 文件中指定证书。在文本编辑器中打开 my.cnf 文件并将以下行添加到 [mysqld] 部分中：

```
[mysqld]
ssl-ca="C:/mysqlCerts/ca-cert.pem"
ssl-cert="C:/mysqlCerts/server-cert.pem"
ssl-key="C:/mysqlCerts/server-key.pem"
```

启用双向 SSL 身份验证

请按照以下步骤为 MySQL 配置双向 SSL 身份验证：

1. 导航到 ServerFlags 目录并创建与服务器标志对应的文件：

```
cd /etc/opt/kaspersky/klnagent_srv/1093/1.0.0.0/ServerFlags/
mkfile KLSRV_MYSQL_OPT_SSL_CA
mkfile KLSRV_MYSQL_OPT_SSL_CERT
mkfile KLSRV_MYSQL_OPT_SSL_KEY
```

2. 编辑创建的文件如下：

   KLSRV_MYSQL_OPT_SSL_CA：指定 ca-cert.pem 文件的路径。

   KLSRV_MYSQL_OPT_SSL_CERT：指定 server-cert.pem 文件的路径。

   KLSRV_MYSQL_OPT_SSL_KEY：指定 server-key.pem 文件的路径。

   如果 server-key.pem 需要密码，请在 ServerFlags 文件夹中创建 KLSRV_MARIADB_OPT_TLS_PASPHRASE 文件并在其中指定密码。

3. 在 my.cnf 文件中指定证书。在文本编辑器中打开 my.cnf 文件并将以下行添加到 [mysqld] 部分中：

```
[mysqld]
ssl-ca="C:/mysqlCerts/ca-cert.pem"
ssl-cert="C:/mysqlCerts/server-cert.pem"
ssl-key="C:/mysqlCerts/server-key.pem"
```

安装 Kaspersky Security Center Linux

该过程描述了如何安装 Kaspersky Security Center Linux。

安装前：

- 安装 DBMS。
- 确保您要安装 Kaspersky Security Center Linux 的设备运行支持的 Linux 分类。

使用安装文件—ksc64_[版本号]_amd64.deb 或 ksc64-[版本号].x86_64.rpm—对应于您设备上的 Linux 版本。您通过从 Kaspersky 网站下载来接收安装文件。

要安装 Kaspersky Security Center Linux：

1. 在命令行中，以拥有 root 权限的账户运行本说明中提供的命令。

2. 创建一个 kladmins 组和一个无特权账户 'ksc'。该账户必须是 'kladmins' 组的成员。为此，请依次运行以下命令：

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

3. 运行 Kaspersky Security Center Linux 安装。根据您的 Linux 发行版，运行以下命令之一：

   - `# apt install /<path>/ksc64_[ 版本号 ]_amd64.deb`
   - `# yum install /<path>/ksc64-[ 版本号 ].x86_64.rpm -y`

4. 运行 Kaspersky Security Center Linux 配置：

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

5. 阅读最终用户授权许可协议 (EULA) 和隐私策略。文本显示在命令行窗口中。按空格键查看下一个文本段。然后，在出现提示时，输入以下值：

   a. 如果您理解并接受 EULA 的条款，请输入“`y`”。如果您不接受 EULA 的条款，请输入“`n`”。要使用 Kaspersky Security Center Linux，您必须接受 EULA 的条款。

   b. 如果您理解并接受隐私策略的条款，并且同意您的数据将按照隐私策略中所述进行处理和传输（包括传输到第三方国家），请输入“`y`”。如果您不接受隐私策略的条款，请输入“`n`”。要使用 Kaspersky Security Center Linux，您必须接受隐私策略的条款。

6. 出现提示时，输入以下设置：

   a. 输入管理服务器 DNS 名称或静态 IP 地址。`127.0.0.1`用于本地数据库安装。

   b. 输入管理服务器 SSL 端口号。默认情况下使用端口 13000。

   c. 评估您要管理的设备的大概数量：

      - 如果有 1 到 100 台联网设备，则输入“1”。
      - 如果有 101 到 1000 台联网设备，则输入“2”。
      - 如果有超过 1000 台联网设备，则输入“3”。

   d. 输入服务的安全组名称。默认情况下，使用“`kladmins`”组。

   e. 输入用于启动管理服务器服务的账户名。该账户必须是输入的安全组的成员。默认情况下，使用“`ksc`”账户。

   f. 输入用于启动其他服务的账户名。该账户必须是输入的安全组的成员。默认情况下，使用“`ksc`”账户。

   g. 选择您安装的与 Kaspersky Security Center Linux 一起使用的 DBMS：

      - 如果您安装了 MySQL 或 MariaDB，请输入 1。
      - 如果您安装了 PostgreSQL 或 Postgres Pro，请输入 2。

   h. 输入安装了数据库的设备的 DNS 名称或 IP 地址。`127.0.0.1` 用于本地 DB 安装。

   i. 输入数据库端口号。该端口用于与管理服务器通信。默认情况下，使用以下端口：

- 端口 3306 用于 MySQL 或 MariaDB
- 端口 5432 用于 PostgreSQL 或 Postgres Pro

j. 输入数据库名称。

k. 输入用于访问数据库的数据库根账户的登录名。

l. 输入用于访问数据库的数据库根账户的密码。
等待服务被添加并自动启动：

- klnagent_srv
- kladminserver_srv
- klactprx_srv
- klwebsrv_srv

m. 创建一个将用作管理服务器管理员的账户。输入用户名和密码。您可以使用以下命令创建新用户：
/opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <password>
密码必须符合以下规则：

- 用户密码不能少于 8 个字符或超过 16 个字符。
- 密码必须包含以下组中三组的字符：
  - 大写字母 (A-Z)
  - 小写字母 (a-z)
  - 数字 (0-9)
  - 特殊字符 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

用户已添加并且 Kaspersky Security Center Linux 已安装。

服务验证

使用以下命令检查服务是否正在运行：

- # systemctl status klnagent_srv.service
- # systemctl status kladminserver_srv.service
- # systemctl status klactprx_srv.service
- # systemctl status klwebsrv_srv.service

以静默模式安装 Kaspersky Security Center Linux

您可以在 Linux 设备上安装 Kaspersky Security Center Linux，方法是使用应答文件以静默模式运行安装，即无需用户参与。应答文件包含一组自定义的安装参数：变量及其各自的值。

安装前：

- 安装数据库管理系统 (DBMS)。
- 确保您要安装 Kaspersky Security Center Linux 的设备运行支持的 Linux 分类。

要以静默模式安装 Kaspersky Security Center Linux：

1. 阅读最终用户授权许可协议。只有在您理解并接受最终用户授权许可协议的条款后，才执行下面的步骤。
2. 创建一个组“kladmins”和一个非特权账户“ksc”，该账户必须是“kladmins”组的成员。为此，请在具有 root 权限的账户下依次运行以下命令：
   ```
   # adduser ksc
   # groupadd kladmins
   # gpasswd -a ksc kladmins
   # usermod -g kladmins ksc
   ```
3. 创建应答文件（TXT 格式），并添加 `VARIABLE_NAME=variable_value` 格式的变量列表到应答文件，每个单独一行。应答文件应包括下表中列出的变量。
4. 用以下命令在包含应答文件全称（例如，包括路径）的根环境中设置 `KLAUTOANSWERS` 环境变量的值：
   ```
   export KLAUTOANSWERS=/tmp/ksc_install/answers.txt
   ```
5. 以静默模式运行 Kaspersky Security Center Linux 安装 — 根据您的 Linux 发行版，运行以下命令之一：
   - `# apt install /<path>/ksc64_[ 版本号 ]_amd64.deb`
   - `# yum install /<path>/ksc64-[ 版本号 ].x86_64.rpm -y`
6. 创建一个使用 Kaspersky Security Center Web Console 的用户。为此，请在具有 root 权限的账户下运行以下命令：
   `/opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <密码>`，其中密码必须至少包含 8 个字符。

用作以静默模式安装 Kaspersky Security Center Linux 的参数的应答文件变量

变量名称	是否必需	描述	可能值
EULA_ACCEPTED	是	确认您理解并接受最终用户授权许可协议的条款。	1
PP_ACCEPTED	是	确认您理解并接受隐私政策的条款。	1
KLSRV_UNATT_SERVERADDRESS	是	管理服务器的 DNS 名称或静态 IP 地址。	DNS 名称或 IP 地址
KLSRV_UNATT_PORT_SRV	否	管理服务器端口号。可选默认值是 14000。	端口号
KLSRV_UNATT_PORT_SRV_SSL	否	管理服务器 SSL 端口号。可选默认值是 13000。	端口号
KLSRV_UNATT_PORT_KLOAPI	否	管理服务器 KLOAPI 端口号。可选，默认值 是 13299.	端口号
KLSRV_UNATT_PORT_GUI	否	管理服务器 GUI 端口号。可选	端口号

		默认值是 13291。	
KLSRV_UNATT_NETRANGETYPE	否	您要管理的设备的大概数量。可选默认值是 1。	1 适用于 1 到 100 设备。 2 适用于 101 到 1,0 联网设备。 3 适用于超过 1,00 网设备。
KLSRV_UNATT_DBMS_TYPE	是	数据库管理系统类型：MySQL（MariaDB）或 Postgres。	mysql 或 postgres
KLSRV_UNATT_DBMS_INSTANCE	是	数据库服务器 IP 地址。	IP 地址
KLSRV_UNATT_DBMS_PORT	是	数据库服务器端口。MySQL (MariaDB) 的默认值为 3306；Postgres 的默认值为 5432。	3306 或者 5432
KLSRV_UNATT_DB_NAME	是	数据库名称。	kav
KLSRV_UNATT_DBMS_LOGIN	是	有权访问数据库的用户的用户名。	
KLSRV_UNATT_DBMS_PASSWORD	是	有权访问数据库的用户的密码。	
KLSRV_UNATT_KLADMINSGROUP	是	服务的安全组名称。	kladmins
KLSRV_UNATT_KLSRVUSER	是	用于启动管理服务器服务的账户名。账户必须是 KLSRV_UNATT_KLADMINSGROUP 变量中指定的安全组的成员。	ksc
KLSRV_UNATT_KLSVCUSER	是	用于启动其他服务的账户名。账户必须是 KLSRV_UNATT_KLADMINSGROUP 变量中指定的安全组的成员。	ksc
如果要将管理服务器部署为 Kaspersky Security Center Linux 故障转移集群，应答文件必须包含以下附加变量			
KLFOC_UNATT_NODE	是	节点编号（1 或 2）。	1 or 2
KLFOC_UNATT_STATE_SHARE_MOUNT_PATH	是	状态共享挂载点。	
KLFOC_UNATT_DATA_SHARE_MOUNT_PATH	是	数据共享挂载点。	
KLFOC_UNATT_CONN_MODE	是	故障转移集群连接模式。	VirtualAdapter 或 ExternalLoadBa
万一 KLFOC_UNATT_CONN_MODE 变量的值为 VirtualAdapter，应答文件必须包含以下附加变量：			
KLFOC_UNATT_CONN_MODE_VA_NAME		虚拟网络适配器名称。	
KLFOC_UNATT_CONN_MODE_VA_IPV4	这些变量之一	虚拟网络适配器 IP 地址。	IP 地址
KLFOC_UNATT_CONN_MODE_VA_IPV6		虚拟网络适配器 IPv6 地址。	IPv6 地址

	是必需项		

在封闭软件环境模式下在 Astra Linux 上安装Kaspersky Security Center Linux

本节介绍如何在 Astra Linux 特别版操作系统上安装Kaspersky Security Center Linux 。

安装前：

- 安装数据库管理系统。
- 确保您要安装 Kaspersky Security Center Linux 的设备运行支持的 Linux 分类。
- 下载kaspersky_astra_pub_key.gpg 应用程序密钥。

使用 ksc64_[version_number]_amd64.deb 安装文件。您通过从 Kaspersky 网站下载来接收安装文件。

以拥有 root 权限的账户运行本说明中提供的命令。

在 Astra Linux 特别版（操作更新 1.7.2）和 Astra Linux 特别版（操作更新 1.6）操作系统上安装Kaspersky Security Center Linux：

1. 打开 /etc/digsig/digsig_initramfs.conf 文件，然后指定以下设置：
   ```
   DIGSIG_ELF_MODE=1
   ```
2. 在命令行中，运行以下命令来安装兼容包：
   ```
   apt install astra-digsig-oldkeys
   ```
3. 为应用程序密钥创建一个目录：
   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```
4. 将应用程序密钥放在上一步创建的目录中：
   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```
5. 更新 RAM 磁盘：
   ```
   update-initramfs -u -k all
   ```
   重新启动系统。
6. 创建一个 kladmins 组和一个无特权账户 'ksc'。该账户必须是 'kladmins' 组的成员。为此，请依次运行以下命令：
   ```
   # adduser ksc
   # groupadd kladmins
   # gpasswd -a ksc kladmins
   # usermod -g kladmins ksc
   ```
7. 运行 Kaspersky Security Center Linux 安装：
   ```
   # apt install /<path>/ksc64_[ 版本号 ]_amd64.deb
   ```

8. 运行 Kaspersky Security Center Linux 配置：

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

9. 阅读最终用户授权许可协议 (EULA) 和隐私策略。文本显示在命令行窗口中。按空格键查看下一个文本段。在出现提示时，输入以下值：

   a. 如果您理解并接受 EULA 的条款，请输入“y”。如果您不接受 EULA 的条款，请输入“n”。要使用 Kaspersky Security Center Linux，您必须接受 EULA 的条款。

   b. 如果您理解并接受隐私策略的条款，并且同意您的数据将按照隐私策略中所述进行处理和传输（包括传输到第三方国家），请输入“y”。如果您不接受隐私策略的条款，请输入“n”。要使用 Kaspersky Security Center Linux，您必须接受隐私策略的条款。

10. 出现提示时，输入以下设置：

    a. 输入管理服务器的 DNS 名称或静态 IP 地址。

    b. 输入管理服务器端口号。默认情况下使用端口 14000。

    c. 输入管理服务器 SSL 端口号。默认情况下使用端口 13000。

    d. 评估您要管理的设备的大概数量：

    - 如果有 1 到 100 台联网设备，则输入“1”。
    - 如果有 101 到 1000 台联网设备，则输入“2”。
    - 如果有超过 1000 台联网设备，则输入“3”。

    e. 输入服务的安全组名称。默认情况下，使用“kladmins”组。

    f. 输入用于启动管理服务器服务的账户名。该账户必须是输入的安全组的成员。默认情况下，使用“ksc”账户。

    g. 输入用于启动其他服务的账户名。该账户必须是输入的安全组的成员。默认情况下，使用“ksc”账户。

    h. 输入安装了数据库的设备的 IP 地址。

    i. 输入数据库端口号。该端口用于与管理服务器通信。默认情况下使用端口 3306。

    j. 输入数据库名称。

    k. 输入用于访问数据库的数据库根账户的登录名。

    l. 输入用于访问数据库的数据库根账户的密码。

    等待服务被添加并自动启动：

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

m. 创建一个将用作管理服务器管理员的账户。输入用户名和密码。

密码必须符合以下规则：

- 用户密码必须最少包含 8 个字符，最多包含 16 个字符。
- 密码必须包含以下组中三组的字符：
  - 大写字母 (A-Z)
  - 小写字母 (a-z)
  - 数字 (0-9)
  - 特殊字符 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

Kaspersky Security Center Linux 已安装，用户已添加。

服务验证

使用以下命令检查服务是否正在运行：

- `# systemctl status klnagent_srv.service`
- `# systemctl status kladminserver_srv.service`
- `# systemctl status klactprx_srv.service`
- `# systemctl status klwebsrv_srv.service`

安装 Kaspersky Security Center Web Console

该部分描述了如何单独安装 Kaspersky Security Center Web Console 服务器 (也叫 Kaspersky Security Center Web Console) 到运行 Linux 操作系统的设备。安装之前，您必须安装数据库管理系统和 Kaspersky Security Center Linux 管理服务器。

> 如果您在封闭软件环境模式下的 Astra Linux 上安装 Kaspersky Security Center Web Console，请按照Astra Linux 特定说明进行操作。

使用与您设备上安装的 Linux 发行版对应的以下安装文件之一：

- 对于 Debian - ksc-web-console-[build_number].x86_64.deb
- 对于基于 RPM 的操作系统 - ksc-web-console-[build_number].x86_64.rpm
- 对于 Alt 8 SP - ksc-web-console-[build_number]-alt8p.x86_64.rpm

您通过从 Kaspersky 网站下载来接收安装文件。

要安装 Kaspersky Security Center Web Console：

1. 确保您要安装 Kaspersky Security Center Web Console 的设备运行支持的 Linux 分类。

2. 阅读最终用户授权许可协议 (EULA)。如果 Kaspersky Security Center Linux 分发包不包含带有 EULA 文本的 TXT 文件，您可以从 卡巴斯基网站 下载文件。如果您不接受授权许可协议的条款，不要安装应用程序。

3. 创建包含参数的响应文件以连接 Kaspersky Security Center Web Console 到管理服务器。命名该文件为 ksc-web-console-setup.json 并将其放置到以下目录：/etc/ksc-web-console-setup.json。

   响应文件的一个例子，它包含最小参数集以及默认地址和端口：

   ```
   {
   "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
   }
   ```

   在 Linux ALT 操作系统上安装 Kaspersky Security Center Web Console 时，必须指定除 8080 以外的端口号，因为端口 8080 被操作系统使用。

   Kaspersky Security Center Web Console 无法使用相同的 .rpm 安装文件更新。如果您要在响应文件中更改设置并使用该文件重新安装应用程序，您必须先卸载该应用程序，然后使用新的响应文件再次安装。

4. 在具有根特权的账户下，根据您的 Linux 分类使用命令行运行 .deb 或 .rpm 安装文件。

   - 要通过 .deb 文件安装或升级 Kaspersky Security Center Web Console，请运行以下命令：
     ```
     $ sudo dpkg -i ksc-web-console-[build_number].x86_64.deb
     ```
   - 要从 .rpm 文件安装 Kaspersky Security Center Web Console，运行以下命令之一：
     ```
     $ sudo rpm -ivh --nodeps ksc-web-console-[build_number].x86_64.rpm
     ```
     或
     ```
     $ sudo alien -i ksc-web-console-[build_number].x86_64.rpm
     ```
   - 要从先前版本的 Kaspersky Security Center Web Console 升级，请运行以下命令之一：
     - 对于运行基于 RPM 的操作系统的设备：
       ```
       $ sudo rpm -Uvh --nodeps --force ksc-web-console-[build_number].x86_64.rpm
       ```
     - 对于运行基于 Debian 的操作系统的设备：
       ```
       $ sudo dpkg -i ksc-web-console-[build_number].x86_64.deb
       ```

   这将开始解包安装文件。请等待安装完成。Kaspersky Security Center Web Console 被安装到以下目录：/var/opt/kaspersky/ksc-web-console。

5. 通过执行以下命令重新启动所有 Kaspersky Security Center Web Console 服务：
   ```
   $ sudo systemctl restart KSC*
   ```

当安装完成时，您可以使用您的浏览器打开和登录 Kaspersky Security Center Web Console。

Kaspersky Security Center Web Console 安装参数

对于在运行 Linux 的设备上安装 Kaspersky Security Center Web Console 服务器，您必须创建响应文件 — 一个包含连接 Kaspersky Security Center Web Console 到管理服务器的参数的 .json 文件。

这里是响应文件的一个例子，它包含最小参数集以及默认地址和端口：

```
{
"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": "Group1:User1",
"managementServiceAccount": "Group1:User2",
"serviceWebConsoleAccount": "Group1:User3",
"pluginAccount": "Group1:User4",
"messageQueueAccount": "Group1:User5"
}
```

在 Linux ALT 操作系统上安装 Kaspersky Security Center Web Console 时，必须指定除 8080 以外的端口号，因为端口 8080 被操作系统使用。

下表描述了可以在响应文件中指定的参数。

安装 Kaspersky Security Center Web Console 到运行 Linux 的设备的参数

参数	描述	可用值
address	Kaspersky Security Center Web Console 服务器的地址（必需）。	字符串值。
port	Kaspersky Security Center Web Console 用于连接到管理服务器的端口号（必需）。	数字值。
defaultLangId	用户界面语言（默认，1033）。	语言数码： • 德语：1031 • 英语：1033 • 西班牙语：3082 • 西班牙语（墨西哥）：2058 • 法语：1036 • 日语：1041 • 哈萨克语：1087

		• 波兰语：1045 • 葡萄牙语（巴西）：1046 • 俄语：1049 • 土耳其语：1055 • 简体中文：4 • 繁体中文：31748 如果没有指定值，则使用 English (en-US)
enableLog	是否启用 Kaspersky Security Center Web Console 活动日志记录。	布尔值： • true—启用日志（默认选中）。 • false—禁用日志。
trusted	允许连接到 Kaspersky Security Center Web Console 的受信任管理服务器列表。每个管理服务器必须使用以下参数定义： • 管理服务器地址 • Kaspersky Security Center Web Console 用以连接到管理服务器的 OpenAPI 端口（默认是 13299） • 管理服务器证书路径 • 将显示在登录窗口的管理服务器名称 参数使用竖线分隔。如果指定了几个管理服务器，使用两个竖线将它们分隔。	以下格式的字符串值： " server address | port | certificat 例如： "X.X.X.X|13299|/cert/server-1.ce 1 ||Y.Y.Y.Y|13299|/cert/server-2.
acceptEula	您是否要接受最终用户授权许可协议(EULA)的条款。包含 EULA 条款的文件和安装文件一起下载。	布尔值： • true – 我已完全阅读、理解并接受最 • false – 我不接受授权许可协议的条款 如果未指定任何值，Kaspersky Security C 向您显示 EULA 并询问您是否同意接受 E
certDomain	如果您要生成新证书，使用该参数指定生成新证书的域名。	字符串值。
certPath	如果您要使用现有证书，使用该参数指定证书文件路径。	字符串值。 指定路径"/var/opt/kaspersky/klnagent_sr 使用现有证书。对于自定义证书，请指定
keyPath	如果您要使用现有证书，使用该参数指定密钥文件路径。	字符串值。

`webConsoleAccount`	运行 KSCWebConsole 服务的账户的名称。	以下格式的字符串值：`"group name:u` 例如：`"Group1:User1"`. 如果未指定任何值，Kaspersky Security C 使用默认名称 `user_management_%uid%`
`managementServiceAccount`	运行 KSCWebConsoleManagement 服务的特权账户的名称。	以下格式的字符串值：`"group name:u` 例如：`"Group1:User1"`. 如果未指定任何值，Kaspersky Security C 使用默认名称 `user_nodejs_%uid%` 创建
`serviceWebConsoleAccount`	运行 KSCSvcWebConsole 服务的账户的名称。	以下格式的字符串值：`"group name:u` 例如：`"Group1:User1"`. 如果未指定任何值，Kaspersky Security C 使用默认名称 `user_svc_nodejs_%uid%`
`pluginAccount`	运行 KSCWebConsolePlugin 服务的账户的名称。	以下格式的字符串值：`"group name:u` 例如：`"Group1:User1"`. 如果未指定任何值，Kaspersky Security C 使用默认名称 `user_web_plugin_%uid%`
`messageQueueAccount`	运行 KSCWebConsoleMessageQueue 服务的账户的名称。	以下格式的字符串值：`"group name:u` 例如：`"Group1:User1"`. 如果未指定任何值，Kaspersky Security C 使用默认名称 `user_message_queue_%u`

如果指定 `webConsoleAccount`、`managementServiceAccount`、`serviceWebConsoleAccount`、`pluginAccount` 或 `messageQueueAccount` 参数，请确保自定义用户账户属于同一安全组。如果未指定这些参数，Kaspersky Security Center Web Console 安装程序会创建一个默认安全组，然后在该组中创建具有默认名称的用户账户。

在封闭软件环境模式下在 Astra Linux 上安装Kaspersky Security Center Linux

该部分描述了如何单独安装 Kaspersky Security Center Web Console 服务器 (也叫 Kaspersky Security Center Web Console) 到 Astra Linux 特别版操作系统。安装之前，您必须安装数据库管理系统和 Kaspersky Security Center Linux 管理服务器。

要安装 Kaspersky Security Center Web Console：

1. 确保您要安装 Kaspersky Security Center Web Console 的设备运行支持的 Linux 分类。
2. 阅读最终用户授权许可协议 (EULA)。如果 Kaspersky Security Center Linux 分发包不包含带有 EULA 文本的 TXT 文件，您可以从 卡巴斯基网站 下载文件。如果您不接受授权许可协议的条款，不要安装应用程序。
3. 创建包含参数的响应文件以连接 Kaspersky Security Center Web Console 到管理服务器。命名该文件为 ksc-web-console-setup.json 并将其放置到以下目录：/etc/ksc-web-console-setup.json。

   响应文件的一个例子，它包含最小参数集以及默认地址和端口：

   ```
   {
   "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
}
```

4. 打开 /etc/digsig/digsig_initramfs.conf 文件，然后指定以下设置：

   ```
   DIGSIG_ELF_MODE=1
   ```

5. 在命令行中，运行以下命令来安装兼容包：

   ```
   apt install astra-digsig-oldkeys
   ```

6. 为应用程序密钥创建一个目录：

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

7. 将应用程序密钥 /opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg 放在上一步创建的目录中：

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

   > 如果 Kaspersky Security Center Linux 分发包不包含 kaspersky_astra_pub_key.gpg 应用程序密钥，您可以通过单击以下链接下载：https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg。

8. 更新 RAM 磁盘：

   ```
   update-initramfs -u -k all
   ```

   重新启动系统。

9. 在具有 root 权限的账户下，使用命令行运行安装文件。您通过从 Kaspersky 网站下载来接收安装文件。

   - 要安装或升级 Kaspersky Security Center Web Console，请运行以下命令：

     ```
     $ sudo dpkg -i ksc-web-console-[build_number].x86_64.deb
     ```

   - 要从先前版本的 Kaspersky Security Center Web Console 升级，请运行以下命令：

     ```
     $ sudo dpkg -i ksc-web-console-[build_number].x86_64.deb
     ```

   这将开始解包安装文件。请等待安装完成。Kaspersky Security Center Web Console 被安装到以下目录：/var/opt/kaspersky/ksc-web-console。

10. 通过执行以下命令重新启动所有 Kaspersky Security Center Web Console 服务：

    ```
    $ sudo systemctl restart KSC*
    ```

当安装完成时，您可以使用您的浏览器打开和登录 Kaspersky Security Center Web Console。

安装 Kaspersky Security Center Web Console，其已连接到安装在 Kaspersky Security Center Linux 故障转移集群节点上的管理服务器

本节介绍如何安装 Kaspersky Security Center Web Console Server（以下也称为 Kaspersky Security Center Web Console），其连接到安装在 Kaspersky Security Center Linux 故障转移集群节点上的管理服务器。在安装 Kaspersky Security Center Web Console 之前，在Kaspersky Security Center Linux 故障转移集群节点上安装数据库管理系统 和 Kaspersky Security Center Linux 管理服务器。

要安装连接到安装在 Kaspersky Security Center Linux 故障转移集群节点上的管理服务器的 Kaspersky Security Center Web Console：

1. 执行 Kaspersky Security Center Web Console 安装的步骤 1 和步骤 2。
2. 在第 3 步，在响应文件中指定受信任的安装参数以允许 Kaspersky Security Center Linux 故障转移集群连接到 Kaspersky Security Center Web Console。此参数的字符串值具有以下格式：
   `“trusted”: "服务器地址|端口|证书路径|服务器名称"`

   指定`trusted`安装参数的组件：

   - **管理服务器地址**。如果您在准备集群节点时创建了从属网络适配器，请使用适配器的 IP 地址作为 Kaspersky Security Center Linux 故障转移集群地址。否则，请指定您使用的第三方负载平衡器的 IP 地址。
   - **管理服务器端口**。Kaspersky Security Center Web Console 用于连接到管理服务器的 OpenAPI 端口（默认 13299）。
   - **管理服务器证书**。管理服务器证书位于 Kaspersky Security Center Linux 故障转移集群的共享数据存储中。证书文件的默认路径：<shared data folder>\1093\cert\klserver.cer。将证书文件从共享数据存储复制到安装 Kaspersky Security Center Web Console 的设备。指定管理服务器证书的本地路径。
   - **管理服务器名称**。将显示在 Kaspersky Security Center Web Console 登录窗口中的 Kaspersky Security Center Linux 故障转移集群名称。
3. 继续 Kaspersky Security Center Web Console 的标准安装。

在安装成功完成后，桌面上将出现一个快捷方式，您可以登录到 Kaspersky Security Center Web Console。

您可以前往**发现和部署 → 未分配的设备**查看集群节点和文件服务器的信息。

Kaspersky Security Center Linux 故障转移集群部署

本节包含有关 Kaspersky Security Center Linux 故障转移集群的常规信息，以及有关在网络中准备和部署 Kaspersky Security Center Linux 故障转移集群的说明。

方案：部署 Kaspersky Security Center Linux 故障转移集群

Kaspersky Security Center Linux 故障转移集群提供 Kaspersky Security Center Linux 的高可用性，并在出现故障时最大限度地减少管理服务器的停机时间。故障转移集群基于安装在两台计算机上的两个相同 Kaspersky Security Center Linux 实例。其中一个实例用作主动节点，另一个实例用作被动节点。主动节点管理客户端设备的保护，而被动节点准备在主动节点出现故障时承担主动节点的所有功能。当出现故障时，被动节点成为主动节点，主动节点成为被动节点。

先决条件

您拥有满足故障转移集群要求的硬件。

Kaspersky 应用程序部署分阶段进行：

1. **为 Kaspersky Security Center Linux 服务创建账户**

在主动节点、被动节点和文件服务器上执行以下步骤：

1. 创建一个名为“kladmins”的域组，并为所有三个组分配相同 GID。
2. 创建一个名为“ksc”的用户账户，并将相同 UID 分配给所有三个用户账户。将创建的账户的主要组设置为“kladmins”。
3. 创建一个名为“rightless”的用户账户，并为所有三个用户账户分配相同 UID。将创建的账户的主要组设置为“kladmins”。

2. **文件服务器准备**

   准备将用作 Kaspersky Security Center Linux 故障转移集群组件的文件服务器。确保该文件服务器满足硬件和软件要求，为 Kaspersky Security Center Linux 数据创建两个共享文件夹，并配置这两个共享文件夹的访问权限。

   操作说明：为 Kaspersky Security Center Linux 故障转移集群准备文件服务器

3. **准备主动和被动节点**

   准备两台具有相同硬件和软件的计算机，它们将用作主动和被动节点。

   操作说明：为 Kaspersky Security Center Linux 故障转移集群准备节点

4. **数据库管理系统 (DBMS) 安装**

   您有两个选项：

   - 如果您想使用 MariaDB Galera Cluster，则 DBMS 不需要专用计算机。在每个节点上安装 MariaDB Galera Cluster。
   - 如果您想使用任何其他受支持的 DBMS，在专用计算机上安装选定的 DBMS。

5. **Kaspersky Security Center Linux 安装**

   在两个节点上均以故障转移集群模式安装 Kaspersky Security Center Linux。必须先在主动节点上安装 Kaspersky Security Center Linux，然后在被动节点上安装。

   此外，您可以在不是集群节点的单独设备上安装 Kaspersky Security Center Web Console。

6. **测试故障转移集群**

   检查您是否正确配置了故障转移集群以及它是否正常工作。例如，您可以停止主动节点上的 Kaspersky Security Center Linux 服务之一：kladminserver、klnagent、ksnproxy、klactprx 或 klwebsrv。服务停止后，保护管理必须自动切换到被动节点。

结果

Kaspersky Security Center Linux 故障转移集群已部署。请熟悉导致主动和被动节点切换的事件。

关于 Kaspersky Security Center Linux 故障转移集群

Kaspersky Security Center Linux 故障转移集群提供 Kaspersky Security Center Linux 的高可用性，并在出现故障时最大限度地减少管理服务器的停机时间。故障转移集群基于安装在两台计算机上的两个相同 Kaspersky Security Center Linux 实例。其中一个实例用作主动节点，另一个实例用作被动节点。主动节点管理客户端设备的保护，而被动节点准备在主动节点出现故障时承担主动节点的所有功能。当出现故障时，被动节点成为主动节点，主动节点成为被动节点。

在 Kaspersky Security Center Linux 故障转移集群中，所有 Kaspersky Security Center Linux 服务都是自动管理的。不要尝试手动重新启动服务。

硬件和软件要求

要部署 Kaspersky Security Center Linux 故障转移集群，您必须拥有以下硬件：

- 两台具有相同硬件和软件的计算机。这两台计算机将用作主动和被动节点。
- 运行 Linux 的文件服务器，带有 EXT4 文件系统。您必须提供一台专用计算机来用作文件服务器。

  确保在文件服务器与主动和被动节点之间提供了高网络带宽。

- 一台具有数据库管理系统 (DBMS) 的计算机。如果使用 MariaDB Galera Cluster 作为 DBMS，则不需要专用计算机。

切换条件

如果主动节点上发生以下任何事件，故障转移集群会将客户端设备的保护管理从主动节点切换到被动节点：

- 由于软件或硬件故障，主动节点损坏。
- 由于维护活动，主动节点暂时停止。
- 至少一个 Kaspersky Security Center Linux 服务（或进程）故障或被用户故意终止。Kaspersky Security Center Linux 服务如下：kladminserver、klnagent、klactprx 和 klwebsrv。
- 主动节点与文件服务器上的存储之间的网络连接中断或终止。

为 Kaspersky Security Center Linux 故障转移集群准备文件服务器

文件服务器是 Kaspersky Security Center Linux 故障转移集群的必需组件。

要准备文件服务器：

1. 确保文件服务器满足硬件和软件要求。
2. 安装和配置 NFS 服务器：
   - 必须在 NFS 服务器设置中为两个节点都启用对文件服务器的访问。
   - NFS 协议的版本必须是 4.0 或 4.1。
   - Linux 内核的最低要求：
     - 3.19.0-25，如果您使用 NFS 4.0
     - 4.4.0-176，如果您使用 NFS 4.1

3. 在文件服务器上，创建两个文件夹并使用 NFS 共享它们。其中一个用于保存有关故障转移集群状态的信息。另一个用于存储 Kaspersky Security Center Linux 的数据和设置。您在配置 Kaspersky Security Center Linux 的安装时将指定共享文件夹的路径。

   运行以下命令：

   ```
   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
   ```

   通过运行以下命令启用自动启动：

   ```
   sudo systemctl enable rpcbind
   ```

4. 重新启动文件服务器。

文件服务器已准备就绪。要部署 Kaspersky Security Center Linux 故障转移集群，请按照此方案中的进一步说明进行操作。

为 Kaspersky Security Center Linux 故障转移集群准备节点

准备两台计算机作为 Kaspersky Security Center Linux 故障转移集群的主动和被动节点。

要为 Kaspersky Security Center Linux 故障转移集群准备节点：

1. 确保有两台符合硬件和软件要求的计算机。这两台计算机将用作故障转移集群的主动和被动节点。

2. 要使节点充当 NFS 客户端，请在每个节点上安装 nfs-utils 包。

   运行以下命令：

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

3. 通过运行以下命令创建挂载点：

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

4. 检查共享文件夹是否可以成功挂载。[可选步骤]

   运行以下命令：

   ```
   sudo mount -t nfs -o vers=4,nolock,local_lock=none,auto,user,rw {服务器}:
   {KlFocStateShare 文件夹的路径/mnt/KlFocStateShare
   sudo mount -t nfs -o vers=4,nolock,local_lock=none,noauto,user,rw {服务器}:
   {KlFocDataShare_klfoc 文件夹的路径} /mnt/KlFocDataShare_klfoc
   ```

   这里，{服务器}:{KlFocStateShare 文件夹的路径} 和 {服务器}:{KlFocDataShare_klfoc 文件夹的路径} 是文件服务器上共享文件夹的网络路径。

   成功挂载共享文件夹后，通过运行以下命令卸载它们：

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

5. 匹配挂载点和共享文件夹：

```
sudo vi /etc/fstab
{服务器}:{KlFocStateShare 文件夹的路径} /mnt/KlFocStateShare nfs
vers=4,nolock,local_lock=none,auto,user,rw 0 0
{服务器}:{KlFocDataShare_klfoc 文件夹的路径} /mnt/KlFocDataShare_klfoc nfs
vers=4,nolock,local_lock=none,noauto,user,rw 0 0
```

这里，{服务器}:{KlFocStateShare 文件夹的路径}和{服务器}:{KlFocDataShare_klfoc 文件夹的路径}是文件服务器上共享文件夹的网络路径。

6. 重新启动两个节点。

7. 通过运行以下命令挂载共享文件夹：

```
mount /mnt/KlFocStateShare
mount /mnt/KlFocDataShare_klfoc
```

8. 确保访问共享文件夹的权限属于 ksc:kladmins。

运行以下命令：

```
sudo ls -la /mnt/
```

9. 在每个节点上，配置一个从属网络适配器。

从属网络适配器可以是物理或虚拟适配器。如果要使用物理网络适配器，请使用标准操作系统工具连接并配置它。如果要使用虚拟网络适配器，请使用第三方软件创建它。

执行以下操作之一：

- 使用虚拟网络适配器。

  a. 使用以下命令检查 NetworkManager 是否用于管理物理适配器：

  ```
  nmcli 设备状态
  ```

  如果物理适配器在输出中显示为不受管理，请配置 NetworkManager 以管理物理适配器。确切的配置步骤取决于您的发行包。

  b. 使用以下命令识别接口：

  ```
  ip a
  ```

  c. 创建一个新的配置文件：

  ```
  nmcli connection add type macvlan dev <physical interface> mode bridge
  ifname <virtual interface> ipv4.addresses <address mask> ipv4.method manual
  autoconnect no
  ```

- 使用物理网络适配器或 hypervisor。在这种情况下，请禁用软件 NetworkManager。

  a. 删除目标接口的 NetworkManager 连接：

  ```
  nmcli con del <connection name>
  ```

  使用以下命令检查目标接口是否有连接：

  ```
  nmcli con show
  ```

  b. 编辑 NetworkManager.conf 文件。找到密钥文件部分并将目标接口分配给 unmanaged-devices 参数。

  ```
  [keyfile]
  unmanaged-devices=interface-name:<interface name>
  ```

c. 重启 NetworkManager：

```
systemctl reload NetworkManager
```

使用以下命令验证目标接口是否不受管理：

```
nmcli dev status
```

- 使用第三方负载平衡器。例如，您可以使用 nginx 服务器。在这种情况下，请执行以下操作：

  a. 提供一台基于 Linux 且安装了 nginx 的专用计算机。

  b. 配置负载平衡。设置主动节点为主服务器，被动节点为备份服务器。

  c. 在 nginx 服务器上，开放所有管理服务器端口：TCP 13000、UDP 13000、TCP 13291、TCP 13299 和 TCP 17000。

节点已准备就绪。要部署 Kaspersky Security Center Linux 故障转移集群，请按照方案中的进一步说明进行操作。

在 Kaspersky Security Center Linux 障转移集群节点上安装 Kaspersky Security Center Linux

此过程描述了如何在 Kaspersky Security Center Linux 故障转移集群的节点上安装 Kaspersky Security Center Linux。Kaspersky Security Center Linux 分别安装在 Kaspersky Security Center Linux 故障转移集群的两个节点上。首先，在主动节点上安装该应用程序，然后在被动节点上安装。安装时，选择哪个节点是主动节点，哪个节点是被动节点。

使用安装文件—ksc64_[版本号]_amd64.deb 或 ksc64-[版本号].x86_64.rpm—对应于您设备上的 Linux 版本。您通过从 Kaspersky 网站下载来接收安装文件。

只有 KLAdmins 域组中的用户可以在每个节点上安装 Kaspersky Security Center Linux。

在主（活动）节点上安装

在主节点上安装 Kaspersky Security Center Linux：

1. 确保您要安装 Kaspersky Security Center Linux 的设备运行支持的 Linux 分类。
2. 在命令行中，以拥有 root 权限的账户运行本说明中提供的命令。
3. 运行 Kaspersky Security Center Linux 安装。根据您的 Linux 发行版，运行以下命令之一：
   - `sudo apt install /<path>/ksc64_[ 版本号 ]_amd64.deb`
   - `sudo yum install /<path>/ksc64-[ 版本号 ].x86_64.rpm -y`
4. 运行 Kaspersky Security Center Linux 配置：

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

5. 阅读最终用户授权许可协议 (EULA) 和隐私策略。文本显示在命令行窗口中。按空格键查看下一个文本段。然后，在出现提示时，输入以下值：

   a. 如果您理解并接受 EULA 的条款，请输入“y”。如果您不接受 EULA 的条款，请输入“n”。要使用 Kaspersky Security Center Linux，您必须接受 EULA 的条款。

   b. 如果您理解并接受隐私策略的条款，并且同意您的数据将按照隐私策略中所述进行处理和传输（包括传输到第三方国家），请输入“y”。如果您不接受隐私策略的条款，请输入“n”。要使用 Kaspersky Security Center Linux，您必须接受隐私策略的条款。

6. 选择“**主集群节点**”作为管理服务器安装模式。

7. 出现提示时，输入以下设置：

   a. 输入状态共享挂载点的本地路径。

   b. 输入数据共享挂载点的本地路径。

   c. 选择故障转移集群连接模式：通过从属网络适配器或外部负载平衡器。

   d. 如果使用从属网络适配器，请输入其名称。

   e. 当系统提示您输入管理服务器 DNS 名称或静态 IP 地址时，请输入从属网络适配器的 IP 地址或外部负载平衡器的 IP 地址。

   f. 输入管理服务器 SSL 端口号。默认情况下使用端口 13000。

   g. 评估您要管理的设备的大概数量：

      - 如果有 1 到 100 台联网设备，则输入“1”。
      - 如果有 101 到 1000 台联网设备，则输入“2”。
      - 如果有超过 1000 台联网设备，则输入“3”。

   h. 输入服务的安全组名称。默认情况下，使用“kladmins”组。

   i. 输入用于启动管理服务器服务的账户名。该账户必须是输入的安全组的成员。默认情况下，使用“ksc”账户。

   j. 输入用于启动其他服务的账户名。该账户必须是输入的安全组的成员。默认情况下，使用“ksc”账户。

   k. 选择您安装的与 Kaspersky Security Center Linux 一起使用的 DBMS：

      - 如果您安装了 MySQL 或 MariaDB，请输入 1。
      - 如果您安装了 PostgreSQL 或 Postgres Pro，请输入 2。

   l. 输入安装了数据库的设备的 DNS 名称或 IP 地址。

   m. 输入数据库端口号。该端口用于与管理服务器通信。默认情况下，使用以下端口：

      - 端口 3306 用于 MySQL 或 MariaDB
      - 端口 5432 用于 PostgreSQL 或 Postgres Pro

n. 输入数据库名称。

o. 输入用于访问数据库的数据库根账户的登录名。

p. 输入用于访问数据库的数据库根账户的密码。
等待服务被添加并自动启动：

- klnagent_srv
- kladminserver_srv
- klactprx_srv
- klwebsrv_srv

q. 创建一个将用作管理服务器管理员的账户。输入用户名和密码。用户密码不能少于 8 个字符或超过 16 个字符。

用户已添加并且 Kaspersky Security Center Linux 已安装在主节点上。

在辅助（被动）节点上安装

要在辅助节点上安装 Kaspersky Security Center Linux：

1. 确保您要安装 Kaspersky Security Center Linux 的设备运行支持的 Linux 分类。
2. 在命令行中，以拥有 root 权限的账户运行本说明中提供的命令。
3. 运行 Kaspersky Security Center Linux 安装。根据您的 Linux 发行版，运行以下命令之一：
   - `sudo apt install /<path>/ksc64_[版本号]_amd64.deb`
   - `sudo yum install /<path>/ksc64-[版本号].x86_64.rpm -y`
4. 运行 Kaspersky Security Center Linux 配置：
   ```
   sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```
5. 阅读最终用户授权许可协议 (EULA) 和隐私策略。文本显示在命令行窗口中。按空格键查看下一个文本段。然后，在出现提示时，输入以下值：
   a. 如果您理解并接受 EULA 的条款，请输入“y”。如果您不接受 EULA 的条款，请输入“n”。要使用 Kaspersky Security Center Linux，您必须接受 EULA 的条款。
   b. 如果您理解并接受隐私策略的条款，并且同意您的数据将按照隐私策略中所述进行处理和传输（包括传输到第三方国家），请输入“y”。如果您不接受隐私策略的条款，请输入“n”。要使用 Kaspersky Security Center Linux，您必须接受隐私策略的条款。
6. 选择”**辅助集群节点**“作为管理服务器安装模式。
7. 出现提示时，输入状态共享挂载点的本地路径。

Kaspersky Security Center Linux 安装在辅助节点上。

服务验证

使用以下命令检查服务是否正在运行：

- `systemctl status klnagent_srv.service`
- `systemctl status kladminserver_srv.service`
- `systemctl status klactprx_srv.service`
- `systemctl status klwebsrv_srv.service`

现在，您可以测试 Kaspersky Security Center Linux 故障转移集群，以确保配置正确并且集群正常工作。

手动启动和停止集群节点

您可能需要停止整个 Kaspersky Security Center Linux 故障转移集群或临时分离集群的一个节点才能进行维护。如果是这种情况，请按照本节中的说明进行操作。请勿尝试通过任何其他方式启动或停止与故障转移集群相关的服务或进程。这可能会导致数据丢失。

启动和停止整个故障转移集群以进行维护

要启动或停止整个故障转移集群：

1. 在活动节点上，转到 /opt/kaspersky/ksc64/sbin。
2. 打开命令行，然后运行以下命令之一：
   - 要停止集群，请运行：`klfoc -stopcluster --stp klfoc`
   - 要启动集群，请运行：`klfoc -startcluster --stp klfoc`

   启动还是停止故障转移集群取决于您运行的命令。

维护其中一个节点

要维护其中一个节点：

1. 在主动节点上，使用 `klfoc -stopcluster --stp klfoc` 命令停止故障转移集群。
2. 在要维护的节点上，转到/opt/kaspersky/ksc64/sbin。
3. 打开命令行，然后运行 `detach_node.sh` 命令将节点从集群中分离。
4. 在主动节点上，使用 `klfoc -startcluster --stp klfoc` 命令启动故障转移集群。
5. 执行维护活动。
6. 在主动节点上，使用 `klfoc -stopcluster --stp klfoc` 命令停止故障转移集群。
7. 在维护的节点上，转到/opt/kaspersky/ksc64/sbin。

8. 打开命令行，然后运行 `attach_node.sh` 命令将节点连接到集群。

9. 在主动节点上，使用 `klfoc -startcluster --stp klfoc` 命令启动故障转移集群。

该节点维护完毕并连接到故障转移集群。

使用 DBMS 的账户

要安装管理服务器并使用它，您需要一个内部 DBMS 账户。此账户允许您访问 DBMS 但需要特定权限。所需权限取决于以下标准：

- DBMS 类型：
  - MySQL 或 MariaDB
  - PostgreSQL 或 Postgres Pro
- 管理服务器数据库创建的方法：
  - **自动**。在安装管理服务器的过程中，您可以使用管理服务器安装程序（简称“安装程序”）自动创建一个管理服务器数据库（以下简称“服务器数据库”）。
  - **手动**。您可以使用第三方应用程序（例如 SQL Server Management Studio）或脚本来创建空数据库。之后，您可以在管理服务器安装期间将此数据库指定为服务器数据库。

为账户授予权限时，请遵循最低权限原则。这意味着授予的权限应以足以执行所需操作为限。

下表包含有关在安装和启动管理服务器之前应授予账户的 DBMS 权限的信息。

MySQL 和 MariaDB

如果您选择 MySQL 或 MariaDB 作为 DBMS，请创建一个 DBMS 内部账户来访问 DBMS，然后授予该账户所需的权限。请注意，数据库创建方法不影响权限集。所需权限如下所列：

- 架构权限：
  - 管理服务器数据库：ALL（不包括 GRANT OPTION）。
  - 系统架构（mysql 和 sys）：SELECT、SHOW VIEW。
  - sys.table_exists 存储过程：EXECUTE（如果您使用 MariaDB 10.5 或更早版本作为 DBMS，则无需授予 EXECUTE 权限）。
- 所有架构的全局权限：PROCESS、SUPER。

有关如何配置账户权限的更多信息，请参阅配置用于 MySQL 和 MariaDB 的 DBMS 账户。

配置管理服务器数据恢复的权限

您授予内部 DBMS 账户的权限足以从备份中恢复管理服务器数据。

PostgreSQL 或 Postgres Pro

如果您选择 PostgreSQL 或 Postgres Pro 作为 DBMS，您可以使用 *postgres* 用户（默认的 Postgres 角色）或创建一个新的 Postgres 角色（以下也称为“角色”）来访问 DBMS。根据服务器数据库的创建方法，如下表所述向角色授予所需权限。有关如何配置角色权限的更多信息，请参阅配置用于 PostgreSQL 或 Postgres Pro 的 DBMS 账户。

Postgres 角色的权限

自动创建数据库		手动创建数据库
postgres 用户不需要额外的权限。	新角色的权限：CREATEDB。	对于新角色： • 针对管理服务器数据库的权限：ALL。 • 针对公共架构中所有表的权限：ALL。 • 针对公共架构中所有序列的特权：ALL。

配置管理服务器数据恢复的权限

若要从备份恢复管理服务器数据，用于访问 DBMS 的 Postgres 角色必须具有针对管理服务器数据库的所有者权限。

配置使用 MySQL 和 MariaDB 的 DBMS 账户

先决条件

在为 DBMS 账户分配权限之前，请执行以下操作：

1. 确保您以本地管理员账户登录系统。
2. 安装 MySQL 或 MariaDB 的使用环境。

配置安装管理服务器的 DBMS 账户

要配置用于安装管理服务器的 DBMS 账户：

1. 在安装 DBMS 时创建的根账户下运行 MySQL 或 MariaDB 的使用环境。
2. 创建一个带密码的内部 DBMS 账户。管理服务器安装程序（以下也简称为“安装程序”）和管理服务器服务将使用此内部 DBMS 账户访问 DBMS。

   要创建带密码的 DBMS 账户，请执行以下命令：

   ```
   /* 创建一个名为 KSCAdmin 的用户并为 KSCAdmin 指定密码 */
   CREATE USER 'KSCAdmin' IDENTIFIED BY '<password>';
   ```

如果您使用 MySQL 8.0 或更早版本作为 DBMS，请注意这些版本不支持“缓存 SHA2 密码”身份验证。将默认身份验证从“缓存 SHA2 密码”更改为“MySQL 本机密码”：

- 要创建使用“MySQL本机密码”身份认证的 DBMS 账户，执行以下命令：

  ```
  CREATE USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<password>';
  ```

- 要更改现有 DBMS 账户的身份验证，执行以下命令：

  ```
  ALTER USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<password>';
  ```

3. 为创建的 DBMS 账户授予以下权限：

   - 架构权限：
     - 管理服务器数据库：ALL（不包括 GRANT OPTION）
     - 系统方案（mysql 和 sys）：SELECT、SHOW VIEW
     - sys.table_exists 存储过程：EXECUTE
   - 所有方案的全局权限：PROCESS、SUPER

   要向创建的 DBMS 账户授予所需的权限，请运行以下脚本：

   ```
   /* Grant privileges to KSCAdmin */
   GRANT USAGE ON *.* TO 'KSCAdmin';
   GRANT ALL ON kav.* TO 'KSCAdmin';
   GRANT SELECT, SHOW VIEW ON mysql.* TO 'KSCAdmin';
   GRANT SELECT, SHOW VIEW ON sys.* TO 'KSCAdmin';
   GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin';
   GRANT PROCESS ON *.* TO 'KSCAdmin';
   GRANT SUPER ON *.* TO 'KSCAdmin';
   ```

   如果您使用 MariaDB 10.5 或更早版本作为 DBMS，则无需授予 EXECUTE 权限。在这种情况下，从脚本中排除以下命令：`GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin'`。

4. 要查看向 DBMS 账户授予的权限的列表，请执行以下命令：

   ```
   SHOW grants for 'KSCAdmin';
   ```

5. 要手动创建管理服务器数据库，请运行以下脚本（此脚本中的管理服务器数据库名称是 *kav*）：

   ```
   CREATE DATABASE kav
   DEFAULT CHARACTER SET utf8
   DEFAULT COLLATE utf8_general_ci;
   ```

   使用您在创建 DBMS 账户的脚本中指定的相同数据库名称。

6. 安装管理服务器。

安装完成后，将创建管理服务器数据库，管理服务器进入就绪状态。

配置使用 PostgreSQL 和 Postgres Pro 的 DBMS 账户

先决条件

在为 DBMS 账户分配权限之前，请执行以下操作：

1. 确保您以本地管理员账户登录系统。
2. 安装 PostgreSQL 和 Postgres Pro 的使用环境。

配置 DBMS 账户以安装管理服务器（自动创建管理服务器数据库）

要配置用于安装管理服务器的 DBMS 账户：

1. 运行 PostgreSQL 和 Postgres Pro 的使用环境。
2. 选择一个 Postgres 角色来访问 DBMS。您可以使用以下角色之一：
   - *postgres* 用户（默认 Postgres 角色）。

     如果您使用 *postgres* 用户，则无需为其授予额外的权限。

     默认情况下， *postgres*用户没有密码。但是，安装 Kaspersky Security Center Linux 需要密码。若要为 *postgres*用户设置密码，请运行以下脚本：

     ```
     ALTER USER user_name WITH PASSWORD '< password >';
     ```

   - 新的 Postgres 角色。

     如果您希望使用新的 Postgres 角色，请创建该角色，然后为其授予 CREATEDB 权限。为此，请运行以下脚本（此脚本中的角色是 *KCSAdmin*）：

     ```
     CREATE USER "KSCAdmin" WITH PASSWORD '< password >' CREATEDB;
     ```

     创建的角色将作为管理服务器数据库（以下也简称为“服务器数据库”）的所有者。
3. 安装管理服务器。

安装完成后，将自动创建服务器数据库，管理服务器进入就绪状态。

配置 DBMS 账户以安装管理服务器（手动创建管理服务器数据库）

要配置用于安装管理服务器的 DBMS 账户：

1. 运行 Postgres 的使用环境。
2. 创建一个新的 Postgres 角色和一个管理服务器数据库。然后为该角色授予管理服务器数据库的所有权限。为此，请以 *postgres* 用户角色登录 *postgres* 数据库，然后运行以下脚本（此脚本中的角色是 *KCSAdmin*，管理服务器数据库名称是 *KAV*）：

   ```
   CREATE USER "KSCAdmin" WITH PASSWORD '<password>';
   CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";
   GRANT ALL PRIVILEGES ON DATABASE "KAV" TO "KSCAdmin";
   ```

   如果发生“新编码 (UTF8) 与模板数据库编码不兼容”错误，请使用以下命令创建数据库：
   ```
   CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin" TEMPLATE template0;
   ```
   instead of:
   ```
   CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";
   ```

3. 为创建的 Postgres 角色授予以下权限：

   - 公共方案中的所有表的权限：ALL
   - 公共方案中的所有序列的权限：ALL

   为此，请以 *postgres* 用户角色登录服务器数据库，然后运行以下脚本（此脚本中的角色是 *KCSAdmin*）：

   ```
   GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "KSCAdmin";
   GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "KSCAdmin";
   ```

4. 安装管理服务器。

安装完成后，管理服务器将使用所创建数据库来存储管理服务器数据。管理服务器进入就绪状态。

用于 Kaspersky Security Center Linux 的证书

本节包含有关 Kaspersky Security Center Linux 证书的信息，并介绍如何为 Kaspersky Security Center Web Console 颁发和更换证书，以及如何在管理服务器与 Kaspersky Security Center Web Console 交互时为管理服务器续订证书。

About Kaspersky Security Center certificates

Kaspersky Security Center uses the following types of certificates to enable a secure interaction between the application components:

- Administration Server certificate
- Web Server certificate
- Kaspersky Security Center Web Console certificate

By default, Kaspersky Security Center uses self-signed certificates (that is, issued by Kaspersky Security Center itself), but you can replace them with custom certificates to better meet the requirements of your organization's network and comply with the security standards. After Administration Server verifies whether a custom certificate meets all applicable requirements, this certificate assumes the same functional scope as a self-signed certificate. The only difference is that a custom certificate is not reissued automatically upon expiration. You replace certificates with custom ones by means of the klsetsrvcert utility or through the Administration Server properties section in Kaspersky Security Center Web Console, depending on the certificate type. When you use the klsetsrvcert utility, you need to specify a certificate type by using one of the following values:

- C—Common certificate for ports 13000 and 13291.
- CR—Common reserve certificate for ports 13000 and 13291.

The maximum validity period for any of the Administration Server certificates must be 397 days or less.

Administration Server certificates

An Administration Server certificate is required for the following purposes:

- Authentication of Administration Server when connecting to Kaspersky Security Center Web Console
- Secure interaction between Administration Server and Network Agent on managed devices
- Authentication when the primary Administration Servers are connected to secondary Administration Servers

The Administration Server certificate is created automatically during installation of the Administration Server component and it is stored in the /var/opt/kaspersky/klnagent_srv/1093/cert/ folder. You specify the Administration Server certificate when you create a response file to install Kaspersky Security Center Web Console. This certificate is called common ("C").

The Administration Server certificate is valid for 397 days. Kaspersky Security Center automatically generates a common reserve ("CR") certificate 90 days before the expiration of the common certificate. The common reserve certificate is subsequently used for seamless replacement of the Administration Server certificate. When the common certificate is about to expire, the common reserve certificate is used to maintain the connection with Network Agent instances installed on managed devices. With this purpose, the common reserve certificate automatically becomes the new common certificate 24 hours before the old common certificate expires.

The maximum validity period for any of the Administration Server certificates must be 397 days or less.

If necessary, you can assign a custom certificate for the Administration Server. For example, this may be necessary for better integration with the existing PKI of your enterprise or for custom configuration of the certificate fields. When replacing the certificate, all Network Agents that were previously connected to Administration Server through SSL will lose their connection and will return "Administration Server authentication error." To eliminate this error, you will have to restore the connection after the certificate replacement.

If the Administration Server certificate is lost, you must reinstall the Administration Server component, and then restore the data in order to recover it.

You can also back up the Administration Server certificate separately from other Administration Server settings in order to move Administration Server from one device to another without data loss.

Mobile certificates

A mobile certificate ("M") is required for authentication of the Administration Server on mobile devices. You specify the mobile certificate in the Administration Server properties.

Also, a mobile reserve ("MR") certificate exists: it is used for seamless replacement of the mobile certificate. Kaspersky Security Center automatically generates this certificate 60 days before the expiration of the common certificate. When the mobile certificate is about to expire, the mobile reserve certificate is used to maintain the connection with Network Agent instances installed on managed mobile devices. With this purpose, the mobile reserve certificate automatically becomes the new mobile certificate 24 hours before the old mobile certificate expires.

If the connection scenario requires the use of a client certificate on mobile devices (connection involving two-way SSL authentication), you can generate those certificates by means of the certificate authority for auto-generated user certificates ("MCA"). Also, in the Administration Server properties, you can specify custom client certificates issued by a different certification authority, while integration with the domain Public Key Infrastructure (PKI) of your organization enables you to issue client certificates by means of your domain certification authority.

Web Server certificate

A special type of certificate is used by Web Server, a component of Kaspersky Security Center Administration Server. This certificate is required for publishing Network Agent installation packages that you subsequently download to managed devices. For this purpose, Web Server can use various certificates.

Web Server uses one of the following certificates, in order of priority:

1. Custom Web Server certificate that you specified manually by means of Kaspersky Security Center Web Console
2. Common Administration Server certificate ("C")

Kaspersky Security Center Web Console certificate

The Server of Kaspersky Security Center Web Console (hereinafter referred to as Web Console) has its own certificate. When you open a website, a browser verifies whether your connection is trusted. The Web Console certificate allows you to authenticate the Web Console and is used to encrypt traffic between a browser and the Web Console.

When you open the Web Console, the browser may inform you that the connection to the Web Console is not private and the Web Console certificate is invalid. This warning appears because the Web Console certificate is self-signed and automatically generated by Kaspersky Security Center. To remove this warning, you can do one of the following:

- Replace the Web Console certificate with a custom one (recommended option). Create a certificate that is trusted in your infrastructure and that meets the requirements for custom certificates.
- Add the Web Console certificate to the list of trusted browser certificates. We recommend that you use this option only if you cannot create a custom certificate.

Requirements for custom certificates used in Kaspersky Security Center Linux

The table below shows the requirements for custom certificates specified for different components of Kaspersky Security Center Linux.

Requirements for Kaspersky Security Center Linux certificates

Certificate type	Requirements	Comments
Common certificate, Common reserve certificate ("C", "CR")	Minimum key length: 2048. Basic constraints: • CA: true • Path Length Constraint: None Key Usage: • Digital signature • Certificate signing • Key encipherment • CRL Signing	Extended Key Usage parameter is optional. Path Length Constraint value may be an integer different from "None," but not less than 1.

	Extended Key Usage (optional): server authentication, client authentication.	
Web Server certificate	Extended Key Usage: server authentication. The PKCS #12 / PEM container from which the certificate is specified includes the entire chain of public keys. The Subject Alternative Name (SAN) of the certificate is present; that is, the value of the `subjectAltName` field is valid. The certificate meets the effective requirements of web browsers imposed on server certificates, as well as the current baseline requirements of the CA/Browser Forum.	Not applicable.
Kaspersky Security Center Web Console certificate	The PEM container from which the certificate is specified includes the entire chain of public keys. The Subject Alternative Name (SAN) of the certificate is present; that is, the value of the `subjectAltName` field is valid. The certificate meets the effective requirements of web browsers to server certificates, as well as the current baseline requirements of the CA/Browser Forum.	Encrypted certificates are not supported by Kaspersky Security Center Web Console.

Reissuing the certificate for Kaspersky Security Center Web Console

Most browsers impose a limit on the validity term of a certificate. To fall within this limit, the validity term of the Kaspersky Security Center Web Console certificate is limited to 397 days. You can replace an existing certificate received from a certification authority (CA) by issuing a new self-signed certificate manually. Alternatively, you can reissue your expired Kaspersky Security Center Web Console certificate.

When you open the Kaspersky Security Center Web Console, the browser may inform you that the connection to the Kaspersky Security Center Web Console is not private and the Kaspersky Security Center Web Console certificate is invalid. This warning appears because the Web Console certificate is self-signed and automatically generated by Kaspersky Security Center Linux. To remove or prevent this warning, you can do one of the following:

- Specify a custom certificate when you reissue it (recommended option). Create a certificate that is trusted in your infrastructure and that meets the requirements for custom certificates.
- Add the Kaspersky Security Center Web Console certificate to the list of trusted browser certificates after you reissue the certificate. We recommend that you use this option only if you cannot create a custom certificate.

To reissue the expired Kaspersky Security Center Web Console certificate:

Reinstall Kaspersky Security Center Web Console by performing one of the following:

- If you want to use the same installation file of Kaspersky Security Center Web Console, remove Kaspersky Security Center Web Console, and then install the same Kaspersky Security Center Web Console version.
- If you want to use an installation file of an upgraded version, run the upgrade command.

The Kaspersky Security Center Web Console certificate is reissued for another validity term of 397 days.

Replacing certificate for Kaspersky Security Center Web Console

By default, when you install Kaspersky Security Center Web Console Server (also referred to as Kaspersky Security Center Web Console), a browser certificate for the application is generated automatically. You can replace the automatically generated certificate with a custom one.

To replace the certificate for Kaspersky Security Center Web Console with a custom one:

1. Create a new response file required for the Kaspersky Security Center Web Console installation.
2. In this file, specify paths to the custom certificate file and the key file by using the `certPath` parameter and the `keyPath` parameter.
3. Reinstall Kaspersky Security Center Web Console by specifying the new response file. Do one of the following:
   - If you want to use the same installation file of Kaspersky Security Center Web Console, remove Kaspersky Security Center Web Console, and then install the same Kaspersky Security Center Web Console version.
   - If you want to use an installation file of an upgraded version, run the upgrade command.

Kaspersky Security Center Web Console works with the specified certificate.

Converting a PFX certificate to the PEM format

To use a PFX certificate in Kaspersky Security Center Web Console, you must first convert it to the PEM format by using any convenient OpenSSL-based cross-platform utility.

To convert a PFX certificate to the PEM format in the Linux operating system:

1. In an OpenSSL-based cross-platform utility, execute the following commands:

   ```
   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. Make sure that the certificate file and the private key are generated to the same directory where the .pfx file is stored.
3. Kaspersky Security Center Web Console does not support passphrase-protected certificates. Therefore, run the following command in an OpenSSL-based cross-platform utility to remove a passphrase from the .pem file:

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

   Do not use the same name for the input and output .pem files.

   As a result, the new .pem file is unencrypted. You do not have to enter a passphrase to use it.

The .crt and .pem files are ready to use, so you can specify them in the Kaspersky Security Center Web Console installer.

场景：指定自定义管理服务器证书

例如，您可以分配自定义管理服务器证书，以便更好地与贵司的现有公钥基础结构 (PKI) 集成，或自定义配置证书字段。最好在安装管理服务器后，快速启动向导完成之前立即替换证书。

管理服务器证书的最长有效期不得超过 397 天。

先决条件

新证书必须以 PKCS#12 格式创建（例如，通过组织的 PKI），并且必须由受信任的证书颁发机构 (CA) 颁发。此外，新证书必须包含整个信任链和私钥，该私钥必须存储在扩展名为 pfx 或 p12 的文件中。对于新证书，必须满足下面列出的要求。

证书类型：普通证书，普通备用证书（“C”，“CR”）

要求：

- 最小密钥长度：2048
- 基本限制：
  - CA：true
  - 路径长度限制：无
    路径长度约束值可以是不同于“无”的整数，但不能小于 1。
- 密钥用法：
  - 数字签名
  - 证书签名
  - 密钥加密
  - CRL 签名
- 扩展密钥用法 (EKU)：服务器身份验证，客户端身份验证。EKU 可选，但如果您的证书包含它，则必须在 EKU 中指定服务器和客户端身份验证数据。

公共 CA 颁发的证书没有证书签名权限。要使用此类证书，请确保您在网络中的分发点或连接网关上安装了网络代理版本 13 或更高版本。否则，您将无法在没有签名权限的情况下使用证书。

阶段

指定管理服务器证书分阶段进行：

1. 替换管理服务器证书

为此目的使用命令行 klsetsrvcert utility。

2. **指定新证书并恢复网络代理与管理服务器的连接**

   当证书被替换时，所有先前通过 SSL 连接到管理服务器的网络代理将丢失它们的连接，并返回“管理服务器身份验证错误。”要指定新证书和恢复连接，使用命令行 klmover utility。

结果

当您结束场景时，管理服务器证书被替换，且服务器得到受管理设备上的网络代理验证。

使用 klsetsrvcert 实用程序替换管理服务器证书

要替换管理服务器证书：

从命令提示符运行以下实用程序：

```
klsetsrvcert [-t <类型> {-i <输入文件> [-p <密码>] [-o <证书验证参数>] | -g <DNS 名称>}]
[-f <时间>][-r <证书颁发机构列表文件>][-l <日志文件>]
```

您无需下载 klsetsrvcert 实用程序。它包含在 Kaspersky Security Center Linux 分发包中。它与以前的 Kaspersky Security Center Linux 版本不兼容。

下表列出了 klsetsrvcert 实用程序参数的说明。

klsetsrvcert 实用工具参数值

参数	参数值
`-t <类型>`	要替换的证书类型。<类型> 参数的可能值： • `C` – 为端口 13000 和 13291 替换普通证书。 • `CR` – 为端口 13000 和 13291 替换普通预留证书。
`-f <时间>`	更改证书的计划，使用格式“DD-MM-YYYY hh:mm”(对于端口 13000 和 13291)。 如果要在到期前更换普通或普通备用证书，请使用此参数。 指定受管理设备必须与新证书上的管理服务器同步的时间。
`-i <输入文件>`	带有 PKCS#12 格式证书的容器（带有扩展名 .p12 或 .pfx 扩展名的文件）。
`-p <密码>`	用于保护 p12 容器的密码。 证书和私钥存储在容器中，因此需要密码才能解密带有容器的文件。
`-o <证书验证参数>`	证书验证参数（以分号分隔）。 要在没有签名权限的情况下使用自定义证书，请在 klsetsrvcert 实用程序中指定 `-o NoCA`。这对于公共 CA 颁发的证书很有用。
`-g <DNS 名称>`	新证书将为指定 DNS 名称创建。
`-r <证书颁发机`	受信任的根证书颁发机构列表，格式 PEM。

构列表文件>	
-l <日志文件>	结果输出文件。默认下，输出被重定向到标准输出流。

例如，要指定"自定义管理服务器证书"，使用以下命令：

```
klsetsrvcert -t C -i <inputfile> -p <密码> -o NoCA
```

证书替换后，所有通过 SSL 连接到管理服务器的网络代理都会失去连接。要恢复它，请使用命令行klmover utility。

为避免丢失网络代理连接，请使用以下命令：

1. 要安装新证书，请执行以下命令：

   ```
   klsetsrvcert -t CR -i <inputfile> -p <password> -o NoCA
   ```

2. 要指定新证书的应用日期，请执行以下命令：

   ```
   klsetsrvcert -f "DD-MM-YYYY hh:mm"
   ```

其中 "DD-MM-YYYY hh:mm" 是比当前日期晚 3-4 周的日期。将证书更改为新证书的时间偏移将允许将新证书被分发给所有网络代理。

使用 klmover 实用程序将网络代理连接到管理服务器

使用命令行 klsetsrvcert 实用程序替换管理服务器证书后，您需要在网络代理和管理服务器之间建立 SSL 连接，因为连接已断开。

要指定新的管理服务器证书并恢复连接：

从命令提示符运行以下实用程序：

```
klmover [-address <服务器地址>] [-pn <端口号>] [-ps <SSL 端口号>] [-nossl] [-cert <证书文件的路径>]
```

当网络代理安装在客户端设备上时，此实用程序会被自动复制到网络代理安装文件夹。

为了防止入侵者将设备移出管理服务器的控制，我们强烈建议为运行 klmover 实用程序启用密码保护。要启用密码保护，请在**网络代理策略设置使用卸载密码**使用卸载密码选项。

klmover 实用程序需要本地管理员权限。对于没有本地管理员权限操作的设备，可以忽略运行 klmover 实用程序的密码保护。

启用**使用卸载密码**还会启用Kaspersky Security Center Web Console 删除工具 (cleaner.exe) 的密码保护。

klmover 实用程序参数的描述如下表所示。

参数	参数值
`-address <服务器地址>`	用于连接的管理服务器的地址。 您可以指定 IP 地址或 DNS 名称。
`-pn <端口号>`	用来建立与管理服务器的非加密连接的端口号。 默认端口号是 14000。
`-ps <SSL 端口号>`	使用 SSL 与管理服务器建立加密连接时使用的 SSL 端口号。 默认端口号是 13000。
`-nossl`	使用非加密连接管理服务器。 如果未使用该键值，网络代理将通过使用加密的 SSL 协议连接至管理服务器。
`-cert <验证文件的路径>`	访问管理服务器时使用指定的证书文件作为身份验证。

定义共享文件夹

安装管理服务器后，您可以在管理服务器属性中指定共享文件夹的位置。默认情况下，在具有管理服务器的设备上创建共享文件夹。然而，在一些情况下(例如高负载或需要从隔离网络访问)，最好放置共享文件夹到专用文件资源。

共享文件夹在网络代理部署中偶尔使用。

共享文件夹必须禁用大小写敏感。

登录到 Kaspersky Security Center Web Console 并登出

您可以在安装管理服务器和 Web Console 服务器后登录到 Kaspersky Security Center Web Console。您必须知道安装过程中指定的管理服务器的 Web 地址和端口号（默认下，端口号是 8080）。在您的浏览器中，JavaScript 必须被启用。

要登录 Kaspersky Security Center Web Console，请执行以下操作：

1. 在您的浏览器中，转到<管理服务器 Web 地址>:<端口号>。
   登录页面显示。
2. 如果您添加若干个受信任的服务器，在管理服务器列表选择您要连接的管理服务器。
   如果您只添加了一个管理服务器，则管理服务器列表被锁定。
3. 执行以下操作之一：
   - 要使用域用户帐户登录管理服务器，请输入域用户的用户名和密码。
     您可以采用以下格式之一输入域用户的用户名：
     - 用户名@ `dns.domain`

- NTDOMAIN\用户名

使用域用户账户登录之前，请轮询域控制器以获取域用户列表。

- 要通过指定管理员的用户名和密码登录管理服务器，请输入内部用户的用户名和密码。
- 如果服务器上创建了一个或多个虚拟管理服务器，并且您要登录到虚拟服务器：

a. 单击**显示虚拟服务器选项**。

b. 输入您在创建虚拟服务器时指定的虚拟管理服务器名称。

c. 输入拥有虚拟管理服务器权限的管理员的用户名和密码。

4. 单击**登录**按钮。

登录后，控制板使用您最后使用的语言和主题显示。您可以通过 Kaspersky Security Center Web Console 导航并使用其操作 Kaspersky Security Center Linux。

注销

要注销 Kaspersky Security Center Web Console，请执行以下操作：

在主菜单中，转到您的账户设置，然后选择**登出**。

Kaspersky Security Center Web Console 被关闭，且登录页面被显示。

更改 Kaspersky Security Center Web Console 界面的语言

您可以选择 Kaspersky Security Center Web Console 界面的语言。

要更改界面语言：

1. 在主菜单中，转到“**设置 → 语言**”。
2. 选择一种受支持的本地化语言。

配置与 Kaspersky Security Center Linux 配合使用的 MySQL x64 服务器

如果将 MySQL 服务器用于 Kaspersky Security Center，请启用对 InnoDB 和 MEMORY 存储以及对 UTF-8 和 UCS-2 编码的支持。

my.cnf 文件的推荐设置

有关 DBMS 配置的更多详细信息，另请参阅帐户配置过程。有关 DBMS 安装的信息，请参阅DBMS 安装过程。

要配置 my.cnf 文件：

1. 在文本编辑器中打开 my.cnf 文件。

2. 将以下行添加到 my.ini 文件的 [mysqld] 部分中：

```
sort_buffer_size=10M
join_buffer_size=20M
tmp_table_size=600M
max_heap_table_size=600M
key_buffer_size=200M
innodb_buffer_pool_size= 真实值不得少于期待 KAV 数据库大小的 80%
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0 ( 在大多数情况下，服务器使用小型事务处理 )
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
```

请注意，在 innodb_buffer_pool_size 值中指定的内存将在服务器启动时分配。如果数据库大小小于指定的缓冲区大小，则只分配所需的内存。已分配内存的实际大小大约比指定的缓冲区大小大 10%。有关详细信息，请参阅 MySQL 文档。

建议使用参数值 innodb_flush_log_at_trx_commit = 0，因为值“1”或“2”会对 MySQL 的运行速度产生负面影响。

快速启动向导

Kaspersky Security Center Linux 允许您对构建集中式管理系统以实施网络安全威胁防护所需的最小设置集合进行调整。该配置使用快速启动向导执行。当向导运行时，您可以对应用程序做以下更改：

- 添加可自动分发至管理组内的设备的密钥文件或激活码。
- 为管理服务器和受管理应用程序的操作事件通知设置邮件传送配置（成功的通知传送需要消息服务在管理服务器和所有接收端设备上运行）。
- 为工作站和服务器创建保护策略，以及为受管理设备的顶级层级创建恶意软件扫描任务、更新下载任务和数据备份任务。

> 快速启动向导仅为其“**受管理设备**”文件夹不包含任何策略的应用程序创建策略。如果已经为受管理设备的顶级层级创建具有相同名称的任务，则快速启动向导不会创建同名任务。

在安装管理服务器后，在第一次连接时，应用程序自动提示您运行快速启动向导。您还可以在任意时刻手动启动快速启动向导。

要手动启动快速启动向导：

1. 在主菜单，单击管理服务器名称旁边的“设置”图标 ()。

   管理服务器属性窗口将打开。

2. 在“**常规**”选项卡上，选择“**常规**”区域。

3. 单击**开始快速启动向导**。

向导提示您执行管理服务器初始化配置。遵照向导的说明操作。使用**下一步**按钮进行向导。

步骤 1：指定互联网连接设置

指定管理服务器的互联网连接设置。您必须配置互联网连接才能使用卡巴斯基安全网络和为 Kaspersky Security Center Linux 及受管理的卡巴斯基应用程序下载反病毒数据库更新。

如果您要在连接到互联网时使用代理服务器，请启用"**使用代理服务器**"选项。如果启用此选项，字段可用于输入设置。为代理服务器连接指定以下设置：

- 地址

  Kaspersky Security Center Linux 用于连接到互联网的代理服务器地址。

- 端口号

  将建立 Kaspersky Security Center Linux 代理服务器连接的端口号。

- 对本地地址不使用代理服务器

  将不会使用代理服务器连接本地网络的设备。

- 代理服务器身份验证

  如果选择该选框，您可以在输入字段中为代理服务器身份验证指定凭证。
  如果选中"**使用代理服务器**"复选框，则该输入字段可用。

- 用户名

  用于与代理服务器建立连接的用户账户（如果选中"**代理服务器身份验证**"复选框，则该字段可用）。

- 密码

  建立代理服务器连接的账户所属的用户所设置的密码（如果选中"**代理服务器身份验证**"复选框，则该字段可用）。
  要查看输入的密码，单击并按住"**显示**"按钮足够长时间。

您可以稍后从快速启动向导单独配置互联网访问。

步骤 2：下载所需更新

所需更新将从 Kaspersky 服务器自动下载。

Step 3. Selecting the assets to secure

Select the protection areas and operating systems that are in use on your network. When you select these options, you specify the filters for application management plug-ins and distribution packages on Kaspersky servers that you can download to install on client devices on your network. Select the options:

- 范围

  You can select the following protection scopes:
  - 工作站
  - 文件服务器和存储
  - **Virtualization**
  - **Embedded systems**
  - **Industrial networks**
  - **Industrial endpoints**

- 操作系统

  You can select the following platforms:
  - Microsoft Windows
  - macOS
  - Android
  - Linux
  - Other

  For information about supported operating systems, refer to Hardware and software requirements for Kaspersky Security Center Web Console.

You can select the Kaspersky application packages from the list of available packages later, separately from the quick start wizard. To simplify the search for the required packages, you can filter the list of available packages by various criteria.

Step 4. Selecting encryption in solutions

The 加密进行中 window is displayed only if you have selected 工作站 as a protection scope.

Kaspersky Endpoint Security for Windows includes encryption tools for information stored on Windows-based client devices. These encryption tools have the Advanced Encryption Standard (AES) implemented with a 256-bit or 56-bit key length.

Download and usage of the distribution package with a 256-bit key length must be performed in compliance with applicable laws and regulations. To download a distribution package of Kaspersky Endpoint Security for Windows that is valid for the needs of your organization, consult the legislation of the country where the client devices of your organization are located.

In the 加密进行中 window, select one of the following encryption types:

- Lite encryption. This encryption type uses a 56-bit key length.
- Strong encryption. This encryption type uses a 256-bit key length.

You can select the distribution package for Kaspersky Endpoint Security for Windows with the required encryption type later, separately from the quick start wizard.

步骤 5：配置受管理应用程序的插件安装

选择要安装的受管理应用程序插件。将显示位于 Kaspersky 服务器上的插件列表。该列表根据在向导的上一步中选择的选项进行筛选。默认情况下，完整列表包括所有语言的插件。要仅显示特定语言的插件，请使用过滤器。插件列表包括以下多列：

- 保护范围

  选定的要保护的区域会显示在此列中。

- 类型

  插件类型会显示在此列中。

- 名称

  将根据您在上一步中选择的保护区域和平台来选择插件。

- 版本

  该列表包括 Kaspersky 服务器上所有版本的插件。默认情况下，将选择最新版本的插件。

- 最新版本

  该列表示插件版本是否为最新。如果显示**true**值，则对应的插件是最新版本。如果显示**false**值，则对应的插件版本更高。

- 操作系统

  此列会显示插件操作系统。

- 语言

  默认情况下，插件的本地化语言由您在安装 Kaspersky Security Center Linux 时选择的语言来定义。您可以在“**显示管理控制台本地化语言或**”下拉列表中指定其他语言。

选择插件后，单击“**下一步**”开始安装。

您可以手动为卡巴斯基应用程序安装管理插件，单独从快速启动向导执行。

快速启动向导会自动安装选定插件。要安装某些插件，您必须接受 EULA 条款。阅读显示的 EULA 文本，选中“**我同意使用卡巴斯基安全网络**”复选框，然后单击“**安装**”按钮。如果您不接受 EULA 条款，则不会安装该插件。

安装所有选定插件后，快速启动向导会自动带您继续下一步。

Step 6. Downloading distribution packages and creating installation packages

Select the distribution packages to download.

Distributives of managed applications may require a specific minimum version of Kaspersky Security Center Linux to be installed.

After you have selected an encryption type for Kaspersky Endpoint Security for Windows, a list of distribution packages of both encryption types is displayed. A distribution package with the selected encryption type is selected in the list. You can select distribution packages of any encryption type. The distribution package language corresponds to the Kaspersky Security Center Linux language. If an application distribution package for the Kaspersky Security Center Linux language does not exist, the English distribution package is selected.

To finish downloading of some distribution packages you must accept EULA. When you click the 接受 button, the text of EULA is displayed. To proceed to the next step of the wizard, you must accept the terms and conditions of the EULA and the terms and conditions of Kaspersky Privacy Policy. If you do not accept the terms and conditions, the downloading of the package is canceled.

After you have accepted the terms and conditions of the EULA and the terms and conditions of Kaspersky Privacy Policy, the downloading of the distribution packages continues. Later, you can use installation packages to deploy Kaspersky applications on client devices.

步骤 7：配置卡巴斯基安全网络

指定设置以转发 Kaspersky Security Center Linux 操作信息到卡巴斯基安全网络知识库。您可以选择以下选项之一：

- 我同意使用卡巴斯基安全网络

  安装在客户端设备上的 Kaspersky Security Center Linux 和受管理应用程序将自动将其操作详情传输到卡巴斯基安全网络。参与卡巴斯基安全网络确保了包含病毒和其他威胁的数据库的快速更新，该数据库确保了对紧急安全威胁的快速响应。

- 我不同意使用卡巴斯基安全网络

  Kaspersky Security Center Linux 和受管理应用程序将不向卡巴斯基安全网络提供任何信息。
  如果选择此选项，则将禁用卡巴斯基安全网络。

您可以稍后设置对卡巴斯基安全网络 (KSN) 的访问，单独从快速启动向导执行。

步骤 8：选择应用程序激活方法

选择以下 Kaspersky Security Center Linux 激活选项之一：

- 通过输入您的激活码

  *激活码*是一串由20个字符数字组成的唯一序列。输入一个激活码可添加一个激活 Kaspersky Security Center Linux 的密钥。购买 Kaspersky Security Center 后，您将通过您指定的电子邮件地址收到激活码。

  若要使用激活码激活应用程序，您需要互联网来建立与 Kaspersky 激活服务器的连接。

  如果选择了此激活选项，则可以启用“**自动部署授权许可密钥到受管理设备**”选项。

  如果启用此选项，授权许可密钥将自动部署到受管理设备。

  如果禁用此选项，则可以稍后在主菜单的 **操作 → 授权许可 → 卡巴斯基授权许可** 部分中将授权许可密钥部署到受管理设备。

- 通过指定密钥文件

  *密钥文件*是 Kaspersky 提供的 .key 扩展名的文件。密钥文件被用来激活应用程序。

  购买 Kaspersky Security Center 后，您将通过您指定的电子邮件地址收到密钥文件。

  若使用密钥文件激活程序，您无需连接至 Kaspersky 激活服务器。

  如果选择了此激活选项，则可以启用“**自动部署授权许可密钥到受管理设备**”选项。

  如果启用此选项，授权许可密钥将自动部署到受管理设备。

  如果禁用此选项，则可以稍后在主菜单的 **操作 → 授权许可 → 卡巴斯基授权许可** 部分中将授权许可密钥部署到受管理设备。

- 通过高推迟应用程序激活

如果您选择延迟应用程序激活，您可以在稍后随时选择“**操作**”→“**授权许可**”来添加授权许可密钥。

当使用从付费 AMI 部署的 Kaspersky Security Center 时，或者对于基于使用的按月付费 SKU，您无法指定密钥文件或输入码。

步骤 9：创建基本的网络保护配置

您可以检查创建的策略和任务列表。

等待策略和任务完成创建，然后转到向导的下一步。

步骤 10：配置邮件通知

配置如何传递有关在 Kaspersky 应用程序在客户端设备上运行期间记录的事件的通知。这些设置将被用作应用程序策略的默认设置。

要配置发生在 Kaspersky 应用程序上的事件的通知传送，使用以下设置：

- 收件人(电子邮件地址)

  应用程序将给其发送通知的用户的邮件地址。您可以输入一个或更多地址；如果您输入多个地址，使用分号分隔。

- SMTP 服务器地址

  您组织邮件服务器的地址。

  如果您输入多个地址，使用分号分隔。您可以使用下列值：

  - IPv4 或 IPv6 地址
  - SMTP 服务器的 DNS 名称

- SMTP 服务器端口

  SMTP 服务器的通信端口号。如果您使用多个 SMTP 服务器，则通过指定的通信端口与它们建立连接。默认端口号是 25。

- 使用 ESMTP 身份验证

  启用 ESMTP 身份验证支持。当选择了该复选框时，您可以在“**用户名**”和“**密码**”字段指定 ESMTP 身份验证设置。默认情况下已清除该选框。

您可以通过单击“**发送测试消息**”按钮测试新邮件通知设置。

步骤 11：关闭快速启动向导

要关闭向导，请单击“**完成**”按钮。

完成快速启动向导后，您可以运行保护部署向导以在网络中的设备上自动安装反病毒应用程序或网络代理。

保护部署向导

要安装 Kaspersky 应用程序，您可以使用保护部署向导。保护部署向导允许使用特别创建的安装包或直接从分发包来远程安装应用程序。

保护部署向导执行以下操作：

- 为应用程序安装下载安装包（如果之前未创建）。安装包位于“**发现和部署**”→“**部署和分配**”→“**安装包**”。在将来，您可以使用该安装包安装程序。
- 为特定设备或管理组创建并启动远程安装任务。新创建的远程安装任务存储在“**任务**”区域中。您可以以后手动启动此任务。任务类型为“**远程安装应用程序**”。

如果您想在装有 SUSE Linux Enterprise Server 15 操作系统的设备上安装网络代理，首先安装 insserv-compat 软件包以配置网络代理。

开始保护部署向导

您可以随时手动启动保护部署向导。

要手动启动保护部署向导，

在主菜单中，转到“**发现和部署 → 部署和分配 → 保护部署向导**”。

保护部署向导启动。使用**下一步**按钮进行向导。

步骤 1：选择安装包

选择您要安装的应用程序安装包。

如果所需应用程序安装包未列出，请单击“**添加**”按钮，然后从列表中选择应用程序。

步骤 2：选择分发密钥文件或激活码的方法

选择分发密钥文件或激活码的方法：

- 不添加授权许可密钥到安装包

  密钥被自动分发到所兼容的所有设备：
  - 如果自动分发在密钥属性中启用。
  - 如果**添加密钥**任务已创建。

- 添加授权许可密钥到安装包

  密钥与安装包一起被分发到设备。

  我们不建议您使用该方法分发密钥，因为将启用对安装包存储库的共享读取访问权限。

如果安装包已经包含密钥文件或激活码，将显示此窗口，但其中只包含授权许可密钥信息。

步骤 3：选择网络代理版本

如果您选择了非网络代理安装包，您也必须安装网络代理，它连接应用程序到 Kaspersky Security Center 管理服务器。

选择网络代理的最新版本。

步骤 4：选择设备

指定要安装应用程序的设备列表：

- 安装到受管理设备

  如果选择该选项，程序将为该设备组创建远程安装任务。

- 选择设备以安装

  该任务被分配到设备分类中的设备。您可以指定现有分类之一。
  例如，您可能要使用该选项在特定操作系统版本的设备上运行任务。

步骤 5：指定远程安装任务设置

在“**远程安装任务设置**”页面，指定应用程序远程安装设置。

在“**强制下载安装包**”设置组中，指定如何将安装程序所需的文件分发到客户端设备中。

- 使用网络代理

  如果启用此选项，安装包通过安装在客户端设备上的网络代理传送到客户端设备。
  如果禁用此选项，则使用客户端的操作系统传送安装包。
  如果任务已分配给安装了网络代理的设备，我们建议您启用此选项。
  默认情况下已启用该选项。

- 通过分发点使用操作系统资源

  如果启用此选项，安装包使用操作系统工具通过分发点传送到客户端设备。如果网络中存在不止一个分发点，那么您可以选择本选项。
  如果启用“**使用网络代理**”选项，仅在网络代理工具不可用时才通过操作系统工具传送文件。
  默认情况下，已经为虚拟管理服务器上创建的远程安装任务启用此选项。
  在未安装网络代理的设备上安装 Windows 应用程序（包括 Windows 网络代理）的唯一方法是使用基于 Windows 的分发点。因此，当您安装 Windows 应用程序时：
  - 选择此选项。
  - 确保为目标客户端设备分配了分发点。
  - 确保分发点基于 Windows。

- 通过管理服务器使用操作系统资源

如果启用此选项，文件将使用客户端设备的操作系统工具通过管理服务器传送到客户端设备。如果客户端设备上未安装网络代理，但是客户端设备与管理服务器在同一网络，则可以启用此选项。

默认情况下已启用该选项。

定义附加设置：

如果已经安装应用程序则不再重新安装

如果启用此选项，则如果选定的应用程序已安装到该客户端设备上，将不再重新安装它。

如果禁用此选项，仍将安装应用程序。

默认情况下已启用该选项。

步骤 6：安装前删除不兼容的应用程序

该步骤仅在您部署的应用程序已知与其他应用程序不兼容时才显示。

如果您想让 Kaspersky Security Center Linux 自动卸载不兼容的应用程序，则选择该选项。

不兼容应用程序列表也被显示。

如果您不选择该选项，应用程序将仅被安装到没有不兼容应用程序的设备。

步骤 7：移动设备到受管理设备

指定设备是否在安装网络代理后必须被移动到管理组。

- 不移动设备

  设备保留在当前所在组中。未被放置在任何组的设备保持未分配。

- 将未分配的设备移动到此组

  设备被移动到您选择的管理组。

默认情况下已选择“**不移动设备**”选项。为了安全起见，您可能需要手动移动设备。

步骤 8：选择访问设备的账户

如果必要，添加要用于启动远程安装任务的账户：

- 不需要账户(网络代理已安装)

如果该选项被选中，您不是必须指定一个账户，并在该账户下运行程序的安装。将使用运行管理服务器服务的账户运行该任务。

如果网络代理未安装在客户端设备，该选项不可用。

- 需要账户(不使用网络代理)

  如果您为其分配远程安装任务的设备上未安装网络代理，请选择此选项。在这种情况下，您可以指定用户账户来安装应用程序。

  要指定运行应用程序安装程序的用户账户，请单击**添加**按钮，选择**本地账户**，然后指定用户账户凭据。

  您可以指定多个用户账户，例如，没有一个账户拥有分配任务所对应的所有设备上的全部所需权限时。在此情况下，已经添加的所有账户都用于从上到下按顺序运行该任务。

步骤 9：开始安装

该页面是向导的最后一步。在该步骤， **远程安装任务**已被成功创建并配置。

默认情况下，未选定“**向导完成时运行任务**”选项。如果您选择该选项， **远程安装任务**将在您完成向导后立即启动。如果您不选择该选项， **远程安装任务**不会启动。您可以以后手动启动此任务。

单击“**确定**”完成保护部署向导的最后一步。

升级 Kaspersky Security Center Linux

您可以在安装了早期版本管理服务器（从版本 13 开始）的设备上安装管理服务器版本 15。当升级至版本 15 时，上一管理服务器版本的所有数据和设置都将被保留下来。

升级 Kaspersky Security Center Linux 之前，请确保您使用管理服务器版本 15 支持的操作系统和 DBMS 版本。如有必要，您可以将管理服务器移动到具有更高版本操作系统和 DBMS 的另一台设备。

您可以使用以下方法之一升级管理服务器的版本：

- 使用 Kaspersky Security Center Linux 安装文件
- 创建管理服务器数据备份，安装新版本的管理服务器，然后备份中恢复管理服务器数据

升级期间，严禁管理服务器和其他应用程序同时使用 DBMS。

如果您的网络包含多个管理服务器，则必须手动升级每个服务器。Kaspersky Security Center Linux 不支持集中升级。

此外，您还必须将 Kaspersky Security Center Web Console 升级到新版本。

从先前版本升级 Kaspersky Security Center Linux 时，支持的卡巴斯基应用程序的所有已安装插件都会保留。管理服务器插件和网络代理插件会自动升级。我们建议在开始升级之前创建管理服务器数据的备份副本。

使用安装文件升级 Kaspersky Security Center Linux

要将管理服务器从以前的版本（从版本 13 开始）升级到版本 15，您可以使用 Kaspersky Security Center Linux 安装文件在早期版本的基础上安装新版本。

要使用安装文件将早期版本的管理服务器升级到版本 15：

1. 从卡巴斯基网站下载包含版本 15 的完整软件包的 Kaspersky Security Center Linux 安装文件：
   - 对于运行基于 RPM 的操作系统的设备 - ksc64-<版本号>.x86_64.rpm
   - 对于运行基于 Debian 的操作系统的设备 - ksc64_<版本号>_amd64.deb
2. 使用您在管理服务器上使用的软件包管理器升级安装包。例如，在具有 root 权限的账户下，可以在命令行终端中使用以下命令：
   - 对于运行基于 RPM 的操作系统的设备：
     ```
     $ sudo rpm -Uvh --nodeps --force ksc64-<版本号>.x86_64.rpm
     ```
   - 对于运行基于 Debian 的操作系统的设备：
     ```
     $ sudo dpkg -i ksc64_<版本号>_amd64.deb
     ```

   成功执行命令后，将创建 /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl 脚本。相关消息显示在终端中。
3. 运行 /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl 脚本来配置升级的管理服务器。

4. 阅读命令行终端中显示的授权许可协议和隐私策略。如果您同意授权许可协议和隐私策略的所有条款：

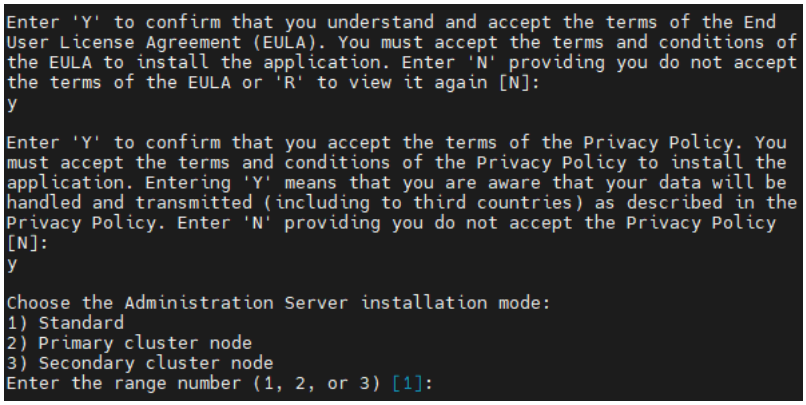
   a. 输入“Y”以确认您已完全阅读、理解并接受 EULA 的条款和条件。

   b. 再次输入“Y”以确认您已完全阅读、理解并接受描述数据处理的隐私策略。

   在您输入两次“Y”后，将继续在您的设备上安装应用程序。

5. 输入“1”选择标准管理服务器安装模式。

   下图显示了最后两个步骤。



接受 EULA 和隐私策略的条款，并在命令行终端中选择标准管理服务器安装模式

   接下来，脚本会配置并完成升级管理服务器。在升级期间，无法更改升级前调整的管理服务器设置。

6. 对于安装了更早版本网络代理的设备，创建并运行用于远程安装新版本网络代理的任务。

   > 我们建议您将 Linux 网络代理升级到与 Kaspersky Security Center Linux 相同的版本。

   完成远程安装任务后，网络代理版本将升级。

通过备份升级 Kaspersky Security Center Linux

要将管理服务器从以前的版本（从版本 13 开始）升级到版本 15，您可以创建管理服务器数据的备份并在安装新版本的 Kaspersky Security Center Linux 后恢复此数据。如果安装期间出现问题，您可以使用升级前创建的管理服务器数据备份恢复先前版本的管理服务器。

要通过备份将早期版本的管理服务器升级到版本 15：

1. 在升级前，使用旧版本的应用程序备份管理服务器数据。
2. 卸载旧版本的 Kaspersky Security Center Linux。
3. 在以前的管理服务器上安装 Kaspersky Security Center Linux 版本 15。
4. 从升级前创建的备份中恢复管理服务器数据。
5. 对于安装了更早版本网络代理的设备，创建并运行用于远程安装新版本网络代理的任务。

我们建议您将 Linux 网络代理升级到与 Kaspersky Security Center Linux 相同的版本。

完成远程安装任务后，网络代理版本将升级。

在 Kaspersky Security Center Linux 障转移集群节点上升级 Kaspersky Security Center Linux

可以在安装了较早版本的管理服务器（从版本 15 起）的每个 Kaspersky Security Center Linux 故障转移集群节点上安装管理服务器版本 14.2。当升级至版本 15 时，上一管理服务器版本的所有数据和设置都将被保留下来。

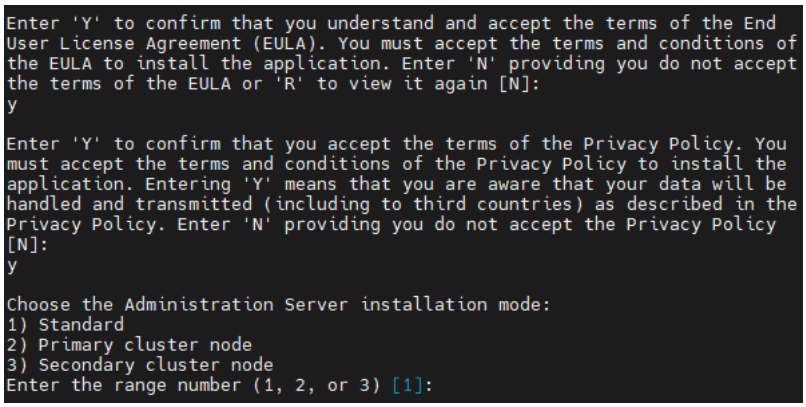
如果您之前在本地设备上安装了 Kaspersky Security Center Linux，您还可以使用安装文件或者通过备份在这些设备上升级 Kaspersky Security Center Linux。

若要在 Kaspersky Security Center Linux 障转移集群节点上升级 Kaspersky Security Center Linux：

1. 从卡巴斯基网站下载包含版本 15 的完整软件包的 Kaspersky Security Center Linux 安装文件：
   - 对于运行基于 RPM 的操作系统的设备 - ksc64-<版本号>-<内部版本号>.x86_64.rpm
   - 对于运行基于 Debian 的操作系统的设备 - ksc64_<版本号>-<内部版本号>_amd64.deb
2. 停止集群。
3. 在集群的主动节点上，使用您在管理服务器上使用的软件包管理器升级安装包。
   例如，在具有 root 权限的账户下，可以在命令行终端中使用以下命令：
   - 对于运行基于 RPM 的操作系统的设备：
     ```
     $ sudo rpm -Uvh --nodeps --force ksc64-<版本号>-<内部版本号>.x86_64.rpm
     ```
   - 对于运行基于 Debian 的操作系统的设备：
     ```
     $ sudo dpkg -i ksc64_<版本号>-<内部版本号>_amd64.deb
     ```

   成功执行命令后，将创建 /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl 脚本。相关消息显示在终端中。
4. 运行 /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl 脚本来配置升级的管理服务器。
5. 阅读命令行终端中显示的授权许可协议和隐私策略。如果您同意授权许可协议和隐私策略的所有条款：
   a. 输入“Y”以确认您已完全阅读、理解并接受 EULA 的条款和条件。
   b. 再次输入“Y”以确认您已完全阅读、理解并接受描述数据处理的隐私策略。

   在您输入两次“Y”后，将继续在您的设备上安装应用程序。
6. 通过输入“2”选择要升级的节点。
   下图显示了最后两个步骤。



接受 EULA 和隐私策略的条款，并在命令行终端中选择安装模式

接下来，脚本会配置并完成升级管理服务器。在升级期间，无法更改升级前调整的管理服务器设置。

7. 在被动节点上执行步骤 3-5。

   在第 6 步，输入“3”以选择节点。

8. 启动集群。

   请注意，您可以在任何节点上启动集群。如果在被动节点上启动集群，它将成为主动节点。

   这样，您就在 Kaspersky Security Center Linux 故障转移集群节点上安装了最新版本的管理服务器。

升级 Kaspersky Security Center Web Console

该文描述了如何升级 Kaspersky Security Center Web Console 服务器 (也叫 Kaspersky Security Center Web Console) 到运行 Linux 操作系统的设备。

如果您需要在封闭软件环境模式下的 Astra Linux 上安装 Kaspersky Security Center Web Console，请按照 Astra Linux 特定说明进行操作。

使用与您设备上安装的 Linux 发行版对应的以下安装文件之一：

- 对于 Debian - ksc-web-console-[build_number].x86_64.deb
- 对于基于 RPM 的操作系统 - ksc-web-console-[build_number].x86_64.rpm
- 对于 Alt 8 SP - ksc-web-console-[build_number]-alt8p.x86_64.rpm

您通过从 Kaspersky 网站下载来接收安装文件。

要升级 Kaspersky Security Center Web Console：

1. 确保您要安装 Kaspersky Security Center Web Console 的设备运行以下一种受支持的 Linux 分类。
2. 阅读并接受最终用户授权许可协议 (EULA)。如果 Kaspersky Security Center Linux 分发包不包含带有 EULA 文本的 TXT 文件，您可以从 卡巴斯基网站 下载文件。如果您不接受授权许可协议的条款，请勿使用安装文件升级 Kaspersky Security Center Web Console 。

3. 使用您在安装 Kaspersky Security Center Web Console 之前准备的相同响应文件。响应文件名称为 ksc-web-console-setup.json，文件位置为 /etc/ksc-web-console-setup.json。

   如果响应文件不存在，请创建一个新的响应文件，其中包含用于将 Kaspersky Security Center Web Console 连接到管理服务器的参数。命名该文件为 ksc-web-console-setup.json，然后将其放置到 /etc 目录中：

   响应文件的一个例子，它包含最小参数集以及默认地址和端口：

   ```
   {
     "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
   }
   ```

   如果您想要升级 Kaspersky Security Center Web Console（其连接到安装在 Kaspersky Kaspersky Security Center Linux 故障转移集群上的管理服务器），请在响应文件中指定受信任的安装参数以允许 Kaspersky Security Center Linux故障转移集群连接到 Kaspersky Security Center Web Console。此参数的字符串值具有以下格式：

   “trusted”："服务器地址|端口|证书路径|服务器名称"

   指定trusted安装参数的组件：

   - **管理服务器地址**。如果您在准备集群节点时创建了从属网络适配器，请使用适配器的 IP 地址作为 Kaspersky Security Center Linux 故障转移集群地址。否则，请指定您使用的第三方负载平衡器的 IP 地址。
   - **管理服务器端口**。Kaspersky Security Center Web Console 用于连接到管理服务器的 OpenAPI 端口（默认 13299）。
   - **管理服务器证书**。管理服务器证书位于 Kaspersky Security Center Linux 故障转移集群的共享数据存储中。证书文件的默认路径：<shared data folder>\1093\cert\klserver.cer。将证书文件从共享数据存储复制到安装 Kaspersky Security Center Web Console 的设备。指定管理服务器证书的本地路径。
   - **管理服务器名称**。将显示在 Kaspersky Security Center Web Console 登录窗口中的 Kaspersky Security Center Linux 故障转移集群名称。

   Kaspersky Security Center Web Console 无法使用相同的 .rpm 安装文件升级。如果您要在响应文件中更改设置并使用该文件重新安装应用程序，您必须先卸载该应用程序，然后使用新的响应文件再次安装。

4. 在具有根特权的账户下，根据您的 Linux 分类使用命令行运行 .deb 或 .rpm 安装文件。

   要从先前版本的 Kaspersky Security Center Web Console 升级，请运行以下命令之一：

   - 对于运行基于 RPM 的操作系统的设备：
     ```
     $ sudo rpm -Uvh --nodeps --force ksc-web-console-[build_number].x86_64.rpm
     ```
   - 对于运行基于 Debian 的操作系统的设备：
     ```
     $ sudo dpkg -i ksc-web-console-[build_number].x86_64.deb
     ```

   这将开始解包安装文件。请等待安装完成。

5. 通过执行以下命令重新启动所有 Kaspersky Security Center Web Console 服务：
   ```
   $ sudo systemctl restart KSC*
   ```

当升级完成时，您可以使用您的浏览器打开和登录 Kaspersky Security Center Web Console。

在封闭软件环境模式下在 Astra Linux 上安装Kaspersky Security Center Web Console

该文描述了如何升级 Kaspersky Security Center Web Console 服务器 (也叫 Kaspersky Security Center Web Console) 到 Astra Linux 特别版操作系统。

要升级 Kaspersky Security Center Web Console：

1. 确保您要安装 Kaspersky Security Center Web Console 的设备运行以下一种受支持的 Linux 分类。

2. 阅读并接受最终用户授权许可协议 (EULA)。如果 Kaspersky Security Center Linux 分发包不包含带有 EULA 文本的 TXT 文件，您可以从 卡巴斯基网站 下载文件。如果您不接受授权许可协议的条款，请勿使用安装文件升级 Kaspersky Security Center Web Console 。

3. 使用您在安装 Kaspersky Security Center Web Console 之前准备的相同响应文件。响应文件名称为 ksc-web-console-setup.json，文件位置为 /etc/ksc-web-console-setup.json。

   如果响应文件不存在，请创建一个新的响应文件，其中包含用于将 Kaspersky Security Center Web Console 连接到管理服务器的参数。命名该文件为 ksc-web-console-setup.json，然后将其放置到 /etc 目录中：

   响应文件的一个例子，它包含最小参数集以及默认地址和端口：

   ```
   {
   "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
   }
   ```

4. 确保在 /etc/digsig/digsig_initramfs.conf 文件中，按如下所示指定`DIGSIG_ELF_MODE`参数：

   ```
   DIGSIG_ELF_MODE=1
   ```

5. 确保安装了`astra-digsig-oldkeys`兼容包。

   如果未安装此软件包，请运行以下命令：

   ```
   apt install astra-digsig-oldkeys
   ```

6. 为应用程序密钥创建一个目录（如果不存在）：

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

7. 将应用程序密钥 /opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg 放在上一步创建的目录中：

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

   > 如果 Kaspersky Security Center Linux 分发包不包含 kaspersky_astra_pub_key.gpg 应用程序密钥，您可以通过单击以下链接下载：https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg。

8. 更新 RAM 磁盘：

   ```
   update-initramfs -u -k all
   ```

   重新启动系统。

9. 在具有 root 权限的账户下，使用命令行运行安装文件。您通过从 Kaspersky 网站下载来接收安装文件。

   要从先前版本的 Kaspersky Security Center Web Console 升级，请运行以下命令：

   ```
   $ sudo dpkg -i ksc-web-console-[build_number].x86_64.deb
   ```

   这将开始解包安装文件。请等待安装完成。

10. 通过执行以下命令重新启动所有 Kaspersky Security Center Web Console 服务：

    ```
    $ sudo systemctl restart KSC*
    ```

当升级完成时，您可以使用您的浏览器打开和登录 Kaspersky Security Center Web Console。

迁移到 Kaspersky Security Center Linux

通过使用此方案，您可以将管理组结构、包含的管理设备和其他组对象（策略、任务、全局任务、标签和设备分类）从 Kaspersky Security Center Windows 转移到 Kaspersky Security Center Linux 的管理下。

限制：

- 只能从 Kaspersky Security Center 14.2 Windows 迁移到 Kaspersky Security Center 15.0 Linux。
- 您只能使用 Kaspersky Security Center Web Console 来执行此方案。

在开始之前，请详细了解 Kaspersky Security Center Linux 的功能和限制：

- Kaspersky Security Center Windows 和 Kaspersky Security Center Linux 之间的功能差异
- Kaspersky Security Center Linux 支持的 Kaspersky 应用程序列表

阶段

迁移方案分阶段进行：

1. **选择迁移方法**

   您可以通过迁移向导迁移到 Kaspersky Security Center Linux。迁移向导步骤取决于 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux 的管理服务器是否排列为层次结构：

   - 使用管理服务器层级进行迁移

     如果 Kaspersky Security Center Windows 管理服务器充当 Kaspersky Security Center Linux 管理服务器的辅助服务器，请选择此选项。您可以在 Kaspersky Security Center Web Console 的单个实例中管理迁移过程并在服务器之间切换。如果您更喜欢此选项，可以将管理服务器排列成层次结构以简化迁移过程。为此，请在开始迁移之前创建层次结构。

   - 使用导出文件（ZIP 存档）进行迁移

     如果 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux 的管理服务器未按层次结构排列，请选择此选项。您使用 Kaspersky Security Center Web Console 的两个实例管理迁移过程：一个实例用于 Kaspersky Security Center Windows，另一个实例用于 Kaspersky Security Center Linux。在这种情况下，您将使用在从 Kaspersky Security Center Windows 导出期间创建和下载的导出文件并将此文件导入到 Kaspersky Security Center Linux。

2. **从 Kaspersky Security Center Windows 导出数据**

   打开 Kaspersky Security Center Windows，然后运行迁移向导。

3. **将数据导入到 Kaspersky Security Center Linux**

   继续运行迁移向导将导出的数据导入到Kaspersky Security Center Linux。如果服务器按层次结构排列，则在同一向导中成功导出后，导入会自动开始。如果服务器未按层次结构排列，您可以在切换到Kaspersky Security Center Linux 后继续运行迁移向导。

4. **执行其他操作以手动将对象和设置从 Kaspersky Security Center Windows 传输到 Kaspersky Security Center Linux（可选步骤）**

   您可能还想传输无法通过迁移向导传输的对象和设置。例如，您还可以执行以下操作：

   - 传输管理服务器和受管理应用程序使用的授权许可密钥
   - 配置管理服务器的全局任务

- 配置网络代理策略设置
- 创建应用程序安装包
- 创建虚拟服务器
- 分配和配置分发点
- 配置设备移动规则
- 配置自动标记设备规则
- 创建应用程序类别

5. **移动 Kaspersky Security Center Linux 管理的导入的受管理设备**

   要完成迁移，请将导入的受管理设备移至 Kaspersky Security Center Linux 的管理下。在当前版本的 Kaspersky Security Center Linux中，您可以通过以下方法之一执行此操作：

   - 通过klmover 实用程序

     使用 klmover 实用程序并指定新管理服务器的连接设置。

   - 通过在受管理设备上安装或重新安装网络代理

     创建新的网络代理安装包，并在安装包属性中指定新管理服务器的连接设置。使用安装包通过远程安装任务在导入的受管理设备上安装网络代理。有关详细信息，请参阅切换受 Kaspersky Security Center Linux 管理的受管理设备。

     您还可以创建并使用独立的安装包在本地安装网络代理。

6. **将网络代理更新到最新版本**

   我们建议您将 Linux 网络代理升级到与 Kaspersky Security Center 相同的版本。

7. **确保受管理设备在新管理服务器上可见**

   在 Kaspersky Security Center Linux 管理服务器上，打开受管理设备列表（**资产(设备)→受管理设备**），然后检查**可见**、**网络代理已安装**和**上一次连接到管理服务器**列中的值。

其他数据迁移方法

除了迁移向导之外，还有其他方法可以传输您当前的对象，但这些方法只允许您传输策略和任务。

- 从 Kaspersky Security Center Windows 导出任务，然后导入任务到 Kaspersky Security Center Linux。
- 从 Kaspersky Security Center Windows 导出特定策略，然后导入政策到 Kaspersky Security Center Linux。相关的策略配置文件与选定的策略一起导出和导入。

从 Kaspersky Security Center Windows 导出组对象

从 Kaspersky Security Center Windows 到 Kaspersky Security Center Linux 的迁移管理组结构、包括的受管理设备和其他组对象，需要您首先选择要导出的数据并创建导出文件。导出文件包含有关要迁移的所有组对象的信息。导出文件将用于以后导入到 Kaspersky Security Center Linux 中。

您可以导出以下对象：

- 受管理应用程序的任务和策略
- 全局任务
- 自定义设备分类
- 管理组结构和包含的设备
- 已分配给迁移设备的标签

开始导出前，请阅读有关迁移到 Kaspersky Security Center Linux 的一般信息。选择迁移方法——使用或不使用 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux 管理服务器的层次结构。

通过迁移向导导出受管理设备和相关组对象：

1. 根据 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux 的管理服务器是否被排列成层次结构，执行以下操作之一：
   - 如果服务器被排列成层次结构，打开 Kaspersky Security Center Web Console，然后切换到 Kaspersky Security Center Windows 的服务器。
   - 如果服务器未排列成层次结构，请打开连接到 Kaspersky Security Center Windows 的 Kaspersky Security Center Web Console。
2. 在主菜单中，转到“**操作 → 迁移**”。
3. 选择**迁移到 Kaspersky Security Center Linux 或 Kaspersky Single Management Platform**启动向导并按照其步骤操作。
4. 选择要导出的管理组或子组。请确保所选的管理组或子组包含的设备不得超过 10,000 台。
5. 选择将导出其任务和策略的受管理应用程序。仅选择 Kaspersky Security Center Linux 支持的应用程序。不受支持的应用程序的对象仍将被导出，但将不可操作。
6. 使用左侧的链接，以选择全局任务、设备分类和要导出的报告。您可通过“**组对象**”链接在导出中排除自定义角色、内部用户和安全组以及自定义应用程序类别。

导出文件（ZIP 存档）已创建。根据您是否使用管理服务器层次结构支持执行迁移，导出文件将保存如下：

- 如果服务器排列成层次结构，导出文件将被保存到Kaspersky Security Center Web Console 服务器上的临时文件夹中。
- 如果服务器未排列成层次结构，则导出文件将被下载到您的设备。

对于具有管理服务器层次结构支持的迁移，导入会在成功导出后自动开始。对于没有管理服务器层次结构支持的迁移，您可以手动将保存的导出文件导入到 Kaspersky Security Center Linux。

将导出文件导入到 Kaspersky Security Center Linux

要传输有关从 Kaspersky Security Center Windows 导出的受管理设备、对象及其设置的信息，必须将其导入到 Kaspersky Security Center Linux 或 Kaspersky XDR Expert。

通过迁移向导导入受管理设备和相关组对象：

1. 根据 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux 的管理服务器是否被排列成层次结构，执行以下操作之一：

   - 如果服务器按层次结构排列，则在导出完成后继续执行迁移向导的下一步。在此向导中成功导出后，导入会自动开始（请参阅本说明的步骤 2）。

   - 如果服务器未按层次结构排列：

     a. 打开连接到 Kaspersky Security Center Linux 的 Kaspersky Security Center Web Console 或 Kaspersky XDR Expert。

     b. 在主菜单中，转到"**操作 → 迁移**"。

     c. 选择您在从 Kaspersky Security Center Windows 导出过程中创建并下载的导出文件（ZIP 存档）。开始上传导出文件。

2. 导出文件上传成功后，即可继续导入。如果要指定其他导出文件，请单击**更改**链接，然后选择所需的文件。

3. Kaspersky Security Center Linux 管理组的整个层次结构将得以显示 。

   选中目标管理组旁边的复选框，导出的管理组的对象（受管理设备、策略、任务和其他组对象）必须还原到该目标管理组。

4. 开始导入组对象。导入期间将无法最小化迁移向导和执行任何并行操作。等待至对象列表中所有项目旁边的刷新图标 (🔄) 均替换为绿色复选标记 (✓)，导入完成。

5. 导入完成后，导出的管理组结构（包括设备详细信息）将显示在所选目标管理组下。如果还原的对象的名称与现有对象的名称相同，则将为还原的对象添加一个增量后缀。

> 如果在迁移的任务中指定了运行该任务的帐户的详细信息，则导入完成后您必须打开该任务并再次输入密码。

如果导入已完成但出现错误，您可以执行以下操作之一：

- 对于具有管理服务器层次结构支持的迁移，您可以再次开始导入导出文件。
- 对于没有管理服务器层次结构支持的迁移，您可以启动迁移向导选择另一个导出文件，然后再次导入。

您可以检查导范围中包含的组对象是否已成功导入到 Kaspersky Security Center Linux。为此，请转到**资产(设备)**部分并确保导入的对象是否出现在相应的子部分中。

请注意，导入的受管理设备显示在**受管理设备**子部分中，但它们在网络中不可见，并且网络代理未安装并在其上运行（**可见**、**网络代理已安装**和**网络代理正在运行**列中的*否*值）。

要完成迁移，您需要将受管理设备切换到Kaspersky Security Center Linux 的管理之下。

将受管理设备切换为受 Kaspersky Security Center Linux 管理

将受管理设备、对象及其设置的信息成功导入Kaspersky Security Center Linux 后，您需要将受管理设备切换到Kaspersky Security Center Linux的管理下才能完成迁移。

在当前版本的 Kaspersky Security Center Linux 中，您可以通过使用 klmover 实用程序或者通过远程安装任务在受管理设备上安装网络代理来移动 Kaspersky Security Center Linux 下的受管理设备。

要通过安装网络代理将受管理设备切换为由Kaspersky Security Center Linux 管理：

1. 切换到 Kaspersky Security Center Windows 的管理服务器。
2. 进入**发现和部署→部署和分配→安装包**，然后打开网络代理现有安装包的属性。

   如果软件包列表中没有网络代理安装包，请下载新的安装包。
3. 在**设置**选项卡上，选择**连接**区域。指定 Kaspersky Security Center Linux 的管理服务器的连接设置。
4. 为导入的受管理设备创建远程安装任务，然后指定重新配置的网络代理安装包。

   您可以通过 Kaspersky Security Center Windows 的管理服务器或通过充当分发点的基于 Windows 的设备安装网络代理。如果您使用管理服务器，请启用**通过管理服务器使用操作系统资源**选项。如果您使用分发点，请启用**通过分发点使用操作系统资源**选项。
5. 运行远程安装任务。

远程安装任务成功完成后，请转至 Kaspersky Security Center Linux 的管理服务器并确保受管理设备在网络中可见，并且网络代理已安装并在其上运行（**可见**、**网络代理已安装**和**网络代理正在运行**列中的*"是"*值）。

配置管理服务器

本节介绍 Kaspersky Security Center 管理服务器的配置过程和属性。

配置 Kaspersky Security Center Web Console 到管理服务器的连接

要设置管理服务器连接端口：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ()。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**连接端口**”区域。

应用程序显示所选服务器的主要连接设置。

配置用于登录 Kaspersky Security Center Linux 的 IP 地址允许列表

默认情况下，用户可以在任何可以打开 Kaspersky Security Center Web Console 的设备上登录 Kaspersky Security Center Linux。但是，您可以配置管理服务器，使用户只能从具有允许 IP 地址的设备进行连接。在这种情况下，即使入侵者窃取了 Kaspersky Security Center Linux 账户，也无法登录 Kaspersky Security Center Linux，因为入侵者设备的 IP 地址不在允许列表中。

当用户登录 Kaspersky Security Center Linux 或运行通过 Kaspersky Security Center Linux OpenAPI 与管理服务器交互的应用程序时，将验证 IP 地址。此时，用户的设备尝试与管理服务器建立连接。如果设备的 IP 地址不在允许列表中，则会发生身份验证错误，并且 KLAUD_EV_SERVERCONNECT 事件将通知您尚未建立与管理服务器的连接。

IP 地址允许列表的要求

仅当以下应用程序尝试连接到管理服务器时才会验证 IP 地址：

- Kaspersky Security Center Web Console 服务器

  如果您通过 Kaspersky Security Center Web Console 登录 Kaspersky Security Center Linux，您可以使用操作系统的标准方式在安装了 Kaspersky Security Center Web Console 服务器 的设备上配置防火墙。然后，如果有人尝试在一台设备上登录 Kaspersky Security Center Linux 并且 Kaspersky Security Center Web Console 服务器安装在另一台设备上，防火墙将有助于防止入侵者干扰。

- 通过 klakaut 自动化对象与管理服务器交互的应用程序
- 通过 OpenAPI 与管理服务器交互的应用程序，例如 Kaspersky Anti Targeted Attack Platform 或 Kaspersky Security for Virtualization

因此，请指定安装了上述应用程序的设备的地址。

您可以设置 IPv4 和 IPv6 地址。您不能指定 IP 地址范围。

如何建立 IP 地址允许列表

如果您之前未设置允许列表，请按照下面的说明操作。

要建立用于登录 Kaspersky Security Center Linux 的 IP 地址允许列表：

1. 在管理服务器设备上，在具有管理员权限的账户下运行命令提示符。
2. 将当前目录更改为 Kaspersky Security Center Linux 安装文件夹（通常为 /opt/kaspersky/ksc64/sbin）。
3. 在根账户下输入以下命令：
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP 地址>" -t s`

   指定满足上述要求的 IP 地址。多个 IP 地址必须用分号隔开。

   如何只允许一台设备连接到管理服务器的示例：

   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0" -t s`

   如何允许多台设备连接到管理服务器的示例：

   `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. 重启管理服务器服务。

您可以在管理服务器上的 Syslog 事件日志中查看您是否已成功配置 IP 地址允许列表。

如何更改 IP 地址允许列表

您可以像第一次建立允许列表那样进行更改。为此，请运行相同的命令并指定一个新的允许列表：

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP 地址>" -t s
```

如果要从允许列表中删除某些 IP 地址，请将其重写。例如，您的允许列表包括以下 IP 地址：192.0.2.0; 198.51.100.0; 203.0.113.0。您要删除 198.51.100.0 IP 地址。为此，在命令提示符处输入以下命令：

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 203.0.113.0" -t s
```

不要忘记重新启动管理服务器服务。

如何重置已配置的 IP 地址允许列表

要重置已配置的 IP 地址允许列表：

1. 在根账户下的命令提示符处输入以下命令：
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "" -t s`
2. 重启管理服务器服务。

之后，不再验证 IP 地址。

指定管理服务器的互联网连接设置

您必须配置互联网连接才能使用卡巴斯基安全网络和为 Kaspersky Security Center Linux 及受管理的卡巴斯基应用程序下载反病毒数据库更新。

要指定管理服务器的互联网访问设置：

1. 在主菜单，单击管理服务器名称旁边的设置图标 ()。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**配置互联网访问**”区域。
3. 如果您要在连接到互联网时使用代理服务器，请启用“**使用代理服务器**”选项。如果启用此选项，字段可用于输入设置。为代理服务器连接指定以下设置：

   - 地址

     Kaspersky Security Center Linux 用于连接到互联网的代理服务器地址。

   - 端口号

     将建立 Kaspersky Security Center Linux 代理服务器连接的端口号。

   - 对本地地址不使用代理服务器

     将不会使用代理服务器连接本地网络的设备。

   - 代理服务器身份验证

     如果选择该选框，您可以在输入字段中为代理服务器身份验证指定凭证。
     如果选中“**使用代理服务器**”复选框，则该输入字段可用。

   - 用户名

     用于与代理服务器建立连接的用户账户（如果选中“**代理服务器身份验证**”复选框，则该字段可用）。

   - 密码

     建立代理服务器连接的账户所属的用户所设置的密码（如果选中“**代理服务器身份验证**”复选框，则该字段可用）。
     要查看输入的密码，单击并按住“**显示**”按钮足够长时间。

您还可以使用快速启动向导配置互联网访问。

管理服务器层级

一些客户公司，例如 MSP，可能运行多个管理服务器。可能不方便管理几个不同的管理服务器，因此可以应用层次结构。在层次结构中，基于 Linux 的管理服务器既可以作为主服务器也可以作为辅助服务器。基于 Linux 的主服务器可以管理基于 Linux 和基于 Windows 的辅助服务器。基于 Windows 的主服务器可以管理基于 Linux 的辅助服务器。

两个管理服务器的“主/从”配置提供了以下选项：

- 一个从属管理服务器从主管理服务器继承策略、任务、用户角色和安装包，从而防止了重复设置。
- 主管理服务器上的设备分类可以包含从属管理服务器的设备。
- 主管理服务器的报告可以包含从属管理服务器的数据（包括详细信息）。
- 主管理服务器可以用作从属管理服务器的更新源。

主管理服务器仅接收来自上面列出的选项范围内的非虚拟从属管理服务器的数据。此限制不适用于虚拟管理服务器，虚拟管理服务器与其主管理服务器共享数据库。

创建管理服务器层级：添加从属管理服务器

在层次结构中，基于 Linux 的管理服务器既可以作为主服务器也可以作为辅助服务器。基于 Linux 的主服务器可以管理基于 Linux 和基于 Windows 的辅助服务器。基于 Windows 的主服务器可以管理基于 Linux 的辅助服务器。

添加从属管理服务器（在未来的主管理服务器上执行）

您可以添加管理服务器作为从属管理服务器，从而建立“主/从属”层级。

要添加可以通过 Kaspersky Security Center Web Console 连接的从属管理服务器：

1. 确保未来主管理服务器的端口 13000 可用于从从属管理服务器接收连接。
2. 在未来主管理服务器上，单击“设置”图标 ( )。
3. 在打开的属性页面上，单击“**管理服务器**”选项卡。
4. 选择您要向其添加管理服务器的管理组名称旁边的复选框。
5. 在菜单行中，单击“**连接从属管理服务器**”。
   “添加从属管理服务器向导”启动。
6. 在向导的第一页，填充以下字段：
   - 从属管理服务器显示名称

     从属管理服务器将显示在层级的名称。如果需要，您可以输入 IP 地址作为名称，也可以使用名称，例如“组 1 的从属服务器”。

   - 从属管理服务器地址(可选)

     指定从属管理服务器的 IP 地址或域名。
     如果启用了“**连接主管理服务器到 DMZ 中的从属管理服务器**”选项，则需要此参数。

   - 管理服务器 SSL 端口

指定主管理服务器上的 SSL 端口号。默认端口号是 13000。

- 管理服务器 API 端口

  指定主管理服务器上的端口号以通过 OpenAPI 接收连接。默认端口号是 13299。

- 连接主管理服务器到 DMZ 中的从属管理服务器

  如果从属管理服务器位于隔离区 (DMZ)，选择该选项。

  如果选择此选项，主管理服务器将发起与从属管理服务器的连接。否则，从属管理服务器将发起与主管理服务器的连接。

- 使用代理服务器

  如果您使用代理服务器连接到从属管理服务器，选择该选项。

  此种情况下，您也必须指定代理服务器的以下设置：

  - 地址
  - 用户名
  - 密码

7. 指定连接设置：

   - 输入将来的主管理服务器的地址。
   - 如果将来的从属管理服务器使用代理服务器，请输入代理服务器地址和用户凭证以连接到代理服务器。

8. 输入对将来的从属管理服务器具有访问权限的用户的凭证。

   确保为您指定的账户禁用两步验证。如果为此账户启用了两步验证，则您仅可从将来的从属服务器创建层级（请参阅下方说明）。这是一个已知问题。

如果连接设置正确，则与将来的从属服务器建立连接，并建立“主/从属”层级。如果连接失败，请检查连接设置或手动指定将来的从属服务器的证书。

连接失败的另一个可能原因是：将来的从属服务器是使用 Kaspersky Security Center Linux 自动生成的自签名证书进行身份验证的。因此，浏览器可能会阻止下载自签名证书。如果是这种情况，您可以执行以下操作之一：

- 对于将来的从属服务器，创建在您的基础架构中受信任且满足自定义证书要求的证书。
- 将将来的从属服务器的自签名证书添加到受信任浏览器证书列表中。我们建议您仅在无法创建自定义证书时才使用此选项。有关将证书添加到受信任证书列表中的信息，请参阅所用浏览器的文档。

向导完成后，“主/从属”层级被建立。主管理服务器和从属管理服务器之间的连接通过端口 13000 建立。主管理服务器的任务和策略被接收和应用。从属管理服务器显示在主管理服务器上，在添加其的管理组中。

添加从属管理服务器（在未来的从属管理服务器上执行）

如果您无法连接到未来从属管理服务器（例如，它临时被断开或无法连接或从属管理服务器的证书文件为自签名），您仍可以添加从属管理服务器。

要添加不可以通过 Kaspersky Security Center Web Console 连接的管理服务器作为从属：

1. 将未来主管理服务器的证书文件发送给未来从属管理服务器所在办公室的系统管理员。（例如，您可以将文件写入闪存驱动器等外部设备，或通过电子邮件发送它。）

   证书文件位于未来的主管理服务器上的 /var/opt/kaspersky/klnagent_srv/1093/cert/ 中。

2. 提示未来从属管理服务器的责任系统管理员做以下事情：

   a. 点击设置图标（）。

   b. 在打开的属性页面上，转到“**常规**”选项卡的“**管理服务器层级**”区域。

   c. 选择**该管理服务器是服务器层级中的从属**选项。

   d. 在“**主管理服务器地址**”字段中，输入将来的主管理服务器的网络名称。

   e. 通过单击“**浏览**”选择先前保存的带有未来主管理服务器证书的文件。

   f. 如有必要，选中“**连接主管理服务器到 DMZ 中的从属管理服务器**”复选框。

   g. 如果通过代理服务器连接到将来的主管理服务器，则选中“**使用代理服务器**”选项并指定连接设置。

   h. 点击“**保存**”。

“主/从属”层级被创建。主管理服务器开始使用端口 13000 从从属管理服务器接收连接。主管理服务器的任务和策略被接收和应用。从属管理服务器显示在主管理服务器上，在添加其的管理组中。

查看从属管理服务器列表

要查看从属（包括虚拟）管理服务器列表：

在主菜单中，单击“设置”图标 () 旁边的管理服务器名称。

从属（包括虚拟）管理服务器下拉列表被显示。

您可以通过单击名称转到任一管理服务器。

管理组也会显示，但它们为灰显，无法在此菜单中进行管理。

如果您在 Kaspersky Security Center Web Console 中连接到主管理服务器，但无法连接到由从属管理服务器管理的虚拟管理服务器，您可以使用以下方法之一：

- 修改现有的 Kaspersky Security Center Web Console 安装，以将从属服务器添加到受信任的管理服务器列表中。然后您将能够在 Kaspersky Security Center Web Console 中连接到该虚拟管理服务器。

1. 在安装了 Kaspersky Security Center Web Console 的设备上，使用具有管理权限的账户运行与您设备上安装的 Linux 发行版相对应的 Kaspersky Security Center Web Console 安装文件。
2. 安装向导将启动。
3. 在向导的第一页，选择**升级**选项。
4. 在**修改类型**页面，选择“**编辑连接设置**”选项。
5. 在**受信任的管理服务器**页面上，添加所需的从属管理服务器。
6. 在向导的最后一页，点击**修改**以应用设置。
7. 在应用程序重新配置成功完成后，点击**完成**按钮。

- 使用 Kaspersky Security Center Web Console 直接连接到在其中创建了虚拟服务器的从属管理服务器。然后您将能够在 Kaspersky Security Center Web Console 中切换到该虚拟管理服务器。

管理虚拟管理服务器

本节介绍管理虚拟管理服务器的以下操作：

- 创建虚拟管理服务器
- 启用和禁用虚拟管理服务器
- 为虚拟管理服务器分配管理员
- 更改客户端设备的管理服务器
- 删除虚拟管理服务器

创建虚拟管理服务器

您可以创建虚拟管理服务器并添加它们到管理组。

要创建和添加虚拟管理服务器：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ()。
2. 在打开的页面上，转到“**管理服务器**”选项卡。
3. 选择您要添加虚拟管理服务器到的管理组。
   虚拟管理服务器将管理选定组（包括子组）中的设备。
4. 在菜单行中，单击“**新虚拟管理服务器**”。
5. 在打开的页面上，定义新虚拟管理服务器的属性：

- 虚拟管理服务器名称。
- 管理服务器连接地址

  您可以指定管理服务器的名称或 IP 地址。

6. 从用户列表中，选择虚拟管理服务器管理员。如果您想，您可以编辑现有账户之一，然后分配其管理员角色，或创建一个新用户账户。
7. 点击“保存”。

新的虚拟管理服务器将创建，添加到管理组并显示在“管理服务器”选项卡上。

如果您在 Kaspersky Security Center Web Console 中连接到主管理服务器，但无法连接到由从属管理服务器管理的虚拟管理服务器，您可以使用以下方法之一：

- 修改现有的 Kaspersky Security Center Web Console 安装，以将从属服务器添加到受信任的管理服务器列表中。然后您将能够在 Kaspersky Security Center Web Console 中连接到该虚拟管理服务器。

  1. 在安装了 Kaspersky Security Center Web Console 的设备上，使用具有管理权限的账户运行与您设备上安装的 Linux 发行版相对应的 Kaspersky Security Center Web Console 安装文件。
  2. 安装向导将启动。
  3. 在向导的第一页，选择升级选项。
  4. 在修改类型页面，选择“编辑连接设置”选项。
  5. 在受信任的管理服务器页面上，添加所需的从属管理服务器。
  6. 在向导的最后一页，点击修改以应用设置。
  7. 在应用程序重新配置成功完成后，点击完成按钮。

- 使用 Kaspersky Security Center Web Console 直接连接到在其中创建了虚拟服务器的从属管理服务器。然后您将能够在 Kaspersky Security Center Web Console 中切换到该虚拟管理服务器。

Enabling and disabling a virtual Administration Server

When you create a new virtual Administration Server, it is enabled by default. You can disable or enable it again at any time. Disabling or enabling a virtual Administration Server is equal to switching off or on a physical Administration Server.

To enable or disable a virtual Administration Server:

1. In the main menu, click the settings icon () next to the name of the required Administration Server.
2. On the page that opens, proceed to the 管理服务器 tab.
3. Select the virtual Administration Server that you want to enable or disable.
4. On the menu line, click the 启用/禁用虚拟管理服务器 button.

The virtual Administration Server state is changed to enabled or disabled, depending on its previous state. The updated state is displayed next to the Administration Server name.

为虚拟管理服务器分配管理员

当您在组织中使用虚拟管理服务器时，可能希望为每个虚拟管理服务器分配一名专门的管理员。例如，当您创建虚拟管理服务器来管理组织的独立办公室或部门时，或者如果您是 MSP 提供商并通过虚拟管理服务器来管理您的租户时，这可能很有用。

当您创建虚拟管理服务器时，它会继承主管理服务器的用户列表和所有用户权限。如果用户有权访问主服务器，则该用户也有权访问虚拟服务器。创建后，您可以单独配置对服务器的访问权限。如果您想要仅为虚拟管理服务器分配管理员，请确保该管理员没有主管理服务器的访问权限。

您可以通过向管理员授予虚拟管理服务器的访问权限来为虚拟管理服务器分配管理员。您可以通过以下方式之一授予所需的访问权限：

- 手动配置管理员的访问权限
- 为管理员分配一个或多个用户角色

要登录 Kaspersky Security Center Web Console，虚拟管理服务器的管理员要指定虚拟管理服务器名称、用户名和密码。Kaspersky Security Center Web Console 会对管理员进行身份验证并打开管理员有权访问的虚拟管理服务器。管理员不能在管理服务器之间切换。

先决条件

在开始之前，请确保满足以下条件：

- 虚拟管理服务器已创建。
- 在主管理服务器上，您已为希望为其分配虚拟管理服务器的管理员创建一个账户。
- 您在“修改对象 ACL right in the **常规功能 → 用户权限**“修改对象 ACL”权限。

手动配置访问权限

要为虚拟管理服务器分配管理员：

1. 在主菜单，切换到所需的虚拟管理服务器：
   a. 单击当前管理服务器名称右侧的 V 形图标 ()。
   b. 选择所需的管理服务器。
2. 在主菜单，单击管理服务器名称旁边的“设置”图标 ()。
   管理服务器属性窗口将打开。
3. 在“**访问权限**”选项卡上，单击“**添加**”按钮。
   系统会打开主管理服务器和当前虚拟管理服务器的用户的统一列表。

4. 从用户列表中，选择要为虚拟管理服务器分配的管理员账户，然后单击“**确定**”按钮。

   应用程序将所选的用户添加到“**访问权限**”选项卡上的用户列表。

5. 选中已添加账户旁边的复选框，然后单击“**访问权限**”按钮。

6. 配置管理员将拥有的虚拟管理服务器的权限。

   要成功进行身份验证，管理员至少必须具有以下权限：

   - “**常规功能 → 基本功能**”功能区域中的**读取**权限
   - “**常规功能 → 虚拟管理服务器**”功能区域中的**读取**权限

应用程序将修改后的用户权限保存到管理员账户中。

通过分配用户角色配置访问权限

或者，您可以通过用户角色向虚拟管理服务器管理员授予访问权限。例如，如果您想在同一个虚拟管理服务器上分配多个管理员，这可能很有用。如果是这种情况，您可以为管理员账户分配相同的一个或多个用户角色，而不是为多个管理员配置相同的用户权限。

通过分配用户角色为虚拟管理服务器分配管理员：

1. 在主管理服务器上，创建一个新的用户角色，然后指定管理员在虚拟管理服务器上必须拥有的所有所需访问权限。您可以创建多个角色，例如，如果您想要单独访问不同的功能区域。

2. 在主菜单，切换到所需的虚拟管理服务器：

   a. 单击当前管理服务器名称右侧的 V 形图标 ( )。

   b. 选择所需的管理服务器。

3. 向管理员账户分配新角色或多个角色。

   应用程序向管理员账户分配角色。

配置对象级别的访问权限

除了分配功能区域级别的访问权限，您还可以在虚拟管理服务器上配置对特定对象的访问，例如对特定管理组或任务的访问。为此，请切换到虚拟管理服务器，然后在对象的属性中配置访问权限。

Changing the Administration Server for client devices

You can change the Administration Server that manages client devices to a different Server using the **更改管理服务器** task. After the task completion, the selected client devices will be put under the management of the Administration Server that you specify. You can switch the device management between the following Administration Servers:

- Primary Administration Server and one of its virtual Administration Servers
- Two virtual Administration Servers of the same primary Administration Server

To change the Administration Server that manages client devices to a different Server:

1. In the main menu, go to 资产(设备) → 任务.
2. Click 添加.

   The New task wizard starts. Proceed through the wizard by using the 下一步 button.
3. For the Kaspersky Security Center application, select the 更改管理服务器 task type.
4. Specify the name for the task that you are creating.

   A task name cannot be more than 100 characters long and cannot include any special characters ("*<>?\:|).
5. Select devices to which the task will be assigned.
6. Select the Administration Server that you want to use to manage the selected devices.
7. Specify the account settings:

   - 默认账户

     The task will be run under the same account as the application that performs this task.

     By default, this option is selected.

   - 指定账户

     Fill in the 账户 and 密码 fields to specify the details of an account under which the task is run. The account must have sufficient rights for this task.

   - 账户

     Account under which the task is run.

   - 密码

     Password of the account under which the task will be run.
8. If on the 完成任务创建 page you enable the 创建完成时打开任务详情 option, you can modify the default task settings. If you do not enable this option, the task is created with the default settings. You can modify the default settings later, at any time.
9. Click the 完成 button.

   The task is created and displayed in the list of tasks.
10. Click the name of the created task to open the task properties window.
11. In the task properties window, specify the general task settings according to your needs.
12. Click the 保存 button.

    The task is created and configured.

13. Run the created task.

After the task is complete, the client devices for which it was created are put under the management of the Administration Server specified in the task settings.

Deleting a virtual Administration Server

When you delete a virtual Administration Server, all of the objects created on the Administration Server, including policies and tasks, will be deleted as well. The managed devices from the administration groups that were managed by the virtual Administration Server will be removed from the administration groups. To return the devices under management of Kaspersky Security Center Linux, run the network polling, and then move the found devices from the Unassigned devices group to the administration groups.

To delete a virtual Administration Server:

1. In the main menu, click the settings icon ( ) next to the name of the Administration Server.
2. On the page that opens, proceed to the 管理服务器 tab.
3. Select the virtual Administration Server that you want to delete.
4. On the menu line, click the 删除 button.

The virtual Administration Server is deleted.

查看连接到管理服务器的日志

操作期间的连接历史和到管理服务器的连接尝试可以被保存到文件。文件中的信息允许您跟踪不仅您的网络基础架构中的连接，还有非授权的到服务器的访问尝试。

要记录连接管理服务器事件：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ( )。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**连接端口**”区域。
3. 启用“**记录管理服务器连接事件**”选项。

所有连入管理服务器的后续事件、身份验证结果和 SSL 错误将被保存到 /var/opt/kaspersky/klnagent_srv/logs/sc.syslog文件。

设置事件存储库中的最大事件数量

在管理服务器属性窗口的“**事件存储库**”区域，您可以通过限制事件记录数和存储期限来编辑管理服务器数据库的事件存储设置。当您指定事件最大数时，应用程序计算用于指定数目的存储空间的大概大小。您可以使用该大概计算来评估您在磁盘上是否具有足够空间以避免数据库溢出。管理服务器数据库的默认容量是 400,000 个事件。最大建议的数据库容量是 45,000,000 个事件。

应用程序每 10 分钟检查一次数据库。如果事件数达到指定的最大值加 10,000，应用程序将删除最旧的事件，以便仅保留指定的最大事件数。

当管理服务器删除旧事件后，它无法保存新事件到数据库。在此时间段内，拒绝事件的信息被写入操作系统日志。新事件被列队，然后在删除操作后被保存到数据库。

要限制存储在管理服务器事件存储库中的事件的数量：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ()。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**事件存储库**”区域。指定存储在数据库中的最大事件数量。
3. 单击“**保存**”按钮。

将管理服务器移动至其他设备

如果需要在新设备上使用管理服务器，可以通过以下方式之一进行移动：

- 将管理服务器和数据库服务器移至新设备。
- 将数据库服务器保留在以前的设备上，仅将管理服务器移至新设备。

要将管理服务器和数据库服务器移至新设备：

1. 在先前设备上，创建管理服务器数据的备份。
   为此，您可以通过 Kaspersky Security Center Web Console 运行数据备份任务或运行 klbackup 实用程序。
2. 选择要安装管理服务器的新设备。确保所选设备上的硬件和软件符合管理服务器、Kaspersky Security Center Web Console 和网络代理的要求。此外，请检查管理服务器上使用的端口是否可用。
3. 在新设备上，安装管理服务器将使用的 DBMS。
   选择 DBMS 时，请考虑管理服务器覆盖的设备数量。
4. 在新设备上安装管理服务器。
   请注意，如果将数据库服务器移至新设备，请将本地地址指定为安装数据库的设备的 IP 地址（安装 Kaspersky Security Center Linux 指令的“h”项）。如果需要将数据库服务器保留在以前的设备上，请在安装 Kaspersky Security Center Linux 指令的“h”项中输入以前的设备的 IP 地址。
5. 安装完成后，在新设备上使用 klbackup 实用程序恢复管理服务器数据。

   如果在先前设备和新设备上使用 SQL Server 作为 DBMS，请注意，新设备上安装的 SQL Server 版本必须不得低于先前设备上安装的 SQL Server 版本。否则，将无法在新设备上恢复管理服务器数据。

6. 打开 Kaspersky Security Center Web Console 并连接到管理服务器。

7. 验证是否所有客户端设备都连接到管理服务器。

8. 从以前的设备中卸载管理服务器和数据库服务器。

Changing DBMS credentials

Sometimes, you may need to change DBMS credentials, for example, in order to perform a credential rotation for security purposes.

To change DBMS credentials in a Linux environment by using the klsrvconfig utility:

1. Launch a Linux command line.

2. Specify the klsrvconfig utility in the opened command line window:

   ```
   sudo /opt/kaspersky/ksc64/sbin/klsrvconfig -set_dbms_cred
   ```

3. Specify a new account name. You should specify credentials of an account that exists in the DBMS.

4. Enter a new password.

5. Specify the new password for confirmation.

The DBMS credentials are changed.

备份复制和管理服务器数据恢复

数据备份允许您将管理服务器从一台设备上转移至其他设备且无数据丢失。通过备份，您可以在将管理服务器数据库移至其他设备时或升级到较新版本的 Kaspersky Security Center Linux 时恢复数据（不支持将管理服务器数据移至 Kaspersky Security Center Windows 的管理之下）。

请注意，已安装的管理插件不会被备份。从备份副本恢复管理服务器数据后，您需要下载并重新安装受管理应用程序的插件。

备份管理服务器数据之前，请检查虚拟管理服务器是否已添加到管理组。如果添加了虚拟管理服务器，请确保在备份之前为该虚拟管理服务器分配了管理员。备份后，您将无法授予管理员对虚拟管理服务器的访问权限。请注意，如果管理员账户凭据丢失，您将无法向虚拟管理员服务器分配新管理员。

您可以使用以下方式之一创建管理服务器数据的备份副本：

- 通过 Kaspersky Security Center Web Console 创建并运行数据备份任务。
- 通过在已安装管理服务器的设备上运行 klbackup 实用程序。该实用程序包含在 Kaspersky Security Center 分发包。管理服务器安装完毕后，该实用程序位于在安装应用程序时指定的目标文件夹的根目录中（通常为 /opt/kaspersky/ksc64/sbin/klbackup）。

以下数据保存在管理服务器的备份副本中：

- 管理服务器数据库（策略、任务、应用程序设置、管理服务器上保存的事件）。

- 有关管理组和客户端设备的结构的配置详情。
- 远程安装的应用程序分发包的存储库。
- 管理服务器证书。

只用使用 klbackup 实用程序才能进行管理服务器恢复。

Creating an Administration Server data backup task

Backup tasks are Administration Server tasks; they are created through the quick start wizard. If a backup task created by the quick start wizard has been deleted, you can create one manually.

The *Backup of Administration Server data* task can only be created in a single copy. If the Administration Server data backup task has already been created for the Administration Server, it is not displayed in the task type selection window.

To create an Administration Server data backup task:

1. In the main menu, go to 资产(设备) → 任务.
2. Click 添加.

   The New task wizard starts.
3. On the first page of the wizard, in the 应用程序 list, select **Kaspersky Security Center 15**, and in the 任务类型 list, select 备份管理服务器数据.
4. On the corresponding page of the wizard, specify the following information:
   - Folder for storage of backup copies
   - Password for the backup (optional)
   - Maximum number of backup copies to save
5. If on the 完成任务创建 page you enable the 创建完成时打开任务详情 option, you can modify the default task settings. If you do not enable this option, the task is created with the default settings. You can modify the default settings later, at any time.
6. Click the 完成 button.

The task is created and displayed in the list of tasks.

使用 klbackup 实用程序备份和恢复数据

您可以使用 Kaspersky Security Center 发布套件中附带的 klbackup 实用程序复制管理服务器数据以作备份和将来恢复之用。

要以静默模式创建备份副本或恢复管理服务器数据，

在已安装管理服务器的设备上，利用命令行和所需密钥运行 klbackup。

实用程序命令行语法：

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

如果在 klbackup 实用程序的命令行中没有指定密码，该实用程序将提示您输入密码。

参数描述：

- `-path BACKUP_PATH` – 在 BACKUP_PATH 文件夹中保存信息或使用 BACKUP_PATH 文件夹中的数据进行恢复（必填参数）。
- `-logfile LOGFILE` – 保存关于管理服务器数据备份和恢复的报告。

  数据库服务器账户和 klbackup 实用程序需要获得更改 BACKUP_PATH 文件夹中数据的权限。
- `-use_ts` – 保存数据时，将数据复制到 BACKUP_PATH 文件夹，将其复制到以 `klbackup YYYY-MM-DD # HH-MM-SS` 格式命名为包含当前系统日期和操作时间的子文件夹。如果未指定键，信息将保存在 BACKUP_PATH 文件夹的根目录。

  当您尝试将信息保存至已存储备份副本的文件夹时，系统会返回错误消息。不会更新任何信息。

  `-use_ts` 键允许您维护管理服务器数据压缩文件。例如，如果 `-path` 键指明文件夹 `C:\KLBackups`，则文件夹 `klbackup 2022/6/19 # 11-30-18` 将存储截至 2022 年 6 月 19 日上午 11:30:18 的管理服务器状态信息。
- `-restore` – 恢复管理服务器数据。系统将基于 BACKUP_PATH 文件夹内包含的信息执行数据恢复。如果没有可用的键，数据将备份在 BACKUP_PATH 文件夹内。
- `-password PASSWORD` – 使用 PASSWORD 参数指定的密码保存或恢复管理服务器证书、加密或解密证书。

  忘记的密码无法被恢复。没有密码要求。密码长度不受限制，并且可以是零长度（无密码）。

  在恢复数据时，您必须指定在备份过程中输入的密码。如果某个共享文件夹的路径在备份任务完成后发生更改，请检查使用数据恢复任务的操作（恢复任务和远程安装任务）。必要时，编辑这些任务的设置。当从备份文件恢复数据时，没有人可以访问管理服务器的共享文件夹。启动 klbackup 实用程序所使用的账户必须对该共享文件夹具有完全访问权限。建议您在新安装的管理服务器上运行该实用程序。
- `-online`—通过创建卷快照来备份管理服务器数据以最小化管理服务器的离线时间。当您使用实用程序恢复数据时，该选项被忽略。

管理服务器维护

管理服务器维护允许您降低数据库容量，提高应用程序的运行和操作可靠性。我们建议您至少每周维护一次管理服务器。

管理服务器通过专用任务进行维护。在维护管理服务器时，应用程序执行以下操作：

- 检查数据库错误。
- 重组数据库索引。

- 更新数据库统计信息。
- 收缩数据库（如果必要）。

管理服务器维护任务支持 MariaDB 版本 10.3 及更高版本。如果您使用 MariaDB 10.2 或更早版本，管理员必须自行维护此 DBMS。

安装 Kaspersky Security Center Linux 时，会自动创建“管理服务器维护”任务。如果“管理服务器维护”任务被删除，您可以手动创建它。

要创建管理服务器维护任务，请执行以下操作：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。
2. 单击“**添加**”按钮。
   “新任务向导”启动。
3. 在向导的“**新任务**”窗口中，选择“**管理服务器维护**”为任务类型并单击“**Next**下一步”按钮。
4. 遵照剩余的向导说明。

新创建的任务显示在任务列表中。一个管理服务器仅可以运行一个“管理服务器维护”任务。如果已经为管理服务器创建了“管理服务器维护”任务，则无法创建新的“管理服务器维护”任务。

删除管理服务器层级

如果不再想拥有管理服务器层级结构，您可以从该层级将其断开连接。

要删除管理服务器层级：

1. 在主菜单，单击主管理服务器名称旁边的“设置”图标 ( )。
2. 在打开的页面上，转到“**管理服务器**选项卡。
3. 在要从其中删除从属管理服务器的管理组中，选择从属管理服务器。
4. 在菜单项目上，单击“**删除**”按钮。
5. 在打开的窗口中，单击“**确定**”以确认您要删除该从属管理服务器。

   先前的主管理服务器和从属管理服务器现在彼此独立。层级不再存在。

访问公共 DNS 服务器

如果无法使用系统 DNS 访问卡巴斯基服务器，Kaspersky Security Center Linux 可以按以下顺序使用这些公共 DNS 服务器：

1. Google Public DNS (8.8.8.8)
2. Cloudflare DNS (1.1.1.1)

3. Alibaba Cloud DNS (223.6.6.6)

4. Quad9 DNS (9.9.9.9)

5. CleanBrowsing (185.228.168.168)

对这些 DNS 服务器的请求可能包含域地址和管理服务器的公共 IP 地址，因为应用程序建立了到 DNS 服务器的 TCP/UDP 连接。如果 Kaspersky Security Center Linux 使用公共 DNS 服务器，则数据处理受相关服务的隐私政策约束。

要通过使用 klscflag 实用程序配置公共 DNS 的使用：

1. 运行命令行，然后将当前目录更改为包含 klscflag 实用程序的目录。klscflag 实用程序位于安装管理服务器的目录中。默认安装路径为/opt/kaspersky/ksc64/sbin。

2. 要禁用公共 DNS 的使用，请在根账户下运行以下命令：

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 1
   ```

3. 要启用公共 DNS 的使用，请在根账户下运行以下命令：

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 0
   ```

Configuring the interface

You can configure the Kaspersky Security Center Web Console interface to display and hide sections and interface elements, depending on the features being used.

To configure the Kaspersky Security Center Web Console interface in accordance with the currently used set of features:

1. In the main menu, go to your account settings, and then select 界面选项.

2. In the 界面选项 window that opens, enable or disable the 显示数据加密和保护 option.

3. Click **Save**.

   After that, the 操作 → 数据加密和保护 section appears in the main menu.

使用 TLS 的加密通信

要修复您组织企业网络中的漏洞，您可以使用 TLS 协议启用流量加密。您可以在管理服务器上启用 TLS 加密协议和支持的密码套件。Kaspersky Security Center Linux 支持 TLS 协议版本 1.0、1.1、1.2 和 1.3。您可以选择所需的加密协议和加密套件。

Kaspersky Security Center Linux 使用自签发证书。您也可以使用您自己的证书。Kaspersky 专家建议使用由受信任证书机构发布的证书。

要在管理服务器上配置允许的加密协议和加密套件：

1. 运行命令行，然后将当前目录更改为包含 klscflag 实用程序的目录。klscflag 实用程序位于安装管理服务器的目录中。默认安装路径为/opt/kaspersky/ksc64/sbin。

2. 使用 SrvUseStrictSslSettings 标志在管理服务器上配置允许的加密协议和加密套件。在根账户下的命令行处执行以下命令：

```
klscflag -fset -pv ".core/.independent" -s Transport -n SrvUseStrictSslSettings -
v <value> -t d
```

指定 SrvUseStrictSslSettings 标志的<value>参数：

- 4 — 仅启用 TLS 1.2 和 TLS 1.3 协议。此外，还启用了具有 TLS_RSA_WITH_AES_256_GCM_SHA384 的密码套件（向后兼容 Kaspersky Security Center 11 需要这些密码套件）。这是默认值。

  TLS 1.2 协议支持的密码套件：

  - ECDHE-RSA-AES256-GCM-SHA384
  - ECDHE-RSA-AES256-SHA384
  - ECDHE-RSA-CHACHA20-POLY1305
  - AES256-GCM-SHA384（具有 TLS_RSA_WITH_AES_256_GCM_SHA384 的密码套件）
  - ECDHE-RSA-AES128-GCM-SHA256
  - ECDHE-RSA-AES128-SHA256

  TLS 1.3 协议支持的密码套件：

  - TLS_AES_256_GCM_SHA384
  - TLS_CHACHA20_POLY1305_SHA256
  - TLS_AES_128_GCM_SHA256
  - TLS_AES_128_CCM_SHA256

- 5 — 仅启用 TLS 1.2 和 TLS 1.3 协议。对于 TLS 1.2 和 TLS 1.3 协议，下面列出的特定密码套件受支持。

  TLS 1.2 协议支持的密码套件：

  - ECDHE-RSA-AES256-GCM-SHA384
  - ECDHE-RSA-AES256-SHA384
  - ECDHE-RSA-CHACHA20-POLY1305
  - ECDHE-RSA-AES128-GCM-SHA256
  - ECDHE-RSA-AES128-SHA256

  TLS 1.3 协议支持的密码套件：

  - TLS_AES_256_GCM_SHA384
  - TLS_CHACHA20_POLY1305_SHA256
  - TLS_AES_128_GCM_SHA256
  - TLS_AES_128_CCM_SHA256

我们不建议使用 0、1、2 或 3 作为 SrvUseStrictSslSettings 标志的参数值。这些参数值对应于不安全的 TLS 协议版本（TLS 1.0 和 TLS 1.1）和不安全的密码套件，仅用于向后兼容早期 Kaspersky Security Center 版本。

3. 重新启动以下 Kaspersky Security Center Linux 服务：
   - 管理服务器
   - Web 服务器
   - 激活代理

这样就启用了使用 TLS 协议的流量加密。

您可以使用 KLTR_TLS12_ENABLED 和 KLTR_TLS13_ENABLED 标志分别启用对 TLS 1.2 和 TLS 1.3 协议的支持。这些标志默认启用。

要启用或禁用对 TLS 1.2 和 TLS 1.3 协议的支持：

1. 运行 klscflag 实用程序。

   运行命令行，然后将当前目录更改为包含 klscflag 实用程序的目录。klscflag 实用程序位于安装管理服务器的目录中。默认安装路径为/opt/kaspersky/ksc64/sbin。

2. 在根账户下的命令行处执行以下命令之一：
   - 使用此命令启用或禁用对 TLS 1.2 协议的支持：

     ```
     klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS12_ENABLED -v <value> -t d
     ```

   - 使用此命令启用或禁用对 TLS 1.3 协议的支持：

     ```
     klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS13_ENABLED -v <value> -t d
     ```

   指定标志的<value>参数：
   - `1` —启用对 TLS 协议的支持。
   - `0` — 禁用对 TLS 协议的支持。

发现网络设备

该部分描述网络设备的搜索和发现。

Kaspersky Security Center Linux 允许您按照指定规则查找设备。您可以保存搜索结果到文本文件。

搜索和发现功能允许您查找以下设备：

- Kaspersky Security Center 管理服务器及其从属管理服务器的管理组中的受管理设备。
- 由 Kaspersky Security Center 管理服务器及其从属管理服务器管理的未分配设备。

情景：发现网络设备

您必须在安装安全应用程序之前执行设备发现。当所有网络设备被发现时，您可以接收它们的信息并通过策略管理。常规网络轮询用于发现是否有新设备以及先前发现的设备是否仍在网络中。

网络设备发现分步骤进行：

1. **初始设备发现**

   完成快速启动向导后，手动执行设备发现。

2. **配置未来轮询**

   确保 IP 范围轮询已启用且轮询计划满足您组织的需要。当配置轮询计划时，使用建议的网络轮询频率。

   如果您的网络包括 IPv6 设备，还可以启用 Zeroconf 轮询。

   如果域中包含联网设备，建议使用域控制器轮询。

3. **设置规则以添加发现的设备到管理组（可选）**

   如果新设备出现在您的网络中，则它们将在定期轮询期间被发现，并自动包含在“**未分配的设备**”组中。如果需要，可以设置自动将这些设备移至“**受管理设备**”组的规则。您也可以建立保留规则。

   如果您跳过该规则设置步骤，所有新发现的设备都将转到“**未分配的设备**”组并保留在那里。如果需要，可以手动将这些设备移动到“**受管理设备**”组。如果您手动将这些设备移动到“**受管理设备**”组，您可以分析每台设备的信息并决定您是否要将它移动到管理组以及移动到哪个组。

结果

完成方案可以导致如下：

- Kaspersky Security Center Linux 管理服务器发现网络中的设备并提供您它们的信息。
- 未来轮询被设置并根据指定的计划工作。

新发现的设备按照配置的规则排列。（或者，如果没有配置规则，设备将保留在**未分配的设备**组中）。

IP 范围轮询

Kaspersky Security Center Linux 尝试使用标准 DNS 请求为指定范围的每个 IPv4 地址执行反向名称解析到 DNS 名称。如果该操作成功，服务器发送 `ICMP ECHO REQUEST`（和 ping 命令相同）到所接收名称。如果设备响应，其信息被添加到 Kaspersky Security Center Linux 数据库。反向名称解析对于排除具有 IP 地址但不是计算机的网络设备是必要的，例如网络打印机或路由器。

该轮询方法依赖正确配置的本地 DNS 服务。它必须具有反向查询域。如果该域未被配置，IP 子网轮询将没有结果。

开始，Kaspersky Security Center Linux 从其所在设备的网络设置获取 IP 轮询范围。如果设备地址是 192.168.0.1 且子网掩码是 255.255.255.0，Kaspersky Security Center Linux 自动包含网络 192.168.0.0/24 到轮询地址。Kaspersky Security Center Linux 从 192.168.0.1 到 192.168.0.254 之间轮询所有地址。

如果仅启用 IP 范围轮询，Kaspersky Security Center Linux 只会发现具有 IPv4 地址的设备。如果您的网络包括 IPv6 设备，请开启设备的 Zeroconf 轮询。

浏览和修改 IP 范围轮询设置

要浏览和修改 IP 范围轮询设置：

1. 在主菜单中，转到“**发现和部署**” → “**发现**” → “**IP 范围**”。
2. 单击“**属性**”按钮。

   IP 轮询属性窗口将开启。
3. 通过使用“**允许轮询**”切换按钮启用或禁用 IP 轮询。
4. 配置轮询计划。默认下，IP 轮询每 420 分钟（七小时）运行一次。

   当指定轮询间隔时，确保该设置不超过 IP 地址生命周期参数值。如果 IP 地址在 IP 地址生命周期中不被轮询所验证，该 IP 地址被从轮询结果中自动删除。默认下，轮询结果的生命期是 24 小时，因为动态 IP 地址（使用 Dynamic Host Configuration Protocol (DHCP)）分配每 24 小时更改一次。

   轮询计划选项：

   - **每 N 天**

     轮询定期运行，按照指定天数间隔，从指定的日期和时间开始。

     默认下，轮询每天运行一次，从当前系统日期和时间开始。
   - **每 N 分钟**

     轮询定期运行，按照指定分钟间隔，从指定的时间开始。
   - **按星期中的天数**

     轮询定期运行，在指定星期的指定时间。
   - **每个月在所选周的指定天**

     轮询定期运行，在指定月日的指定时间。
   - **运行错过的任务**

如果在计划轮询期间管理服务器被切换掉或不可用，管理服务器可以在切换回来后立即启动轮询，或者等待下次计划轮询。

如果启用该选项，管理服务器在它切换回来后立即启动轮询。

如果禁用该选项，管理服务器等待下一次计划轮询。

默认情况下已禁用该选项。

5. 单击“**保存**”按钮。

属性包保存并应用到所有 IP 范围。

手动运行轮询

要立即运行轮询，

单击**开始轮询**。

添加和修改 IP 范围

开始，Kaspersky Security Center Linux 从其所在设备的网络设置获取 IP 轮询范围。如果设备地址是 192.168.0.1 且子网掩码是 255.255.255.0，Kaspersky Security Center Linux 自动包含网络 192.168.0.0/24 到轮询地址。Kaspersky Security Center Linux 从 192.168.0.1 到 192.168.0.254 之间轮询所有地址。您可以修改自动定义的 IP 范围或添加自定义 IP 范围。

您只能创建 IPv4 地址范围。如果启用 Zeroconf 轮询，Kaspersky Security Center Linux 将轮询整个网络。

要添加新 IP 范围：

1. 在主菜单中，转到“**发现和部署**” → “**发现**” → “**IP 范围**”。
2. 要添加新 IP 范围，请单击“**添加**”按钮。
3. 在打开的窗口，指定以下设置：

- **IP 范围名称**

  IP 范围名称。您可能想指定 IP 范围本身作为名称，例如，"192.168.0.0/24"。

- **IP 间隔或子网地址和掩码**

  通过指定开始和结束地址或子网地址和子网掩码设置 IP 范围。您也可以通过点击“**浏览**”按钮选择现有 IP 范围之一。

- **IP 地址生命周期(小时)**

  当指定该参数时，确保它超过轮询计划中设置的轮询间隔。如果 IP 地址在 IP 地址生命周期中不被轮询所验证，该 IP 地址被从轮询结果中自动删除。默认下，轮询结果的生命期是 24 小时，因为动态 IP 地址（使用 Dynamic Host Configuration Protocol (DHCP)）分配每 24 小时更改一次。

4. 如果要轮询已添加的子网或区间，则选择“**启用 IP 范围轮询**”。否则，您添加的子网或间隔将不被轮询。

5. 单击“**保存**”按钮。

新 IP 范围被添加到 IP 范围列表。

您可以使用“**开始轮询**”按钮分别对每个 IP 范围运行轮询。默认下，轮询结果的寿命是 24 小时，且等于 IP 地址生命周期设置。

要添加子网到现有 IP 范围：

1. 在主菜单中，转到“**发现和部署**” → “**发现**” → “**IP 范围**”。

2. 点击您要添加到子网的 IP 范围名称。

3. 在打开的窗口中，单击“**添加**”按钮。

4. 通过使用地址或者掩码指定子网，或者通过使用 IP 范围中的第一个和最后一个 IP 地址。或者，单击“**浏览**”按钮来添加一个现有子网。

5. 单击“**保存**”按钮。

新子网被添加到 IP 范围。

6. 单击“**保存**”按钮。

IP 范围的新设置被保存。

您可以添加无限多的子网。命名 IP 范围不被允许重叠，IP 范围中的非命名子网没有此限制。您可以对每个 IP 范围独立启用和禁用轮询。

Zeroconf 轮询

只有基于 Linux 的分发点支持此轮询类型。

Kaspersky Security Center Linux 可以轮询具有 IPv6 地址的设备的网络。在这种情况下，不指定 IP 范围，并且 Kaspersky Security Center Linux 使用零配置网络（也称为 *Zeroconf*）轮询整个网络。要开始使用 Zeroconf，您必须在轮询网络的 Linux 设备（管理服务器或分发点）上安装 avahi-browse 实用程序。

要启用 Zeroconf 轮询：

1. 在主菜单中，转到“**发现和部署**” → “**发现**” → “**IP 范围**”。

2. 单击“**属性**”按钮。

3. 在打开的窗口中，开启“**使用 Zeroconf 轮询 IPv6 网络**”切换按钮。

之后，Kaspersky Security Center Linux 将开始轮询您的网络。在这种情况下，指定的 IP 范围将被忽略。

域控制器轮询

Kaspersky Security Center Linux 支持轮询 Microsoft Active Directory 域控制器和 Samba 域控制器。对于 Samba 域控制器， Samba 4 用作 Active Directory 域控制器。

当您轮询域控制器时，管理服务器或分发点会检索有关域中包含的设备的域结构、用户账户、安全组和 DNS 名称的信息。

如果所有联网设备都是域的成员，我们建议使用域控制器轮询。如果某些联网设备未包含在域中，则域控制器轮询无法发现这些设备。

先决条件

在轮询域控制器之前，请确保启用以下协议：

- 简单身份验证和安全层 (SASL)
- 轻量级目录访问协议 (LDAP)

确保域控制器设备上的以下端口可用：

- 389 用于 SASL
- 636 用于 TLS

使用管理服务器进行域控制器轮询

要使用管理服务器轮询域控制器：

1. 在主菜单中，转到**发现和部署** → **发现** → **域控制器**。
2. 单击**轮询设置**。
   域控制器轮询设置窗口将打开。
3. 选择**启用域控制器轮询**选项。
4. 在**轮询指定域**中，单击**添加**，然后指定域控制器的地址和用户凭据。
5. 如有必要，请在**域控制器轮询设置**窗口中指定轮询计划。默认间隔是一小时。下次轮询接收的数据会完全替换旧数据。
   有以下轮询计划选项可用：
   - **每 N 天**
     轮询定期运行，按照指定天数间隔，从指定的日期和时间开始。
     默认下，轮询每天运行一次，从当前系统日期和时间开始。
   - **每 N 分钟**
     轮询定期运行，按照指定分钟间隔，从指定的时间开始。
   - **按星期中的天数**

轮询定期运行，在指定星期的指定时间。

- 每个月在所选周的指定天

  轮询定期运行，在指定月日的指定时间。

- 运行错过的任务

  如果在计划轮询期间管理服务器被切换掉或不可用，管理服务器可以在切换回来后立即启动轮询，或者等待下次计划轮询。

  如果启用该选项，管理服务器在它切换回来后立即启动轮询。

  如果禁用该选项，管理服务器等待下一次计划轮询。

  默认情况下已禁用该选项。

如果您更改域安全组中的用户账户，这些更改将在您轮询域控制器一小时后显示在 Kaspersky Security Center Linux 中。

6. 单击**保存**以应用更改。
7. 如果您要立即执行轮询，请单击“**开始轮询**”按钮。

使用分发点进行域控制器轮询

您还可以使用分发点轮询域控制器。基于 Windows 或 Linux 的受管理设备可以充当分发点。

对于 Linux 分发点，支持对 Microsoft Active Directory 域控制器和 Samba 域控制器进行轮询。
对于 Windows 分发点，仅支持 Microsoft Active Directory 域控制器的轮询。
使用 Mac 分发点进行轮询不受支持。

要使用分发点配置域控制器轮询：

1. 打开分发点属性。
2. 选择**域控制器轮询**部分。
3. 选择**启用域控制器轮询**选项。
4. 选择要轮询的域控制器。

   如果您使用 Linux 分发点，请在**轮询指定域**部分中单击**添加**，然后指定域控制器的地址和用户凭据。

   如果您使用 Windows 分发点，则可以选择以下选项之一：

   - **轮询当前域**
   - **轮询整个域森林**
   - **轮询指定域**

5. 如果需要，单击**设置轮询计划**按钮以指定轮询计划选项。

   轮询仅根据指定的时间表开始。无法手动启动轮询。

轮询完成后，域结构将显示在**域控制器**部分。

如果设置并启用了设备移动规则，则新发现的设备将自动包含在“**受管理设备**”组中。如果未启用移动规则，新发现的设备将自动包含在“**未分配的设备**”组。

发现的用户账户可用于Kaspersky Security Center Web Console 中的域身份验证。

身份验证和连接到域控制器

与域控制器初始连接时，管理服务器会识别连接协议。该协议用于将来与域控制器的所有连接。

与域控制器的初始连接过程如下：

1. 管理服务器尝试通过 TLS 连接到域控制器。

   默认情况下不需要证书验证。将 KLNAG_LDAP_TLS_REQCERT 标志设置为 1 以强制执行证书验证。

   默认情况下，使用与操作系统相关的证书颁发机构 (CA) 路径来访问证书链。使用 KLNAG_LDAP_SSL_CACERT 标志指定自定义路径。

2. 如果 TLS 连接失败，管理服务器将尝试通过 SASL (DIGEST-MD5) 连接到域控制器。

3. 如果 SASL (DIGEST-MD5) 连接失败，管理服务器将使用通过非加密 TCP 连接的简单身份验证来连接到域控制器。

您可以使用 klscflag 实用程序来配置标志。

运行命令行，然后将当前目录更改为包含 klscflag 实用程序的目录。klscflag 实用程序位于安装管理服务器的目录中。默认安装路径为/opt/kaspersky/ksc64/sbin。
例如，以下命令可强制执行证书验证：

```
klscflag -fset -pv klserver -n KLNAG_LDAP_TLS_REQCERT -t d -v 1
```

配置 Samba 域控制器

Kaspersky Security Center Linux 支持仅在 Samba 4 上运行的 Linux 域控制器。

Samba 域控制器支持与 Microsoft Active Directory 域控制器相同的架构扩展。您可以使用 Samba 4 架构扩展启用 Samba 域控制器与 Microsoft Active Directory 域控制器完全兼容。这是一个可选操作。

> 我们建议启用 Samba 域控制器与 Microsoft Active Directory 域控制器完全兼容。这将确保 Kaspersky Security Center Linux 和 Samba 域控制器之间的正确交互。

要启用 Samba 域控制器与 Microsoft Active Directory 域控制器完全兼容：

1. 执行以下命令以使用 RFC2307 架构扩展：

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. 在 Samba 域控制器中启用架构更新。为此，请将以下行添加到 /etc/samba/smb.conf 文件中：

```
dsdb:schema update allowed = true
```

> 如果架构更新完成时出现错误，则需要对充当架构主机的域控制器执行完整还原。

如果要正确轮询 Samba 域控制器，您必须在 /etc/samba/smb.conf 文件中指定`netbios name`和`workgroup`参数。

在客户端设备上使用 VDI 动态模式

虚拟基础架构可以使用临时虚拟机部署企业网络。Kaspersky Security Center Linux 检测到临时虚拟机和他们在管理服务器数据库的附加信息。用户使用完临时虚拟机后，这些虚拟机将从虚拟架构中移除。然而，以后虚拟机的记录可以保存在管理服务器数据库中。此外，不存在的虚拟机可能会显示在 Kaspersky Security Center Web Console 中。

为了防止不存在的虚拟机被保存，Kaspersky Security Center Linux 支持动态模式的虚拟桌面基础架构 (VDI)。管理员可以在被安装到临时虚拟机的网络代理安装包的属性中启用支持动态 VDI。

当临时虚拟机被禁用，网络代理通知管理服务器该虚拟机已被禁用。如果虚拟机被成功禁用，它将从连接到管理服务器的设备列表中被移除。如果虚拟机被禁用错误，网络代理没有发送禁用虚拟机的通知到管理服务器，使用备份方案。使用这个方案，和管理服务器尝试同步三次未成功后，虚拟机从连接管理服务器的设备列表移除。

在网络代理安装包属性中启用 VDI 动态模式

要启用 VDI 动态模式，请执行以下操作：

1. 在主菜单中，转到 “**发现和部署**” → “**部署和分配**” → “**安装包**”。
2. 在网络代理安装包的上下文菜单中，选择“**属性**”。
   属性窗口将打开。
3. 在**属性**窗口中，选择**高级**区域。
4. 在“**高级**”区域中，选择“**启用 VDI 动态模式**”选项。

要安装网络代理的设备成为 VDI 的一部分。

将组成 VDI 的设备移至管理组

要将组成 VDI 的设备移至管理组，请执行以下操作：

1. 转到 **资产(设备)** → **移动规则**。
2. 单击**添加**。
3. 在**规则条件**选项卡上，选择**虚拟机**选项卡。
4. 将**这是一台虚拟机**规则设置为**是**，将**虚拟桌面基础架构的一部分**设置为**是** 。

5. 单击“保存”。

部署最佳实践

Kaspersky Security Center Linux 是一个分发的应用程序。Kaspersky Security Center Linux 包含以下应用程序：

- 管理服务器 — 核心组件，设计用于管理组织设备和在 DBMS 中存储数据。
- Kaspersky Security Center Web Console 是管理员的基本工具。您可以在安装了管理服务器的同一台设备上或在其他设备上安装 Kaspersky Security Center Web Console。
- 网络代理 — 设计用于管理安装在设备上的安全应用程序，同时获取设备信息并传输该信息到管理服务器。网络代理安装在组织设备上。

Kaspersky Security Center Linux 在组织网络上的部署运行如下：

- 管理服务器的安装
- 在管理员设备上安装 Kaspersky Security Center Web Console
- 网络代理和企业设备上安全应用程序的安装

强化指南

Kaspersky Security Center Linux 设计用于在组织网络中集中执行基本的管理和维护任务。该应用程序使管理员可以访问有关组织网络安全级别的详细信息。Kaspersky Security Center Linux 允许您配置使用卡巴斯基应用程序构建的所有保护组件。

Kaspersky Security Center Linux 管理服务器拥有对客户端设备保护管理的完全访问权限，是组织安全系统中最重要的组件。因此，管理服务器需要增加保护方法。

强化指南描述了配置 Kaspersky Security Center Linux 及其组件的建议和功能，旨在降低其危害的风险。

强化指南包含以下信息：

- 选择管理服务器架构
- 配置与管理服务器的安全连接
- 配置访问管理服务器的账户
- 管理服务器保护的管理
- 管理客户端设备保护
- 配置受管理应用程序的保护
- 管理服务器维护
- 将信息传输到第三方应用程序

管理服务器部署

管理服务器架构

一般来说，集中式管理架构的选择取决于受保护设备的位置、相邻网络的访问、数据库更新的交付方案等。

在架构开发的初始阶段，我们建议熟悉 Kaspersky Security Center Linux 组件以及他们之间的互动，以及数据流量和端口使用的模式。

基于此信息，您可以形成一个架构指定：

- 管理服务器位置和网络连接
- 管理员工作区的组织以及连接到管理服务器的方法
- 网络代理及防护软件的部署方法
- 使用分发点
- 使用虚拟管理服务器
- 使用管理服务器层级
- 反病毒数据库更新方案
- 其他信息流

选择用于安装管理服务器的设备

我们建议将管理服务器安装在组织基础架构的专用服务器上。如果服务器上没有安装其他第三方软件，您可以根据 Kaspersky Security Center Linux 的要求配置安全设置而不依赖于第三方软件的要求。

您可以在物理服务器或虚拟服务器上部署管理服务器。请确保所选设备满足硬件和软件要求。

限制将管理服务器安装在域控制器、终端服务器或用户设备上

我们强烈不建议将管理服务器安装在域控制器、终端服务器或用户设备上。

我们建议您提供网络关键节点的功能分离。这种方法允许您在节点出现故障或受到损害时保持不同系统的可操作性。同时，您可以为每个节点创建不同的安全策略。

用于安装和运行管理服务器的账户

在部署管理服务器期间，需要创建两个非特权账户。管理服务器中包含的服务将在这些非特权账户下运行。为账户授予权限时，请遵循最低权限原则。避免在“kladmins”组中包含不必要的账户。

您还需要创建一个内部 DBMS 账户。管理服务器使用此内部 DBMS 账户来访问选定的 DBMS。

所需账户及其权利集取决于所选的 DBMS 类型和管理服务器数据库创建方法。

连接安全

TLS 的使用

我们建议禁止与管理服务器的不安全连接。例如，您可以在管理服务器设置中禁止使用 HTTP 的连接。

请注意，默认情况下，管理服务器的几个 HTTP 端口是关闭的。其余端口用于管理服务器 Web 服务器 (8060)。此端口可受管理服务器设备的防火墙设置限制。

严格的 TLS 设置

建议使用 1.2 及以后版本的 TLS 协议，限制或禁止不安全的加密算法。

您可以配置管理服务器使用的加密协议 (TLS)。请注意，在发布管理服务器版本时，默认配置加密协议设置以确保安全的数据传输。

限制访问管理服务器数据库

我们建议限制访问管理服务器数据库。例如，只允许从管理服务器设备进行访问。这可降低管理服务器数据库因已知漏洞而受到损害的可能性。

您可以根据使用的数据库的操作说明配置参数，也可以在防火墙上提供关闭的端口。

配置允许连接到管理服务器的 IP 地址允许列表

默认情况下，用户可以从安装了 Kaspersky Security Center Web Console 的任何设备登录Kaspersky Security Center Linux。您可以配置管理服务器，使用户只能从具有允许 IP 地址的设备进行连接。

账户和身份验证

通过管理服务器使用两步验证

Kaspersky Security Center Linux 为 Kaspersky Security Center Web Console 的用户提供两步验证，基于 RFC 6238 标准（TOTP：基于时间的一次性密码算法）。

为您自己的账户启用两步验证后，每次登录 Kaspersky Security Center Web Console 时，都需要输入用户名、密码和附加的一次性安全代码。要接收一次性安全代码，您必须在计算机或移动设备上安装认证应用程序。

有支持 RFC 6238 标准的软件和硬件验证器（令牌）。例如，软件验证器包括 Google Authenticator、Microsoft Authenticator、FreeOTP。

我们强烈建议不要在与管理服务器建立连接的同一台设备上安装验证器应用程序。您可以在移动设备上安装验证器应用程序。

对操作系统使用双重身份验证

我们建议使用令牌、智能卡或其他方法（如果可能）在管理服务器设备上使用多重身份验证 (MFA) 进行身份验证。

禁止保存管理员密码

如果您使用 Kaspersky Security Center Web Console，我们不建议在用户设备上安装的浏览器中保存管理员密码。

内部用户账户的身份验证

默认情况下，管理服务器内部用户账户的密码必须遵守以下规则：

- 密码必须是8 到 16 位字符长度。
- 密码必须包含以下组中三组的字符：
  - 大写字母 (A-Z)
  - 小写字母 (a-z)
  - 数字 (0-9)
  - 特殊字符 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- 密码不可以包含任何空格、Unicode 字符以及“.”和“@”按先后顺序的组合。

默认下，允许的最大密码输入尝试次数是 10。您可以更改允许的密码输入尝试次数。

Kaspersky Security Center Linux 用户可以输入无效密码的次数有限。达到限制后，用户账户被锁定一小时。

管理服务器的专用管理组

我们建议为管理服务器创建一个专门的管理组。授予该组特殊访问权限并为其创建特殊安全策略。

为避免故意降低管理服务器的安全级别，我们建议限制可以管理专用管理组的账户列表。

限制主管理员角色的分配

由 kladduser 实用程序创建的用户在管理服务器的访问控制列表 (ACL) 中被分配为主管理员角色。我们建议避免将主管理员角色分配给大量用户。

配置对应用程序功能的访问权限

我们建议为每个用户或用户组灵活配置对 Kaspersky Security Center Linux 功能的访问权限。

基于角色的访问控制允许通过使用一组预定义的权限创建标准用户角色并根据用户的职责范围将这些角色分配给用户。

基于角色的访问控制模型的主要优点：

- 易于管理
- 角色层级

- 最小特权方法
- 职责分离

您可以根据职位为某些员工分配内置角色，或创建全新的角色。

在配置角色时，注意与改变管理服务器设备保护状态和远程安装第三方软件相关的权限：

- 对管理组进行管理。
- 管理服务器操作。
- 远程安装。
- 更改用于存储事件和发送通知的参数。
  此权限允许您设置在事件发生时在管理服务器设备上运行脚本或可执行模块的通知。

使用单独的账户进行远程安装应用程序

除了访问权限的基本区分外，我们建议限制所有账户（主管理员或其他专用账户除外）进行应用程序远程安装。

我们建议使用单独的账户进行远程安装应用程序。您可以分配角色或者权限给单独账户。

定期审核所有用户

我们建议对管理服务器设备上的所有用户进行定期审核。这使您能够应对与可能损害设备相关的某些类型的安全威胁。

管理服务器保护的管理

选择管理服务器保护软件

根据管理服务器部署的类型和一般保护策略，选择应用程序来保护管理服务器设备。

如果您在专用设备上部署管理服务器，我们建议选择 Kaspersky Endpoint Security 应用程序来保护管理服务器设备。这可让您应用所有可用技术来保护管理服务器设备，包括行为分析模块。

如果管理服务器安装在基础设施中存在的设备上并且之前曾用于其他任务，我们建议考虑以下保护软件：

- Kaspersky Industrial CyberSecurity for Nodes。我们建议在包含在工业网络中的设备上安装此应用程序。Kaspersky Industrial CyberSecurity for Nodes 是一个应用程序，具有与各种工业软件制造商的兼容性证书。
- 推荐的安全产品。如果管理服务器安装在装有其他软件的设备上，我们建议考虑该软件供应商对安全产品兼容性的建议（可能已经有选择安全解决方案的建议，您可能需要配置信任区域）。

为保护应用程序创建单独的安全策略

我们建议为保护管理服务器设备的应用程序创建单独的安全策略。此策略必须不同于客户端设备的安全策略。这可让您为管理服务器指定最合适的安全设置，而不会影响其他设备的保护级别。

我们建议将设备分组，然后将管理服务器设备放入一个单独的组中，您可以为其创建特殊的安全策略。

保护模块

如果与管理服务器安装在同一设备上的第三方软件的供应商没有特别建议，我们建议激活并配置所有可用的保护模块（在检查这些保护模块的运行一段时间后）。

配置管理服务器设备的防火墙

在管理服务器设备上，我们建议配置防火墙以限制设备数量，管理员可以从这些设备通过 Kaspersky Security Center Web Console 连接到管理服务器。

默认情况下，管理服务器使用端口13299 接收来自 Kaspersky Security Center Web Console 的连接。我们建议限制可以使用该端口管理管理服务器的设备数量。

管理客户端设备保护

限制将授权许可密钥添加到安装包

安装包存储在管理服务器共享文件夹的 Packages 子文件夹中。如果将授权许可密钥添加到安装包，则所有对此文件夹具有读取权限的用户都可以访问该授权许可密钥（直接或通过管理服务器中嵌入的Web 服务器）。

为避免泄露授权许可密钥，我们不建议将授权许可密钥添加到安装包中。

我们推荐使用将授权许可密钥自动分发到受管理设备，通过受管理应用程序的“添加授权许可密钥”任务进行部署，并手动将激活码或密钥文件添加到设备。

在管理组之间移动设备的自动规则

我们建议限制使用自动规则在管理组之间移动设备。

如果您使用自动规则移动设备，这可能会导致策略的传播，这些策略为移动的设备提供比重新定位前的设备更多的权限。

此外，将客户端设备移动到另一个管理组可能会导致策略设置的传播。这些策略设置可能不适合分发给访客和不受信任的设备。

此建议不适用于将设备一次性初始分配给管理组。

分发点和连接网关的安全要求

安装了网络代理的设备可以充当分发点并执行以下功能：

- 将从管理服务器收到的更新和安装包分发到组内的客户端设备。
- 在客户端设备上执行第三方软件和卡巴斯基应用程序的远程安装。

- 轮询网络以检测新设备并更新现有设备的信息。分发点可以使用与管理服务器相同的设备检测方法。

在组织的网络上放置分发点用于：

- 降低管理服务器负载
- 流量优化
- 让管理服务器能够访问网络中难以到达的设备

考虑到可用功能，我们建议保护充当分发点的设备免受任何类型的未经授权的访问（包括物理访问）。

限制自动分配分发点

为了简化管理并保持网络的可操作性，我们建议使用分发点的自动分配。但是，对于工业网络和小型网络，我们建议您避免自动分配分发点，因为（例如）用于推送远程安装任务的账户的私人信息可以通过操作系统转移到分发点。

对于工业网络和小型网络，您可以手动分配设备作为分发点。

您还可以查看分发点活动报告。

配置受管理应用程序的保护

受管理应用程序策略

我们建议为每种类型使用的应用程序和 Kaspersky Security Center Linux 组件（网络代理、Kaspersky Endpoint Security for Windows、Kaspersky Endpoint Security for Linux、Kaspersky Endpoint Agent 等）创建一个策略。此组策略必须应用于所有受管理设备（根管理组）或根据配置的移动规则新的受管理设备将自动移动到其中的单独组。

指定用于禁用保护和卸载应用程序的密码

我们强烈建议启用密码保护，以防止入侵者禁用或卸载卡巴斯基安全应用程序。在支持密码保护的平台上，您可以为 Kaspersky Endpoint Security、网络代理和其他卡巴斯基应用程序设置密码。启用密码保护后，我们建议通过关闭"锁"来锁定相应设置。

指定将客户端设备手动连接到管理服务器的密码（klmover 实用程序）

klmover 实用程序允许您手动将客户端设备连接到管理服务器。在客户端设备上安装网络代理时，自动将该实用程序复制到网络代理安装文件夹。

为了防止入侵者将设备移出管理服务器的控制，我们强烈建议为运行 klmover 实用程序启用密码保护。要启用密码保护，请在**网络代理策略设置使用卸载密码**使用卸载密码选项。

klmover 实用程序需要本地管理员权限。对于没有本地管理员权限操作的设备，可以忽略运行 klmover 实用程序的密码保护。

启用**使用卸载密码**还会启用Kaspersky Security Center Web Console 删除工具 (cleaner.exe) 的密码保护。

配置卡巴斯基安全网络

在受管理应用程序的所有策略和管理服务器属性中，我们建议启用卡巴斯基安全网络 (KSN) 的使用并接受 KSN 声明。更新或升级管理服务器时，您可以接受更新后的 KSN 声明。在某些情况下，当法律或其他法规禁止使用云服务时，您可以禁用 KSN。

定期扫描受管理设备

对于所有设备组，我们建议创建一个定期运行完整设备扫描的任务。

发现新设备

我们建议正确配置设备发现设置：设置与域控制器的集成，并指定用于发现新设备的 IP 地址范围。

出于安全目的，您可以使用包含所有新设备的默认管理组和影响该组的默认策略。

管理服务器维护

备份管理服务器数据

数据备份允许您在不丢失数据的情况下恢复管理服务器数据。

默认情况下，数据备份任务在管理服务器安装后自动创建并定期执行，从而将备份保存在适当的目录中。
数据备份任务的设置可以更改如下：

- 备份频率增加
- 指定保存副本的特殊目录
- 更改备份副本的密码

如果您将备份副本存储在不同于默认目录的特殊目录中，我们建议限制该目录的访问控制列表 (ACL)。管理服务器账户和管理服务器数据库的账户必须具有此目录的写入权限。

管理服务器维护

管理服务器维护允许您降低数据库容量，提高应用程序的运行和操作可靠性。我们建议您至少每周维护一次管理服务器。

管理服务器通过专用任务进行维护。在维护管理服务器时，应用程序执行以下操作：

- 检查数据库错误
- 重组数据库索引
- 更新数据库统计信息
- 收缩数据库（如果必要）

安装操作系统更新和第三方软件更新

我们强烈建议您定期为管理服务器设备上的操作系统和第三方软件安装软件更新。

客户端设备不需要持续连接到管理服务器，因此在安装更新后重新启动管理服务器设备是安全的。管理服务器停机期间在客户端设备上注册的所有事件都会在连接恢复后发送给它。

事件传输到第三方系统

监控和报告

为了及时响应安全问题，我们建议配置监控和报告功能。

导出事件到 SIEM 系统

为了在重大损害发生之前快速检测安全问题，我们建议在 SIEM 系统中使用事件导出。

审计事件的电子邮件通知

Kaspersky Security Center Linux 允许您接收受管理设备上安装的管理服务器和 Kaspersky 应用程序在操作期间发生的事件信息。为了及时响应紧急情况，我们建议配置管理服务器以发送有关其发布的审计事件、关键事件、故障事件和警告的通知。

由于这些事件是系统内事件，因此可以预期它们的数量很少，这非常适用于邮件。

部署准备

该部分描述了在部署 Kaspersky Security Center Linux 之前必须采取的操作。

计划 Kaspersky Security Center Linux 部署

该部分介绍了根据以下标准在组织网络中部署 Kaspersky Security Center Linux 组件的最方便选项：

- 设备总数
- 在组织或地理上拆分的单元（本地办公室、分支）
- 由狭窄通道连接的网络拆分网络
- 需要到管理服务器的互联网访问

部署保护系统的常规方案

本部分描述了使用 Kaspersky Security Center 的企业网络保护系统的标准部署方案。

系统必须防止任何非授权的访问。我们建议您为您的操作系统安装所有可用更新，然后再安装应用程序到您的设备并物理保护管理服务器和分发点。

您可以使用 Kaspersky Security Center 部署保护系统到企业网络，通过以下部署方案：

- 通过 Kaspersky Security Center Web Console 部署保护系统。

  Kaspersky 应用程序自动安装在客户端设备上，并通过 Kaspersky Security Center 自动连接到管理服务器。

- 使用在 Kaspersky Security Center 中生成的独立安装包手动部署保护系统。

  手动在客户端设备和管理员工作站中安装 Kaspersky 应用程序；在安装网络代理时指定客户端设备与管理服务器的连接设置。

  该部署方法建议在远程安装不可用时使用。

Kaspersky Security Center 不支持使用 Microsoft Active Directory® 组策略进行部署。

关于在组织网络中规划 Kaspersky Security Center Linux 的部署

一台管理服务器最多可支持 20,000 台设备（使用 MariaDB 作为 DBMS）。如果组织网络中的设备总数超过 20,000，必须在网络中部署多个管理服务器，并合并到一个方便集中管理的层级。

如果组织包含大规模有各自管理员的远程本地办公室（分支），则适合在这些办公室部署管理服务器。否则，此类办公室必须被视为通过低吞吐量通道连接的独立网络，请参见“标准配置：由自己管理员运行的多个大规模办公室”部分。

当使用由狭窄通道连接的拆分网络时，可以分配一个或几个网络代理作为分发点来节省流量（参见分发点数量计算表格）。这种情况下，一个拆分网络中的所有设备都从此本地更新中心上获取更新。实际分发点可以从管理服务器（默认情景）和互联网上的卡巴斯基服务器下载更新（参见“标准配置：多个小型远程办公室”）。

“Kaspersky Security Center Linux 标准配置”部分提供了 Kaspersky Security Center Linux 标准配置的详细描述。当计划部署时，根据组织架构选择最合适的标准配置。

在部署计划阶段，必须考虑到特别证书 X.509 到管理服务器的分配。X.509 证书到管理服务器的分配可能用在以下情况（部分列表）：

- 通过 SSL 终端代理或使用反向代理检查安全套接层（SSL）
- 在证书字段中指定所需值
- 提供所需的证书加密长度

选择企业保护结构

组织保护结构的选择根据以下因素进行定义：

- 组织的网络拓扑。
- 组织结构。

- 负责网络保护的员工的数量及其责任分配。
- 可用于分配以便保护管理组件的硬件资源。
- 可用于分配以便维护组织网络内部保护组件运行的通信通道的吞吐量。
- 在组织网络中执行关键管理操作的时间限制。关键管理操作，包括分发反病毒数据库和修改客户端设备的策略。

在选择保护结构时，建议您首先评估可用来操作集中式保护系统的网络和硬件资源。

要分析网络和硬件基础架构，建议您遵照以下过程：

1. 定义将部署保护的网络的以下设置：
   - 网段数量。
   - 各个网段之间的通信通道的速度。
   - 每个网段中的受管理设备的数量。
   - 可用于分配以便维护保护运行的每个通信通道的吞吐量。
2. 确定为所有受管理设备执行主要管理操作的最大允许时间。
3. 分析来自步骤 1 和步骤 2 的信息以及来自管理系统负载测试的数据。根据分析，回答以下问题：
   - 是否可以用单个管理服务器服务所有客户端，或者是否需要一个管理服务器层级?
   - 需要哪种管理服务器硬件配置以便用在项目 2 中指定的时间限制内处理所有客户端?
   - 是否需要使用分发点来减少通信通道的负载?

在获取上述问题的答案之后，您可以编辑组织保护所允许的一组结构。

在组织的网络中，您可以使用下列标准保护结构之一：

- 一个管理服务器。将所有客户端设备连接至单个管理服务器。管理服务器充当分发点。
- 一个包含分发点的管理服务器。将所有客户端设备连接至单个管理服务器。某些联网的客户端设备作为分发点运行。
- 管理服务器层级。每个网段都分配了单独的管理服务器，作为管理服务器常规层次结构的一部分。主管理服务器充当分发点。
- 包含分发点的管理服务器层级。每个网段都分配了单独的管理服务器，作为管理服务器常规层次结构的一部分。某些联网的客户端设备作为分发点运行。

Kaspersky Security Center Linux 的标准配置

该部分描述了以下用于组织网络中的 Kaspersky Security Center Linux 组件部署的标准配置：

- 单一办公室

- 几个大规模办公室，被地理拆分并由自己的管理员运行
- 多个小办公室，被地理拆分

标准配置：单一办公室

可以在组织网络中部署一个或多个管理服务器。管理服务器数量可以基于可用硬件或受管理设备总数来选择。

一台管理服务器最多可支持 20,000 台设备（使用 MariaDB 作为 DBMS）。考虑今后增加受管理设备的数量的可能性：最好连接较少设备到单一管理服务器。

管理服务器可以被部署在内部网络或 DMZ 中，具体取决于管理服务器是否需要互联网连接。

如果使用了多个服务器，建议您合并它们到一个层级。使用管理服务器层级时，允许您避免冗余策略和任务、处理整个受管理设备集合，使其如同被单一管理服务器管理一样：例如，搜索设备、创建设备分类和创建报告。

标准配置：由自己管理员运行的几个大规模办公室

如果组织有多个地理位置分散的大规模办公室，则必须考虑在每个办公室部署管理服务器的选项。每个办公室可以部署一台或多台管理服务器，具体取决于可用的客户端设备和硬件的数量。此种情况下，每个办公室可以被视为“标准配置：单一办公室”。为了简化管理，建议将所有管理服务器合并到一个层次结构（可能是多层）中。

如果一些员工带着他们的设备（笔记本电脑）在办公室之间移动，请在网络代理策略中创建网络代理连接配置文件。请注意，网络代理连接配置文件仅支持 Windows 和 macOS 设备。

标准配置：多个小远程办公室

该标准配置适用于总部办公室以及许多可通过互联网与总部办公室联系的远程小型办公室。每个远程办公室可能位于 Network Address Translation (NAT) 之外，例如，两个远程办公室之间无法建立连接，因为它们是隔离的。

总部办公室必须部署一个管理服务器，必须为所有其他办公室分配一个或多个分发点。如果办公室通过互联网连接，最好为分发点创建*将更新下载至分发点存储库*任务，这样它们将从卡巴斯基服务器、本地或网络文件夹直接下载更新，而不是从管理服务器下载。

如果远程办公室的一些设备不能直接访问管理服务器（例如，到管理服务器的访问是通过互联网提供但是一些设备没有互联网连接），分发点必须被切换到连接网关模式。此种情况下，远程办公室设备上的网络代理将被通过网关而不是直接连接到管理服务器，为了后期同步。

作为管理服务器，很可能无法轮询远程办公室网络，最好把该功能转给分发点。

管理服务器将无法发送通知到远程办公室 NAT 以外的受管理设备的端口 15000 UDP。要解决该问题，可以在作为分发点的设备的属性中启用持续连接到管理服务器模式（“**不断开与管理服务器的连接**”复选框）。如果分发点总数不超过 300 则该模式可用。使用推送服务器以确保受管理设备和管理服务器之间存在持续连接。有关详细信息，请参阅以下主题：启用推送服务器。

选择 DBMS

下表列出了有效 DBMS 选项，以及它们的使用建议和限制。

DBMS	建议和限制
MySQL（参见支持的版本）	如果您打算为少于 20,000 台设备运行单个管理服务器，请使用此 DBMS。
MariaDB（参见支持的版本）	如果您打算为少于 20,000 台设备运行单个管理服务器，请使用此 DBMS。
PostgreSQL、Postgres Pro（查看支持的版本）	如果您打算为少于 50,000 台设备运行单个管理服务器，请使用此 DBMS。

对于如何安装所选 DBMS 的信息，请参考其文档。

建议禁用软件清单任务并禁用（在卡巴斯基 Endpoint Security 策略设置中）管理服务器对已启动应用程序的通知。

如果您决定安装 PostgreSQL 或 Postgres Pro DBMS，请确保您为超级用户指定了密码。如果未指定密码，管理服务器可能无法连接到数据库。

如果您安装 MariaDB、PostgreSQL 或 Postgres Pro，请使用建议的设置以确保 DBMS 正常运行。

提供到管理服务器的互联网访问

以下情况需要到管理服务器的互联网访问：

- 定期更新 Kaspersky 数据库、软件模块和应用程序
- 更新第三方软件

  默认情况下，管理服务器不需要互联网连接就可以在受管理设备上安装 Microsoft 软件更新。例如，受管理设备可以直接从 Microsoft 更新服务器下载 Microsoft 软件更新，也可以从组织的网络中部署了 Microsoft Windows Server Update Services (WSUS) 的 Windows Server 下载。在以下情况下，管理服务器必须连接到互联网：

  - 将管理服务器用作 WSUS 服务器时
  - 要安装除 Microsoft 软件以外的第三方软件的更新
- 修复第三方软件漏洞

  管理服务器需要互联网连接才能执行以下任务：

  - 针对 Microsoft 软件漏洞生成推荐的修复程序列表。该列表由 Kaspersky 专家创建并定期更新。
  - 修复除 Microsoft 软件以外的第三方软件的漏洞。
- 管理漫游用户的设备（便携式电脑）
- 在远程办公室管理设备
- 与位于远程办公室的主管理服务器或从属管理服务器交互
- 管理移动设备

该部分描述了通过互联网提供到管理服务器的访问的典型方法。着眼于提供到管理服务器的互联网访问的每种情况都可能需要一个管理服务器专用证书。

互联网访问：本地网络上的管理服务器

如果管理服务器位于组织内部网络，则最好通过端口转发使管理服务器的 TCP 端口 13000 可从外部访问。如果需要移动设备管理，则最好使 TCP 端口 13292 可被访问。

互联网访问：DMZ 中的管理服务器

如果管理服务器位于组织网络的 DMZ 中，它不能访问组织内部网络。因此，以下限制被应用：

- 管理服务器无法检测新设备。
- 管理服务器无法通过在组织内部网络设备上强制安装来运行网络代理初始化部署。
- 这仅应用到网络代理初始化安装上。任何网络代理的后续升级或安全应用程序安装可以被管理服务器运行。

请注意， Kaspersky Security Center Linux 不支持使用 Microsoft Windows 组策略进行部署。

您可以使用位于组织网络上的分发点。要在没有网络代理的设备上运行初始化部署，您首先要在其中一台设备上安装网络代理，然后给它分配分发点状态。结果，在其他设备上的网络代理初始化安装将通过该分发点由管理服务器运行。

要确保将通知成功发送到组织内部网络中受管理设备的端口 15000 UDP，您必须使用分发点覆盖整个网络。在被分配的分发点的属性中，选择**不断开与管理服务器的连接**复选框。因此，管理服务器将建立一个到分发点的持续连接，同时这些分发点能够发送通知到组织内部网络（可以是 IPv4 或 IPv6 网络）中的设备的端口 15000 UDP。

互联网访问：DMZ 中作为连接网关的网络代理

管理服务器可以位于组织的内部网络，在该网络的 DMZ 中，可以有一个将网络代理作为反向连接网关运行的设备（管理服务器建立到网络代理的连接）。此种情况下，以下条件必须被满足以确保互联网访问：

- 网络代理必须安装在该 DMZ 中的设备上。当您安装网络代理时，在安装向导的“**连接网关**”窗口，选择“**使用网络代理作为 DMZ 连接网关**”。
- 必须将安装了连接网关的设备添加为分发点。添加连接网关时，在“**添加分发点**”窗口中选择“**选择**”→“**按地址在 DMZ 中添加连接网关**”选项。
- 要使用互联网连接将外部台式机连接到管理服务器，必须更正网络代理的安装包。在创建的安装包的属性中，选择“**高级**”→“**通过使用连接网关连接到管理服务器**”选项，然后指定新创建的连接网关。

对于 DMZ 中的连接网关，管理服务器创建与管理服务器证书一同签署的证书。如果管理员决定分配自定义证书到管理服务器，它必须在连接网关在 DMZ 中被创建之前完成。

如果一些员工使用可以连接到管理服务器的便携式电脑，最好在网络代理策略中为网络代理创建交换规则。

关于分发点

安装了网络代理的设备可以用作分发点。在此模式下，网络代理可以分发更新，这些更新可以从管理服务器或卡巴斯基服务器检索。在后一种情况下，为分发点配置更新下载。

在组织网络中部署分发点可以带来以下好处：

- 降低管理服务器负载。
- 优化流量。
- 让管理服务器能够访问组织网络中难以到达的设备。NAT 以外分发点的可用性(与管理服务器有关)允许管理服务器运行以下操作：
  - 在 IPv4 或 IPv6 网络上通过 UDP 向设备发送通知
  - 轮询 IPv4 或 IPv6 网络
  - 执行初始部署
  - 用作推送服务器

为每个管理组分配分发点。此种情况下，分发点的范围包括管理组及其所有子组中的所有设备。然而，作为分发点的设备可能不包含在它被分配的管理组。

您可以让分发点作为连接网关工作。此种情况下，分发点范围内的设备将通过网关连接到管理服务器，而不是直接连接到管理服务器。该模式适合用在不允许管理服务器和受管理设备之间建立直接连接的场合中。

计算分发点的数量和配置

网络包含越多的客户端设备，就需要越多的分发点。我们建议您禁用分发点的自动分配。当分发点的自动分配被启用时，如果客户端设备数量很大，管理服务器就分配分发点并定义其配置。

使用单独分配的分发点

如果您计划使用特定设备作为分发点(就是，单独分配的服务器)，您可以不使用分发点的自动分配。此种情况下，确保您要分配为分发点的设备具有足够的剩余磁盘空间卷，不定期关闭，且禁用了睡眠模式。

网络中基于网络设备数量被专门分配的包含单一网段的分发点的数量

网段中的客户端设备的数量	分发点数量
少于 300	0（不分配分发点）
大于 300	可接受：(N/10,000 + 1)，建议：(N/5,000 + 2)，N 是网络设备数量

网络中基于网络设备数量被专门分配的包含多个网段的分发点的数量

每个网段中的客户端设备的数量	分发点数量
少于 10	0（不分配分发点）
10–100	1
大于 100	可接受：(N/10,000 + 1)，建议：(N/5,000 + 2)，N 是网络设备数量

使用标准客户端设备（工作站）作为分发点

如果您计划使用标准客户端设备（就是，工作站）作为分发点，我们建议您按照所示分配分发点（参见下表），以便避免通信渠道和管理服务器过载。

网络中基于网络设备数量作为分发点工作的包含单一网段的工作站的数量

网段中的客户端设备的数量	分发点数量
少于 300	0（不分配分发点）
大于 300	(N/300 + 1)，N 是网络设备数量；至少有三台分发点

网络中基于网络设备数量作为分发点工作的包含多个网段的工作站的数量

每个网段中的客户端设备的数量	分发点数量
少于 10	0（不分配分发点）
10–30	1
31–300	2
大于 300	(N/300 + 1)，N 是网络设备数量；至少有三台分发点

如果分发点被关闭(或由于某些原因不可用)，其范围内的受管理设备可以访问管理服务器以更新。

虚拟管理服务器

基于物理管理服务器，可以创建多个虚拟管理服务器，它们与从属管理服务器相似。相比于基于访问控制列表（ACLs）的任意访问模式，虚拟管理服务器模式功能更强大并且提供更高度隔离。除了具有策略和任务的已分配设备的专用管理组结构外，每个虚拟管理服务器还具有自己的未分配设备组、自己的报告集、选定的设备和事件、安装包、移动规则等。虚拟管理服务器的功能范围既可以被服务提供商 (xSP) 用来最大限度地隔离客户，也可以为具有复杂工作流和众多管理员的大型组织所用。

虚拟管理服务器与从属管理服务器非常相似，但是有以下不同点：

- 虚拟管理服务器缺少多数全局设置和自己的 TCP 端口。
- 虚拟管理服务器没有从属管理服务器。
- 虚拟管理服务器没有其他虚拟管理服务器。
- 物理管理服务器可以查看它所有虚拟管理服务器的设备、组、事件和受管理设备上的对象（隔离区条目、应用程序注册表等等）。
- 虚拟管理服务器仅可以扫描连接了分发点的网络。

用于与外部服务交互的网络设置

Kaspersky Security Center Linux 使用以下网络设置与外部服务交互。

网络设置

网络设置	地址	描述
端口：443	activation-v2.kaspersky.com/activationservice/activationservice.svc	应用程序激活。

协议： HTTPS		
端口： 443 协议： HTTPS	https://s00.upd.kaspersky.com https://s01.upd.kaspersky.com https://s02.upd.kaspersky.com https://s03.upd.kaspersky.com https://s04.upd.kaspersky.com https://s05.upd.kaspersky.com https://s06.upd.kaspersky.com https://s07.upd.kaspersky.com https://s08.upd.kaspersky.com https://s09.upd.kaspersky.com https://s10.upd.kaspersky.com https://s11.upd.kaspersky.com https://s12.upd.kaspersky.com https://s13.upd.kaspersky.com https://s14.upd.kaspersky.com https://s15.upd.kaspersky.com https://s16.upd.kaspersky.com https://s17.upd.kaspersky.com https://s18.upd.kaspersky.com https://s19.upd.kaspersky.com https://cm.k.kaspersky-labs.com	更新卡巴斯基数据库、软件模块和应用程序。
端口： 443 协议： HTTPS	https://downloads.upd.kaspersky.com	• 更新卡巴斯基数据库、软件模块和应用程序。 • 检查卡巴斯基服务器是否可访问。在下载卡巴斯基数据库和软件模块之前，Kaspersky Security Center Linux 会检查卡巴斯基服务器是否可访问。如果无法使用系统 DNS 访问服务器，应用程序将使用公共 DNS 服务器。
端口： 80 协议： HTTP	http://p00.upd.kaspersky.com http://p01.upd.kaspersky.com http://p02.upd.kaspersky.com http://p03.upd.kaspersky.com http://p04.upd.kaspersky.com http://p05.upd.kaspersky.com http://p06.upd.kaspersky.com http://p07.upd.kaspersky.com http://p08.upd.kaspersky.com http://p09.upd.kaspersky.com http://p10.upd.kaspersky.com	更新卡巴斯基数据库、软件模块和应用程序。

	http://p11.upd.kaspersky.com http://p12.upd.kaspersky.com http://p13.upd.kaspersky.com http://p14.upd.kaspersky.com http://p15.upd.kaspersky.com http://p16.upd.kaspersky.com http://p17.upd.kaspersky.com http://p18.upd.kaspersky.com http://p19.upd.kaspersky.com http://downloads0.kaspersky-labs.com http://downloads1.kaspersky-labs.com http://downloads2.kaspersky-labs.com http://downloads3.kaspersky-labs.com http://downloads4.kaspersky-labs.com http://downloads5.kaspersky-labs.com http://downloads6.kaspersky-labs.com http://downloads7.kaspersky-labs.com http://downloads8.kaspersky-labs.com http://downloads9.kaspersky-labs.com http://downloads.kaspersky-labs.com http://cm.k.kaspersky-labs.com	
端口：443 协议：HTTPS	ds.kaspersky.com	使用卡巴斯基安全网络。
端口：443、1443 协议：HTTPS	ksn-a-stat-geo.kaspersky-labs.com ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com	使用卡巴斯基安全网络。
协议：HTTPS	click.kaspersky.com redirect.kaspersky.com	打开界面中的链接。
端口：80 协议：HTTP	http://crl.kaspersky.com http://ocsp.kaspersky.com	公钥基础设施 (PKI)。
端口：443 协议：HTTPS	https://ipm-klca.kaspersky.com	营销公告。

为了让 Kaspersky Security Center Linux 与外部服务正确交互，请考虑以下建议：
- 组织的网络设备和代理服务器上的端口 443 和 1443 必须允许未加密的网络流量。
- 当管理服务器与卡巴斯基更新服务器和卡巴斯基安全网络服务器交互时，必须避免用证书替换劫持网络流量（MITM 攻击）。

要使用 klscflag 实用程序通过 HTTP 或 HTTPS 协议下载更新：

1. 运行命令行，然后将当前目录更改为包含 klscflag 实用程序的目录。klscflag 实用程序位于安装管理服务器的目录中。默认安装路径为/opt/kaspersky/ksc64/sbin。
2. 如果您想通过 HTTP 协议下载更新，请在根账户下运行以下命令之一：

   - 在安装了管理服务器的设备上：

     ```
     klscflag -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 1
     ```

   - 在分发点上：

     ```
     klscflag -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 1
     ```

   如果您想通过 HTTPS 协议下载更新，请在根账户下运行以下命令之一：

   - 在安装了管理服务器的设备上：

     ```
     klscflag -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 0
     ```

   - 在分发点上：

     ```
     klscflag -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 0
     ```

部署网络代理和安全应用程序

要管理组织设备，您必须在其上安装网络代理。部署分发的 Kaspersky Security Center Linux 到组织设备通常开始于在其上安装网络代理。

在 Microsoft Windows XP 中，网络代理可能无法正确执行以下操作：直接从卡巴斯基服务器（作为分发点）下载更新以及充当 KSN 代理服务器（作为分发点）。

初始化部署

如果已经有网络代理安装在设备，在该设备上远程安装应用程序通过该网络代理运行。要安装的应用程序分发包通过网络代理和管理服务器之间的通信渠道，与管理员定义的安装设置一并传输。为了传递分发包，您可以使用中继分发节点，即分发点、组播传递等。有关如何在已安装网络代理的受管理设备上安装应用程序的更多详细信息，请参阅本节下文。

您可以在运行 Windows 的设备上执行网络代理初始化安装，使用以下方法之一：

- 使用应用程序远程安装的第三方工具。
- 通过克隆带有操作系统和网络代理的管理员硬盘驱动器镜像：使用 Kaspersky Security Center Linux 提供的工具处理磁盘镜像或使用第三方工具。

- 使用 Windows 组策略：使用标准 Windows 组策略管理工具、或在自动模式下，通过 Kaspersky Security Center Linux 远程安装任务的专用选项。
- 在强制模式，使用 Kaspersky Security Center Linux 远程安装任务的特殊选项。
- 通过发送设备用户链接到 Kaspersky Security Center Linux 生成的独立包。独立包是包含所选应用程序分发包的定义了设置的可执行模块集合。
- 在设备上手动运行应用程序安装程序。

在 Microsoft Windows 以外的平台上，网络代理在受管理设备上的初始化安装必须通过可用的第三方工具执行。您可以升级网络代理到新版本或安装其他 Kaspersky 应用程序到非 Windows 平台，使用网络代理(已经安装在设备)执行远程安装任务。此种情况下，安装和在 Windows 设备上的安装相同。

当选择部署应用程序到受管理网络的方法和策略时，您必须考虑很多因素（部分列表）：

- 组织网络的配置。
- 设备总数。
- 在组织网络的设备出席、不是任何活动目录域成员、在设备上具有管理员权限的统一账户的出席。
- 管理服务器和设备通道的容量。
- 管理服务器和远程子网之间的通信类型以及那些子网中的网络通道容量。
- 部署之初应用在远程设备上的安全设置(例如 UAC 和简单文件共享模式的使用)。

配置安装程序

在开始部署 Kaspersky 应用程序到网络之前，您必须指定安装设置，就是在应用程序安装过程中定义的设置。当安装网络代理时，您应该指定最小值、连接管理服务器的地址，也可能需要一些高级设置。取决于您选择的安装方法，您可以用不同方法定义设置。最简单的方法(在所选设备上的手动交互式安装)，所有相关设置可以通过安装程序用户界面进行定义。

该定义设置的方法不适用于在设备组上的应用程序静默安装。通常情况下，管理员必须集中指定设置值；这些值可能用于在所选网络设备上的静默安装。

安装包

定义应用程序安装设置的第一个和主要的方法是通用的，因此适用于所有安装方法，用 Kaspersky Security Center Linux 工具和多数第三方工具。该方法包括在 Kaspersky Security Center Linux 中创建应用程序安装包。

安装包使用以下方法生成：

- 基于包含的*描述符*(带有 .kud 扩展名的包含了安装和结果分析规则以及其他信息的文件)从指定的分发包自动生成
- 来自安装程序的可执行文件或本地格式（.msi、.deb、.rpm）的安装程序，适用于标准或受支持的应用程序

生成的安装包以包含子文件夹和文件的文件夹形式分层级组织。除了原始分发包，安装包包含可编辑设置(包含安装程序设置和是否在安装结束时重启操作系统等处理规则)以及小的辅助模块。

单独支持的应用程序的安装设置值可以在创建安装包时在 Kaspersky Security Center Web Console 的用户界面定义。当通过 Kaspersky Security Center Linux 工具执行远程应用程序安装时，安装包被传送到设备，因此运行应用程序安装程序使得所有管理员定义的设置对该应用程序可用。当使用第三方工具安装 Kaspersky 应用程序时，您仅需要确保设备上整个安装包的可用性，即是分发包和其设置的可用性。安装包被 Kaspersky Security Center Linux 创建并存储在共享文件夹下的专用子文件夹。

不在安装包参数中显示授权账户的任何细节。

不支持使用 Microsoft Windows 的组策略进行部署。

在 Kaspersky Security Center Linux 安装之后，一些安装包被自动生成；它们可用于安装并包含网络代理和 Microsoft Windows 安全应用程序包。

尽管应用程序授权许可密钥可以在安装包属性中设置，但是建议您避免使用此授权许可分发方法，因为这样容易获取对安装包的读访问权限。您应该使用自动分发的授权许可密钥，或使用授权许可密钥安装任务。

关于 Kaspersky Security Center Linux 中的远程安装任务

Kaspersky Security Center Linux 提供了远程安装应用程序的不同装置，它们作为远程安装任务实现（强制安装、通过复制硬盘驱动器镜像安装）。您可以为指定管理组和特定设备或设备分类创建远程安装任务（此类任务显示在 Kaspersky Security Center Web Console 的**任务**文件夹中）。当创建任务时，您可以选择安装包(网络代理和/或其他应用程序的安装包)以用此任务安装，并指定定义远程安装方法的设置。此外，您可以使用远程安装向导，基于远程安装任务和结果监控。

管理组的任务影响指定组的设备和所有管理组子组的设备。如果任务中启用了相应设置，任务将覆盖组及其任何子组中包括的从属管理服务器的设备。

特定设备的任务在每一次运行时根据分类内容刷新客户端设备列表。如果分类包含连接到从属管理服务器的设备，任务也将在那些设备上运行。对于那些设置的详情和安装方法请参加以下。

要确保远程安装任务在连接到从属管理服务器的设备上成功操作，您必须使用转发任务提前转发您任务使用的安装包到对应的从属管理服务器。

通过捕获和复制设备镜像来部署

如果您需要安装网络代理到必须安装（或重新安装）操作系统和其他软件的设备，您可以使用捕获和复制设备镜像的机制。

要通过捕获和复制硬盘驱动器来执行部署：

1. 创建安装了操作系统和相关软件的“参考”设备，包含网络代理和安全应用程序。
2. 在设备上捕获参考镜像并通过 Kaspersky Security Center Linux 专用任务分发该镜像到新设备。

   要捕获和安装磁盘映像，请使用组织中可用的第三方工具。

使用第三方工具复制磁盘镜像

当应用第三方工具捕获安装了网络代理的设备镜像时，使用以下方法之一：

- 在参考设备上，停止网络代理服务并使用 -dupfix 参数运行 klmover 实用工具。实用工具 klmover 包含在网络代理安装包中。在镜像捕获操作完成之前请避免任何网络代理服务的运行。
- 请确保 klmover 将使用 -dupfix 参数运行(强制需求)在目标设备网络代理服务第一次运行之前，在镜像部署后的操作系统第一次启动时。实用工具 klmover 包含在网络代理安装包中。
- 使用网络代理磁盘克隆模式。

如果硬盘驱动器映像被错误地复制，可以解决此问题。

您还可以捕获未安装网络代理的设备的镜像。为此，在目标设备上执行镜像部署，然后部署网络代理。如果使用此方法，请使用设备中的独立安装包提供对网络文件夹的访问权限。

网络代理磁盘克隆模式

克隆参考设备的硬盘驱动器是在新设备上安装软件的流行方法。如果网络代理以标准模式运行在参考设备的硬盘驱动器上，会发生以下问题：

带有网络代理的参考磁盘镜像被部署到新设备后，它们以单一设备显示在 Kaspersky Security Center Web Console 中。该问题发生是因为克隆过程导致新设备保持相同的内部数据，这将允许管理服务器在 Kaspersky Security Center Web Console 中将设备关联到其自己的记录。

一个特别的*网络代理磁盘克隆模式*允许您避免克隆后在 Kaspersky Security Center Web Console 中错误显示新设备的问题。在您通过克隆磁盘部署软件（带有网络代理）到新设备时使用该模式。

在磁盘克隆模式下，网络代理保持运行，但是不连接到管理服务器。当退出克隆模式时，网络代理删除内部数据，这将导致管理服务器关联多个设备到 Kaspersky Security Center Web Console 中的单一记录。在完成参考设备镜像的克隆时，新设备显示在 Kaspersky Security Center Web Console 属性中（在个别记录下）。

网络代理磁盘克隆模式使用方案

1. 管理员安装网络代理到参考设备。
2. 管理员使用 klnagchk 实用工具检查网络代理到管理服务器的连接。
3. 管理员启用网络代理磁盘克隆模式。
4. 管理员安装软件和补丁到设备，并重启所需的次数。
5. 管理员克隆参考设备的硬盘驱动器到任意数量的设备。
6. 每个克隆的副本必须满足以下条件：
    a. 设备名称必须更改。
    b. 设备必须重启。

c. 磁盘克隆模式必须被禁用。

使用 klmover 工具启用和禁用磁盘克隆模式

要启用或禁用网络代理磁盘克隆模式：

1. 在您必须克隆的安装了网络代理的设备上运行 klmover 工具。
   klmover 工具位于网络代理安装文件夹。
2. 要启用磁盘克隆模式，在 Windows 命令行输入以下命令：`klmover -cloningmode 1`。
   网络代理切换到磁盘克隆模式。
3. 要请求磁盘克隆模式的当前状态，在命令行输入以下命令：`klmover -cloningmode`。
   工具显示是否磁盘克隆模式已启用或禁用。
4. 要禁用磁盘克隆模式，在命令行输入以下命令：`klmover -cloningmode 0`。

通过 Kaspersky Security Center Linux 远程安装任务的强制部署

如果您需要立即开始部署网络代理或其他应用程序，不等待目标设备下一次登录到域，或如果有任何非活动目录域的目标设备可用，您可以通过 Kaspersky Security Center Linux 远程安装任务强制安装所选的安装包。

此种情况下，您可以明确指定目标设备(使用列表)，或通过选择它们所属的 Kaspersky Security Center Linux 管理组，或通过基于指定标准创建设备分类。安装开始时间定义在任务计划中。如果任务属性中启用了**运行错过的任务**，任务可以在设备开启时立即运行，或设备被移动到目标管理组时立即运行。

该类型安装涉及到复制文件到设备上的管理资源(admin$)和在其上运行支持服务的远程注册。只有指定的分发点才能从管理资源在 Windows 设备上执行强制部署。以下条件必须在此种情况下被满足：

- 设备必须可以从管理服务器或分发点连接。
- 目标设备的名称解析必须在网络中运行正常。
- 设备上的管理共享(admin$)必须保持启用。
- 服务器系统服务必须在目标设备上运行(默认下是运行的)。
- 目标设备上必须打开以下端口以允许通过 Windows 工具远程访问：TCP 139, TCP 445, UDP 137 和 UDP 138。
- 简单文件共享必须在目标设备上禁用。
- 在目标设备上，访问共享和安全模块必须被设置为 *经典 – 本地用户身份验证*，不能是 *仅访客 – 本地用户访客身份验证*。
- 目标设备必须是域成员，或带有管理员权限的统一账户必须提前在目标设备上被创建。

工作组中的设备可以根据以上需求通过使用 riprep 实用工具进行调整，相关描述参见卡巴斯基技术支持网站。

在未分配到任何 Kaspersky Security Center Linux 管理组的新设备上进行安装时，您可以打开远程安装任务属性并指定网络代理安装后设备要移动到的管理组。

当创建组任务时，记住每个组任务都影响所选组的潜逃组中的所有设备。因此，您必须避免在子组中的重复安装任务。

自动安装是创建应用程序强制安装任务的最简单方法。为此，打开管理组属性，打开安装包列表并选择必须在该组中设备上安装的包。结果，所选安装包将被自动安装在该组和其所有子组中的所有设备上。包被安装的时间间隔取决于网络吞吐量和网络设备总数。

强制安装也可以在设备无法被管理服务器直接访问时应用：例如，设备在隔离网络中，或者设备在本地网络但管理服务器在 DMZ。要能够强制安装，您必须为每个隔离网络提供分发点。

使用分发点作为本地安装中心也可以用在与管理服务器具有窄通道通信的子网设备上的安装，此时子网中的通道带宽很高。然而，该安装方法给作为分发点的设备增加了大量负载。因此，建议您带有高性能存储单元的高性能设备作为分发点。而且，文件夹 /var/opt/kaspersky/klnagent_srv/ 所在分区的磁盘剩余空间必须超过所安装应用程序的分发包的总大小的好几倍。

运行 Kaspersky Security Center Linux 创建的独立包

以上描述的网络代理和其他应用程序的初始化部署方法无法总被实现，因为不可能满足所有可应用条件。此种情况下，您可以通过 Kaspersky Security Center Linux 创建通用可执行文件，叫做*独立安装包*，使用管理员准备的带有相关安装设置的安装包。独立安装包存储在 Kaspersky Security Center Linux 共享文件夹。

您可以使用 Kaspersky Security Center Linux 来给所选用户发送包含该共享文件夹文件链接的电子邮件，提示他们运行该文件(在交互模式或静默模式)。您可以附加独立安装包到电子邮件，然后发送它到对 Kaspersky Security Center Linux 共享文件夹没有访问权限的设备用户。管理员也可以复制独立包到可移动驱动器，将其传送到相关设备然后稍后运行。

您可以从网络代理包或其他应用程序包创建独立包(例如，安全应用程序)。如果独立包从网络代理和其他应用程序创建，安装和网络代理一起启动。

当创建带有网络代理的独立包时，您可以指定当网络代理安装完成时，新设备(未分配到任何管理组的设备)将被自动移动到的管理组。

独立包可以在交互模式下运行(默认)，显示应用程序安装结果，或者可以运行在静默模式(以参数 "-s" 运行)。静默模式可以用在从脚本安装，例如操作系统镜像部署后要运行的脚本。静默模式安装的结果决定与进程返回代码。

在安装有网络代理的设备上远程安装应用程序

如果连接到主管理服务器（或任何其从属管理服务器）的可操作网络代理被安装到设备，您可以升级该设备上的网络代理，以及通过网络代理安装、升级或卸载支持的应用程序。

您可以在远程安装任务的属性中启用“**使用网络代理**”选项。

如果选择此选项，带有管理员定义的安装设置的安装包将被通过网络代理和管理服务器之间的通信渠道传输到目标设备。

要优化管理服务器负载和最小化管理服务器和设备之间的流量，最好为每个远程网络或每个多播域分配分发点（请参见“关于分发点”部分和“创建管理组结构和分配分发点”部分）。此种情况下，安装包和安装设置通过分发点从管理服务器分发到目标设备。

而且，您可以使用分发点来多播传送安装包，这将允许您在部署应用程序时显著降低网络流量。

当通过网络代理和管理服务器之间的通信渠道传输安装包到目标设备时，所有准备传输的安装包都将被缓存在 /var/opt/kaspersky/klnagent_srv/1093/.working/ 文件夹。当使用多个不同类型的大安装包并涉及大量分发点时，该文件夹的尺寸将显著增长。

文件不能从 FTServer 文件夹手动删除。当原始安装包被删除时，对应数据将被自动从 FTServer 文件夹删除。

分发点接收的数据保存在文件夹 /var/opt/kaspersky/klnagent_srv/1103/ 中。

文件不能从 $FTCITmp 文件夹手动删除。使用该文件夹数据的任务完成后，该文件夹的内容将被永久删除。

因为安装包从中转存储库以优化传输的格式通过管理服务器与网络代理之间的通信渠道进行分发，原始文件夹里的安装包不允许更改。这些更改将不会被管理服务器自动注册。如果您需要手动修改安装包的文件(尽管建议您避免此方案)，您必须在 Kaspersky Security Center Web Console 中编辑安装包的任何设置。在 Kaspersky Security Center Web Console 中编辑安装包的设置会导致管理服务器在目标设备传输缓存中更新安装包镜像。

在远程安装任务中管理设备重启

设备经常需要在完成应用程序远程安装时重启(尤其在 Windows)。

如果您使用 Kaspersky Security Center Linux 远程安装任务，在新任务向导或所创建任务的属性窗口（**操作系统重启**区域）中，您可以选择 Windows 设备要求重启时执行的操作：

- **不重启设备**。此种情况下，自动重启不会运行。要完成安装，您必须重启设备(例如，手动或通过设备管理任务)。所需重启的信息将被保存在任务结果和设备状态。该选项适用于在需要持续操作的服务器和其他设备上的安装任务。
- **重启设备**。此种情况下，如果完成安装需要重启，设备总是被自动重启。该选项适用于允许中断操作(关机或重启)的设备上的安装任务。
- **提示用户操作**。此种情况下，客户端设备上将显示重启提醒，提示用户手动重启设备。可以为该选项定义一些高级设置：用户消息文本、消息显示频率以及强制重启（不需要用户确认）的时间间隔。**提示用户操作**最适用于用户需要选择最合适重启时间的工作站。

安全应用程序安装包上的数据库更新

开始保护部署之前，您必须注意要随安全应用程序的分发包一起更新反病毒数据库(包块模块和自动补丁)。最好在开始部署之前更新应用程序安装包中的数据库(例如， 通过使用所选安装包上下文菜单中的相关命令)。这将减少目标设备在完成保护部署后所需的重启次数。

监控部署

要监控 Kaspersky Security Center Linux 部署并确保受管理设备上安装了安全应用程序和网络代理，请使用监控和报告功能：

- 使用仪表板的部署小部件实时监控部署。
- 使用报告获取详细信息。

配置安装程序

该部分提供了 Kaspersky Security Center Linux 安装程序文件和安装设置的信息，以及如何在静默模式安装管理服务器和网络代理的建议。

常规信息

适用于 Windows 设备的 Kaspersky Security Center Linux 组件的安装程序基于 Windows Installer 技术构建。MSI 包是安装程序的核心。该格式的包允许使用 Windows Installer 的所有好处：可量测性、补丁系统可用性、转换系统、通过第三方解决方案集中安装以及在操作系统中透明注册。

在静默模式下安装(带有响应文件)

网络代理安装程序可以使用响应文件工作(ss_install.xml)，其中整合了不需要用户参与的静默模式安装参数。ss_install.xml 文件位于与 MSI 包相同的文件夹；在静默模式安装时被自动使用。您可以通过命令行参数"/s"启用静默安装模式。

一个大概例子运行如下：

```
setup.exe /s
```

> 在以静默模式启动安装程序之前，请阅读最终用户授权许可协议 (EULA)。如果 Kaspersky Security Center Linux 分发包不包含带有 EULA 文本的 TXT 文件，您可以从 卡巴斯基网站 下载文件。

ss_install.xml 文件 Kaspersky Security Center Linux 安装程序参数的内部格式的实例。分发包包含带有默认参数的 ss_install.xml 文件。

> 请不要手动修改 ss_install.xml 文件。该文件可以通过 Kaspersky Security Center Linux 工具修改，当在 Kaspersky Security Center Web Console 中编辑安装包参数时。

通过 setup.exe 的部分安装配置

当通过 setup.exe 运行应用程序安装时，您可以添加 MSI 任何属性的值到 MSI 包。

该命令显示如下：

```
例如：
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

管理服务器安装参数

下表介绍了在静默模式下安装 Kaspersky Security Center Linux 时可以配置的属性。

静默模式下安装管理服务器的参数

变量名称	是否必需	描述	可能值
EULA_ACCEPTED	是	确认您理解并接受最终用户授权许可协议的条款。	1
PP_ACCEPTED	是	确认您理解并接受隐私政策的条款。	1
KLSRV_UNATT_SERVERADDRESS	是	管理服务器的 DNS 名称或静态 IP 地址。	DNS 名称或 IP 地址
KLSRV_UNATT_PORT_SRV	否	管理服务器端口号。可选默认值是 14000。	端口号
KLSRV_UNATT_PORT_SRV_SSL	否	管理服务器 SSL 端口号。可选默认值是 13000。	端口号
KLSRV_UNATT_PORT_KLOAPI	否	管理服务器 KLOAPI 端口号。可选，默认值 是 13299.	端口号
KLSRV_UNATT_PORT_GUI	否	管理服务器 GUI 端口号。可选默认值是 13291。	端口号
KLSRV_UNATT_NETRANGETYPE	否	您要管理的设备的大概数量。可选默认值是 1。	1 适用于 1 到 100 个联设备。 2 适用于 101 到 1000 网设备。 3 适用于超过 1000 个网设备。
KLSRV_UNATT_DBMS_TYPE	是	数据库管理系统类型：MySQL（MariaDB）或 Postgres。	mysql 或 postgres
KLSRV_UNATT_DBMS_INSTANCE	是	数据库服务器 IP 地址。	IP 地址
KLSRV_UNATT_DBMS_PORT	是	数据库服务器端口。MySQL (MariaDB) 的默认值为 3306；Postgres 的默认值为 5432。	3306 或者 5432
KLSRV_UNATT_DB_NAME	是	数据库名称。	kav
KLSRV_UNATT_DBMS_LOGIN	是	有权访问数据库的用户的用户名。	
KLSRV_UNATT_DBMS_PASSWORD	是	有权访问数据库的用户的密码。	
KLSRV_UNATT_KLADMINSGROUP	是	服务的安全组名称。	kladmins
KLSRV_UNATT_KLSRVUSER	是	用于启动管理服务器服务的账户名。账户必须是 KLSRV_UNATT_KLADMINSGROUP 变量中指定的安全组的成员。	ksc

KLSRV_UNATT_KLSVCUSER	是	用于启动其他服务的账户名。账户必须是 KLSRV_UNATT_KLADMINSGROUP 变量中指定的安全组的成员。	ksc
如果要将管理服务器部署为 Kaspersky Security Center Linux 故障转移集群，应答文件必须包含以下附加变量：			
KLFOC_UNATT_NODE	是	节点编号（1 或 2）。	1 or 2
KLFOC_UNATT_STATE_SHARE_MOUNT_PATH	是	状态共享挂载点。	
KLFOC_UNATT_DATA_SHARE_MOUNT_PATH	是	数据共享挂载点。	
KLFOC_UNATT_CONN_MODE	是	故障转移集群连接模式。	VirtualAdapter 或 ExternalLoadBalar
万一 KLFOC_UNATT_CONN_MODE 变量的值为 VirtualAdapter，应答文件必须包含以下附加变量：			
KLFOC_UNATT_CONN_MODE_VA_NAME	这些变量之一是必需项	虚拟网络适配器名称。	
KLFOC_UNATT_CONN_MODE_VA_IPV4		虚拟网络适配器 IP 地址。	IP 地址
KLFOC_UNATT_CONN_MODE_VA_IPV6		虚拟网络适配器 IPv6 地址。	IPv6 地址

网络代理安装参数

下表描述了安装网络代理时您可以配置的 MSI 属性。所有参数都是可选的，除了 EULA 和服务器地址。

静默模式下安装网络代理的参数

MSI 属性	描述	可用值
EULA	是否接受授权许可协议条款	• 1 – 我已完全阅读、理解并接受最终用户授权许可协议的条款。 • 0 – 我不接受授权许可协议的条款（将不会执行安装）。 • 没有值 – 我不接受授权许可协议的条款（将不会执行安装）。
DONT_USE_ANSWER_FILE	从响应文件读取安装设置	• 1–不使用。 • 其它值或没有值 – 读取。

INSTALLDIR	网络代理安装文件夹路径	字符串值。
SERVERADDRESS	管理服务器地址(必需)	字符串值。
SERVERPORT	连接管理服务器的端口号	数字值。
SERVERSSLPORT	使用 SSL 协议加密连接到管理服务器的端口号	数字值。
USESSL	是否使用 SSL 连接	• 1 – 使用。 • 其它值或没有值 – 不使用。
OPENUDPPORT	是否打开 UDP 端口	• 1 – 打开。 • 其它值或没有值 – 不打开。
UDPPORT	UDP 端口号	数字值。
USEPROXY	是否使用代理服务器	• 1 – 使用。 • 其它值或没有值 – 不使用。
PROXYLOCATION (PROXYADDRESS:PROXYPORT)	连接到代理服务器的代理地址和端口号	字符串值。
PROXYLOGIN	连接代理服务器的账户	字符串值。
PROXYPASSWORD	用于连接到代理服务器的账户密码（不要在安装包参数中指定授权账户的任何细节。）	字符串值。
GATEWAYMODE	连接网关使用模式	• 0 – 不使用连接网关。 • 1 – 使用该网络代理作为连接网关。 • 2 – 使用连接网关连接到管理服务器。
GATEWAYADDRESS	连接网关地址	字符串值。
CERTSELECTION	接收证书的方法	• GetOnFirstConnection – 从管理服务器接收证书。 • GetExistent – 如果选中此选项则选择现有证书，必须指定 CERTFILE 属性。
CERTFILE	证书文件路径	字符串值。
VMVDI	启用虚拟桌面基础架构（VDI）的动态模式	• 1 – 启用。

		• 0 – 不启用。 • 没有值 – 不启用。
LAUNCHPROGRAM	安装后是否启动网络代理服务	• 1 – 启动。 • 其它值或没有值 – 不启动。
NAGENTTAGS	网络代理标签（优先级高于响应文件中给定的标签）	字符串值。

虚拟基础架构

Kaspersky Security Center Linux 支持虚拟机的使用。您可以在每台虚拟机上安装网络代理和安全应用程序，并可以在虚拟机监控程序级别保护虚拟机。在第一种情况下，您可以使用标准安全应用程序或 Kaspersky Security for Virtualization Light Agent 来保护您的虚拟机。在第二种情况下，您可以使用 Kaspersky Security for Virtualization Agentless。

Kaspersky Security Center Linux 支持虚拟机回滚到先前状态。

降低虚拟机负载的窍门

当安装网络代理到虚拟机时，建议您禁用一些对虚拟机没有用的 Kaspersky Security Center Linux 功能。

在虚拟机或用于生成虚拟机的模版上安装网络代理时，建议执行以下操作：

- 如果要运行远程安装，则在网络代理安装包的属性窗口的“**高级**”区域中，选择“**优化 VDI 设置**”选项。
- 如果要通过向导运行交互式安装，则在向导窗口中选择“**为虚拟基础架构优化网络代理设置**”选项。

选择这些选项将改变网络代理设置，因此以下功能在默认情况下保持禁用状态（在应用策略之前）：

- 获取已安装软件的信息
- 获取硬件信息
- 获取检测到的漏洞信息
- 获取需要更新的信息

通常，这些功能对于虚拟机不必要，因为它们使用统一软件和虚拟硬件。

禁用该功能是不可逆的。如果需要任何被禁用的功能，您可以通过网络代理策略启用它，或通过网络代理本地设置。网络代理本地设置通过 Kaspersky Security Center Web Console 中相关设备的上下文菜单可用。

对动态虚拟机的支持

Kaspersky Security Center Linux 支持动态虚拟机。如果虚拟架构部署在组织网络，动态（临时）虚拟机可以被用在特定情况。动态虚拟机基于管理员提供的模板以独立名称创建。用户使用了虚拟机一段时间，然后关闭虚拟机，则该虚拟机将从虚拟基础架构中删除。如果 Kaspersky Security Center Linux 部署在组织网络，安装了网络代理的虚拟机将被添加到管理服务器数据库。在您关闭虚拟机后，对应的条目必须从管理服务器数据库中删除。

要运行自动删除虚拟机上的条目的功能，在动态虚拟机的模板上安装网络代理时，请选中“**启用 VDI 动态模式**”选项：

- 对于远程安装—在网络代理安装包的属性窗口（高级区域）
- 对于交互式安装 — 在“网络代理安装向导”中进行

> 当安装网络代理到物理设备时，不要选中“**启用 VDI 动态模式**”选项。

如果您要在删除虚拟机后将动态虚拟机的事件存储在管理服务器一段时间，那么，在管理服务器属性窗口，在“**事件存储库**”区域，选择“**设备被删除后存储事件**”选项并指定事件的最大存储期限（天）。

对虚拟机复制的支持

复制安装了网络代理的虚拟机或从安装了网络代理的模板创建虚拟机，和捕获和复制硬盘驱动器镜像的网络代理部署相同。因此，常规情况下，当复制虚拟机时，您需要执行与通过复制磁盘镜像部署网络代理时相同的操作。

然而，以下描述的两种情况展示了自动检测复制的网络代理。由于以上原因，您不必运行“通过捕获和复制设备磁盘镜像部署”中描述的复杂操作：

- “**启用 VDI 动态模式**”选项在网络代理被安装时选中：在操作系统每次重启后，该虚拟机将被认为是新设备，无论是否被复制。
- 以下 Hypervisor 之一被使用：VMware™、HyperV® 或 Xen®：网络代理通过更改的虚拟硬件 ID 检测虚拟机的复制。

> 虚拟硬件更改分析并不绝对可靠。在广泛应用该方法之前，您必须在小组虚拟机上测试您组织中使用的当前 hypervisor 版本。

对网络代理设备文件系统回滚的支持

Kaspersky Security Center Linux 是一个分发的应用程序。在安装了网络代理的设备上回滚文件系统到先前状态将导致数据不同步和 Kaspersky Security Center Linux 功能不正常。

文件系统(或一部分)可以在以下情况下回滚：

- 当复制硬件驱动器镜像时。
- 当通过虚拟架构恢复虚拟机状态时。
- 当从备份副本或恢复点恢复数据时。

安装了网络代理的设备上的第三方软件影响 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ 文件夹的情景仅是 Kaspersky Security Center Linux 的关键情景。因此，如果可能，您必须总是从恢复进程中排除该文件夹。

因此一些组织的工作规则提供了对设备文件系统的回滚，对安装了网络代理的设备的文件系统回滚的支持被添加到了 Kaspersky Security Center Linux，从版本 10 Maintenance Release 1 开始(管理服务器和网络代理必须是版本 10 Maintenance Release 1 或更新)。当检测到时，这些设备被自动连接到管理服务器，带有完整数据清除和完整同步。

默认下，对文件系统回滚检测的支持在 Kaspersky Security Center Linux 中被启用。

尽量不要回滚网络代理设备的 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ 文件夹，因为完整数据的重新同步需要大量资源。

系统状态回滚在管理服务器设备上是不允许的。管理服务器使用的数据库的回滚也是不允许的。

您可以仅可以使用标准的 klbackup 实用工具从备份副本恢复管理服务器状态。

应用程序的本地安装

此部分介绍仅可在本地设备上安装的应用程序的安装过程。

要在所选客户端设备上执行应用程序本地安装，您必须具有此设备的管理员权限。

要在所选客户端设备上本地安装应用程序：

1. 在客户端设备上安装网络代理并配置客户端设备和管理服务器之间的连接。
2. 按照这些应用程序的指南说明，在设备上安装相关的应用程序。
3. 为每个在管理员工作站上安装的应用程序安装管理插件。

Kaspersky Security Center Linux 还支持使用独立安装包进行应用程序本地安装。Kaspersky Security Center Linux 不支持所有 Kaspersky 应用程序的安装。

网络代理的本地安装

要在设备上本地安装网络代理：

1. 在设备上，运行从互联网下载的分发包中的 setup.exe 文件。

   提示您选择要安装的 Kaspersky 程序的窗口将打开。

2. 在应用程序选择窗口中，单击“**仅安装 Kaspersky Security Center 15 网络代理**”链接以启动网络代理安装向导。遵照向导的说明操作。

   在安装向导运行期间，您可以指定网络代理高级设置（见下）。

3. 如果您想使用您的设备作为指定管理组的连接网关，在安装向导的“**连接网关**”窗口，选中“**使用网络代理作为 DMZ 连接网关**”。

4. 要在虚拟机上安装时配置网络代理：

a. 如果您计划从虚拟机镜像创建动态虚拟机，为虚拟桌面基础架构(VDI)启用网络代理动态模式。为此，请在安装向导的“**高级设置**”窗口中选择“**启用 VDI 动态模式**”选项。

如果您不想从虚拟机镜像创建动态虚拟机，跳过此步。

b. 优化网络代理的 VDI 操作。为此，请在安装向导的“**高级设置**”窗口中选择“**优化 VDI 设置**”选项。

计算机启动时扫描可执行文件中是否有漏洞将被禁用。另外，会禁用发送关于以下对象的信息至管理服务器：

- 硬件注册表
- 设备上安装的应用程序
- 必须安装在本地客户端设备上的 Microsoft Windows 更新
- 在本地客户端设备上检测到的软件漏洞

而且，您将可以在网络代理属性或网络代理策略设置中启用此信息的发送。

安装向导完成后，网络代理被安装在设备。

您可以查看网络代理服务的属性，还可以使用标准的 Microsoft Windows 工具（计算机管理\服务）来启动、停止或监控网络代理活动。

在静默模式下安装网络代理

网络代理可以在静默模式下安装，即，无需交互式输入安装参数。静默安装使用网络代理的 Windows Installer 数据包 (MSI)。MSI 文件位于 Kaspersky Security Center Linux 分发包，在 Packages\NetAgent\exec 文件夹。

要在静默模式下将网络代理安装至本地设备：

1. 阅读最终用户授权许可协议。只有在您理解并接受最终用户授权许可协议的条款后，才使用下面的命令。
2. 运行命令

```
msiexec /i "Kaspersky Network Agent.msi" /qn <setup_parameters>
```

其中“`setup_parameters`”是一系列参数，其各自的值用空格隔开 (`PROP1=PROP1VAL PROP2=PROP2VAL`)。

在参数列表中，您必须包含 `EULA=1`。否则网络代理不会被安装。

如果您正在使用 Kaspersky Security Center 11 和更高版本的标准连接设置以及远程设备上的网络代理，请运行以下命令：

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

`/l*vx` 是写入日志的键。该日志在网络代理安装期间创建，保存在 C:\windows\temp\nag_inst.log。

除了 nag_inst.log，应用程序还会创建 $klssinstlib.log 文件，其中包含安装日志。此文件存储在 %windir%\temp 或 %temp% 文件夹中。为了进行故障排除，您或 Kaspersky 技术支持专家可能同时需要两个日志文件 - nag_inst.log 和 $klssinstlib.log。

如果您需要另外指定用于连接到管理服务器的端口，请运行以下命令：

```
```

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1 SERVERPORT=14000
```

参数 SERVERPORT 对应于连接到管理服务器的端口号。

网络代理安装参数区域中列出了在静默模式下安装网络代理时可用到的参数名称和可能的值。

应用程序管理插件的本地安装

要安装应用程序管理插件：

在按照了管理控制台的设备上，运行可执行文件 klcfginst.exe。该文件包含于应用程序分发包中。

klcfginst.exe 包含在可通过 Kaspersky Security Center Linux 管理的所有应用程序里。向导可方便进行安装，并且无需手动配置设置。

以静默模式安装应用程序

要以静默模式安装应用程序：

1. 打开 Kaspersky Security Center 的主应用程序窗口。
2. 在控制台树的“**远程安装**”文件夹中的“**安装包**”子文件夹中，选择相关应用程序的安装包，或者为该应用程序创建新安装包。

   安装包将存储于管理服务器的共享文件夹下的“安装包服务”文件夹中。每个安装包都对应一个独立的子文件夹。

3. 以下列方式之一打开所需安装包的存储文件夹：
   - 通过将相关安装包对应的文件夹从管理服务器复制到客户端设备。然后在客户端设备上打开复制的文件夹。
   - 通过从客户端设备打开对应于管理服务器预安装包的共享文件夹。

   如果共享文件位于安装了 Microsoft Windows Vista 的设备上，请为“**用户账户控制：以管理员批准模式运行所有管理员**”设置选择值“**已禁用**”（“**开始**” → “**控制面板**” → “**管理**” → “**本地安全策略**” → “**安全设置**”）。

4. 部署选择的程序，执行下面的操作：
   - 对于 Kaspersky Anti-Virus for Windows Workstations、Kaspersky Anti-Virus for Windows Servers 和 Kaspersky Security Center，打开 exec 子文件夹并用 /s 键值运行可执行文件（带 .exe 扩展名的文件）。
   - 对于其他 Kaspersky 应用程序，请在打开的文件夹中，以 /s 键值运行可执行文件（带 .exe 扩展名的文件）。

以 EULA=1 和 PRIVACYPOLICY=1 参数运行可执行文件表示您已完全阅读、理解并接受最终用户授权许可协议和隐私策略的条款。您也知道并同意您的数据将按照隐私策略中所述进行处理和传输（包括传输到第三方国家）。授权许可协议和隐私策略的文本包含在 Kaspersky Security Center Linux 分发包中。必须接受授权许可协议和隐私策略的条款才能安装程序或升级上一版本程序。

使用独立包安装应用程序

Kaspersky Security Center 允许您为应用程序创建独立安装包。独立安装包是一个位于 Web 服务器上的可执行文件。它可由电子邮件发送，也可以其他方式传送传送到客户端设备。收到的文件可以在本地客户端设备上运行，并且安装程序不涉及 Kaspersky Security Center。

要使用独立安装包安装应用程序：

1. 连接至必要的管理服务器。
2. 在控制台树的“**远程安装**”文件夹中，选择“**安装包**”子文件夹。
3. 在工作区中，选择所需应用程序的安装包。
4. 使用下列方式之一，启动独立安装包的创建过程：
   - 在安装包的上下文菜单中，选择“**创建独立安装包**”。
   - 通过在安装包的工作区中单击“**创建独立安装包**”链接。

   独立安装包创建向导启动。遵照向导的说明操作。

   在向导的最后一步，选择一种方法将独立安装包传输至客户端设备。
5. 将独立安装包传输至客户端设备。
6. 在客户端设备上运行独立安装包。

这样，应用程序将以独立包所指定的设置，安装在客户端设备上。

当您创建独立安装包时，它会自动发布在 Web 服务器上。已创建的独立安装包列表中会显示用于下载独立包的链接。您可以取消发布选中的独立包，也可以重新在 Web 服务器上发布。默认情况下，使用端口 8060 下载独立安装包。

网络代理安装包设置

要配置网络代理安装包：

1. 在控制台树的“**远程安装**”文件夹中，选择“**安装包**”子文件夹。

   默认情况下，“ **远程安装**”文件夹是“**高级**”文件夹的子文件夹。
2. 在网络代理安装包的上下文菜单中，选择“**属性**”。

“网络代理安装包属性”窗口将开启。

常规

“**常规**”区域显示有关安装包的常规信息：

- 安装包名称
- 为其创建该安装包的应用程序的名称和版本
- 安装包大小
- 安装包创建日期
- 安装包文件夹的路径

设置

本区域显示为确保网络代理在安装后就能正确工作所需的设置。该区域的设置仅在运行 Windows 的设备上可用。

在“**目标文件夹**”设置组，您可以选择要安装网络代理的客户端设备。

- 安装到默认文件夹

  如果选择该选项，网络代理将安装在 <驱动器>:\Program Files\Kaspersky Lab\NetworkAgent 文件夹中。如果该文件夹不存在，系统会自动创建。

  默认情况下已选定该选项。

- 安装到指定文件夹

  如果选择该选项，则网络代理将安装到输入字段中指定的文件夹中。

在以下设置组中，您可以设置网络代理远程卸载任务的密码：

- 使用卸载密码

  如果启用此选项，通过单击“**修改**”按钮，可以输入卸载密码（仅适用于运行 Windows 操作系统的设备上的网络代理）。

  默认情况下已禁用该选项。

- 状态

  密码状态：**密码已设置**或**密码未设置**。

  默认情况下，该密码未指定。

- 保护网络代理服务免遭非授权的卸载或终止，并防止设置更改

当启用该选项时，网络代理被安装到受管理设备之后，没有所需权限组件无法被卸载或重新配置。网络代理服务无法被停止。此选项对域控制器没有影响。

启用此选项可保护以本地管理员权限操作的工作站上的网络代理。

默认情况下已禁用该选项。

- 对未定义状态的组件自动安装可应用更新和补丁

  如果启用此选项，将自动安装为管理服务器、网络代理、Kaspersky Security Center Web Console、Exchange 移动设备服务器和 iOS MDM 服务器下载的所有更新和补丁。

  如果禁用此选项，所有已下载的更新和补丁只有在状态更改为“*已批准*”后才会更新。带有*未定义*状态的更新和补丁将不被安装。

  默认情况下已启用该选项。

连接

在该区域中，您可以配置网络代理至管理服务器的连接：要建立连接，您可以使用 SSL 或 UDP 协议。要配置连接，请指定以下设置：

- 管理服务器

  安装了管理服务器的设备地址。

- 端口

  用于连接的端口号。

- SSL 端口

  用于通过 SSL 协议的连接的端口号。

- 使用服务器证书

  如果启用此选项，网络代理访问管理服务器时的身份验证将使用证书文件，您可以通过单击“**浏览**”按钮来指定该证书文件。

  如果禁用此选项，将在网络代理第一次连接到“**服务器地址**”字段指定的地址时从管理服务器接收证书文件。

  我们建议不禁用此选项，因为网络代理在连接到管理服务器时自动接收管理服务器证书被认为是不安全的。

  默认情况下已选中该选框。

- 使用 SSL

  如果启用此选项，则使用 SSL 协议通过安全端口连接管理服务器。

  默认情况下已禁用该选项。我们建议您不要禁用此选项，以便您的连接保持安全。

- 使用 UDP 端口

  如果启用此选项，网络代理将通过 UDP 端口连接至管理服务器。这允许管理客户端设备并接收有关它们的信息。

  UDP 端口必须在安装网络代理的受管理设备上开放。因此，我们建议您不要禁用此选项。

  默认情况下已启用该选项。

- UDP 端口号

  在该字段中，可以指定使用 UDP 协议连接管理服务器到网络代理的端口。

  默认 UDP 端口 15000。

- 在 Microsoft Windows 防火墙中打开网络代理端口

  如果启用此选项，网络代理使用的 UDP 端口将被添加到 Microsoft Windows 防火墙排除列表中。

  默认情况下已启用该选项。

高级

在“**高级**”区域，您可以配置如何使用连接网关。为此目的，您可以执行以下操作：

- 使用网络代理作为非管制区域 (DMZ) 中的连接网关以连接到管理服务器，与之通信，以及 在数据传输过程中保持网络代理上的数据安全。
- 使用连接网关连接到管理服务器以减少与管理服务器的连接数。在这种情况下，请在“**连接网关地址**”字段中输入将充当连接网关的设备的地址。
- 如果您的网络包含虚拟机，请配置虚拟桌面基础架构 (VDI) 的连接。为此目的，请执行以下操作：
  - 启用 VDI 动态模式

    如果启用此选项，将针对虚拟机上安装的网络代理启用虚拟桌面基础架构 (VDI) 的动态模式。

    默认情况下已禁用该选项。

  - 优化 VDI 设置

    如果启用此选项，网络代理设置中将禁用以下功能：
    - 获取已安装软件的信息
    - 获取硬件信息
    - 获取检测到的漏洞信息
    - 获取需要更新的信息

    默认情况下已禁用该选项。

附加组件

在该区域,您可以为网络代理同时安装选择附加组件。

标签

"**标签**"区域显示网络代理安装后可以被添加到客户端设备的关键字列表。您可以在列表中添加和删除标签以及重命名它们。

如果标签旁的复选框被选中，该标签在网络代理安装过程中被自动添加到受管理设备。

如果标签旁的复选框被清空，该标签在网络代理安装过程中不被自动添加到受管理设备。您可以手动添加该标签到设备。

当从列表中删除标签时，它被自动从所有添加了该标签的设备上删除。

修订历史

在该区域，您可以查看安装包修订历史。您可以比较修订、查看修订、保存修订到文件和添加/编辑修订描述。

对特别操作系统可用的网络代理安装包设置在下表中给出。

网络代理安装包设置

属性区域	Windows	Mac	Linux
常规	✓	✓	✓
设置	✓	–	–
连接	✓	✓ （"在 Microsoft Windows 防火墙中打开网络代理端口"和"仅使用代理服务器自动检测"选项除外）	✓ （"在 Microsoft Windows 防火墙中打开网络代理端口"和"仅使用代理服务器自动检测"选项除外）
高级	✓	✓	✓
附加组件	✓	✓	✓
标签	✓	✓ （自动标记规则除外）	✓ （自动标记规则除外）
修订历史	✓	✓	✓

Kaspersky Endpoint Security 设备扫描组任务的手动设置

快速启动向导创建扫描设备的组任务。如果自动指定的组扫描任务计划不适合您的组织，您必须根据组织采用的工作场所规则手动设置最方便的计划。

例如，为任务分配"**在星期五下午 7:00 运行**"计划，并且取消选中"**运行错过的任务**"复选框。这意味着如果组织中的设备在星期五关闭，例如在下午 6:30 关闭，设备扫描任务将永远不会运行。在这种情况下，您需要手动设置组扫描任务。

管理客户端设备

该部分说明如何管理管理组中的设备。

Settings of a managed device

To view the settings of a managed device:

1. In the main menu, go to 资产(设备) → 受管理设备.

   The list of managed devices is displayed.

2. In the list of managed devices, click the link with the name of the required device.

The properties window of the selected device is displayed.

The following tabs are displayed in the upper part of the properties window representing the main groups of the settings:

- 常规

This tab comprises the following sections:

- The 常规 section displays general information about the client device. Information is provided on the basis of data received during the last synchronization of the client device with the Administration Server:
  - 名称

    In this field, you can view and modify the client device name in the administration group.
  - 描述

    In this field, you can enter an additional description for the client device.
  - 设备状态

    Status of the client device assigned on the basis of the criteria defined by the administrator for the status of anti-virus protection on the device and the activity of the device on the network.
  - 设备所有者

    Name of the device owner. You can assign or remove a user as a device owner by clicking the 管理设备所有者 link.
  - 完整组名称

    Administration group, which includes the client device.
  - 反病毒数据库上次更新

    Date the anti-virus databases or applications were last updated on the device.
  - 连接到管理服务器

    Date and time Network Agent installed on the client device last connected to the Administration Server.
  - 上一次可见

    Date and time the device was last visible on the network.
  - 网络代理版本

    Version of the installed Network Agent.
  - 创建日期

Date of the device creation within Kaspersky Security Center Linux.

- 不断开与管理服务器的连接

  If this option is enabled, continuous connectivity between the managed device and the Administration Server is maintained. You may want to use this option if you are not using push servers, which provide such connectivity.

  If this option is disabled and push servers are not in use, the managed device only connects to the Administration Server to synchronize data or to transmit information.

  The maximum total number of devices with the 不断开与管理服务器的连接 option selected is 300.

  This option is disabled by default on managed devices. This option is enabled by default on the device where the Administration Server is installed and stays enabled even if you try to disable it.

- The 网络 section displays the following information about the network properties of the client device:
  - IP 地址

    Device IP address.

  - Windows 域

    Workgroup that contains the device.

  - DNS 名称

    Name of the DNS domain of the client device.

  - NetBIOS 名称

    Name of the client device.

  - IPv6 地址
- The 系统 section provides information about the operating system installed on the client device:
  - 操作系统
  - CPU 架构
  - 设备名称
  - 虚拟机类型

    The virtual machine manufacturer.

  - 作为 VDI 一部分的动态虚拟机

This row displays whether the client device is a dynamic virtual machine as part of VDI.

- The 保护 section provides the following information about the current status of anti-virus protection on the client device:
  - 可见

    Visibility status of the client device.

  - 设备状态

    Status of the client device assigned on the basis of the criteria defined by the administrator for the status of anti-virus protection on the device and the activity of the device on the network.

  - 状态描述

    Status of the client device protection and connection to Administration Server.

  - 保护状态

    This field shows the current status of real-time protection on the client device.

    When the status changes on the device, the new status is displayed in the device properties window only after the client device is synchronized with the Administration Server.

  - 上一次全盘扫描

    Date and time the last malware scan was performed on the client device.

  - 检测到的病毒

    Total number of threats detected on the client device since installation of the anti-virus application (first scan), or since the last reset of the threat counter.

  - 清除失败的对象

    Number of unprocessed files on the client device.

    This field ignores the number of unprocessed files on mobile devices.

  - 磁盘加密状态

    The current status of file encryption on the local drives of the device. For a description of the statuses, see the Kaspersky Endpoint Security for Windows Help.

    Files can be only encrypted on the managed devices on which Kaspersky Endpoint Security for Windows is installed.

- The 应用程序定义的设备状态 section provides information about the device status that is defined by the managed application installed on the device. This device status can differ from the one defined by Kaspersky Security Center Linux.

- 应用程序

  This tab lists all Kaspersky applications installed on the client device. You can click the application name to view general information about the application, a list of events that have occurred on the device, and the application settings.

- 活动策略和策略配置文件

  This tab lists the policies and policy profiles which are currently active on the managed device.

- 任务

  In the 任务 tab, you can manage client device tasks: view the list of existing tasks, create new ones, remove, start, and stop tasks, modify their settings, and view execution results. The list of tasks is provided based on data received during the last session of client synchronization with the Administration Server. The Administration Server requests the task status details from the client device. If connection is not established, the status is not displayed.

- 事件

  The 事件 tab displays events logged on the Administration Server for the selected client device.

- 安全问题

  In the 安全问题 tab, you can view, edit, and create security issues for the client device. Security issues can be created either automatically, through managed Kaspersky applications installed on the client device, or manually by the administrator. For example, if some users regularly move malware from their removable drives to devices, the administrator can create a security issue. The administrator can provide a brief description of the case and recommended actions (such as disciplinary actions to be taken against a user) in the text of the security issue, and can add a link to the user or users.

  A security issue for which all of the required actions have been taken is called *processed*. The presence of unprocessed security issues can be chosen as the condition for a change of the device status to *Critical* or *Warning*.

  This section contains a list of security issues that have been created for the device. Security issues are classified by severity level and type. The type of a security issue is defined by the Kaspersky application, which creates the security issue. You can highlight processed security issues in the list by selecting the check box in the **Processed** column.

- 标签

  In the 标签 tab, you can manage the list of keywords that are used for finding client devices: view the list of existing tags, assign tags from the list, configure auto-tagging rules, add new tags and rename old tags, and remove tags.

- 高级

This tab comprises the following sections:

- 应用程序注册表. In this section, you can view the registry of applications installed on the client device and their updates; you can also set up the display of the applications registry.

  Information about installed applications is provided if Network Agent installed on the client device sends required information to the Administration Server. You can configure sending of information to the Administration Server in the properties window of Network Agent or its policy, in the 存储库 section.

  Clicking an application name opens a window that contains the application details and a list of the update packages installed for the application.

- 可执行文件. This section displays executable files found on the client device.

- 分发点. This section provides a list of distribution points with which the device interacts.

  - 导出到文件

    Click the **Export to file** button to save to a file a list of distribution points with which the device interacts. By default, the application exports the list of devices to a CSV file.

  - 属性

    Click the **Properties** button to view and configure the distribution point with which the device interacts.

- 硬件注册表. In this section, you can view information about hardware installed on the client device.

- 远程诊断. In this section, you can perform remote diagnostics of client devices.

创建管理组

安装 Kaspersky Security Center 后，管理组层次结构仅包含一个名为“**受管理设备**”的管理组。当创建管理组层次结构时，您可以将设备和虚拟机添加到“**受管理设备**”组，并添加嵌套组（请参见下图）。

查看管理组层次结构

要创建管理组，请执行以下操作：

1. 在主菜单中，转到“**资产(设备)**” → “**组层级**”。

2. 在管理组结构中，选择要包括新管理组的管理组。

3. 单击“**添加**”按钮。

4. 在打开的“**新管理组名称**”窗口中，输入组的名称，然后单击“**添加**”按钮。

一个具有指定名称的新管理组将出现在管理组层次结构中。

要创建管理组结构：

1. 在主菜单中，转到“**资产(设备)**” → “**组层级**”。

2. 单击“**导入**”按钮。

新管理组结构向导启动。遵照向导的说明。

设备移动规则

建议通过*设备移动规则*自动分配设备到管理组。设备移动规则由三个主要部分组成：名称、执行条件（带设备属性的逻辑表达式）和目标管理组。如果设备属性满足规则执行条件，则规则移动设备到目标管理组。

所有设备移动规则都有优先级。管理服务器检查设备属性以查看它们是否满足每条规则的执行条件（升序优先级）。如果设备属性满足某条规则的执行条件，设备被移动到目标组，至此规则处理在该设备上完成。如果设备属性满足多个规则的条件，设备被移动到具有高优先级的规则的目标组。

设备移动规则可以被间接创建。例如，在安装包或远程安装任务的属性中，您可以指定安装网络代理后设备必须被移动到的管理组。而且，设备移动规则可以被 Kaspersky Security Center Linux 管理员明确创建，在**资产(设备)** → **移动规则**区域中。

默认下，设备移动规则用于设备到管理组的一次性初始分配。该规则仅将设备从未分配的设备组中移动一次。如果某个设备曾经被此规则移动，则此规则永远不会再次移动该设备，即使您手动将该设备放回未分配的设备组也是如此。这是应用移动规则的推荐方法。

您可以移动已经被分配的设备到一些管理组。为此，在规则的属性中，请清空“**仅移动不属于任何管理组的设备**”复选框。

应用移动规则到已经分配到一些管理组中的设备会显著增加管理服务器负载。

仅移动不属于任何管理组的设备复选框在自动创建的移动规则的属性中被锁定。当您添加*远程安装应用程序*任务或创建独立安装包时，会创建此类规则。

您可以创建重复影响单一设备的移动规则。

我们强烈建议您避免从一个组重复移动单一设备到另一个组(例如，为了应用特别策略到该设备，运行特别组任务，或者通过特别分发点更新设备)。

此类方案不被支持，因为它们显著增加了管理服务器负载和网络流量。这些方案也与 Kaspersky Security Center Linux 的操作原则冲突（尤其在访问权限、事件和报告方面）。必须找到其他解决方案，例如，通过使用策略配置文件、设备分类的任务、根据标准方案分配更新代理，等等。

创建设备移动规则

您可以设置设备移动规则，即自动分配设备到管理组的规则。

要创建移动规则：

1. 在主菜单中，转到**资产(设备)** → **移动规则**。
2. 单击**添加**。
3. 在打开的窗口中，在"**常规**"选项卡上指定以下信息：

- 规则名称

  输入新规则名称。
  如果您正复制规则，新规则与源规则名称相同，但是索引格式 () 被添加到名称，例如：(1)。

- 管理组

  选择要自动移动设备的管理组。

- 激活的规则

  如果启用该选项，规则被启用并在被保存后开始工作。
  如果禁用该选项，规则被创建，但不被启用。直到您启用该选项它才工作。

- 仅移动不属于任何管理组的设备

  如果启用该选项，仅未分配的设备将被移动到所选组。
  如果禁用该选项，已经属于其他管理组的设备以及未分配的设备将被移动到所选组。

- 应用规则

  您可以选择以下选项之一：
  - **对每台设备运行一次**
    规则对匹配标准的每台设备应用一次。
  - **对每台设备运行一次，然后在每次网络代理重新安装时**
    规则对匹配标准的每台设备应用一次，然后仅在网络代理被重新安装到这些设备时。
  - **持续应用规则**
    规则根据管理服务器自动设置的计划被应用（通常每几个小时）。

4. 在"**规则条件**"选项卡上，指定至少一个标准，设备将依据该标准移至管理组。
5. 单击"**保存**"。

移动规则被创建。它显示在移动规则列表。

列表上的位置越高，规则的优先级越高。要提高或降低移动规则的优先级，请使用鼠标在列表中分别向上或向下移动规则。

如果设备属性满足多个规则的条件，设备被移动到具有高优先级的规则的目标组。

复制设备移动规则

您可以复制移动规则，例如，如果您要对不同目标管理组拥有几个相同规则。

要复制现有移动规则：

1. 执行以下操作之一：
   - 在主菜单中，转到**资产(设备) → 移动规则**。
   - 在主菜单中，转到**"发现和部署 → 部署和分配 → 移动规则"**。

   移动规则列表被显示。
2. 选择您要复制的规则旁边的复选框。
3. 单击**复制**。
4. 在打开的窗口中的**"常规"**选项卡上更改以下信息或不进行任何更改（如果您仅想复制规则而不更改其设置）：
   - 规则名称

     输入新规则名称。
     如果您正复制规则，新规则与源规则名称相同，但是索引格式 () 被添加到名称，例如：(1)。
   - 管理组

     选择要自动移动设备的管理组。
   - 激活的规则

     如果启用该选项，规则被启用并在被保存后开始工作。
     如果禁用该选项，规则被创建，但不被启用。直到您启用该选项它才工作。
   - 仅移动不属于任何管理组的设备

     如果启用该选项，仅未分配的设备将被移动到所选组。
     如果禁用该选项，已经属于其他管理组的设备以及未分配的设备将被移动到所选组。
   - 应用规则

您可以选择以下选项之一：

- **对每台设备运行一次**
  规则对匹配标准的每台设备应用一次。
- **对每台设备运行一次，然后在每次网络代理重新安装时**
  规则对匹配标准的每台设备应用一次，然后仅在网络代理被重新安装到这些设备时。
- **持续应用规则**
  规则根据管理服务器自动设置的计划被应用（通常每几个小时）。

5. 在“**规则条件**”选项卡上，为您希望自动移动的设备指定至少一个标准。
6. 单击“**保存**”。

新移动规则被创建。它显示在移动规则列表。

设备移动规则的条件

当创建或复制将客户端设备移动到管理组的规则时，在“**规则条件**”选项卡上设置移动设备的条件。要确定移动哪些设备，可以使用以下标准：

- 分配给客户端设备的标签。
- 网络参数。例如，您可以移动具有指定范围内 IP 地址的设备。
- 安装在客户端设备上的受管理应用程序，例如网络代理或管理服务器。
- 虚拟机，即客户端设备。

您可以在下面找到有关如何在设备移动规则中指定此信息的说明。

如果在规则中指定多个条件，AND 逻辑运算符将生效并且所有条件同时适用。如果不选择任何选项或将某些字段留空，则此类条件不适用。

标签选项卡

在该选项卡上，可以基于先前添加到客户端设备描述的设备标签配置设备移动规则。为此，请选择所需标签。此外，还可以启用以下选项：

- 应用到没有指定标签的设备

  如果启用此选项，则具有指定标签的所有设备都将从设备移动规则中排除。如果禁用此选项，则设备移动规则应用于具有所有选定标签的设备。

  默认情况下已禁用该选项。

- 如果至少一个指定的标签匹配则应用

如果启用此选项，则设备移动规则将应用于具有至少一个选定标签的客户端设备。如果禁用此选项，则设备移动规则应用于具有所有选定标签的设备。

默认情况下已禁用该选项。

网络选项卡

在此选项卡上，可以指定设备移动规则考虑的设备的网络数据：

- 设备的 DNS 名称

  要移动的客户端设备的 DNS 域名。如果网络包含 DNS 服务器，请填写此字段。

  如果为您用于 Kaspersky Security Center Linux 的数据库设置了区分大小写的排序规则，请在指定设备 DNS 名称时保持大小写。否则，设备移动规则将不起作用。

- DNS 域

  设备移动规则应用于指定主 DNS 后缀中包含的所有设备。如果网络包含 DNS 服务器，请填写此字段。

- IP 范围

  如果启用此选项，您可以输入应该包括相关设备的 IP 范围的初始和最终 IP 地址。

  默认情况下已禁用该选项。

- 用于连接管理服务器的 IP 地址

  如果启用此选项，则可以设置客户端设备用于连接到管理服务器的 IP 地址。为此，请指定包含所有必要 IP 地址的 IP 范围。

  默认情况下已禁用该选项。

- 连接配置文件已更改

  您可以选择以下值之一：

  - **是**。设备移动规则仅应用于连接配置文件已更改的客户端设备。
  - **否**。设备移动规则仅应用于连接配置文件未更改的客户端设备。
  - **未选择值**。条件不适用。

- 由不同管理服务器管理

您可以选择以下值之一：

- **是**。设备移动规则仅应用于由其他管理服务器管理的客户端设备。这些服务器与配置了设备移动规则的服务器不同。
- **否**。设备移动规则仅应用于当前管理服务器管理的客户端设备。
- **未选择值**。条件不适用。

应用程序选项卡

在此选项卡上，可以根据客户端设备上安装的受管理应用程序和操作系统来配置设备移动规则：

- 网络代理已安装

  您可以选择以下值之一：
  - **是**。设备移动规则仅应用于安装了网络代理的客户端设备。
  - **否**。设备移动规则仅应用于未安装网络代理的客户端设备。
  - **未选择值**。条件不适用。

- 应用程序

  指定应在客户端设备上安装哪些受管理应用程序，以便设备移动规则应用于这些设备。例如，您可以选择**Kaspersky Security Center 15 网络代理**或**Kaspersky Security Center 15 管理服务器**。

  如果不选择任何受管理应用程序，则条件不适用。

- 操作系统版本

  您可以根据操作系统版本剔除客户端设备。为此，请指定应在客户端设备上安装的操作系统。结果是，设备移动规则应用于具有选定操作系统的客户端设备。

  如果不启用此选项，则条件不适用。默认情况下，禁用该选项。

- 操作系统 bit 大小

您可以按操作系统位数来剔除客户端设备。在"**操作系统 bit 大小**"字段中，您可以选择以下值之一：

- **未知**
- **x86**
- **AMD64**
- **IA64**

要检查客户端设备的操作系统位数：

1. 在主菜单中，转到**资产(设备)** → **受管理设备**区域。
2. 在右侧单击**列设置**按钮（ ）。
3. 选择**操作系统 bit 大小**选项，然后单击**保存**按钮。
   之后，将显示每个受管理设备的操作系统位数。

- 操作系统服务包版本

在该字段中，您可以指定操作系统的更新包版本（采用 *X.Y* 格式），这将决定将移动规则应用到设备的方式。默认情况下，不指定版本值。

- 用户证书

您可以选择以下值之一：

- **已安装**。设备移动规则仅应用于具有移动证书的移动设备。
- **未安装**。设备移动规则仅应用于没有移动证书的移动设备。
- **未选择值**。条件不适用。

- 操作系统内部版本

该设置仅应用到 Windows 操作系统。

您可以指定所选操作系统是否必须具有相等、更早或更晚的版本号。您也可以为除指定内部版本号外的所有内部版本号配置设备移动规则。

- 操作系统发布号

该设置仅应用到 Windows 操作系统。

您可以指定所选操作系统必须具有相同、更早还是更晚的版本号。您也可以为除指定版本号外的所有版本号配置设备移动规则。

虚拟机选项卡

在该选项卡上，可以根据客户端设备是否是虚拟机或虚拟桌面基础架构 (VDI) 的一部分来配置设备移动规则：

- 这是一台虚拟机

  在该下拉列表中，可以选择以下选项之一：
  - **N/A**。条件不适用。
  - **否**。移动非虚拟机设备。
  - **是**。移动虚拟机设备。

- 虚拟机类型
- 虚拟桌面基础架构的一部分

  在该下拉列表中，可以选择以下选项之一：
  - **N/A**。条件不适用。
  - **否**。移动不属于 VDI 的设备。
  - **是**。移动属于 VDI 的设备。

域控制器选项卡

在此选项卡上，您可以指定需要移动域组织单元中包含的设备。您还可以从指定域组织单元的所有子组织单元移动设备：

- 设备包含在以下组织单元中

  如果启用此选项，则设备移动规则将应用于该选项下的列表中指定的域控制器组织单元中的设备。
  默认情况下已禁用该选项。

- 包括子组织单元

  如果启用此选项，选择范围将包括指定域控制器组织单元的所有子组织单元中的设备。
  默认情况下已禁用该选项。

- 将设备从子单元移动到对应子组
- 创建对应于新检测到设备的容器的子组
- 删除域中不存在的子组
- 设备包含在以下域安全组中

如果启用此选项，设备移动规则将应用于该选项下的列表中指定的域安全组中的设备。
默认情况下已禁用该选项。

Adding devices to an administration group manually

You can move devices to administration groups automatically by creating device moving rules or manually by moving devices from one administration group to another or by adding devices to a selected administration group. This section describes how to manually add devices to an administration group.

To add manually one or more devices to a selected administration group:

1. In the main menu, go to 资产(设备) → 受管理设备.
2. Click the **Current path:** `<current path>` link above the list.
3. In the window that opens, select the administration group to which you want to add the devices.
4. Click the 添加设备 button.
   The Move devices wizard starts.
5. Make a list of the devices that you want to add to the administration group.

   You can add only devices for which information has already been added to the Administration Server database either upon connection of the device or after device discovery.

   Select how you want to add devices to the list:

   - Click the 添加设备 button, and then specify the devices in one of the following ways:
     - Select devices from the list of devices detected by the Administration Server.
     - Specify a device IP address or an IP range.
     - Specify a device DNS name.

       The device name field must not contain space characters, backspace characters, or the following prohibited characters: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %
   - Click the 从文件导入设备 button to import a list of devices from a .txt file. Each device address or name must be specified on a separate line.

     The file must not contain space characters, backspace characters, or the following prohibited characters: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %
6. View the list of devices to be added to the administration group. You can edit the list by adding or removing devices.

7. After making sure that the list is correct, click the 下一步 button.

The wizard processes the device list and displays the result. The successfully processed devices are added to the administration group and are displayed in the list of devices under names generated by Administration Server.

Moving devices or clusters to an administration group manually

You can move devices from one administration group to another, or from the group of unassigned devices to an administration group.

You can also move clusters or server arrays from one administration group to another. When you move a cluster or server array to another group, all of its nodes move with it, because a cluster and any of its nodes always belong to the same administration group. When you select a single cluster node on the 设备 tab, the 移动到组 button becomes unavailable.

To move one or several devices or clusters to a selected administration group:

1. Open the administration group from which you want to move the devices. To do this, perform one of the following:
   - To open an administration group, in the main menu, go to 资产(设备) → 受管理设备, click the path link in the 当前路径 field, and select an administration group in the left-side pane that opens.
   - To open the 未分配的设备 group, in the main menu, go to 发现和部署 → 未分配的设备.
2. If the administration group contains clusters or server arrays, the 受管理设备 section is divided into two tabs—the 设备 tab and the 集群和服务器阵列 tab. Open the tab for the object that you want to move.
3. Select the check boxes next to the devices or clusters that you want to move to a different group.
4. Click the 移动到组 button.
5. In the hierarchy of administration groups, select the check box next to the administration group to which you want to move the selected devices or clusters.
6. Click the 移动 button.

The selected devices or clusters are moved to the selected administration group.

关于集群和服务器阵列

Kaspersky Security Center Linux 支持集群技术。如果网络代理向管理服务器发送信息确认组成服务器阵列的客户端设备上已安装该应用程序，则该客户端设备就成为一个集群节点。

如果管理组包含集群或服务器阵列，则**受管理设备**页面将显示两个选项卡：一个用于单个设备，另一个用于集群和服务器阵列。受管理设备被检测为集群节点后，集群将被作为单独对象添加到**集群和服务器阵列**选项卡。

集群或服务器阵列节点与其他受管理设备一起列在**设备**选项卡上。您可以将节点作为单个设备查看属性并执行其他操作，但不能删除集群节点或将其从集群中单独移动到另一个管理组。您只能删除或移动整个集群。

您可以对集群或服务器阵列执行以下操作：

- 查看属性
- 将集群或服务器阵列移至另一个管理组

  当您将集群或服务器阵列移动到另一个组时，其所有节点都会随之移动，因为集群及其任何节点始终属于同一管理组。
- 删除

  仅当集群或服务器阵列不在组织网络中存在时，删除该集群或服务器阵列才合理。如果集群在您的网络上仍然可见，并且网络代理和卡巴斯基安全应用程序仍然安装在集群节点上， Kaspersky Security Center Linux 会自动将已删除的集群及其节点返回到受管理设备列表。

集群或服务器阵列的属性

要查看集群或服务器阵列的设置：

1. 在主菜单中，转到**资产(设备) → 受管理设备 → 集群和服务器阵列**。

   集群和服务器阵列的列表将显示。
2. 单击所需集群或服务器阵列的名称。

所选集群或服务器阵列的属性窗口将显示。

常规

常规部分显示有关集群或服务器阵列的常规信息。信息基于上一次集群节点与管理服务器之间的同步接收的数据来提供：

- 名称
- 描述
- Windows 域

  Windows 域或工作组，包含集群或服务器阵列。
- NetBIOS 名称

  集群或服务器阵列的 Windows 网络名称。
- DNS 名称

  集群或服务器阵列的 DNS 域名称。

任务

在“任务”选项卡中，您可以管理分配给集群或者服务器阵列的任务：查看现有任务列表；创建新任务；删除、启动和停止任务；修改任务设置；查看执行结果。列出的任务与安装在集群节点上的卡巴斯基安全应用程序相关。Kaspersky Security Center Linux 从集群节点接收任务列表和任务状态详细信息。如果未建立连接，则不显示状态。

节点

此选项卡显示集群或服务器阵列中包含的节点列表。您可以单击节点名称来查看设备属性窗口。

卡巴斯基应用程序

属性窗口还可能包含其他选项卡，其中包含与集群节点上安装的卡巴斯基安全应用程序相关的信息和设置。

分发点和连接网关的调整

Kaspersky Security Center Linux 中的管理组结构执行以下功能：

- 设置策略范围
  将相关设置应用到设备还有一种方式：使用*策略配置文件*。
- 设置组任务范围
  还有一个不基于管理组层级定义组任务范围的方法：使用设备分类的任务和特定设备的任务。
- 设置设备、虚拟管理服务器和从属管理服务器的访问权限。
- 分配分发点

当建立管理组结构时，您必须考虑到组织网络的拓扑以便最优分配分发点。分发点的最优分发允许您在企业网络中保存流量。

根据组织图表和网络拓扑，以下标准配置可以被应用到管理组结构：

- 单一办公室
- 多个小远程分办公室

作为分发点的设备必须被保护，包括物理保护，以防范非授权的访问。

分发点的标准配置：单一办公室

在标准“单一办公室”配置中，所有设备都在组织网络中，因此它们能看见彼此。组织网络可能包含几部分(网络或网段)，由窄通道连接。

有以下构建管理组结构的方法：

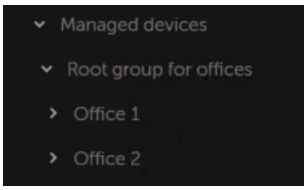
- 构建管理组结构涉及到网络拓扑。管理组结构可能不精确反映网络拓扑。网络各部分之间以及特定管理组相互匹配。您可以使用分发点自动分配或手动分配它们。

- 不考虑网络拓扑而构建管理组结构。此种情况下，您必须禁用分发点自动分配，然后为网络中每个部分的根管理组分配一个或几个设备作为分发点，例如为“**受管理设备**”组。所有分发点将处于相同级别，并将掌控组织网络中所有设备的相同范围。此种情况下，每个网络代理都将连接到具有最短路由的分发点。分发点的路由可以使用 tracert 使用工具跟踪。

分发点的标准配置：多个小远程办公室

该标准配置可用于多个小型远程办公室，它们可能通过互联网与总部联络。每个远程办公室都位于 NAT 之外，就是说，从一个远程办公室到另一个远程办公室的连接是不可能的，因为办公室是彼此隔离的。

配置必须在管理组中体现：必须为每个远程办公室创建各自的管理组(下图中的组**办公室 1**和**办公室 2**)。



远程办公室包含在管理组结构

必须指定一个或多个分发点给每个办公室的对应管理组。分发点必须是远程办公室中具有足够剩余磁盘空间的设备。部署在**办公室 1**组的设备，例如，将访问分配到**办公室 1**管理组的分发点。

如果一些用户在办公室之间移动他们的便携电脑，您必须在远程办公室选择两个或更多设备(除了现有的分发点)并分配它们作为等级管理组的分发点(上图中**办公室根组**)。

例如：便携式电脑部署在**办公室 1**管理组，然后被移动到对应于**办公室 2** 管理组的办公室。在移动便携式电脑后，网络代理试图访问分配到**办公室 1**组的分发点，但是那些分发点不可用。然后，网络代理开始尝试访问分配到**办公室根组**的分发点。因为远程办公室是彼此隔离的，尝试访问分配到**办公室根组**管理组的分发点仅在网络代理尝试访问**办公室 2** 组中的分发点时才会成功。就是说，便携式电脑将保持在原始办公室对应的管理组，但是将使用它当时所在办公室的分发点。

计算分发点的数量和配置

网络包含越多的客户端设备，就需要越多的分发点。我们建议您禁用分发点的自动分配。当分发点的自动分配被启用时，如果客户端设备数量很大，管理服务器就分配分发点并定义其配置。

使用单独分配的分发点

如果您计划使用特定设备作为分发点(就是，单独分配的服务器)，您可以不使用分发点的自动分配。此种情况下，确保您要分配为分发点的设备具有足够的剩余磁盘空间卷，不定期关闭，且禁用了睡眠模式。

网络中基于网络设备数量被专门分配的包含单一网段的分发点的数量

网段中的客户端设备的数量	分发点数量
少于 300	0（不分配分发点）
大于 300	可接受：(N/10,000 + 1)，建议：(N/5,000 + 2)，N 是网络设备数量

网络中基于网络设备数量被专门分配的包含多个网段的分发点的数量

每个网段中的客户端设备的数量	分发点数量

少于 10	0（不分配分发点）
10–100	1
大于 100	可接受：(N/10,000 + 1)，建议：(N/5,000 + 2)，N 是网络设备数量

使用标准客户端设备（工作站）作为分发点

如果您计划使用标准客户端设备（就是，工作站）作为分发点，我们建议您按照所示分配分发点（参见下表），以便避免通信渠道和管理服务器过载。

网络中基于网络设备数量作为分发点工作的包含单一网段的工作站的数量

网段中的客户端设备的数量	分发点数量
少于 300	0（不分配分发点）
大于 300	(N/300 + 1)，N 是网络设备数量；至少有三台分发点

网络中基于网络设备数量作为分发点工作的包含多个网段的工作站的数量

每个网段中的客户端设备的数量	分发点数量
少于 10	0（不分配分发点）
10–30	1
31–300	2
大于 300	(N/300 + 1)，N 是网络设备数量；至少有三台分发点

如果分发点被关闭(或由于某些原因不可用)，其范围内的受管理设备可以访问管理服务器以更新。

自动分配分发点

我们建议您自动分配分发点。此种情况下，Kaspersky Security Center Linux 将自行选择哪个设备要被分配为分发点。

要自动分配分发点：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ()。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**分发点**”区域。
3. 选择“**自动分配分发点**”选项。

   如果自动指派设备做为分发点被启用，您无法手动配置分发点，也不能编辑分发点列表。

4. 单击“**保存**”按钮。

管理服务器便自动指派和配置分发点。

手动分配分发点

Kaspersky Security Center Linux 允许您手动指定设备做为分发点。

我们建议您自动分配分发点。此种情况下，Kaspersky Security Center Linux 将自行选择哪个设备要被分配为分发点。然后，如果您由于一些原因必须不自动分配分发点（例如，如果您要使用单独分配的服务器），您可以在计算数量和配置后手动分配分发点。

作为分发点的设备必须被保护，包括物理保护，以防范非授权的访问。

要手动指派设备做为分发点：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ()。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**分发点**”区域。
3. 选择“**手动分配分发点**”选项。
4. 单击“**分配**”按钮。
5. 选择您要制作分发点的设备。
   选择设备时，请牢记分发点的操作功能以及设备做为分发点的需求。
6. 选择您要包含在所选分发点范围的管理组。
7. 单击“**确定**”按钮。
   您添加的分发点将显示在“**分发点**”区域的分发点列表中。
8. 在列表中单击新添加的分发点以打开其属性窗口。
9. 在属性窗口中配置分发点：
   - **常规**区域中包含用于设定分发点与客户端设备进行交互的设置。
     - SSL 端口

       客户端设备与分发点之间，使用 SSL 进行安全连接的 SSL 端口号。
       默认情况下使用端口 13000。

     - 使用多点传送

       如果启用此选项，将使用 IP 多点传送自动向组内的客户端设备上分发安装包。
       IP 多点传送减少了将应用程序从安装包安装到一组客户端设备所需的时间，但是增加了在将应用程序安装到单个客户端设备时的安装时间。

     - IP 多点传送地址

用于多点传送的 IP 地址。您可以定义范围是 224.0.0.0 – 239.255.255.255 的 IP 地址

默认情况下，Kaspersky Security Center Linux 自动分配一个在给定范围内的唯一 IP 多播地址。

- IP 多点传送端口号

  IP 多点传送的端口号。

  默认情况下，端口号指定为 15001。如果运行管理服务器的设备指定为分发点，端口 13001 默认用于 SSL 连接。

- 远程设备的分发点地址

  远程设备连接到分发点所用的 IPv4 地址。

- 部署更新

  更新被从以下来源分发到受管理设备：

  - 此分发点（如果启用此选项）。
  - 其他分发点、管理服务器或 Kaspersky 更新服务器（如果禁用此选项）。

  如果您使用分发点来部署更新，则可以节省流量，因为您减少了下载次数。此外，您可以减轻管理服务器上的负载并在分发点之间重新定位负载。你可以计算分发点的数量以便网络优化流量和负载。

  如果禁用此选项，管理服务器上的更新下载和加载次数可能会增加。默认情况下已启用该选项。

- 部署安装包

  安装包被从以下来源分发到受管理设备：

  - 此分发点（如果启用此选项）。
  - 其他分发点、管理服务器或 Kaspersky 更新服务器（如果禁用此选项）。

  如果使用分发点部署安装包，您可以节省流量，因为减少了下载次数。此外，您可以减轻管理服务器上的负载并在分发点之间重新定位负载。你可以计算分发点的数量以便网络优化流量和负载。

  如果禁用此选项，管理服务器上的安装包下载和加载次数可能会增加。默认情况下已启用该选项。

- 运行推送服务器

  在 Kaspersky Security Center Linux 中，分发点可以用作通过移动协议管理的设备和由网络代理管理的设备的推送服务器。例如，如果您希望能强制 KasperskyOS 设备与管理服务器同步，则必须启用推送服务器。推送服务器与启用该推送服务器的分发点具有相同的受管理设备范围。如果为同一个管理组分配了多个分发点，则可以在每个分发点上都启用推送服务器。在这种情况下，管理服务器会平衡分发点之间的负载。

- 推送服务器端口

  推送服务器的端口号。您可以指定任何未占用的端口号。

- 在“**范围**”区域中，指定分发点将向其分发更新的管理组。
- 在“**更新源**”区域中，可以选择分发点的更新源：
  - 更新源

    选择分发点的更新源：
    - 要允许分发点从管理服务器接收更新，请选择“**从管理服务器检索**”。
    - 要允许分发点使用任务接收更新，请选择“**使用更新下载任务**”，然后指定“*将更新下载至分发点存储库*”任务：
      - 如果设备上已存在此类任务，请在列表中选择该任务。
      - 如果设备上尚不存在此类任务，请单击“**创建任务**”链接创建任务。“新任务向导”启动。遵照向导的说明操作。
  - 下载差异文件

    该选项启用下载 diff 文件功能。

    默认情况下已启用该选项。
- 在**互联网连接设置**子区域，您可以指定互联网连接设置：
  - 使用代理服务器

    如果选择该选框，您可以在输入字段中配置代理服务器连接。
    默认情况下已清除该选框。
  - 代理服务器地址

    代理服务器地址。
  - 端口号

    用于连接的端口号。
  - 对本地地址不使用代理服务器

    如果启用此选项，将不使用代理服务器连接本地网络的设备。
    默认情况下已禁用该选项。
  - 代理服务器身份验证

    如果选择该选框，您可以在输入字段中为代理服务器身份验证指定凭证。
    默认情况下已清除该选框。

- 用户名

  建立连接代理服务器的用户账户。

- 密码

  任务运行时使用的账户的密码。

- 在“**KSN 代理**”区域，您可以配置应用程序使用分发点从受管理设备转发 KSN 请求：

  - 在分发点端启用 KSN 代理

    KSN 代理服务运行在用作分发点的设备上。使用该功能重新分发和优化网络流量。

    分发点发送列在卡巴斯基安全网络声明中的 KSN 统计信息到 Kaspersky。

    默认情况下已禁用该选项。启用该选项仅在**使用管理服务器作为代理服务器** 和 **我同意使用卡巴斯基安全网络**选项在管理服务器属性窗口中被启用时起作用。

    您可以分配活动被动集群节点到分发点并在该节点上启用 KSN 代理服务器。

  - 转发 KSN 请求到管理服务器

    分发点从受管理设备转发 KSN 请求到管理服务器。

    默认情况下已启用该选项。

  - 通过互联网直接访问 KSN 云/KPSN

    分发点从受管理设备转发 KSN 请求到 KSN 云或 KPSN。分发点本身上生成的 KSN 请求也直接发送到 KSN 云或 KPSN。

  - 当连接到 KPSN 时忽略代理服务器设置

    如果您在分发点属性或网络代理策略中配置了代理服务器设置，但您的网络架构要求您直接使用 KPSN，则启用此选项。否则，从受管理应用程序的请求无法到达 KPSN。

    如果您选择“**通过互联网直接访问 KSN 云/KPSN**”选项，则此选项可用。

  - 端口

    受管理设备将用于连接到 KSN 代理服务器的 TCP 端口号。默认端口号是 13111。

  - 使用 UDP 端口

    如果需要受管理设备通过 UDP 端口连接到 KSN 代理，则启用“**使用 UDP 端口**”选项并指定 UDP 端口号。默认情况下已启用该选项。

  - UDP 端口

受管理设备将用于连接到 KSN 代理服务器的 UDP 端口号。连接到 KSN 代理的默认 UDP 端口是 15111。

- 在“连接网关”区域中，可以配置分发点，充当网络代理实例和管理服务器之间连接的网关：
  - 连接网关

    如果由于您的网络组织而无法在管理服务器和网络代理之间建立直接连接，您可以使用分发点作为管理服务器和网络代理之间的连接网关。

    如果您需要分发点充当网络代理和管理服务器之间的连接网关，请启用此选项。默认情况下已禁用该选项。

  - 从管理服务器建立连接到网关(如果网关位于 DMZ 中)

    如果管理服务器位于隔离区域 (DMZ) 之外，在局域网中，安装在远程设备上的网络代理无法连接到管理服务器。您可以使用分发点作为具有反向连接的连接网关（管理服务器建立到分发点的连接）。

    如果您需要将管理服务器连接到 DMZ 中的连接网关，请启用此选项。

  - 为 Kaspersky Security Center Web Console 打开本地端口

    如果您需要 DMZ 中的连接网关为位于 DMZ 中或互联网上的 Web Console 打开一个端口，请启用此选项。指定将用于从 Web Console 连接到分发点的端口号。默认端口号是 13299。

    如果启用“从管理服务器建立连接到网关(如果网关位于 DMZ 中)”选项，则此选项可用。

  - 为移动设备打开端口(仅管理服务器 SSL 身份验证)

    如果您需要连接网关为移动设备打开一个端口并指定移动设备将用于连接到分发点的端口号，请启用此选项。默认端口号是 13292。建立连接时，仅对管理服务器进行身份验证。

  - 为移动设备打开端口(双向 SSL 身份验证)

    如果您需要连接网关打开一个端口，该端口将用于管理服务器和移动设备的双向身份验证，请启用此选项。指定以下参数：

    - 移动设备将用于连接到分发点的端口号。默认端口号是 13293。
    - 移动设备将使用的连接网关的 DNS 域名。用逗号分隔域名。指定的域名将包含在分发点证书中。如果移动设备使用的域名与分发点证书中的通用名称不匹配，则移动设备不会连接到分发点。

      默认 DNS 域名是连接网关的 FQDN 名称。

- 配置分发点的域控制器轮询。
  - 域控制器轮询

您可以对域控制器启用设备发现。

如果选择**启用域控制器轮询**选项，则可以选择要轮询的域控制器并为其指定轮询计划。

如果使用 Linux 分发点，请在**轮询指定域**部分中单击**添加**，然后指定域控制器的地址和用户凭据。

如果使用 Windows 分发点，则可以选择以下选项之一：

- **轮询当前域**
- **轮询整个域森林**
- **轮询指定域**

- 按分发点配置 IP 范围轮询。
  - **IP 范围轮询**

    您可以针对 IPv4 范围和 IPv6 网络启用设备发现。

    如果启用"**启用范围轮询**"选项，则可以添加扫描范围并为其设置计划。您可以添加 IP 范围到已扫描范围列表。

    如果启用"**使用 Zeroconf 轮询 IPv6 网络**"选项，分发点将使用零配置网络（也称为 *Zeroconf*）自动轮询 IPv6 网络。在这种情况下，指定的 IP 范围将被忽略，因为分发点会轮询整个网络。如果分发点运行 Linux，则**使用 Zeroconf 轮询 IPv6 网络**选项可用。要使用 Zeroconf IPv6 轮询，您必须在分发点上安装 avahi-browse 实用程序。

- 在**高级**区域，指定分发点必须使用以存储发布数据的文件夹。
  - **使用默认的文件夹**

    如果您选择此选项，应用程序使用分发点上的网络代理安装文件夹。

  - **使用指定的文件夹**

    如果您选择该选项，则可以在下面的字段中指定该文件夹的路径。它可以是分发点上的本地文件夹，也可以是企业网络中任何设备上的目录。

    分发点上用于运行网络代理的用户账户必须具有对指定文件夹的访问权限以进行读写操作。

10. 单击"**确定**"按钮。

所选设备作为分发点运行。

修改管理组的分发点列表

您可以查看为特定管理组分配的分发点列表并通过添加或删除分发点来修改列表。

要查看和修改分配给管理组的分发点列表：

1. 在主菜单中，转到 "**资产(设备)**" → "**受管理设备**"。

2. 在受管理设备列表上方的**当前路径**字段中，单击路径链接。

3. 在打开的左侧窗格中，选择您要查看其分配的分发点的管理组。
   这将启用**分发点**菜单项。

4. 在主菜单中，转到**"资产(设备)"** → **"分发点"**。

5. 要为管理组添加新的分发点，请单击**分配**按钮。

6. 要删除分配的分发点，请从列表中选择设备并单击**取消分配**按钮。

根据于您的修改，新分发点被添加到列表或现有分发点被从列表删除。

Enabling a push server

In Kaspersky Security Center Linux, a distribution point can work as a push server for the devices managed through the mobile protocol and for the devices managed by Network Agent. For example, a push server must be enabled if you want to be able to force synchronization of KasperskyOS devices with Administration Server. A push server has the same scope of managed devices as the distribution point on which the push server is enabled. If you have several distribution points assigned for the same administration group, you can enable push server on each of the distribution points. In this case, Administration Server balances the load between the distribution points.

You might want to use distribution points as push servers to make sure that there is continuous connectivity between a managed device and the Administration Server. Continuous connectivity is needed for some operations, such as running and stopping local tasks, receiving statistics for a managed application, or creating a tunnel. If you use a distribution point as a push server, you do not have to use the **Do not disconnect from the Administration Server** option on managed devices or send packets to the UDP port of the Network Agent.

A push server supports the load of up to 50,000 simultaneous connections.

To enable push server on a distribution point:

1. In the main menu, click the settings icon ( ) next to the name of the required Administration Server.
   The Administration Server properties window opens.

2. On the 常规 tab, select the 分发点 section.

3. Click the name of the distribution point on which you want to enable the push server.
   The distribution point properties window opens.

4. On the 常规 section, enable the 运行推送服务器 option.

5. In the 推送服务器端口 field, type the port number. You can specify number of any unoccupied port.

6. In the **Address for remote hosts** field, specify the IP address or the name of the distribution point device.

7. Click the 确定 button.

The push server is enabled on the selected distribution point.

About device statuses

Kaspersky Security Center Linux assigns a status to each managed device. The particular status depends on whether the conditions defined by the user are met. In some cases, when assigning a status to a device, Kaspersky Security Center Linux takes into consideration the device's visibility flag on the network (see the table below). If Kaspersky Security Center Linux does not find a device on the network within two hours, the visibility flag of the device is set to *Not Visible*.

The statuses are the following:

- *Critical* or *Critical/Visible*
- *Warning* or *Warning/Visible*
- *OK* or *OK/Visible*

The table below lists the default conditions that must be met to assign the *Critical* or *Warning* status to a device, with all possible values.

Conditions for assigning a status to a device

Condition	Condition description	Available values
安全应用程序未安装	Network Agent is installed on the device, but a security application is not installed.	• Toggle button is on. • Toggle button is off.
检测到太多病毒	Some viruses have been found on the device by a task for virus detection, for example, the Malware scan task, and the number of viruses found exceeds the specified value.	More than 0.
实时保护级别与管理员设置的级别不同	The device is visible on the network, but the real-time protection level differs from the level set (in the condition) by the administrator for the device status.	• Stopped. • Paused. • Running.
恶意软件扫描已长时间未执行	The device is visible on the network and a security application is installed on the device, but neither the *Malware scan* task nor a local scan task has been run within the specified time interval. The condition is applicable only to devices that were added to the Administration Server database 7 days ago or earlier.	More than 1 day.
数据库已过期	The device is visible on the network and a security application is installed on the device, but the anti-virus databases have not been updated on this device within the specified time interval. The condition is applicable only to devices that were added to the Administration Server database 1 day ago or earlier.	More than 1 day.
长时间没有连接	Network Agent is installed on the device, but the device has not connected to an Administration Server within the specified time interval, because the device was turned off.	More than 1 day.
检测到活	The number of unprocessed objects in the 活动威胁 folder exceeds the	More than 0

动威胁	specified value.	items.
需要重新启动	The device is visible on the network, but an application requires the device restart longer than the specified time interval and for one of the selected reasons.	More than 0 minutes.
安装了不兼容的应用程序	The device is visible on the network, but software inventory performed through Network Agent has detected incompatible applications installed on the device.	• Toggle button is off. • Toggle button is on.
授权许可已过期	The device is visible on the network, but the license has expired.	• Toggle button is off. • Toggle button is on.
授权许可即将过期	The device is visible on the network, but the license will expire on the device in less than the specified number of days.	More than 0 days.
无效的加密状态	Network Agent is installed on the device, but the device encryption result is equal to the specified value.	• Does not comply with the policy due to the user's refusal (for external devices only). • Does not comply with the policy due to an error. • Restart is required when applying the policy. • No encryption policy is specified. • Not supported. • When applying the policy.
检测到未处理的安	Some unprocessed security issues have been found on the device. Security issues can be created either automatically, through managed Kaspersky	• Toggle button is off.

全问题	applications installed on the client device, or manually by the administrator.	• Toggle button is on.
应用程序定义的设备状态	The status of the device is defined by the managed application.	• Toggle button is off. • Toggle button is on.
设备磁盘空间不足	Free disk space on the device is less than the specified value or the device could not be synchronized with the Administration Server. The *Critical* or *Warning* status is changed to the *OK* status when the device is successfully synchronized with the Administration Server and free space on the device is greater than or equal to the specified value.	More than 0 MB.
设备已失去管理	During device discovery, the device was recognized as visible on the network, but more than three attempts to synchronize with the Administration Server failed.	• Toggle button is off. • Toggle button is on.
保护已禁用	The device is visible on the network, but the security application on the device has been disabled for longer than the specified time interval. In this case, the state of the security application is *stopped* or *failure*, and differs from the following: *starting*, *running*, or *suspended*.	More than 0 minutes.
安全应用程序没有运行	The device is visible on the network and a security application is installed on the device but is not running.	• Toggle button is off. • Toggle button is on.

Kaspersky Security Center Linux allows you to set up automatic switching of the status of a device in an administration group when specified conditions are met. When the specified conditions are met, the client device is assigned one of the following statuses: *Critical* or *Warning*. When the specified conditions are not met, the client device is assigned the *OK* status.

Different statuses may correspond to different values of one condition. For example, by default, if the 数据库已过期 condition has the **More than 3 days** value, the client device is assigned the *Warning* status; if the value is **More than 7 days**, the *Critical* status is assigned.

If you upgrade Kaspersky Security Center Linux from the previous version, the values of the 数据库已过期 condition for assigning the status to *Critical* or *Warning* do not change.

When Kaspersky Security Center Linux assigns a status to a device, for some conditions (see the Condition description column) the visibility flag is taken into consideration. For example, if a managed device was assigned the *Critical* status because the 数据库已过期 condition was met, and later the visibility flag was set for the device, then the device is assigned the *OK* status.

配置设备状态切换

您可以更改条件以将*严重*或*警告*状态分配给设备。

要启用更改设备状态到严重：

1. 通过下列方式之一打开属性窗口：
   - 在“**策略**”文件夹，在管理服务器策略的上下文菜单中选择“**属性**”。
   - 在管理组的上下文菜单中选择**属性**。
2. 在打开的**属性**窗口中，在“**区域**”窗格中选择“**设备状态**”。
3. 在右侧窗格中的“**设置状态为“严重”，如果这些被指定**”区域，从列表中选择条件旁边的复选框。

   > 您只能更改未在在父策略中锁定的设置。

4. 为所选条件设置所需的值。
   您可以为某些（但不是全部）条件设置值。
5. 单击“**确定**”。

满足指定条件时，受管理设备被分配*严重*状态。

要启用更改设备状态到警告：

1. 通过下列方式之一打开属性窗口：
   - 在“**策略**”文件夹，在管理服务器策略的上下文菜单中选择“**属性**”。
   - 在管理组的上下文菜单中选择**属性**。
2. 在打开的**属性**窗口中，在“**区域**”窗格中选择“**设备状态**”。
3. 在右侧窗格中的“**设置状态为“警告”，如果这些被指定**”区域，从列表中选择条件旁边的复选框。

   > 您只能更改未在在父策略中锁定的设置。

4. 为所选条件设置所需的值。
   您可以为某些（但不是全部）条件设置值。
5. 单击“**确定**”。

满足指定条件时，受管理设备被分配*警告*状态。

设备分类

*设备分类*是根据特定条件筛选设备的工具。您可以使用设备分类管理几个设备：例如，查看仅查看这些设备的报告或移动所有这些设备到其他组。

Kaspersky Security Center Linux 提供大量的*预定义分类*（例如，**处于"严重"状态的设备**，**保护已禁用**，**检测到活动威胁**）。预定义分类无法被删除。您也可以创建和配置附加*用户定义分类*。

在用户定义分类中，您可以设置搜索范围并选择所有设备、受管理设备、或者未分配的设备。搜索参数在条件中指定。在设备分类中，您可以创建带有不同搜索参数的多个条件。例如，您可以创建两个条件并指定不同的 IP 范围。如果多个条件被指定，分类显示满足任意条件的设备。相比之下，条件中的搜索参数是附加的。如果 IP 范围和已安装应用程序名称都被指定在一个条件，仅安装了应用程序且 IP 地址处于指定范围的设备被显示。

从设备分类中查看设备列表

Kaspersky Security Center Linux 允许您从设备分类中查看设备列表。

若要从设备分类中查看设备列表：

1. 在主菜单中，转到"**资产(设备)** → **设备分类**或者**发现和部署** → **设备分类**"区域。
2. 在分类列表中，单击设备分类的名称。
   该页面会显示一个表格，其中包含有关设备分类中包含的设备的信息。
3. 您可以按如下方式对设备表中的数据进行分组和筛选：
   - 单击设置图标 ( )，然后选择要在表中显示的列。
   - 单击筛选图标 ( )，然后在调用的菜单中指定并应用筛选条件。
     筛选出的设备表将显示。

您可以在设备分类中选择一个或多个设备，然后单击**新任务**按钮以创建将被应用于这些设备的任务。

要将设备分类中的选定设备移动到另一个管理组，请单击**移动到组**按钮，然后选择目标管理组。

Creating a device selection

To create a device selection:

1. In the main menu, go to **资产(设备)** → **设备分类**.
   A page with a list of device selections is displayed.
2. Click the **添加** button.
   The **设备分类设置** window opens.
3. Enter the name of the new selection.
4. Specify the group that contains the devices to be included in the device selection:
   - **查找任何设备**—Searching for devices that meet the selection criteria and included in the **受管理设备** or **未分配的设备** group.
   - **查找受管理设备**—Searching for devices that meet the selection criteria and included in the **受管理设备** group.

- 查找未分配的设备—Searching for devices that meet the selection criteria and included in the 未分配的设备 group.

You can enable the 包含来自从属管理服务器的数据 check box to enable searching for devices that meet the selection criteria and managed by secondary Administration Servers.

5. Click the 添加 button.
6. In the window that opens, specify conditions that must be met for including devices in this selection, and then click the 确定 button.
7. Click the 保存 button.

The device selection is created and added to the list of device selections.

Configuring a device selection

To configure a device selection:

1. In the main menu, go to 资产(设备) → 设备分类.

   A page with a list of device selections is displayed.
2. Select the relevant user-defined device selection, and click the 属性 button.

   The 设备分类设置 window opens.
3. On the 常规 tab, click the 新条件 link.
4. Specify conditions that must be met for including devices in this selection.
5. Click the 保存 button.

The settings are applied and saved.

Below are descriptions of the conditions for assigning devices to a selection. Conditions are combined by using the OR logical operator: the selection will contain devices that comply with at least one of the listed conditions.

常规

In the 常规 section, you can change the name of the selection condition and specify whether that condition must be inverted:

反转分类条件

If this option is enabled, the specified selection condition will be inverted. The selection will include all devices that do not meet the condition.

By default, this option is disabled.

网络基础架构

In the 网络 subsection, you can specify the criteria that will be used to include devices in the selection according to their network data:

- 设备名称

  Windows network name (NetBIOS name) of the device, or the IPv4 or IPv6 address.

- 域

  Displays all devices included in the specified workgroup.

- 管理组

  Displays devices included in the specified administration group.

- 描述

Text in the device properties window: in the 描述 field of the 常规 section.

To describe text in the 描述 field, you can use the following characters:

- Within a word:
  - *****. Replaces any string with any number of characters.

    Example:

    To describe words such as **Server** or **Server's**, you can enter **Server***.
  - **?.** Replaces any single character.

    Example:

    To describe phrases such as **SUSE Linux Enterprise Server 12** or **SUSE Linux Enterprise Server 15**, you can enter **SUSE Linux Enterprise Server 1?**.

    Asterisk (*****) or question mark (**?**) cannot be used as the first character in the query.
- To find several words:
  - Space. Displays all the devices whose descriptions contain any of the listed words.

    Example:

    To find a phrase that contains **Secondary** or **Virtual** words, you can include **Secondary Virtual** line in your query.
  - **+**. When a plus sign precedes a word, all search results will contain this word.

    Example:

    To find a phrase that contains both **Secondary** and **Virtual**, enter the **+Secondary+Virtual** query.
  - **-**. When a minus sign precedes a word, no search results will contain this word.

    Example:

    To find a phrase that contains **Secondary** and does not contain **Virtual**, enter the **+Secondary-Virtual** query.
  - **"<some text>"**. Text enclosed in quotation marks must be present in the text.

    Example:

    To find a phrase that contains **Secondary Server** word combination, you can enter **"Secondary Server"** in the query.

- IP 范围

  If this option is enabled, you can enter the initial and final IP addresses of the IP range in which the relevant devices must be included.

  By default, this option is disabled.

- 由不同管理服务器管理

Select one of the following values:

- 是. A device moving rule only applies to client devices managed by other Administration Servers. These Servers are different from the Server on which you configure the device moving rule.
- 否. The device moving rule only applies to client devices managed by the current Administration Server.
- **No value is selected**. The condition does not apply.

In the 域控制器 subsection, you can configure criteria for including devices into a selection based on domain membership:

- 设备在域组织单元中

  If this option is enabled, the selection includes devices from the domain organizational unit specified in the entry field.

  By default, this option is disabled.

- 该设备是域安全组成员

  If this option is enabled, the selection includes devices from the domain security group specified in the entry field.

  By default, this option is disabled.

In the 网络活动 subsection, you can specify the criteria that will be used to include devices in the selection according to their network activity:

- 作为分发点

  In the drop-down list, you can set up the criterion for including devices in the selection when performing search:

  - 是. The selection includes devices that act as distribution points.
  - 否. Devices that act as distribution points are not included in the selection.
  - **No value is selected**. The criterion will not be applied.

- 不断开与管理服务器的连接

  In the drop-down list, you can set up the criterion for including devices in the selection when performing search:

  - 已启用. The selection will include devices on which the 不断开与管理服务器的连接 check box is selected.
  - 已禁用. The selection will include devices on which the 不断开与管理服务器的连接 check box is cleared.
  - **No value is selected**. The criterion will not be applied.

- 连接配置文件已切换

  In the drop-down list, you can set up the criterion for including devices in the selection when performing search:

  - 是. The selection will include devices that connected to the Administration Server after the connection profile was switched.
  - 否. The selection will not include devices that connected to the Administration Server after the connection profile was switched.
  - **No value is selected**. The criterion will not be applied.

- 上一次连接到管理服务器

  You can use this check box to set a search criterion for devices according to the time they last connected to the Administration Server.

  If this check box is selected, in the entry fields you can specify the time interval (date and time) during which the last connection was established between Network Agent installed on the client device and the Administration Server. The selection will include devices that fall within the specified interval.

  If this check box is cleared, the criterion will not be applied.

  By default, this check box is cleared.

- 网络轮询时检测到新设备

  Searches for new devices that have been detected by network polling over the last few days.

  If this option is enabled, the selection only includes new devices that have been detected by device discovery over the number of days specified in the 检测周期 **(**天**)** field.

  If this option is disabled, the selection includes all devices that have been detected by device discovery.

  By default, this option is disabled.

- 设备可见

  In the drop-down list, you can set up the criterion for including devices in the selection when performing search:

  - 是. The application includes in the selection devices that are currently visible in the network.
  - 否. The application includes in the selection devices that are currently invisible in the network.
  - **No value is selected**. The criterion will not be applied.

设备状态

In the 受管理设备状态 subsection, you can configure criteria for including devices into a selection based on the description of the devices status from a managed application:

- 设备状态

  Drop-down list in which you can select one of the device statuses: *正常*, *严重*, or *警告*.

- 实时保护状态

  Drop-down list, in which you can select the real-time protection status. Devices with the specified real-time protection status are included in the selection.

- **Device status description**

  In this field, you can select the check boxes next to conditions that, if met, assign one of the following statuses to the device: *正常*, *严重*, or *警告*.

In the 受管理应用程序组件的状态 subsection, you can configure criteria for including devices in a selection according to the statuses of components in managed applications:

- 数据泄漏防护状态

  Search for devices by the status of Data Leakage Prevention (*设备上无数据*, *已停止*, *正在启动*, *已暂停*, *运行中*, *失败*).

- 协作服务器保护状态

  Search for devices by the status of server collaboration protection (*设备上无数据*, *已停止*, *正在启动*, *已暂停*, *运行中*, *失败*).

- 邮件服务器的反病毒保护状态

  Search for devices by the status of Mail Server protection (*设备上无数据*, *已停止*, *正在启动*, *已暂停*, *运行中*, *失败*).

- 端点传感器状态

  Search for devices by the status of the Endpoint Sensor component (*设备上无数据*, *已停止*, *正在启动*, *已暂停*, *运行中*, *失败*).

In the 影响受管理应用程序状态的问题 subsection, you can specify the criteria that will be used to include devices in the selection according to the list of possible problems detected by a managed application. If at least one problem that you select exists on a device, the device will be included in the selection. When you select a problem listed for several applications, you have the option to select this problem in all of the lists automatically.

You can select check boxes for descriptions of statuses from the managed application; upon receipt of these statuses, the devices will be included in the selection. When you select a status listed for several applications, you have the option to select this status in all of the lists automatically.

系统详情

In the 操作系统 section, you can specify the criteria that will be used to include devices in the selection according to their operating system type.

- 平台类型

If the check box is selected, you can select an operating system from the list. Devices with the specified operating systems installed are included in the search results.

- 操作系统服务包版本

  In this field, you can specify the package version of the operating system (in the *X.Y* format), which will determine how the moving rule is applied to the device. By default, no version value is specified.

- 操作系统 **bit** 大小

  In the drop-down list, you can select the architecture for the operating system, which will determine how the moving rule is applied to the device (未知, **x86**, **AMD64**, or **IA64**). By default, no option is selected in the list so that the operating system's architecture is not defined.

- 操作系统内部版本

  This setting is applicable to Windows operating systems only.

  The build number of the operating system. You can specify whether the selected operating system must have an equal, earlier, or later build number. You can also configure searching for all build numbers except the specified one.

- 操作系统发布号

  This setting is applicable to Windows operating systems only.

  The release identifier (ID) of the operating system. You can specify whether the selected operating system must have an equal, earlier, or later release ID. You can also configure searching for all release ID numbers except the specified one.

In the 虚拟机 section, you can set up the criteria to include devices in the selection according to whether these are virtual machines or part of virtual desktop infrastructure (VDI):

- 这是一台虚拟机

  In the drop-down list, you can select the following options:

  - 未定义.
  - 否. Find devices that are not virtual machines.
  - 是. Find devices that are virtual machines.

- **Virtual machine type**

In the drop-down list, you can select the virtual machine manufacturer.

This drop-down list is available if the 是 or 不重要 value is selected in the 这是一台虚拟机 drop-down list.

- 虚拟桌面基础架构的一部分

  In the drop-down list, you can select the following options:

  - 未定义.
  - 否. Find devices that are not part of Virtual Desktop Infrastructure.
  - 是. Find devices that are part of the Virtual Desktop Infrastructure (VDI).

In the 硬件注册表 subsection, you can configure criteria for including devices into a selection based on their installed hardware:

Ensure that the lshw utility is installed on Linux devices from which you want to fetch hardware details. Hardware details fetched from virtual machines may be incomplete depending on the hypervisor used.

- 设备

  In the drop-down list, you can select a unit type. All devices with this unit are included in the search results.

  The field supports the full-text search.

- 供应商

  In the drop-down list, you can select the name of a unit manufacturer. All devices with this unit are included in the search results.

  The field supports the full-text search.

- 设备名称

  The device with the specified name is included in the selection.

- 描述

  Description of the device or hardware unit. Devices with the description specified in this field are included in the selection.

  A device's description in any format can be entered in the properties window of that device. The field supports the full-text search.

- 设备制造商

  Name of the device manufacturer. Devices produced by the manufacturer specified in this field are included in the selection.

  You can enter the manufacturer's name in the properties window of a device.

- 序列号

  All hardware units with the serial number specified in this field will be included in the selection.

- 清单号

  Equipment with the inventory number specified in this field will be included in the selection.

- 用户

  All hardware units of the user specified in this field will be included in the selection.

- 位置

  Location of the device or hardware unit (for example, at the HQ or a branch office). Computers or other devices that are deployed at the location specified in this field will be included in the selection.

  You can describe the location of a device in any format in the properties window of that device.

- CPU 时钟频率 (MHz)，从

  The minimum clock rate of a CPU. Devices with a CPU that matches the clock rate range specified in the entry fields (inclusive) will be included in the selection.

- CPU 时钟频率 (MHz)，到

  The maximum clock rate of a CPU. Devices with a CPU that matches the clock rate range specified in the entry fields (inclusive) will be included in the selection.

- 虚拟 CPU 内核数量，从

  The minimum number of virtual CPU cores. Devices with a CPU that matches the range of the virtual cores number specified in the entry fields (inclusive) will be included in the selection.

- 虚拟 CPU 内核数量，到

  The maximum number of virtual CPU cores. Devices with a CPU that matches the range of the virtual cores number specified in the entry fields (inclusive) will be included in the selection.

- 硬盘卷(GB)，从

  The minimum volume of the hard drive on the device. Devices with a hard drive that matches the volume range specified in the entry fields (inclusive) will be included in the selection.

- 硬盘卷(GB)，到

  The maximum volume of the hard drive on the device. Devices with a hard drive that matches the volume range specified in the entry fields (inclusive) will be included in the selection.

- 内存大小(MB)，从

  The minimum size of the device RAM. Devices with RAM that matches the size range specified in the entry fields (inclusive) will be included in the selection.

- 内存大小(MB)

  The maximum size of the device RAM. Devices with RAM that matches the size range specified in the entry fields (inclusive) will be included in the selection.

第三方软件详情

In the 应用程序注册表 subsection, you can set up the criteria to search for devices according to applications installed on them:

- 应用程序名称

  Drop-down list in which you can select an application. Devices on which the specified application is installed, are included in the selection.

- 应用程序版本

  Entry field in which you can specify the version of selected application.

- 供应商

  Drop-down list in which you can select the manufacturer of an application installed on the device.

- 应用程序状态

  A drop-down list in which you can select the status of an application (*Installed*, *Not installed*). Devices on which the specified application is installed or not installed, depending on the selected status, will be included in the selection.

- 根据更新查找

  If this option is enabled, search will be performed using the details of updates for applications installed on the relevant devices. After you select the check box, the 应用程序名称, 应用程序版本, and 应用程序状态 fields change to 更新名称, 更新版本, and 状态 respectively.

  By default, this option is disabled.

- 不兼容安全应用程序名称

  Drop-down list in which you can select third-party security applications. During the search, devices on which the specified application is installed, are included in the selection.

- 应用程序标签

In the drop-down list, you can select the application tag. All devices that have installed applications with the selected tag in the description are included in the device selection.

- 应用到没有指定标签的设备

  If this option is enabled, the selection includes devices with descriptions that contain none of the selected tags.

  If this option is disabled, the criterion is not applied.

  By default, this option is disabled.

In the 漏洞和更新 subsection, you can specify the criteria that will be used to include devices in the selection according to their Windows Update source:

WUA 已切换到管理服务器

You can select one of the following search options from the drop-down list:

- 是. If this option is selected, the search results will include devices that receive updates through Windows Update from the Administration Server.
- 否. If this option is selected, the results will include devices that receive updates through Windows Update from another sources.

卡巴斯基应用程序详情

In the 卡巴斯基应用程序 subsection, you can configure criteria for including devices in a selection based on the selected managed application:

- 应用程序名称

  In the drop-down list, you can set a criterion for including devices in a selection when search is performed by the name of a Kaspersky application.

  The list provides only the names of applications with management plug-ins installed on the administrator's workstation.

  If no application is selected, the criterion will not be applied.

- 应用程序版本

  In the entry field, you can set a criterion for including devices in a selection when search is performed by the version number of a Kaspersky application.

  If no version number is specified, the criterion will not be applied.

- 关键更新名称

  In the entry field, you can set a criterion for including devices in a selection when search is performed by application name or by update package number.

  If the field is left blank, the criterion will not be applied.

- Application status

  A drop-down list in which you can select the status of an application (*Installed*, *Not installed*). Devices on which the specified application is installed or not installed, depending on the selected status, will be included in the selection.

- 选择模块上次更新的时间段

  You can use this option to set a criterion for searching devices by time of the last update of modules of applications installed on those devices.

  If this check box is selected, in the entry fields you can specify the time interval (date and time) during which the last update of modules of applications installed on those devices was performed.

  If this check box is cleared, the criterion will not be applied.

  By default, this check box is cleared.

- 设备通过管理服务器管理

  In the drop-down list, you can include in the selection the devices managed through Kaspersky Security Center Linux:

  - 是. The application includes in the selection devices managed through Kaspersky Security Center Linux.
  - 否. The application includes devices in the selection if they are not managed through Kaspersky Security Center Linux.
  - **No value is selected**. The criterion will not be applied.

- 安全应用程序已安装

  In the drop-down list, you can include in the selection all devices with the security application installed:

  - 是. The application includes in the selection all devices with the security application installed.
  - 否. The application includes in the selection all devices with no security application installed.
  - **No value is selected**. The criterion will not be applied.

In the 反病毒保护 subsection, you can set up the criteria for including devices in a selection based on their protection status:

- 数据库发布日期

  If this option is selected, you can search for client devices by anti-virus database release date. In the entry fields you can set the time interval, on the basis of which the search is performed.

  By default, this option is disabled.

- 数据库记录数

If this option is enabled, you can search for client devices by number of database records. In the entry fields you can set the lower and upper threshold values for anti-virus database records.

By default, this option is disabled.

- 上一次扫描

  If this check option is enabled, you can search for client devices by time of the last malware scan. In the entry fields you can specify the time period within which the last malware scan was performed.

  By default, this option is disabled.

- 检测到的威胁

  If this option is enabled, you can search for client devices by number of viruses detected. In the entry fields you can set the lower and upper threshold values for the number of viruses found.

  By default, this option is disabled.

In the 加密 subsection, you can configure the criterion for including devices in a selection based on the selected encryption algorithm:

加密算法

Advanced Encryption Standard (AES) symmetrical block cipher algorithm. In the drop-down list, you can select the encryption key size (56-bit, 128-bit, 192-bit, or 256-bit).

Available values: *AES56*, *AES128*, *AES192*, and *AES256*.

The 应用程序组件 subsection contains the list of components of those applications that have corresponding management plug-ins installed in Kaspersky Security Center Web Console.

In the 应用程序组件 subsection, you can specify criteria for including devices in a selection according to the statuses and version numbers of the components that refer to the application that you select:

- 状态

Search for devices according to the component status sent by an application to the Administration Server. You can select one of the following statuses: *N/A*, *Stopped*, *Paused*, *Starting*, *Running*, *Failed*, *Not installed*, *Not supported by license*. If the selected component of the application installed on a managed device has the specified status, the device is included in the device selection.

Statuses sent by applications:

- *Stopped*—The component is disabled and not working at the moment.
- *Paused*—The component is suspended, for example, after the user has paused protection in the managed application.
- *Starting*—The component is currently in the process of initialization.
- *Running*—The component is enabled and working properly.
- *Failed*—An error has occurred during the component operation.
- *Not installed*—The user did not select the component for installation when configuring custom installation of the application.
- *Not supported by license*—The license does not cover the selected component.

Unlike other statuses, the *N/A* status is not sent by applications. This option shows that the applications have no information about the selected component status. For example, this can happen when the selected component does not belong to any of the applications installed on the device, or when the device is turned off.

- 版本

Search for devices according to the version number of the component that you select in the list. You can type a version number, for example `3.4.1.0`, and then specify whether the selected component must have an equal, earlier, or later version. You can also configure searching for all versions except the specified one.

标签

In the 标签 section, you can configure criteria for including devices into a selection based on key words (tags) that were previously added to the descriptions of managed devices:

如果至少一个指定的标签匹配则应用

If this option is enabled, the search results will show devices with descriptions that contain at least one of the selected tags.

If this option is disabled, the search results will only show devices with descriptions that contain all the selected tags.

By default, this option is disabled.

To add tags to the criterion, click the 添加 button, and select tags by clicking the 标签 entry field. Specify whether to include or exclude the devices with the selected tags in the device selection.

- 必须被包含

  If this option is selected, the search results will display the devices whose descriptions contain the selected tag. To find devices, you can use the asterisk, which stands for any string with any number of characters.

  By default, this option is selected.

- 必须被排除

  If this option is selected, the search results will display the devices whose descriptions do not contain the selected tag. To find devices, you can use the asterisk, which stands for any string with any number of characters.

用户

In the 用户 section, you can set up the criteria to include devices in the selection according to the accounts of users who have logged in to the operating system.

- 最后一次登录系统的用户

  If this option is enabled, you can select the user account for configuring the criterion. The search results include devices on which the selected user performed the last login to the system.

- 登录系统至少一次的用户

  If this option is enabled, click the 浏览 button to specify a user account. The search results include devices on which the specified user logged in to the system at least once.

从设备分类中导出设备列表

Kaspersky Security Center Linux 允许您将设备分类中的设备信息保存并导出为 CSV 或 TXT 文件。

若要从设备分类中导出设备列表：

1. 从设备分类中打开包含设备的表格。
2. 使用以下方法之一选择要导出的设备：
   - 要选择特定设备，请选中它们旁边的复选框。
   - 要从当前表格页面选择所有设备，请选中设备表格表头中的复选框，然后选中**全选当前页面**复选框。
   - 要从表中选择所有设备，请选中设备表格表头中的复选框，然后选择**全选**复选框。
3. 单击**导出到 CSV**或**导出到 TXT**按钮。表中包含的有关所选设备的所有信息都将被导出。

请注意，如果您将筛选条件应用于设备表，则只有来自显示列的筛选数据将被导出。

在分类中从管理组中删除设备

在使用设备分类时，你可以直接从管理组中删除设备，而不是切换到包含这些设备的管理组。

要从管理组删除设备，请执行以下操作：

1. 在主菜单中，转到“**资产(设备) → 设备分类**或者**发现和部署 → 设备分类**”。
2. 在分类列表中，单击设备分类的名称。
   该页面会显示一个表格，其中包含有关设备分类中包含的设备的信息。
3. 选择要删除的设备，然后单击“**删除**”。
   所选设备即从相应管理组中删除。

设备标签

该部分描述了设备标签，提供了创建和修改它们以及手动或自动标记设备的说明。

关于设备标签

Kaspersky Security Center Linux 允许您*标记*设备。标签是设备标志，可以用于分组、描述或查找设备。分配到设备的标签可以用于创建分类、查找设备以及分发设备到管理组。

您可以手动或自动标记设备。当您要标记单个设备时可以使用手动标记。自动标记由 Kaspersky Security Center Linux 利用指定标记规则来执行。

当指定条件被满足时，设备被自动标记。单个规则对应于每个标记。规则应用到设备网络属性、操作系统、设备上安装的应用程序以及其他设备属性。例如，您可以设置规则以分配 `[CentOS]` 标签到运行 CentOS 操作系统的所有设备。然后，您可以在创建设备分类时使用该标签；这将帮助您整理所有 CentOS 设备，并给它们分配任务。

在以下情况下标签从设备上被自动删除：

- 当设备停止满足分配标签的规则的条件时。
- 当分配标签的规则被禁用或删除时。

每个管理服务器的标签列表和规则列表是独立的，包括主管理服务器和从属虚拟管理服务器。规则仅被应用到来自创建规则的相同管理服务器的设备。

创建设备标签

要创建设备标签：

1. 在主菜单中，转到“**资产(设备) → 标签 → 设备标签**“。

2. 单击**添加**。
   新标签窗口打开。
3. 在“**标签**”字段中，输入标签名称。
4. 单击“**保存**”保存设置。

新标签出现在设备标签列表。

重命名设备标签

要重命名设备标签：

1. 在主菜单中，转到“**资产(设备) → 标签 → 设备标签**“。
2. 点击您要重命名的标签名称。
   标签属性窗口打开。
3. 在“**标签**”字段中，更改标签名称。
4. 单击“**保存**”保存设置。

更新的标签出现在设备标签列表。

删除设备标签

要删除设备标签：

1. 在主菜单中，转到“**资产(设备) → 标签 → 设备标签**“。
2. 在列表中，选择您想要删除的设备标签。
3. 单击“**删除**”按钮。
4. 在打开的窗口中，单击“**是**”。

设备标签被删除。删除的标签被从其分配的所有设备上自动删除。

> 您已删除的标签不会自动从自动标记规则中删除。标签被删除后，它仅在设备第一次满足标签分配条件时被分配到新设备。

> 如果此标记由应用程序或网络代理分配给设备，则已删除的标记不会自动从设备中删除。要从您的设备中删除标签，请使用 klscflag 实用程序。

查看分配了标签的设备

要查看分配了标签的设备：

1. 在主菜单中，转到“**资产(设备)** → **标签** → **设备标签**”。
2. 单击您要查看所分配设备的标签旁边的“**查看设备**”链接。

   设备列表仅显示分配了标签的设备。

要返回设备标签列表，点击您浏览器的**后退**按钮。

查看分配到设备的标签

要查看分配到设备的标签：

1. 在主菜单中，转到 “**资产(设备)**” → “**受管理设备**”。
2. 点击您要查看其标签的设备名称。
3. 在打开的设备属性窗口中，选择“**标签**”选项卡。

   分配给所选设备的标签列表被显示。

您可以分配其他标签到设备或删除已经分配的标签。您也可以查看管理服务器上存在的所有设备标签。

手动标记设备

要手动分配标签到设备：

1. 查看分配到您要分配其他标签的设备的标签。
2. 单击**添加**。
3. 在打开的窗口中，执行以下操作之一：
   - 要创建和分配新标签，请选择“**创建新标签**”，然后指定新标签的名称。
   - 要选择现有标签，请选择“**分配现有标签**”，然后在下拉列表中选择所需标签。
4. 单击“**正常**”应用更改。
5. 单击“**保存**”保存设置。

   所选的标签被分配到设备。

从设备上删除分配的标签

要从设备上删除标签：

1. 在主菜单中，转到“**资产(设备)**” → “**受管理设备**”。
2. 点击您要查看其标签的设备名称。
3. 在打开的设备属性窗口中，选择“**标签**”选项卡。
4. 选择您要删除的条目旁边的复选框。
5. 在列表顶部，单击**取消分配标签**按钮。
6. 在打开的窗口中，单击“**是**”。

标签从设备上删除。

未分配的设备标签不被删除。如果您想，您可以手动删除它。

您不能手动删除应用程序或网络代理分配给设备的标签。要删除这些标签，请使用 klscflag 实用程序。

查看自动标记设备规则

要查看自动标记设备规则，

做以下任意：

- 在主菜单中，转到“**资产(设备)** → **标签** → **自动标记规则**”。
- 在主菜单中，转到“**资产(设备)** → **标签** → **设备标签**”，然后单击“**设置自动标记规则**”链接。
- 查看分配给设备的标签，然后单击“**设置**”按钮。

自动标记设备规则列表出现。

编辑自动标记设备规则

要编辑自动标记设备规则：

1. 查看自动标记设备规则。
2. 点击您要编辑的规则名称。

规则设置窗口打开。

3. 编辑规则的常规属性：

   a. 在“**规则名称**”字段中，更改规则名称。
   名称不能包括 256 个以上字符。

   b. 做以下任意：

   - 通过将切换按钮切换到“**规则已启用**”来启用规则。
   - 通过将切换按钮切换到“**规则已禁用**”来禁用规则。

4. 做以下任意：

   - 如果要添加新条件，请单击“**添加**”按钮，然后在打开的窗口中指定新条件的设置。
   - 如果要编辑现有条件，请单击要编辑的条件名称，然后编辑条件设置。
   - 如果要删除条件，请选中要删除的条件名称旁边的复选框，然后单击“**删除**”。

5. 在条件设置窗口中单击“**确定**”。

6. 单击“**保存**”保存设置。

编辑的规则显示在列表。

创建自动标记设备规则

要创建自动标记设备规则：

1. 查看自动标记设备规则。

2. 单击**添加**。
新规则设置窗口打开。

3. 配置规则的常规属性：

   a. 在“**规则名称**”字段中，输入规则名称。
   名称不能包括 256 个以上字符。

   b. 执行以下操作之一：

   - 通过将切换按钮切换到“**规则已启用**”来启用规则。
   - 通过将切换按钮切换到“**规则已禁用**”来禁用规则。

   c. 在“**标签**”字段中，输入新设备标签名称或从列表中选择现有设备标签之一。
   名称不能包括 256 个以上字符。

4. 在条件区域中，单击“**添加**”按钮以添加新条件。

新条件设置窗口打开。

5. 输入条件名称。

   名称不能包括 256 个以上字符。名称必须在规则内唯一。

6. 设置根据以下条件的规则触发。您可以选择多个条件。

   - **网络**—设备的网络属性，例如设备的 DNS 名称，或设备是否属于某个 IP 子网。

     如果为您用于 Kaspersky Security Center Linux 的数据库设置了区分大小写的排序规则，请在指定设备 DNS 名称时保持大小写。否则，自动标记规则将不起作用。

   - **应用程序**—设备上是否存在网络代理，操作系统类型、版本和架构。
   - **虚拟机**—设备属于特定类型的虚拟机。
   - **应用程序注册表**—设备上是否存在不同供应商的应用程序。

7. 单击“**确定**”保存更改。

   如果必要，您可以为一个规则设置多个条件。此种情况下，在满足至少一个条件时，标签将被分配到设备。

8. 单击“**保存**”保存设置。

所创建的规则被强加到被所选管理服务器管理的设备。如果设备的设置满足规则条件，标签被分配到设备。

然后，规则被应用到以下情况：

- 自动和间歇性，取决于服务器负载
- 在您编辑规则之后
- 当您手动运行规则时
- 在管理服务器检测到满足规则条件的设备设置的更改或包含此设备的组设置的更改后

您可以创建多个标记规则。如果您创建了多个标记规则且规则对应的条件同时被满足，单个设备可以被分配多个标签。您可以在设备属性中查看所有分配的标签列表。

为自动标记设备运行规则

当规则运行时，规则属性中指定的标签被分配到满足相同规则中指定条件的设备。您仅可以运行活动规则。

要为自动标记设备运行规则：

1. 查看自动标记设备规则。
2. 选择您要运行的活动规则旁边的复选框。
3. 单击**运行规则**按钮。

   所选规则被运行。

删除自动标记设备规则

要删除自动标记设备规则：

1. 查看自动标记设备规则。
2. 选择您要删除的规则旁边的复选框。
3. 单击**删除**。
4. 在打开的窗口中，单击“**删除**”。

所选规则被删除。规则属性中指定的标签从所有所分配的设备上取消分配。

未分配的设备标签不被删除。如果您想，您可以手动删除它。

Data encryption and protection

Data encryption reduces the risk of unintentional leakage of sensitive and corporate data if your laptop or hard drive is stolen or lost. Also, data encryption allows you to prevent access by unauthorized users and applications.

You can use the data encryption feature if your network includes Windows-based managed devices with Kaspersky Endpoint Security for Windows installed. In this case, you can manage the following types of encryption:

- BitLocker Drive Encryption on devices running a Windows operating system for servers
- Kaspersky Disk Encryption on devices running a Windows operating system for workstations

By using these components of Kaspersky Endpoint Security for Windows, you can, for example, enable or disable encryption, view the list of encrypted drives, or generate and view reports about encryption.

To configure encryption, define the Kaspersky Endpoint Security for Windows policy in Kaspersky Security Center Linux. Kaspersky Endpoint Security for Windows performs encryption and decryption according to the active policy. For detailed instructions on how to configure rules and for a description of encryption features, see the Kaspersky Endpoint Security for Windows Help.

Encryption management for a hierarchy of Administration Servers is currently not available in the Web Console. Use the primary Administration Server to manage encrypted devices.

You can show or hide some of the interface elements related to the encryption management feature by using the user interface settings.

Viewing the list of encrypted drives

In Kaspersky Security Center Linux, you can view details about encrypted drives and devices that are encrypted at the drive level. After the information on a drive is decrypted, the drive is automatically removed from the list.

To view the list of encrypted drives,

In the main menu, go to 操作 → 数据加密和保护 → 加密驱动器.

If the section is not on the menu, this means that it is hidden. In the user interface settings, enable the 显示数据加密和保护 option to display the section.

You can export the list of encrypted drives to a CSV or TXT file. To do this, click the 导出到 **CSV** or 导出到 **TXT** button.

Viewing the list of encryption events

When running data encryption or decryption tasks on devices, Kaspersky Endpoint Security for Windows sends Kaspersky Security Center Linux information about events of the following types:

- Cannot encrypt or decrypt a file, or create an encrypted archive, due to a lack of free disk space.
- Cannot encrypt or decrypt a file, or create an encrypted archive, due to license issues.
- Cannot encrypt or decrypt a file, or create an encrypted archive, due to missing access rights.
- The application has been prohibited from accessing an encrypted file.
- Unknown errors.

To view a list of events that occurred during data encryption on devices,

In the main menu, go to 操作 → 数据加密和保护 → 加密事件.

If the section is not on the menu, this means that it is hidden. In the user interface settings, enable the 显示数据加密和保护 option to display the section.

You can export the list of encrypted drives to a CSV or TXT file. To do this, click the 导出到 **CSV** or 导出到 **TXT** button.

Alternatively, you can examine the list of encryption events for every managed device.

To view the encryption events for a managed device:

1. In the main menu, go to 资产**(**设备**)** → 受管理设备.
2. Click on the name of a managed device.
3. On the 常规 tab, go to the 保护 section.
4. Click the 查看数据加密错误 link.

Creating and viewing encryption reports

You can generate the following reports:

- 受管理设备加密状态报告. This report provides details about the data encryption of various managed devices. For example, the report shows the number of devices to which the policy with configured encryption rules applies. Also, you can find out, for instance, how many devices need to be rebooted. The report also contains information about the encryption technology and algorithm for every device.
- 大容量存储设备加密状态报告. This report contains similar information as the report on the encryption status of managed devices, but it provides data only for mass storage devices and removable drives.
- 加密驱动器访问权限报告. This report shows which user accounts have access to encrypted drives.
- 文件加密错误报告. This report contains information about errors that occurred when the data encryption or decryption tasks were run on devices.
- 加密文件访问被阻止报告. This report contains information about blocking application access to encrypted files. This report is helpful if an unauthorized user or application tries to access encrypted files or drives.

You can generate any report in the 监控和报告 → 报告 section. Alternatively, in the 操作 → 数据加密和保护 section, you can generate the following encryption reports:

- 大容量存储设备加密状态报告
- 加密驱动器访问权限报告
- 文件加密错误报告

To generate an encryption report in the 数据加密和保护 section:

1. Make sure that you enabled the 显示数据加密和保护 option in the Interface options.
2. In the main menu, go to 操作 → 数据加密和保护.
3. Open one of the following sections:
   - 加密驱动器 generates the report on encryption status of mass storage devices or the report on rights to access encrypted drives.
   - 加密事件 generates the report on file encryption errors.
4. Click the name of the report that you want to generate.

The report generation starts.

Granting access to an encrypted drive in offline mode

A user can request access to an encrypted device, for example, when Kaspersky Endpoint Security for Windows is not installed on the managed device. After you receive the request, you can create an access key file and send it to the user. All of the use cases and detailed instructions are provided in the Kaspersky Endpoint Security for Windows Help.

To grant access to an encrypted drive in offline mode:

1. Get a request access file from a user (a file with the FDERTC extension). Follow the instructions in the Kaspersky Endpoint Security for Windows Help to generate the file in Kaspersky Endpoint Security for Windows.
2. In the main menu, go to 操作 → 数据加密和保护 → 加密驱动器.

   A list of encrypted drives appears.
3. Select the drive to which the user requested access.
4. Click the 授予移动模式设备访问权限 button.
5. In the window that opens, select the Kaspersky Endpoint Security for Windows plug-in.
6. Follow the instructions provided in the Kaspersky Endpoint Security for Windows Help (see the instructions for Kaspersky Security Center Web Console at the end of the section).

After that, the user applies the received file to access the encrypted drive and read data stored on the drive.

更改客户端设备的管理服务器

对于特定客户端设备，您可以将管理服务器更改为不同的管理服务器。为此，请使用“*更改管理服务器*”任务。

要更改管理客户端设备的管理服务器：

1. 连接至管理设备的管理服务器。
2. 创建管理服务器更改任务。

   “新任务向导”启动。遵照向导的说明操作。在新任务向导的“**新任务**”窗口中，选择“**Kaspersky Security Center 15**”应用程序和“**更改管理服务器**”任务类型。之后，指定要更改管理服务器的设备：

   - 分配任务到管理组

     任务被分配到包含在管理组中的设备。您可以指定现有组之一或者创建新组。

     例如，您可能要使用该选项运行发送消息到用户任务，如果消息针对包含在特定管理组中的设备。

   - 手动指定设备地址或从列表导入地址

     您可以指定要为其分配任务的设备的 DNS 名称、IP 地址和 IP 子网。

     您可能要使用该选项以对特定子网执行任务。例如，您可能要安装特定应用程序到会计设备，或者扫描疑似被感染子网中的设备。

   - 分配任务到设备分类

该任务被分配到设备分类中的设备。您可以指定现有分类之一。

例如，您可能要使用该选项在特定操作系统版本的设备上运行任务。

3. 运行创建的任务。

为其创建任务的客户端设备，在任务执行完毕后，将由任务设置中指定的管理服务器进行管理。

如果管理服务器支持加密和数据保护，并且您正在创建*更改管理服务器*任务，将显示警告。警告声明如果有加密数据存储在设备，在新服务器开始管理设备之后，用户将仅可以访问他之前使用过的加密数据。除此之外，将不会提供对加密数据的访问权限。有关不提供加密数据访问权限的情况的详细说明，请参见 Kaspersky Endpoint Security for Windows 帮助。

当设备显示不活动时查看和配置操作

如果组中的客户端设备不活动，您可以获取关于它的通知。您也可以自动删除此类设备。

要在组中设备显示不活动时查看或配置操作：

1. 在主菜单中，转到“**资产(设备)**” → “**组层级**”。
2. 点击所需管理组的名称。

   管理组属性窗口将开启。
3. 在属性窗口中，转到“**设置**”选项卡。
4. 在“**继承**”区域中，启用或禁用以下选项：

   - 从父组继承

     该区域的设置将从包含客户端设备的父组继承。如果启用该选项，“**网络中的设备活动**”下的设置将被锁定以阻止更改。

     该选项仅在管理组拥有父组时可用。

     默认情况下已启用该选项。

   - 在子组中强制继承设置

     该设置值将被分发到子组，但在子组的属性中这些设置被锁定。

     默认情况下已禁用该选项。
5. 在“**设备活动**”区域中，启用或禁用以下选项：

   - 当设备处于非活动状态超过指定天数时，通知管理员

如果启用该选项，管理员接收不活动设备的通知。您可以指定**设备在网络上已长时间没有活动**事件被创建的时间间隔。默认时间间隔是 7 天。

默认情况下已启用该选项。

- 当设备处于非活动状态超过指定天数时，从组中删除设备

  如果启用该选项，您可以指定设备被从组中自动移除的时间间隔。默认时间间隔是 60 天。

  默认情况下已启用该选项。

6. 点击“**保存**”。

您的更改已保存并应用。

发送消息到设备用户

要发送消息到设备用户：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。
2. 单击**添加**。

   “新任务向导”启动。
3. 在**任务类型**下拉列表中，选择**将消息发送至用户**。
4. 选择一个选项以指定管理组、设备分类或应用程序任务的设备。
5. 运行创建的任务。

任务完成后，创建的消息将被发送给选定设备用户。**将消息发送至用户**任务仅对 Windows 设备可用。

远程开启、关闭和重启客户端设备

Kaspersky Security Center Linux 允许您远程管理客户端设备：开机、关机和重启。

要远程管理客户端设备：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。
2. 单击**添加**。

   “新任务向导”启动。
3. 在“**任务类型**”下拉列表中，选择“**管理设备**”。
4. 选择一个选项以指定管理组、设备分类或应用程序任务的设备。
5. 选择命令（打开、关闭或重新启动）。（可选）为关闭和重新启动命令指定用户提示消息以及**在该时间后强制关闭阻止会话中的应用程序(分钟)**选项。

6. 运行创建的任务。

任务完成后，选定设备将执行所选命令（开启、关闭或重启）。

部署 Kaspersky 应用程序

本节介绍通过 Kaspersky Security Center Web Console 在组织中的客户端设备上部署 Kaspersky 应用程序。

方案：Kaspersky 应用程序部署

此方案说明如何通过 Kaspersky Security Center Web Console 部署 Kaspersky 应用程序。您可以使用快速启动向导和保护部署向导，或者您可以手动完成所有必要步骤。

以下应用程序可以使用 Kaspersky Security Center Web Console 进行部署：

- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Windows

阶段

Kaspersky 应用程序部署分阶段进行：

1. **下载应用程序的管理 Web 插件**

   此阶段由快速启动向导处理。如果您选择不运行向导，请手动下载插件。

2. **下载并创建安装包**

   此阶段由快速启动向导处理。

   通过快速启动向导可以下载带有管理Web 插件的安装包。如果在运行向导时未选择此选项，或者根本没有运行向导，则必须手动下载安装包。

   如果在某些设备（例如远程员工的设备）上无法通过 Kaspersky Security Center Linux 安装卡巴斯基应用程序，则可以为应用程序创建独立安装包。如果您使用独立软件包安装卡巴斯基应用程序，则不必创建和运行远程安装任务，也不必为 Kaspersky Endpoint Security for Windows 创建和配置任务。

   或者，您可以从卡巴斯基网站下载网络代理和安全应用程序的分发包。如果由于某种原因无法远程安装应用程序，您可以使用下载的分发包在本地安装应用程序。

3. **创建、配置和运行远程安装任务**

   此步骤是保护部署向导的一部分。如果您选择不运行保护部署向导，您必须手动创建该任务并手动配置它。

   您也可以为不同管理组或不同设备分类手动创建几个远程安装任务。您可以在这些任务中部署应用程序的不同版本。

   确保您网络中的所有设备均已被发现；然后运行远程安装任务。

   > 如果您想在装有 SUSE Linux Enterprise Server 15 操作系统的设备上安装网络代理，首先安装 insserv-compat 软件包以配置网络代理。

4. **创建和配置任务**

   必须配置 Kaspersky Endpoint Security 的“*更新*”任务。

   该步骤是快速启动向导的一部分：任务被使用默认设置自动创建和配置。如果您未运行向导，您必须手动创建该任务并手动配置它。如果您使用快速启动向导，请确保任务的计划符合您的要求。（默认情况下，任务的预定开始设置为**手动**，但您可能希望选择其他选项。）

5. 创建策略

   手动或通过快速启动向导为 Kaspersky Endpoint Security 创建策略。您可以使用策略默认设置；您也可以根据需要随时修改策略默认设置。

6. 验证结果

   确保部署成功完成：您的每个应用程序都拥有策略和任务，这些应用程序被安装到受管理设备。

结果

完成方案可以导致如下：

- 所选应用程序的所有所需策略和任务被创建。
- 任务计划根据您的需要被配置。
- 所选应用程序被部署，或者计划在所选客户端设备上部署。

添加 Kaspersky 应用程序的管理插件

要部署 Kaspersky 应用程序（例如 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Windows），您必须添加并安装该应用程序的管理 Web 插件。

要下载 Kaspersky 应用程序的 Web 管理插件：

1. 在主菜单中，转到**设置 → Web 插件**。
2. 在打开的窗口中，单击“**添加**”按钮。
   可用插件列表被显示。
3. 在可用插件列表中，通过点击其名称选择您要下载的插件（例如，Kaspersky Endpoint Security for Linux）。
   插件描述页面被显示。
4. 在插件描述页面，点击“**安装插件**”。
5. 当安装完成时，点击“**确定**”。

管理 Web 插件使用默认配置进行下载并显示在管理 Web 插件列表中。

您可以从文件添加插件以及更新下载的插件。您可以从卡巴斯基网站下载管理 Web 插件。

要从文件下载或更新管理 Web 插件：

1. 在主菜单中，转到**设置 → Web 插件**。
2. 指定插件文件和文件签名：
   - 单击**从文件添加**以从文件下载插件。
   - 单击**从文件更新**以从文件下载插件更新。

3. 指定文件和文件签名。

4. 下载指定的文件。

管理 Web 插件被从文件下载并显示在管理 Web 插件列表。

下载和创建 Kaspersky 应用程序的安装包

如果管理服务器可以访问 Internet，则可以从 Kaspersky Web 服务器创建 Kaspersky 应用程序的安装包。

要下载并创建 Kaspersky 应用程序的安装包：

1. 执行以下操作之一：

   - 在主菜单中，转到**“发现和部署” → “部署和分配” → “安装包”** 。
   - 在主菜单中，转到**“操作”→ “存储库” → “安装包”**。

   您可以在屏幕通知列表中查看关于 Kaspersky 应用程序的新安装包的通知。如果有关于新安装包的通知，您可以点击通知旁边的链接并转到可用安装包列表。

   此时会显示管理服务器上可用的安装包的列表。

2. 单击**添加**。

   新安装包向导启动。使用**下一步**按钮进行向导。

3. 在向导的第一页上，选择**“为卡巴斯基应用程序创建安装包”**。

   将显示 Kaspersky Web 服务器上的可用安装包列表。该列表仅包含与当前版本的 Kaspersky Security Center Linux 兼容的应用程序的安装包。

4. 单击安装包名称。例如，Kaspersky Endpoint Security for Linux。

   带有安装包信息的窗口打开。

   > 如果符合适用的法律法规，您可以下载并使用包含实施强加密的加密工具的安装包。要下载可满足组织需求的有效 Kaspersky Endpoint Security for Windows 安装包，请参考组织的客户端设备所在国家/地区的法律。

5. 阅读信息，然后单击**“下载并创建安装包”**按钮。

   如果分发包无法转换为安装包，将显示**“下载分发包”**按钮而不是**“下载并创建安装包”**。

   下载安装包到管理服务器开始。您可以关闭向导的窗口或继续执行说明的下一步。如果关闭向导的窗口，下载过程将在后台模式下继续。

   如果要跟踪安装包下载过程：

   a. 在主菜单中，转到**“操作 → 存储库 → 安装包 → 进行中()“**。

   b. 在表的**“下载进度”**列和**“下载状态列”**中跟踪操作进度。

   该过程完成后，安装包将添加到**“已下载”**选项卡上的列表中。如果下载过程停止并且下载状态切换为**“接受 EULA**，则单击安装包名称，然后继续执行说明的下一步。

如果所选分发包中包含的数据大小超过当前限制，将显示错误消息。您可以更改限制值，然后继续创建安装包。

6. 对于一些 Kaspersky 应用程序，下载过程中将显示“**显示 EULA**”按钮。如果它不显示，做以下操作：

   a. 点击“**显示 EULA**”按钮以阅读最终用户授权许可协议（EULA）。

   b. 阅读屏幕上显示的 EULA，然后单击“**接受**”。
   在您接受 EULA 后，下载继续。如果您单击“**拒绝**”，下载将停止。

7. 下载完成后，单击“**关闭**”按钮。

所选安装包将下载到管理服务器共享文件夹及 Packages 子文件夹。下载后，安装包出现在安装包列表。

从文件创建安装包

您可以使用自定义安装包执行以下操作：

- 在客户端设备上安装任何应用程序（例如文本编辑器），例如通过任务。
- 创建独立安装包。

自定义安装包是一个包含一组文件的文件夹。创建自定义安装包的源是*存档文件*。存档文件包含一个或多个必须包含在自定义安装包中的文件。

创建自定义安装包时，您可以指定命令行参数，例如以静默模式安装应用程序。

要创建自定义安装包：

1. 执行以下操作之一：

   - 在主菜单中，转到“**发现和部署**” → “**部署和分配**” → “**安装包**”。
   - 在主菜单中，转到“**操作**”→ “**存储库**” → “**安装包**”。

   此时会显示管理服务器上可用的安装包的列表。

2. 单击**添加**。
   新安装包向导启动。使用**下一步**按钮进行向导。

3. 在向导的第一页上，选择“**从文件创建安装包**”。

4. 在向导的下一页上，指定安装包名称，然后单击“**浏览**”按钮。

5. 在打开的窗口中，选择可用磁盘上的压缩文件。
   您可以上传 ZIP、CAB、TAR 或 TAR.GZ 压缩文件。无法从 SFX（自解压存档）文件创建安装包。
   开始上传文件到管理服务器。

6. 如果您指定了 Kaspersky 应用程序的文件，则系统可能会提示您阅读并接受该应用程序的最终用户授权许可协议 (EULA)。要继续，您必须接受 EULA。仅当您完全阅读、理解并接受 EULA 条款后，才选中“**接受该最终用**

户授权许可协议的条款和条件"选项。

此外，系统还可能会提示您阅读并接受隐私策略。要继续，您必须接受隐私策略。仅当您理解并同意您的数据将按照隐私策略中所述进行处理和传输（包括传输到第三方国家）后，才选中"**我接受隐私策略**"选项。

7. 在向导的下一页上，选择一个文件（从所选压缩文件中提取的文件列表中选择），然后指定可执行文件的命令行参数。

   您可以指定命令行参数，以静默模式从安装包中安装应用程序。指定命令行参数是可选的。

   创建安装包的过程将开始。

   该向导将在过程完成时通知您。

   如果未创建安装包，则会显示相应的消息。

8. 单击**完成**按钮关闭向导。

您创建的安装包将下载到管理服务器共享文件夹的 Packages 子文件夹中。下载后，安装包出现在安装包列表。

在管理服务器上的可用安装包列表中，通过单击带有自定义安装包名称的链接，您可以：

- 查看安装包的以下属性：
  - **名称**。自定义安装包名称。
  - **源**。应用程序供应商名称。
  - **应用程序**。打包到自定义安装包中的应用程序名称。
  - **版本**。应用程序版本。
  - **语言**。打包到自定义安装包中的应用程序的语言。
  - **大小(MB)** 。安装包的大小。
  - **操作系统**安装包适合的操作系统的类型。
  - **创建日期**。安装包创建日期。
  - **修改日期**。安装包修改日期。
  - **类型**。安装包的类型。
- 更改命令行参数。

创建独立安装包

您和组织中的设备用户可以使用独立安装包在设备上手动安装应用程序。

独立安装包是一个可执行文件 (Installer.exe)，您可以将其存储在 Web 服务器或共享文件夹中，通过电子邮件发送或通过另一种方式传输到客户端设备。在客户端设备上，用户可以在本地运行接收到的文件以安装应用程序，而无需涉及 Kaspersky Security Center Linux。您可以为 Kaspersky 应用程序和第三方应用程序创建独立安装包。要为第三方应用程序创建独立安装包，必须创建自定义安装包。

确保独立安装包不适用于第三方。

要创建独立安装包：

1. 执行以下操作之一：

   - 在主菜单中，转到 “**发现和部署**” → “**部署和分配**” → “**安装包**”。
   - 在主菜单中，转到“**操作**”→ “**存储库**” → “**安装包**”。

   此时会显示管理服务器上可用的安装包的列表。

2. 在安装包列表中选择安装包，然后在列表上方单击“**部署**”按钮。

3. 选择**使用独立包**选项。

   独立安装包创建向导启动。使用**下一步**按钮进行向导。

4. 在向导的第一页，如果要将网络代理与所选应用程序一起安装，请确保已启用“**网络代理和该应用程序一起安装**”选项。

   默认情况下已启用该选项。如果不确定设备上是否安装了网络代理，建议启用此选项。如果设备上已经安装了网络代理，则在安装带有网络代理的独立安装包之后，网络代理将更新为较新的版本。

   如果禁用此选项，则网络代理将不会安装在设备上，并且该设备将不受管理。

   如果管理服务器上已经存在用于所选应用程序的独立安装包，则向导会通知您这一事实。在这种情况下，您必须选择以下操作之一：

   - **创建独立安装包**。例如，如果要为新的应用程序版本创建独立安装包，并且还希望保留为先前的应用程序版本创建的独立安装包，请选择此选项。新的独立安装包位于另一个文件夹中。
   - **使用现有的独立安装包**。如果要使用现有的独立安装包，请选择此选项。安装包创建过程将不会开始。
   - **重新编译现有的独立安装包**。如果要再次为同一应用程序创建独立安装包，请选择此选项。独立安装包位于同一文件夹中。

5. 在向导的“**移动到受管理设备列表**”页面上，默认情况下已选择“**不移动设备**”选项。如果您不希望在安装网络代理后将客户端设备移至任何管理组，则不要更改选项选择。

   如果要在安装网络代理后移动客户端设备，请选择“**将未分配的设备移动到此组**”选项并指定要将客户端设备移至的管理组。默认情况下，设备移至“**受管理设备**”组。

6. 在向导的下一页上，完成独立安装包创建过程后，单击“**完成**”按钮。

   “独立安装包创建向导”关闭。

此时会创建独立安装包，并将其放置在管理服务器共享文件夹的 PkgInst 子文件夹中。您可以通过单击安装包列表上方的“**查看独立包列表**”按钮来查看独立包列表。

Changing the limit on the size of custom installation package data

The total size of data unpacked during creation of a custom installation package is limited. The default limit is 1 GB.

If you attempt to upload an archive file that contains data exceeding the current limit, an error message is displayed. You might have to increase this limit value when creating installation packages from large distribution packages.

To change the limit value for the custom installation package size:

1. On the Administration Server device, run the command prompt under the account that was used to install Administration Server.

2. Change your current directory to the Kaspersky Security Center Linux installation folder (usually, /opt/kaspersky/ksc64/sbin).

3. Depending on the type of Administration server installation, enter one of the following commands under the root account:

   - Normal local installation:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <number of bytes>
     ```

   - Installation on the Kaspersky Security Center Linux failover cluster:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <number of bytes> --stp
     klfoc
     ```

   Where <number of bytes> is a number of bytes in hexadecimal or decimal format.

   For example, if the required limit is 2 GB, you can specify the decimal value 2147483648 or the hexadecimal value 0x80000000. In this case, for a local installation of Administration Server, you can use the following command:

   ```
   klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v 2147483648
   ```

The limit on the size of custom installation package data is changed.

Installing Network Agent for Linux in silent mode (with an answer file)

You can install Network Agent on Linux devices by using an answer file—a text file that contains a custom set of installation parameters: variables and their respective values. Using this answer file allows you to run an installation in silent mode, that is, without user participation.

To perform installation of Network Agent for Linux in silent mode:

1. Prepare the relevant Linux device for remote installation. Download and create the remote installation package, by using a .deb or .rpm package of Network Agent, by means of any suitable package management system.

2. If you want to install Network Agent on devices with the SUSE Linux Enterprise Server 15 operating system, install the insserv-compat package first to configure Network Agent.

3. Read the End User License Agreement. Follow the steps below only if you understand and accept the terms of the End User License Agreement.

4. Set the value of the KLAUTOANSWERS environment variable by entering the full name of the answer file (including the path), for example, as follows:

   ```
   export KLAUTOANSWERS=/tmp/nagent_install/answers.txt
   ```

5. Create the answer file (in TXT format) in the directory that you have specified in the environment variable. Add to the answer file a list of variables in the VARIABLE_NAME=variable_value format, each variable on a separate

line.

For correct usage of the answer file, you must include in it a minimum set of the three required variables:

- KLNAGENT_SERVER
- KLNAGENT_AUTOINSTALL
- EULA_ACCEPTED

You can also add any optional variables to use more specific parameters of your remote installation. The following table lists all of the variables that can be included in the answer file:

Variables of the answer file used as parameters of Network Agent for Linux installation in silent mode

Variables of the answer file used as parameters of Network Agent for Linux installation in silent mode

Variable name	Required	Description	Possible values
KLNAGENT_SERVER	Yes	Contains the Administration Server name presented as fully qualified domain name (FQDN) or IP address.	DNS name or IP address.
KLNAGENT_AUTOINSTALL	Yes	Defines whether silent installation mode is enabled.	1—Silent mode is enabled; the user is not prompted for any actions during installation. Other—Silent mode is disabled; the user may be prompted for actions during installation.
EULA_ACCEPTED	Yes	Defines whether the user accepts the End User License Agreement (EULA) of Network Agent; when missing, can be interpreted as non-acceptance of the EULA.	1—I confirm that I have fully read, understand, and accept the terms and conditions of this End User License Agreement. Other or not specified—I do not accept the terms of the License Agreement (installation is not performed).
KLNAGENT_PROXY_USE	No	Defines whether connection with the Administration Server will use proxy settings. The default value is 0.	1—Proxy settings are used. Other—Proxy settings are not used.
KLNAGENT_PROXY_ADDR	No	Defines the address of the proxy server used for connection with the Administration Server.	DNS name or IP address.
KLNAGENT_PROXY_LOGIN	No	Defines the user name used for login to the proxy server.	Any existing user name.
KLNAGENT_PROXY_PASSWORD	No	Defines the user password used for login to the proxy server.	Any set of alphanumeric characters allowed by the password format in the operating system.
KLNAGENT_VM_VDI	No	Defines whether Network Agent is installed on an image	1—Network Agent is installed on an

		for creation of dynamic virtual machines.	image, which is subsequently used for creation of dynamic virtual machines. Other—No image is used during installation.
KLNAGENT_VM_OPTIMIZE	No	Defines whether the Network Agent settings are optimal for hypervisor.	1—The default local settings of Network Agent are modified so that they allow optimized usage on hypervisor.
KLNAGENT_TAGS	No	Lists the tags assigned to the Network Agent instance.	One or multiple tag names separated with semicolon.
KLNAGENT_UDP_PORT	No	Defines the UDP port used by Network Agent. The default value is 15000.	Any existing port number.
KLNAGENT_PORT	No	Defines the non-TLS port used by Network Agent. The default value is 14000.	Any existing port number.
KLNAGENT_SSLPORT	No	Defines the TLS port used by Network Agent. The default value is 13000.	Any existing port number.
KLNAGENT_USESSL	No	Defines whether Transport Layer Security (TLS) is used for connection.	1 (default)—TLS is used. Other—TLS is not used.
KLNAGENT_GW_MODE	No	Defines whether connection gateway is used.	1 (default)—The current settings are not modified (at the first call, no connection gateway is specified). 2—No connection gateway is used. 3—Connection gateway is used. 4—The Network Agent instance is used as connection gateway in demilitarized zone (DMZ).
KLNAGENT_GW_ADDRESS	No	Defines the address of the connection gateway. The	DNS name or IP address.

		value is applicable only if KLNAGENT_GW_MODE=3.	

6. Install Network Agent:

   - To install Network Agent from an RPM package to a 32-bit operating system, execute the following command:
     `# rpm -i klnagent-<build number>.i386.rpm`
   - To install Network Agent from an RPM package to a 64-bit operating system, execute the following command:
     `# rpm -i klnagent64-<build number>.x86_64.rpm`
   - To install Network Agent from an RPM package on a 64-bit operating system for the Arm architecture, execute the following command:
     `# rpm -i klnagent64-<build number>.aarch64.rpm`
   - To install Network Agent from a DEB package to a 32-bit operating system, execute the following command:
     `# apt-get install ./klnagent_<build number>_i386.deb`
   - To install Network Agent from a DEB package to a 64-bit operating system, execute the following command:
     `# apt-get install ./klnagent64_<build number>_amd64.deb`
   - To install Network Agent from a DEB package on a 64-bit operating system for the Arm architecture, execute the following command:
     `# apt-get install ./klnagent64_<build number>_arm64.deb`

   Installation of Network Agent for Linux starts in silent mode; the user is not prompted for any actions during the process.

准备在封闭软件环境模式下运行 Astra Linux 的设备以安装网络代理

在封闭软件环境模式下运行 Astra Linux 的设备上安装网络代理之前，您必须执行两个准备过程：下面说明中的一个和适用于任何 Linux 设备的常规准备步骤。

在您开始之前：

- 确保您要在上面安装 Network Agent for Linux 的设备运行受支持的 Linux 分类。
- 从卡巴斯基网站下载必要的网络代理安装文件。

以拥有 root 权限的账户运行本说明中提供的命令。

要准备在封闭软件环境模式下运行 Astra Linux 的设备来安装网络代理：

1. 打开 /etc/digsig/digsig_initramfs.conf 文件，然后指定以下设置：
   `DIGSIG_ELF_MODE=1`
2. 在命令行中，运行以下命令来安装兼容包：
   `apt install astra-digsig-oldkeys`

3. 为应用程序密钥创建一个目录：

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. 将应用程序密钥 /opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg 放在上一步创建的目录中：

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

   如果 Kaspersky Security Center Linux 分发包不包含 kaspersky_astra_pub_key.gpg 应用程序密钥，您可以通过单击以下链接下载：https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg。

5. 更新 RAM 磁盘：

   ```
   update-initramfs -u -k all
   ```

   重新启动系统。

6. 执行任何 Linux 设备通用的准备步骤。

设备准备好。您现在可以继续安装网络代理。

Viewing the list of stand-alone installation packages

You can view the list of stand-alone installation packages and properties of each stand-alone installation package.

To view the list of stand-alone installation packages for all installation packages:

Above the list, click the 查看独立包列表 button.

In the list of stand-alone installation packages, their properties are displayed as follows:

- 包名称. Stand-alone installation package name that is automatically formed as the application name included in the package and the application version.
- 应用程序名称. Application name included in the stand-alone installation package.
- 应用程序版本.
- 网络代理安装包名称. The property is displayed only if Network Agent is included in the stand-alone installation package.
- 网络代理版本. The property is displayed only if Network Agent is included in the stand-alone installation package.
- 大小. File size in MB.
- 组. Name of the group to which the client device is moved after Network Agent installation.
- 创建日期. Date and time of the stand-alone installation package creation.
- 修改日期. Date and time of the stand-alone installation package modification.
- 路径. Full path to the folder where the stand-alone installation package is located.

- 网址. Web address of the stand-alone installation package location.
- 文件哈希. The property is used to certify that the stand-alone installation package was not changed by third-party persons and a user has the same file you have created and transferred to the user.

To view the list of stand-alone installation packages for specific installation package:

Select the installation package in the list and, above the list, click the 查看独立包列表 button.

In the list of stand-alone installation packages, you can do the following:

- Publish a stand-alone installation package on the Web Server by clicking the 发布 button. Published stand-alone installation package is available for downloading for users whom you sent the link to the stand-alone installation package.
- Cancel publication of a stand-alone installation package on the Web Server by clicking the 取消发布 button. Unpublished stand-alone installation package is available for downloading only for you and other administrators.
- Download a stand-alone installation package to your device by clicking the 下载 button.
- Send email with the link to a stand-alone installation package by clicking the 通过电子邮件发送 button.
- Remove a stand-alone installation package by clicking the 删除 button.

将安装包分发至从属管理服务器

Kaspersky Security Center Linux 允许您创建安装包用于卡巴斯基应用程序和第三方应用程序，以及将安装包分发至客户端设备并从包中安装应用程序。要优化主管理服务器上的负载，您可以将安装包分发至从属管理服务器。之后，从属服务器将安装包传输到客户端设备，然后您可以在客户端设备上远程安装应用程序。

要将安装包分发至从属管理服务器：

1. 请确保从属管理服务器连接至主管理服务器。
2. 在主菜单中，转到“**资产(设备)**” → “**任务**”。
   将显示任务列表。
3. 单击“**添加**”按钮。
   “新任务向导”启动。遵照向导的说明。
4. 在**新任务**页面的 **应用程序**下拉列表中，选择**Kaspersky Security Center**。然后，从**任务类型**下拉列表中选择**分发安装包**，然后指定任务名称。
5. 在“ **任务范围**”页面，通过以下方式之一选择任务分配到的设备：
   - 如果要为特定管理组中的所有从属管理服务器创建任务，选择该组，然后为它创建组任务。
   - 如果要为特定的从属管理服务器创建任务，选择这些服务器，然后为它们创建任务。
6. 在“**分发的安装包**”页面，选择要复制到从属管理服务器的安装包。
7. 指定一个账户，以该账户来运行“*分发安装包*”任务。您可以使用您的账户并保持“**默认账户**”选项为启用状态。或者，您可以指定另一个用于运行该任务并具有必要访问权限的账户。为此，请选择“**指定账户**”选项，然后输

入该账户的凭据。

8. 在**完成任务创建**页面上，您可以启用**创建完成时打开任务详情**选项以打开任务属性窗口，然后修改默认任务设置。或者，您可以稍后随时配置任务设置。

9. 单击"**完成**"按钮。

   为了将安装包分发至从属管理服务器而创建的任务显示在任务列表中。

10. 您可以手动运行该任务，或者等待任务按照您在任务设置中指定的时间表启动。

任务完成后，所选的安装包将复制到指定的从属管理服务器。

准备 Linux 设备并在 Linux 设备上远程安装网络代理

网络代理安装包括两个步骤：

- Linux 设备准备
- 网络代理远程安装

Linux 设备准备

要准备运行 Linux 的设备以远程安装网络代理：

1. 确保目标 Linux 设备上安装了以下软件：
   - Sudo
   - Perl 语言解释器版本 5.10 或更高版本
2. 测试设备配置：
   a. 检查是否您可以通过 SSH 客户端（例如 PuTTY）连接到设备。

      如果您无法连接到设备，打开文件 /etc/ssh/sshd_config 并确保以下设置具有以下相关值：

      ```
      PasswordAuthentication no
      ChallengeResponseAuthentication yes
      ```

      > 如果您可以毫无问题地连接到设备，请不要修改 /etc/ssh/sshd_config 文件；否则在运行远程安装任务时可能会遇到 SSH 认证失败的情况。

      保存文件（如果必要）并使用 `sudo service ssh restart` 命令重启 SSH 服务。

   b. 禁用要连接设备的用户账户的 sudo 密码。

   c. 使用 sudo 的 `visudo` 命令打开 sudoers 配置文件。

      在您打开的文件中，找到以 `%sudo` 开头的行（如果您使用 CentOS 操作系统，则以 `%wheel` 开头）。在该行下方指定以下内容：`<用户名> ALL = (ALL) NOPASSWD: ALL`。此种情况下，`<用户名>` 是将用于通过 SSH 连接设备的用户账户。如果您使用的是 Astra Linux 操作系统，请在 /etc/sudoers 文件中添加包含以下文本的最后一行： `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

d. 保存并关闭 sudoers 文件。

e. 通过 SSH 再次连接设备并确保 Sudo 服务不提示您输入密码；您可以使用 `sudo whoami` 命令来操作。

3. 打开 /etc/systemd/logind.conf 文件，然后做以下操作：

- 指定"no"作为 KillUserProcesses 设置的值：`KillUserProcesses=no`。
- 对于 KillExcludeUsers 设置，输入要执行远程安装的账户的用户名，例如，`KillExcludeUsers=root`。

如果目标设备正在运行 Astra Linux，请在 `/home/<用户名>/.bashrc` 文件中添加 `export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` 字符串，其中 `< 用户名 >` 是用于使用 SSH 进行设备连接的用户账户。

要应用更改的设置，重启 Linux 设备或执行以下命令：

```
$ sudo systemctl restart systemd-logind.service
```

4. 如果您想在装有 SUSE Linux Enterprise Server 15 操作系统的设备上安装网络代理，首先安装 insserv-compat 软件包以配置网络代理。

5. 如果要在封闭软件环境模式下运行 Astra Linux 操作系统的设备上安装网络代理，请执行额外的步骤来准备 Astra Linux 设备。

网络代理远程安装

要在 Linux 设备上远程安装网络代理：

1. 下载并创建安装包：

a. 在设备上安装之前，请确保该包安装了所有的先决条件（程序和库）。

您可以自行查看每个包的先决条件，使用 Linux 分发包的实用工具。关于更多实用工具的详情，请参考您的操作系统文档。

b. 使用应用程序界面或从卡巴斯基网站下载网络代理安装包。

c. 要创建远程安装包，使用以下文件：

- klnagent.kpd
- akinstall.sh
- 网络代理的 .deb 或 .rpm 包

2. 使用以下设置创建远程安装任务：

- 在新任务向导的**设置**页面，选择**通过管理服务器使用操作系统资源**复选框。清空所有其他复选框。
- 在"**选择账户以运行任务**"页面，请指定通过 SSH 进行设备连接的用户账户设置。

3. 运行远程安装任务。使用 `su` 命令的选项保护环境：`-m, -p, --preserve-environment`。

如果您在早于 20 版本的 Fedora 设备上使用 SSH 安装网络代理，可能返回错误。此种情况下，为了成功安装网络代理，请在 /etc/sudoers 文件注释出默认选项（用注释符号将其围住以防止其被解析）。对于可能导致 SSH 连接问题的默认选项的详细说明，请参考 Bugzilla bugtracker 网站。

使用远程安装任务安装应用程序

Kaspersky Security Center Linux 允许您远程安装应用程序到设备，使用远程安装任务。那些任务通过专门向导被创建被分配到设备。要更快和更便捷地分配任务到设备，您可以在向导窗口中指定设备，使用以下方法之一：

- **分配任务到管理组**。此种情况下，任务被分配到先前创建的管理组中的设备。
- **手动指定设备地址或从列表导入地址**。您可以指定要为其分配任务的设备的 DNS 名称、IP 地址和 IP 子网。
- **分配任务到设备分类**。此种情况下，任务被分配到先前创建的分类中的设备。您可以指定默认分类或您所创建的自定义分类。

要想在未安装网络代理的设备上正确进行远程安装，必须打开下列端口：a) TCP 139 和 445；b) UDP 137 和 138。默认情况下，域中所有设备的这些端口均已打开。它们被远程安装准备实用程序自动打开。

远程安装应用程序

本节包含有关如何在管理组、具有特定地址的设备或选择的设备上远程安装应用程序的信息。

要在特定设备上安装应用程序：

1. 在主菜单中，转到**资产(设备)** → **任务**。
2. 单击**添加**。
   “新任务向导”启动。
3. 在**任务类型**字段中，选择**远程安装应用程序**。
4. 您可以选择以下选项之一：

   - 分配任务到管理组

     任务被分配到包含在管理组中的设备。您可以指定现有组之一或者创建新组。
     例如，您可能要使用该选项运行发送消息到用户任务，如果消息针对包含在特定管理组中的设备。

   - 手动指定设备地址或从列表导入地址

     您可以指定要为其分配任务的设备的 DNS 名称、IP 地址和 IP 子网。
     您可能要使用该选项以对特定子网执行任务。例如，您可能要安装特定应用程序到会计设备，或者扫描疑似被感染子网中的设备。

   - 分配任务到设备分类

     该任务被分配到设备分类中的设备。您可以指定现有分类之一。
     例如，您可能要使用该选项在特定操作系统版本的设备上运行任务。

*远程安装应用程序*任务为指定设备创建。如果您选择了"**分配任务到管理组**"选项，则任务是组任务。

5. 在**任务范围**步骤，指定管理组、具有特定地址的设备或设备分类。
   可用设置取决于在上一步中选择的选项。

6. 在**安装包**步骤中，指定以下设置：

   - 在"**选择安装包**"字段中，选择要安装的应用程序的安装包。
   - 在"**强制下载安装包**"设置组中，指定如何将安装程序所需的文件分发到客户端设备中。
     - 使用网络代理

       如果启用此选项，安装包通过安装在客户端设备上的网络代理传送到客户端设备。
       如果禁用此选项，则使用客户端的操作系统传送安装包。
       如果任务已分配给安装了网络代理的设备，我们建议您启用此选项。
       默认情况下已启用该选项。

     - 通过分发点使用操作系统资源

       如果启用此选项，安装包使用操作系统工具通过分发点传送到客户端设备。如果网络中存在不止一个分发点，那么您可以选择本选项。
       如果启用"**使用网络代理**"选项，仅在网络代理工具不可用时才通过操作系统工具传送文件。
       默认情况下，已经为虚拟管理服务器上创建的远程安装任务启用此选项。
       在未安装网络代理的设备上安装 Windows 应用程序（包括 Windows 网络代理）的唯一方法是使用基于 Windows 的分发点。因此，当您安装 Windows 应用程序时：
       - 选择此选项。
       - 确保为目标客户端设备分配了分发点。
       - 确保分发点基于 Windows。

     - 通过管理服务器使用操作系统资源

       如果启用此选项，文件将使用客户端设备的操作系统工具通过管理服务器传送到客户端设备。如果客户端设备上未安装网络代理，但是客户端设备与管理服务器在同一网络，则可以启用此选项。
       默认情况下已启用该选项。

   - 在**同时下载的最大数量**字段中，指定管理服务器可以同时向其传输文件的最大允许客户端设备数。
   - 在**安装尝试最大数量**字段中，指定安装程序运行的最大允许次数。
     如果超过参数中指定的尝试次数，Kaspersky Security Center Linux 将不再在设备上启动安装程序。若要重新启动*远程安装应用程序*任务，请增加**安装尝试最大数量**参数的值然后启动任务。或者，您可以创建新的"*远程安装应用程序*"任务。
   - 定义附加设置：
     - 如果已经安装应用程序则不再重新安装

如果启用此选项，则如果选定的应用程序已安装到该客户端设备上，将不再重新安装它。

如果禁用此选项，仍将安装应用程序。

默认情况下已启用该选项。

- 下载之前验证操作系统类型

  在将文件传输到客户端设备之前，Kaspersky Security Center Linux 将检查安装实用程序设置是否适用于客户端设备的操作系统。如果设置不适用，Kaspersky Security Center Linux 不会传输文件，也不会尝试安装应用程序。例如，要将某个应用程序安装到某个管理组的设备（这些设备运行各种操作系统），可以将安装任务分配给管理组，然后启用此选项以跳过操作系统与所需设备不同的设备。

- 提示用户关闭运行中应用程序

  运行应用程序可能会阻止客户端设备重启。例如，如果文档在文档处理应用程序中被编辑且未被保存，则应用程序不允许设备重启。

  如果启用该选项，锁定设备上的此类应用程序在设备重启前被强制关闭。结果，用户可能丢失他们未保存的更改。

  如果禁用该选项，锁定设备不被重启。该设备上的任务状态显示设备需要重启。用户必须手动关闭所有运行在锁定设备上的应用程序并重启这些设备。

  默认情况下已禁用该选项。

- 选择要在哪些设备上安装应用程序：

  - 在所有设备上安装

    应用程序将被安装到由其他管理服务器管理的设备。

    默认情况下已选中该选项。如果您在网络中只有一个管理服务器，您不必更改该设置。

  - 仅安装到通过该管理服务器管理的设备

    应用程序将仅被安装到由该管理服务器管理的设备。如果您在网络中有多个管理服务器且需要避免它们之间的冲突，请选择该选项。

- 指定设备是否在安装后必须被移动到管理组：

  - 不移动设备

    设备保留在当前所在组中。未被放置在任何组的设备保持未分配。

  - 移动未分配的设备到所选组 (仅可以选择单一组)

    设备被移动到您选择的管理组。

  注意默认情况下已选择“**不移动设备**”选项。为了安全起见，您可能需要手动移动设备。

7. 在向导的这一步，指定在安装应用程序期间是否必须重新启动设备：

- 不重启设备

  如果选择该选项，安全应用程序安装后设备不被重启。

- 重启设备

  如果选择该选项，安全应用程序安装后设备将被重启。

8. 如有必要，在**选择账户以访问设备**步骤，添加将用于启动*远程安装应用程序*任务的账户：

   - 不需要账户(网络代理已安装)

     如果该选项被选中，您不是必须指定一个账户，并在该账户下运行程序的安装。将使用运行管理服务器服务的账户运行该任务。

     如果网络代理未安装在客户端设备，该选项不可用。

   - 需要账户(不使用网络代理)

     如果您为其分配远程安装任务的设备上未安装网络代理，请选择此选项。在这种情况下，您可以指定用户账户来安装应用程序。

     要指定运行应用程序安装程序的用户账户，请单击**添加**按钮，选择**本地账户**，然后指定用户账户凭据。

     您可以指定多个用户账户，例如，没有一个账户拥有分配任务所对应的所有设备上的全部所需权限时。在此情况下，已经添加的所有账户都用于从上到下按顺序运行该任务。

9. 在**完成任务创建**步骤中，单击**完成**按钮以创建任务并关闭向导。

   如果启用了"**创建完成时打开任务详情**"选项，将打开任务设置窗口。在此窗口中，您可以检查任务参数、修改它们或配置任务启动计划（如有必要）。

10. 在任务列表中，选择已创建的任务，然后单击**启动**。

    或者等待任务按照您在任务设置中指定的时间表启动。

远程安装任务完成后，选定的应用程序即安装在指定设备上。

在从属管理服务器上安装应用程序

要在从属管理服务器上安装应用程序：

1. 与控制相关从属管理服务器的管理服务器建立连接。

2. 确保每个所选的从属管理服务器上都有与要安装的应用程序对应的安装包。如果在任何从属服务器上都找不到安装包，请分发它。为此，创建一个任务类型为**分发安装包**任务。

3. 创建在从属管理服务器上远程安装应用程序的任务。选择**将应用程序远程安装到从属管理服务器**任务类型。

   "新任务向导"将创建一个任务，用于在特定从属管理服务器上远程安装向导中选择的应用程序。

4. 手动运行该任务，或者按照任务设置中指定的计划等待任务启动。

远程安装任务完成后，选定的应用程序即安装在从属管理服务器上。

Specifying settings for remote installation on Unix devices

When you install an application on a Unix device by using a remote installation task, you can specify Unix-specific settings for the task. These settings are available in the task properties after the task is created.

To specify Unix-specific settings for a remote installation task:

1. In the main menu, go to 资产(设备) → 任务.
2. Click the name of the remote installation task for which you want to specify the Unix-specific settings.

   The task properties window opens.
3. Go to 应用程序设置 → **Unix** 特定的设置.
4. Specify the following settings:

   - 为根账户设置密码(仅对通过 SSH 的部署)

     If the `sudo` command cannot be used on the target device without specifying the password, select this option, and then specify the password for the root account. Kaspersky Security Center Linux transmits the password in an encrypted form to the target device, decrypts the password, and then starts the installation procedure on behalf of the root account with the specified password.

     Kaspersky Security Center Linux does not use the account or the specified password to create an SSH connection.

   - 指定目标设备上具有执行权限的临时文件夹的路径(仅对通过 SSH 的部署)

     If the /tmp directory on the target device does not have the execute permission, select this option, and then specify the path to the directory with the execute permission. Kaspersky Security Center Linux uses the specified directory as a temporary directory to access via SSH. The application places the installation package in the directory and runs the installation procedure.
5. Click the 保存 button.

The specified task settings are saved.

替换第三方安全应用程序

通过 Kaspersky Security Center Linux 进行卡巴斯基安全应用程序的安装可能需要卸载与正在安装的应用程序不兼容的第三方软件。Kaspersky Security Center Linux 提供几种卸载第三方应用程序的方法。

当配置应用程序远程安装时卸载不兼容应用程序

您可以在保护部署向导中配置安全应用程序远程安装时启用“**自动卸载不兼容的应用程序**”选项。当该选项被启用时，Kaspersky Security Center Linux 在安装安全应用程序到受管理设备之前卸载不兼容的应用程序。

通过专用任务卸载不兼容的应用程序

要卸载不兼容的应用程序，使用*远程卸载应用程序*任务。该任务应该在安全应用程序安装任务运行之前运行在设备。例如，在安装任务中，可以选择“**在完成其他任务时**”作为计划类型，其中其他任务为“*远程卸载应用程序*”。

该卸载方法在安全应用程序无法正确卸载不兼容应用程序时是很有用的。

Removing applications or software updates remotely

You can remove applications or software updates on managed devices that run Linux remotely only by using Network Agent.

To remove applications or software updates remotely from selected devices:

1. In the main menu, go to 资产(设备) → 任务.
2. Click 添加.

   The 新任务向导 starts. Proceed through the wizard by using the 下一步 button.
3. In the 应用程序 drop-down list, select Kaspersky Security Center.
4. In the 任务类型 list, select the 远程卸载应用程序 task type.
5. In the 任务名称 field, specify the name of the new task.

   A task name cannot be more than 100 characters long and cannot include any special characters ("*<>?\:|).
6. Select the devices to which the task will be assigned.

   Go to the next step of the wizard.
7. Select what kind of software you want to remove, and then select specific applications, updates, or patches that you want to remove:

   - 卸载受管理应用程序

     A list of Kaspersky applications is displayed. Select the application that you want to remove.

   - 从应用程序注册表中卸载应用程序

By default, Network Agents send the Administration Server information about the applications installed on the managed devices. The list of installed applications is stored in the applications registry.

To select an application from the applications registry:

a. Click the 要卸载的应用程序 field, and then select the application that you want to remove.

b. Specify the uninstallation options:

- 卸载模式

  Select how you want to remove the application:

  - 自动定义卸载命令

    If the application has an uninstallation command defined by the application vendor, Kaspersky Security Center Linux uses this command. We recommend that you select this option.

  - 指定卸载命令

    Select this option if you want to specify your own command for the application uninstallation.

    > We recommend that you first try to remove the application by using the 自动定义卸载命令 option. If the uninstallation through the automatically defined command fails, then use your own command.

    Type an installation command into the field, and then specify the following option:

    仅当未自动检测到默认命令时使用此命令进行卸载

    > Kaspersky Security Center Linux checks whether or not the selected application has an uninstallation command defined by the application vendor. If the command is found, Kaspersky Security Center Linux will use it instead of the command specified in the 应用程序卸载命令 field.
    >
    > We recommend that you enable this option.

- 应用程序成功卸载后执行重启

  > If the application requires the operating system to be restarted on the managed device after successful uninstallation, the operating system is restarted automatically.

- 卸载指定的应用程序更新、补丁或第三方应用程序

A list of updates, patches, and third-party applications is displayed. Select the item that you want to remove.

The displayed list is a general list of applications and updates, and it does not correspond to the applications and updates installed on the managed devices. Before selecting an item, we recommend that you ensure that the application or update is installed on the devices defined in the task scope. You can view the list of devices on which the application or update is installed, via the properties window.

To view the list of devices:

a. Click the name of the application or update.

The properties window opens.

b. Open the 设备 section.

You can also view the list of installed applications and updates in the device properties window.

8. Specify how client devices will download the Uninstallation utility:

- 使用网络代理

The files are delivered to client devices by Network Agent installed on those client devices.

If this option is disabled, the files are delivered using the Linux operating system tools.

We recommend that you enable this option if the task has been assigned to devices that have Network Agents installed.

- 通过管理服务器使用操作系统资源

The option is obsolete. Use the 使用网络代理 or 通过分发点使用操作系统资源 option instead.

The files are transmitted to client devices by using the Administration Server operating system tools. You can enable this option if no Network Agent is installed on the client device, but the client device is on the same network as the Administration Server.

- 通过分发点使用操作系统资源

The files are transmitted to client devices by using operating system tools through distribution points. You can enable this option if there is at least one distribution point on the network.

If the 使用网络代理 option is enabled, the files are delivered by using operating system tools only if Network Agent tools are unavailable.

- 同时下载的最大数量

The maximum allowed number of client devices to which Administration Server can simultaneously transmit the files. The larger this number, the faster the application will be uninstalled, but the load on Administration Server is higher.

- 尝试卸载的最大次数

If, when running the *远程卸载应用程序* task, Kaspersky Security Center Linux fails to uninstall an application on a managed device within the number of installer runs specified by the parameter, Kaspersky Security Center Linux stops delivering the Uninstallation utility to this managed device and does not start the installer on the device anymore.

The 尝试卸载的最大次数 parameter allows you to save the resources of the managed device, as well as reduce traffic (uninstallation, MSI file run, and error messages).

Recurring task start attempts may indicate a problem on the device and which prevents uninstallation. The administrator should resolve the problem within the specified number of uninstallation attempts and then restart the task (manually or by a schedule).

If uninstallation is not achieved eventually, the problem is considered unresolvable and any further task starts are seen as costly in terms of unnecessary consumption of resources and traffic.

When the task is created, the attempts counter is set to `0`. Each run of the installer that returns an error on the device increments the counter reading.

If the number of attempts specified in the parameter has been exceeded and the device is ready for application uninstallation, you can increase the value of the 尝试卸载的最大次数 parameter and start the task to uninstall the application. Alternatively, you can create a new *远程卸载应用程序* task.

- 下载之前验证操作系统类型

  Before transmitting the files to client devices, Kaspersky Security Center Linux checks if the Installation utility settings are applicable to the operating system of the client device. If the settings are not applicable, Kaspersky Security Center Linux does not transmit the files and does not attempt to install the application. For example, to install some application to devices of an administration group that includes devices running various operating systems, you can assign the installation task to the administration group, and then enable this option to skip devices that run an operating system other than the required one.

Go to the next step of the wizard.

9. Specify the operating system restart settings:

- 不重启设备

  Client devices are not restarted automatically after the operation. To complete the operation, you must restart a device (for example, manually or through a device management task). Information about the required restart is saved in the task results and in the device status. This option is suitable for tasks on servers and other devices where continuous operation is critical.

- 重启设备

  Client devices are always restarted automatically if a restart is required for completion of the operation. This option is useful for tasks on devices that provide for regular pauses in their operation (shutdown or restart).

- 提示用户操作

The restart reminder is displayed on the screen of the client device, prompting the user to restart it manually. Some advanced settings can be defined for this option: text of the message for the user, the message display frequency, and the time interval after which a restart will be forced (without the user's confirmation). This option is most suitable for workstations where users must be able to select the most convenient time for a restart.

By default, this option is selected.

- 重复提示间隔(分钟)
- 在该时间后重启(分钟)

- 强行关闭锁定会话中的应用程序

Running applications may prevent a restart of the client device. For example, if a document is being edited in a word processing application and is not saved, the application does not allow the device to restart.

If this option is enabled, such applications on a locked device are forced to close before the device restart. As a result, users may lose their unsaved changes.

If this option is disabled, a locked device is not restarted. The task status on this device states that a device restart is required. Users have to manually close all applications running on locked devices and restart these devices.

By default, this option is disabled.

Go to the next step of the wizard.

10. If necessary, add the accounts that will be used to start the remote uninstallation task:

- 不需要账户(网络代理已安装)

If this option is selected, you do not have to specify the account under which the application installer will be run. The task will run under the account under which the Administration Server service is running.

If Network Agent has not been installed on client devices, this option is not available.

- 需要账户(不使用网络代理)

Select this option if Network Agent is not installed on the devices for which you assign the *Uninstall application remotely* task.

Specify the user account under which the application installer will be run. Click the 添加 button, select 账户, and then specify the user account credentials.

You can specify multiple user accounts if, for example, none of them have all the required rights on all devices for which you assign the task. In this case, all added accounts are used for running the task, in consecutive order, top-down.

11. At the 完成任务创建 step of the wizard, enable the 创建完成时打开任务详情 option to modify the default task settings.

    If you do not enable this option, the task will be created with the default settings. You can modify the default settings later.

12. Click the 完成 button.

The wizard creates the task. If you enabled the 创建完成时打开任务详情 option, the task properties window automatically opens. In this window, you can specify the general task settings and, if required, change the settings specified during task creation.

> You can also open the task properties window by clicking the name of the created task in the list of tasks.

The task is created, configured, and displayed in the list of tasks at 资产(设备) → 任务.

13. To run the task, select it in the task list, and then click the 开始 button.

    You can also set a task start schedule on the 计划 tab of the task properties window.

    For a detailed description of scheduled start settings, refer to the general task settings.

After the task is completed, the selected application is removed from the selected devices.

准备运行 SUSE Linux Enterprise Server 15 的设备以安装网络代理

要在装有 SUSE Linux Enterprise Server 15 操作系统的设备上安装网络代理：

在安装网络代理之前，运行以下命令：

```
$ sudo zypper install insserv-compat
```

这使您能够安装 insserv-compat 软件包并正确配置网络代理。

> 运行 `rpm -q insserv-compat` 命令来检查软件包是否已经安装。

如果您的网络包含大量运行 SUSE Linux Enterprise Server 15 的设备，您可以使用配置和管理公司基础架构的专用软件。通过使用此软件，您可以一次在所有必要的设备上自动安装 insserv-compat 软件包。例如，您可以使用 Puppet、Ansible、Chef，也可以制作自己的脚本 — 使用任何方便的方法。

如果设备没有 SUSE Linux Enterprise 的 GPG 签名密钥，您可能会遇到以下警告：`Package header is not signed!` 选择`i`选项忽略警告。

准备好 SUSE Linux Enterprise Server 15 设备后，部署并安装网络代理。

为远程安装准备 Windows 设备。Riprep 实用程序

远程安装应用程序到客户端设备时可能会因下列原因返回错误：

- 该任务已成功在该设备上执行。在此情况下，该任务无需再执行。
- 任务开始后，设备被关闭。在此情况下，请打开设备并重新启动此任务。
- 管理服务器与客户端设备上安装的网络代理之间无连接。要确定问题原因，请使用客户端设备的远程诊断实用程序 (klactgui)。
- 如果设备上未安装网络代理，远程安装过程中可能出现下列问题：

- 客户端设备启用了“**禁用简单文件共享**”。
- 客户端设备上未运行服务器服务。
- 客户端设备上的相关端口被关闭。
- 用于执行任务的账户权限不足。

要解决在无网络代理的客户端设备安装应用程序时出现的问题， 请使用专门用于为远程安装准备设备的实用程序 (riprep)。

使用 riprep 实用程序准备 Windows 设备进行远程安装。要下载该实用程序，请单击此链接：https://media.kaspersky.com/utilities/CorporateUtilities/KSC/riprep.exe

此实用程序用于为远程安装准备设备，且该设备不运行 Microsoft Windows XP Home Edition。

以交互模式为远程安装准备 Windows 设备

要以交互模式为远程安装准备 Windows 设备：

1. 在客户端设备上运行 riprep.exe 文件。
2. 在远程安装准备实用程序窗口中，选择以下选项：
   - **禁用简单文件共享**
   - **启动管理服务器服务**
   - **打开端口**
   - **添加账户**
   - **禁用用户账户控制 (UAC)**（仅适用于运行 Microsoft Windows Vista、Microsoft Windows 7 或 Microsoft Windows Server 2008 的设备）
3. 单击“**开始**”按钮。

在此实用程序主窗口的底部将显示远程安装设备准备的阶段。

如果您选择了“**添加账户**”选项，则创建账户时，系统将提示您输入账户名称和密码。这样，将会创建一个属于本地管理组的本地账户。

如果您选中了“**禁用用户账户控制 (UAC)**”选项，则即使在实用程序启动前已禁用 UAC，也将尝试禁用用户账户控制。在禁用 UAC 后，您将被提示重启设备。

以静默模式为远程安装准备 Windows 设备

要以静默模式为远程安装准备 Windows 设备：

从命令行中，以相关的一组键值运行客户端设备上的 riprep.exe 文件。

实用程序命令行语法：

```
riprep.exe [-silent] [-cfg CONFIG_FILE] [-tl traceLevel]
```

参数描述：

- `-silent` – 以静默模式启动实用程序。
- `-cfg CONFIG_FILE` – 定义实用程序配置，其中 `CONFIG_FILE` – 是配置文件的路径（带 .ini 后缀的文件）。
- `-tl traceLevel` – 定义跟踪级别，其中 `traceLevel` – 是介于 0 至 5 的数字。如果未指定具体键值，将使用数值 0。

您可以以静默模式启动实用程序来执行下列任务：

- 禁用文件简单共享
- 启动客户端设备上的服务器服务
- 打开端口
- 创建本地账户
- 禁用用户账户控制 (UAC)

在 `-cfg` 键中指定的配置文件中，您可以为远程安装设备准备指定参数。要定义这些参数，请在配置文件中添加下列信息：

- 在“`Common`”区域中，指定要执行的任务：
  - `DisableSFS` – 禁用简单文件共享（0 – 任务被禁用；1– 任务被启用）。
  - `StartServer` – 启动服务器服务（0 – 任务被禁用；1– 任务被启用）。
  - `OpenFirewallPorts` – 打开必要的端口（0 – 任务被禁用；1– 任务被启用）。
  - `DisableUAC` – 禁用用户账户控制 (UAC)（0 – 任务被禁用；1– 任务被启用）。
  - `RebootType` – 定义禁用 UAC 时需要重启设备时的操作。您可以使用下列值：
    - 0 – 不重启设备。
    - 1– 如果 UAC 在启动此实用程序之前启用，则重启设备。
    - 2 – 如果 UAC 在启动此实用程序之前启用，则强制重启。
    - 4 – 总是重启设备。
    - 5 – 总是强制重启设备。
- 在“`UserAccount`”区域中，指定账户名称（`user`）及其密码（`Pwd`）。

配置文件上下文示例：

```
[Common]
DisableSFS=0
```

```
StartServer=1
OpenFirewallPorts=1
[UserAccount]
user=Admin
Pwd=Pass123
```

实用程序执行完毕后，实用程序启动文件夹中将创建下列文件：

- riprep.txt – 操作报告，列出了实用程序在各阶段的操作及其原因。
- riprep.log – 跟踪文件（如果跟踪级别被设为 0 以上，则创建此文件）。

授权许可

此部分提供下列信息：

- 与 Kaspersky Security Center Linux 授权许可相关的一般概念
- 有关受管理卡巴斯基应用程序授权许可管理的说明

关于 Kaspersky Security Center Linux 的授权许可

本节介绍与 Kaspersky Security Center Linux 授权许可有关的一般概念。

关于最终用户授权许可协议

最终用户授权许可协议（授权许可协议或 EULA）是您和 AO Kaspersky Lab 之间具有约束力的合作协议，其中规定了您使用该程序应遵守的条款。

在您开始使用应用程序之前请认真阅读授权许可协议。

Kaspersky Security Center Linux 及其组件（例如网络代理）具有自己的 EULA。

您可以使用以下方法查看 Kaspersky Security Center Linux 最终用户授权许可协议的条款：

- 在 Kaspersky Security Center 安装期间。
- 如果阅读包含在 Kaspersky Security Center 分发包的 license.txt 文档。
- 如果阅读在 Kaspersky Security Center 安装文件夹的 license.txt 文档。
- 通过从卡巴斯基网站下载 license.txt 文件。

您可以使用以下方法查看 Network Agent for Linux 的最终用户授权许可协议的条款：

- 从 Kaspersky Web 服务器下载网络代理分发包期间。
- 在安装 Linux 网络代理期间。
- 阅读 Linux 网络代理分发包中包含的 license.txt 文档。
- 阅读 Linux 网络代理安装文件夹中的 license.txt 文档。
- 通过从卡巴斯基网站下载 license.txt 文件。

当您安装程序时同意了最终用户授权许可协议，这表明您接受了最终用户授权许可协议的条款。如果您不接受授权许可协议的条款，请取消应用程序安装且不再使用应用程序。

关于授权许可

*授权许可*是根据签名授权许可合约（最终用户授权许可协议）条款授予的在有限时间内使用 Kaspersky Security Center Linux 的权限。

服务范围和有效期取决于根据其使用应用程序的授权许可。

提供以下授权许可类型：

- *试用*

  用于试用该程序的免费授权许可。试用版授权许可通常拥有较短的有效期。

  试用版授权许可过期后，Kaspersky Security Center Linux 的所有功能都会被禁用。要继续使用该程序，您需要购买商业版的授权许可。

  您只能在试用授权许可下使用该应用程序一个试用期。

- *商业*

  付费授权许可。

  当商业授权许可到期时，应用程序的主要功能将被禁用。要继续使用 Kaspersky Security Center，您必须续费您的商业授权许可。商业授权许可过期后，您将无法继续使用该应用程序，必须将其从设备中删除。

  我们建议在授权许可过期之前进行续费，以确保保护不受中断，防御所有安全威胁。

关于授权许可证书

*授权许可证书*是随着您收到的一个密钥文件和激活码一起的文档。

授权许可证书包含下面的提供授权许可的信息：

- 授权许可密钥或订购号
- 授予授权许可的用户信息
- 可以使用提供的授权许可激活的应用程序信息
- 授权许可单元数量限制（例如，在该授权许可下，设备上的应用程序可以被使用）
- 授权许可期限的开始日期
- 授权许可到期日期或授权许可期限
- 授权许可类型

关于授权许可密钥

*授权许可密钥*由一系列数位组成，您可以依据最终用户授权许可协议的条款使用它们激活并使用程序。授权许可密钥由 Kaspersky 专家生成。

您可以使用下面的方法添加一个授权许可密钥到应用程序：通过应用*密钥文件*或输入*激活码*。为程序添加授权许可后，将在程序界面中显示该授权许可密钥的唯一字母数字序列。

如果违反授权许可协议的条款，Kaspersky 可能会阻止授权许可密钥。如果授权许可已被阻止，要使用程序，您需要添加另外一个授权许可密钥。

授权许可密钥可以是活动密钥或附加（备用）密钥。

*活动授权许可密钥*是应用程序当前使用的授权许可密钥。活动授权许可密钥可以被添加为商业授权许可。应用程序只能拥有一个活动授权许可密钥。

*附加（或备用）授权许可密钥*是允许用户使用应用程序，但是当前未使用的授权许可密钥。与当前授权许可密钥相关联的授权许可过期时，附加授权许可密钥将自动成为当前活动授权许可密钥。只有在添加了活动授权许可密钥之后，才可以添加附加授权许可密钥。

试用授权许可密钥仅可以被当作活动授权许可密钥添加。试用授权许可密钥不可以被当作附加授权许可密钥添加。

Viewing the Privacy Policy

The Privacy Policy is available online at https://www.kaspersky.com/products-and-services-privacy-policy.

The Privacy Policy is also available offline:

- You can read the Privacy Policy before Installing Kaspersky Security Center Linux.
- The Privacy Policy text is included in the license.txt file, in the Kaspersky Security Center Linux installation folder.
- The privacy_policy.txt file is available on a managed device, in the Network Agent installation folder.
- You can unpack the privacy_policy.txt file from the Network Agent distribution package.

Kaspersky Security Center 授权许可选项

Kaspersky Security Center 作为 Kaspersky 应用程序的一部分提供，用于保护公司网络。您也可以从卡巴斯基网站下载。

使用 Kaspersky Security Center 您可以做以下事情：

- 创建一个管理服务器层级结构来管理组织网络以及远程办公室网络或客户组织网络。
  *客户端组织*是指由服务提供商确保反病毒保护的一种组机构。
- 创建一个管理组层级结构以整体的形式管理一组选定的客户端设备。
- 管理基于 Kaspersky 程序构建的反病毒保护系统。
- 由 Kaspersky 和其他软件供应商执行应用程序的远程安装。
- 将 Kaspersky 应用程序的授权许可密钥集中部署到客户端设备、监控其使用情况，以及续订授权许可。
- 接收有关程序和设备运行的统计信息和报告。
- 接收有关 Kaspersky 程序操作中严重事件的通知。
- 管理存储在 Windows 设备的硬盘驱动器和可移动驱动器上的信息的加密。
- 管理用户对 Windows 设备上的加密数据的访问。

- 创建已连接至组织网络的硬件清查列表。
- 集中管理被安全应用程序移动到隔离区或备份区中的文件，以及安全应用程序已经推迟处理的文件。

关于密钥文件

*密钥文件*是 Kaspersky 提供的 .key 扩展名的文件。密钥文件设计用于通过添加授权许可密钥激活应用程序。

在购买 Kaspersky Security Center 或预定试用版本的 Kaspersky Security Center 后，您通过您指定的邮件地址可以收到密钥文件。

您不需要连接到 Kaspersky 激活服务器以使用密钥文件激活应用程序。

如果密钥文件被意外删除，您可以恢复它。您可能需要密钥文件来注册 Kaspersky CompanyAccount。

若要恢复您的密钥文件，执行下面任何的操作：

- 联系授权许可销售商。
- 使用您有效的激活码，通过卡巴斯基网站接收密钥文件。

关于数据提供

本地处理的数据

Kaspersky Security Center Linux 设计用于在组织网络中集中执行基本的管理和维护任务。Kaspersky Security Center Linux 为管理员提供组织网络安全级别详细信息的访问权限；Kaspersky Security Center Linux 允许管理员配置基于 Kaspersky 应用程序的所有保护组件。Kaspersky Security Center Linux 执行以下主要功能：

- 检测组织网络中的设备及其用户
- 创建用于设备管理的管理组层级
- 在设备上安装 Kaspersky 应用程序
- 管理已安装应用程序的设置和任务
- 在设备上激活 Kaspersky 应用程序
- 管理用户账户
- 查看设备上的 Kaspersky 应用程序运行信息
- 查看报告

为执行其主要功能，Kaspersky Security Center Linux 可以接收、存储和处理以下信息：

- 通过扫描 Active Directory 或 Samba 域控制器或通过扫描 IP 间隔收到的有关组织网络上的设备的信息。管理服务器独立获取数据或从网络代理接收数据。

- 来自 Active Directory 和 Samba 的有关组织单位、域、用户和组的信息。管理服务器自行获取数据或从被分配充当分发点的网络代理接收数据。
- 受管理设备详细信息。网络代理将下面列出的数据从设备传输到管理服务器。用户在 Kaspersky Security Center Web Console 界面中输入设备的显示名称和说明：
  - 用于设备识别的受管理设备及其组件的技术说明：设备显示名称和描述、Windows 域名和类型（用于属于 Windows 域的设备）、Windows 环境中的设备名称（用于属于 Windows 域的设备）、DNS 域和 DNS 名称、IPv4 地址、IPv6 地址、网络位置、MAC 地址、操作系统类型、设备是否为虚拟机以及虚拟机监控程序类型，以及设备是否为动态虚拟机（作为 VDI 的一部分）。
  - 审计受管理设备所需的受管理设备及其组件的其他说明：操作系统体系结构、操作系统供应商、操作系统内部版本号、操作系统发行版 Id、操作系统位置文件夹、虚拟机类型（如果设备是虚拟机）、管理设备的虚拟管理服务器的名称。
  - 受管理设备上的操作的详细信息：上次更新的日期和时间、设备在网络中最后一次可见的时间、重新启动等待状态以及设备打开的时间。
  - 设备用户账户及其工作会话的详细信息。
- 通过在受管理设备上运行远程诊断接收到的数据：跟踪文件、系统信息、设备上安装的卡巴斯基应用程序的详细信息、转储文件、事件日志、从卡巴斯基技术支持接收到的运行诊断脚本的结果。
- 分发点运行统计数据（如果设备是分发点）。网络代理将数据从设备传输到管理服务器。
- 用户在 Kaspersky Security Center Web Console 中输入的分发点设置。
- 设备上安装的 Kaspersky 应用程序的详细信息。受管理应用程序通过网络代理将数据从设备传输到管理服务器：
  - 受管理设备上安装的 Kaspersky 应用程序的设置：Kaspersky 应用程序名称和版本、状态、实时保护状态、上次设备扫描日期和时间、检测到的威胁数、无法清除的对象数、应用程序组件的可用性和状态、Kaspersky 应用程序设置和任务的详细信息、当前和备用授权许可密钥的信息、应用程序安装日期和 ID。
  - 应用程序操作统计信息：与受管理设备上的 Kaspersky 应用程序组件状态变化有关的事件和与应用程序组件发起的任务的性能有关的事件。
  - Kaspersky 应用程序定义的设备状态。
  - Kaspersky 应用程序分配的标签。
- Kaspersky Security Center Linux 组件和 Kaspersky 受管理应用程序的事件中包含的数据。网络代理将数据从设备传输到管理服务器。
- 策略和策略配置文件中显示的 Kaspersky Security Center Linux 组件和 Kaspersky 受管理应用程序的设置。用户在 Kaspersky Security Center Web Console 界面中输入数据。
- Kaspersky Security Center Linux 组件和 Kaspersky 受管理应用程序的任务设置。用户在 Kaspersky Security Center Web Console 界面中输入数据。
- 系统管理功能处理的数据。网络代理将以下信息从设备传输到管理服务器：
  - 有关在受管理设备上检测到的硬件的信息（硬件注册表）。
  - 有关在受管理设备上安装的软件的信息（软件注册表）。软件可以与应用程序控制功能在设备上检测到的有关可执行文件的信息进行比较。

- 应用程序的用户类别。用户在 Kaspersky Security Center Web Console 界面中输入数据。
- “应用程序控制”功能在受管理设备上检测到的可执行文件的详细信息。受管理应用程序通过网络代理将数据从设备传输到管理服务器。相应应用程序的帮助文件中提供了完整的数据列表。
- 有关加密的 Windows 设备和加密状态的信息。受管理应用程序通过网络代理将数据从设备传输到管理服务器。
- 使用 Kaspersky 应用程序的数据加密功能在 Windows 设备上执行的数据加密的错误详细信息。受管理应用程序通过网络代理将数据从设备传输到管理服务器。相应应用程序的帮助文件中提供了完整的数据列表。
- 备份区中放置的文件的详细信息。受管理应用程序通过网络代理将数据从设备传输到管理服务器。相应应用程序的帮助文件中提供了完整的数据列表。
- 隔离区中放置的文件的详细信息。受管理应用程序通过网络代理将数据从设备传输到管理服务器。相应应用程序的帮助文件中提供了完整的数据列表。
- Kaspersky 专家为进行详细分析而请求的文件详细信息。受管理应用程序通过网络代理将数据从设备传输到管理服务器。相应应用程序的帮助文件中提供了完整的数据列表。
- 安装或连接到受管理设备并被“设备控制”功能检测到的外部设备（内存单元、信息传输工具、信息硬拷贝工具和连接总线）的详细信息。受管理应用程序通过网络代理将数据从设备传输到管理服务器。相应应用程序的帮助文件中提供了完整的数据列表。
- 有关加密设备和加密状态的信息。受管理应用程序通过网络代理将数据从设备传输到管理服务器。
- 有关设备上数据加密错误的信息。加密由卡巴斯基应用程序的加密数据功能执行。受管理应用程序通过网络代理将数据从设备传输到管理服务器。相应应用程序的在线帮助中提供了完整的数据列表。
- 受管理可编程逻辑控制器 (PLC) 列表。受管理应用程序通过网络代理将数据从设备传输到管理服务器。相应应用程序的帮助文件中提供了完整的数据列表。
- 创建威胁发展链所需的数据。受管理应用程序通过网络代理将数据从设备传输到管理服务器。相应应用程序的帮助文件中提供了完整的数据列表。
- 输入的激活码和密钥文件的详细信息。用户在管理控制台或 Kaspersky Security Center Web Console 界面中输入数据。
- 用户账户：名称、说明、全名、电子邮件地址、主要电话号码和密码。用户在 Kaspersky Security Center Web Console 界面中输入数据。
- 管理对象的修订历史。用户在 Kaspersky Security Center Web Console 界面中输入数据。
- 已删除的管理对象的注册表。用户在 Kaspersky Security Center Web Console 界面中输入数据。
- 从文件创建的安装包以及安装设置。用户在 Kaspersky Security Center Web Console 界面中输入数据。
- 在 Kaspersky Security Center Web Console 中显示 Kaspersky 公告所需的数据。用户在 Kaspersky Security Center Web Console 界面中输入数据。
- Kaspersky Security Center Web Console 中的受管理应用程序插件运行所需的数据，以及这些插件在常规运行期间保存在管理服务器数据库中的数据。相应应用程序的帮助文件中介绍了提供数据的描述和方式。
- Kaspersky Security Center Web Console 用户设置：界面的本地化语言和主题、监控面板显示设置、有关通知状态（已读/未读）的信息、电子表格中的列状态（显示/隐藏）、训练模式进度。用户在 Kaspersky Security Center Web Console 界面中输入数据。

- 受管理设备与 Kaspersky Security Center Linux 组件的安全连接的证书。用户在 Kaspersky Security Center Web Console 界面中输入数据。
- 用户已接受卡巴斯基法律协议条款的信息。
- 用户在 Kaspersky Security Center Web Console 或程序界面 Kaspersky Security Center OpenAPI 中输入的管理服务器数据。
- 用户在 Kaspersky Security Center Web Console 界面中输入的任何数据。

如果应用以下方法之一，则上面列出的数据可以在 Kaspersky Security Center Linux 中显示：

- 用户在 Kaspersky Security Center Web Console 界面中输入数据。
- 网络代理会自动从设备接收数据，并将其传输到管理服务器。
- 网络代理接收由 Kaspersky 受管理应用程序检索的数据，并将其传输到管理服务器。Kaspersky 受管理应用程序处理的数据列表在相应应用程序的帮助文件中提供。
- 管理服务器自行获取有关联网设备的信息，或从被分配充当分发点的网络代理接收数据。

列出的数据存储在管理服务器数据库中。用户名和密码以加密格式存储。

本地处理的所有数据都只能通过 Dump 文件、跟踪文件或 Kaspersky Security Center Linux 组件的日志文件（包括安装程序和实用程序创建的日志文件）传输到 Kaspersky。

Kaspersky Security Center Linux 组件的转储文件、跟踪文件或日志文件包含管理服务器、网络代理和 Kaspersky Security Center Web Console 的任意数据。这些文件可能包含个人或机密数据。Dump 文件、跟踪文件或日志文件以非加密形式存储在设备上。Dump 文件、跟踪文件或日志文件不会自动传输到卡巴斯基，但是管理员可以在技术支持要求下手动传输数据到 Kaspersky 以便解决 Kaspersky Security Center Linux 的表现问题。

Kaspersky 按照法律和相应的 Kaspersky 规则来保护所收到的任何信息。数据均通过安全渠道传输。

单击管理控制台或 Kaspersky Security Center Web Console 中的链接，即表示用户同意自动传输以下数据：

- Kaspersky Security Center Linux 代码
- Kaspersky Security Center Linux 版本
- Kaspersky Security Center Linux 本地化
- 授权许可 ID
- 授权许可类型
- 授权许可是否是通过合作伙伴购买的

通过每个链接提供的数据列表取决于链接的目的和位置。

Kaspersky 以匿名形式使用接收的数据，并且只用于常规统计。摘要统计根据原始收到的信息自动生成，不包含任何个人或机密数据。一旦积累了新数据，就会擦除以前的数据（一年一次）。摘要统计无限存储。

关于订阅

*Kaspersky Security Center Linux 订阅*是在所选设置（订阅过期时间、受保护设备数量）下使用程序的订购。您可以和您的服务提供商（例如，互联网提供商）注册您的 Kaspersky Security Center Linux 订阅。订阅可以自动或手动续费，您也可以取消订阅。

订阅可以是限期的（例如，一年）或不限期的。如果要在限期订阅后继续使用 Kaspersky Security Center，您必须续费订阅。无限制订阅如果已经预付给服务提供商了，则会在到期日自动续费。

当受限制订阅过期时，可为您提供一个使产品继续工作的宽限期以便您及时续费。宽限期的可用性和期限由服务提供商提供。

要在订阅下使用 Kaspersky Security Center Linux，您必须应用从服务提供商收到的激活码。

您仅可以在订阅过期后或者取消订阅后为 Kaspersky Security Center Linux 申请不同的激活码。

取决于服务提供商，订阅管理可能的操作也会不同。服务提供商可以不提供订阅宽限期，因此程序会失去它的功能。

订阅激活码无法用于激活 Kaspersky Security Center 的早期版本。

在订阅下使用应用程序时，Kaspersky Security Center Linux 在指定时间间隔自动尝试访问激活服务器，直到订阅过期。如果无法使用系统 DNS 访问服务器，应用程序将使用公共 DNS 服务器。您可以在服务提供商网站续费您的订阅。

激活 Kaspersky Security Center Linux

您可以激活授权许可功能以使用 Kaspersky Security Center Linux 的附加功能。有两种方法可以完成此任务：使用管理服务器快速启动向导或管理服务器属性。

要激活 Kaspersky Security Center Linux 的授权许可功能：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ()。

   管理服务器属性窗口将打开。

2. 在“**常规**”选项卡上，选择“**授权许可密钥**”区域。

3. 在**当前授权许可**下，单击**选择**按钮。

4. 在打开的窗口中，选择要用于激活 Kaspersky Security Center Linux 的授权许可密钥。如果未列出授权许可密钥，请单击**添加新授权许可密钥**按钮，然后指定新的授权许可密钥。

5. 如有必要，您还可以添加备用授权许可密钥。为此，请在**备用授权许可密钥**下，单击**选择**按钮，然后选择现有授权许可密钥或添加新授权许可密钥。请注意，如果没有活动授权许可密钥，则无法添加备用授权许可密钥。

6. 单击“**保存**”按钮。

受管理卡巴斯基应用程序的授权许可

此部分描述了使用受管理 Kaspersky 应用程序的授权许可密钥时相关的 Kaspersky Security Center 功能。

Kaspersky Security Center Linux 允许您集中为客户端设备上的 Kaspersky 应用程序分发授权许可密钥、监控其使用情况，以及续订授权许可。

使用 Kaspersky Security Center 添加授权许可密钥时，该密钥的设置会保存在管理服务器上。应用程序会根据该信息生成一份授权许可密钥使用情况的报告，并通知管理员密钥属性中指定的授权许可期满日期，以及是否违反此限制。您可以在管理服务器设置内配置授权许可密钥使用情况的通知。

受管理应用程序的授权许可

安装到受管理设备上的 Kaspersky 应用程序必须通过将密钥文件或激活码应用到每个应用程序来获得授权。密钥文件或激活码可以按以下方法部署：

- 自动部署
- 受管理应用程序安装包
- 受管理应用程序的“添加授权许可密钥”任务
- 受管理应用程序的手动激活

您可以通过上面列出的任何方法添加新的活动或备用授权许可密钥。卡巴斯基应用程序当前使用一个活动密钥并存储一个备用密钥以在活动密钥到期后应用。您为其添加授权许可密钥的应用程序可定义密钥是活动密钥还是备用密钥。密钥定义不依赖于您用于添加新授权许可密钥的方法。

自动部署

如果您使用不同的受管理应用程序，且您必须将特定密钥文件或激活码部署到设备，请选择其他方法部署激活码或密钥文件。

Kaspersky Security Center 允许您自动部署可用授权许可密钥到设备。例如，三个授权许可密钥被存储在管理服务器存储库。您已对所有三个授权许可密钥启用了**自动分发的授权许可密钥**。Kaspersky 安全应用程序—例如，Kaspersky Endpoint Security for Linux— 被安装到组织设备。发现必须部署授权许可密钥的新设备。应用程序决定，例如，存储库中的两个授权许可密钥可以被部署到设备：授权许可密钥 *Key_1*和授权许可密钥 *Key_2*。这些授权许可密钥之一被部署到设备。此种情况下，无法预见两个授权许可密钥中的哪个将被部署到设备，因为自动部署授权许可密钥不提供给任何管理员活动。

当部署授权许可密钥时，设备为该授权许可密钥重新计算。您必须确保部署授权许可密钥的设备数量不超过授权许可限制。如果设备数量超过授权许可限制，所有不被授权许可覆盖的设备将被分配*严重*状态。

部署之前，密钥文件或激活码必须添加到管理服务器存储库。

说明：

- 添加授权许可密钥到管理服务器存储库
- 自动分发授权许可密钥

请注意，在以下情况下，自动分发的授权许可密钥可能不会显示在虚拟管理服务器存储库中：

- 授权许可密钥对于应用程序无效。
- 虚拟管理服务器没有受管理设备。
- 授权许可密钥已用于由另一个虚拟管理服务器管理的设备，并且已达到设备数量限制。

添加密钥文件或激活码到受管理应用程序安装包

对于安全应用程序，该选项不被推荐。添加到安装包的密钥文件或激活码可能被盗用。

如果您使用安装包安装受管理应用程序，您可以在该安装包中或在应用程序策略中指定激活码或密钥文件。授权许可密钥将在下一次设备与管理服务器同步时被部署到受管理应用程序。

操作说明：将授权许可密钥添加到安装包

通过为受管理应用程序添加授权许可密钥任务来进行部署

如果您选择使用为受管理应用程序添加授权许可密钥任务，您可以选择要部署到设备的授权许可密钥并以任何便捷的方法选择设备—例如，通过选择管理组或设备分类。

部署之前，密钥文件或激活码必须添加到管理服务器存储库。

说明：

- 添加授权许可密钥到管理服务器存储库
- 部署授权许可密钥到客户端设备

手动添加激活码或密钥文件到设备

您可以激活本地安装的 Kaspersky 应用程序，通过使用应用程序界面提供的工具。请参考已安装应用程序的文档。

添加授权许可密钥到管理服务器存储库

要添加授权许可密钥到管理服务器存储库：

1. 在主菜单中，转到“**操作**” → “**授权许可**” → “**卡巴斯基授权许可**”。
2. 单击“**添加**”按钮。
3. 选择您要添加的内容：
   - **添加密钥文件**
     单击“**选择密钥文件**”按钮并浏览到您要添加的 .key 文件。
   - **输入激活码**
     在文本字段指定激活码并单击“**发送**”按钮。
4. 单击“**关闭**”按钮。

授权许可密钥或几个授权许可密钥被添加到管理服务器存储库。

部署授权许可密钥到客户端设备

Kaspersky Security Center Web Console 允许您自动或通过添加授权许可密钥任务将授权许可密钥分发至客户端设备。

在部署之前，请将授权许可密钥添加到管理服务器存储库。

要通过添加密钥任务将授权许可密钥分发到客户端设备：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。
2. 单击**添加**。
   新任务向导启动。使用**下一步**按钮进行向导。
3. 在**应用程序**下拉列表中，选择要为其添加授权许可密钥的应用程序。
4. 在**任务类型**列表中选择**添加密钥**任务。
5. 在**任务名称**字段中，指定新任务的名称。
6. 选择要将任务分配到的设备。
7. 在向导的**选择授权许可密钥**步骤中，单击**添加密钥**链接以添加授权许可密钥。
8. 在密钥添加窗格中，使用以下选项之一添加授权许可密钥：

   仅当您在创建添加密钥任务之前未将授权许可密钥添加到管理服务器存储库时，才需要添加授权许可密钥。

   - 选择**输入激活码**选项以输入激活码，然后执行以下操作：

     a. 指定激活码，然后单击**发送**按钮。
     有关授权许可密钥的信息将显示在密钥添加窗格中。

     b. 单击“**保存**”按钮。

     如果您想要自动将授权许可密钥分发到受管理设备，请启用**自动分发授权许可密钥到受管理设备**选项。

     密钥添加窗格将关闭。

   - 选择**添加密钥文件**选项以添加密钥文件，然后执行以下操作：

     a. 单击**选择密钥文件**按钮。

     b. 在打开的窗口中，选择一个密钥文件，然后单击“**打开**”按钮。
     有关授权许可密钥的信息将显示在授权许可密钥添加窗格中。

c. 单击“**保存**”按钮。

> 如果您想要自动将授权许可密钥分发到受管理设备，请启用**自动分发授权许可密钥到受管理设备**选项。

密钥添加窗格将关闭。

9. 在密钥表中选择授权许可密钥。
10. 如果您想将此密钥用作备用密钥，请在向导的**授权许可信息**步骤中启用“**用作备用密钥**”选项。
    在这种情况下，备用密钥将在活动密钥过期后被应用。
11. 在向导的“**完成任务创建**”步骤启用“**创建完成时打开任务详情**”选项以修改默认任务设置。
    如果您不启用该选项，任务将使用默认设置创建。您可以稍后修改默认设置。
12. 单击“**完成**”按钮。
    向导将创建任务。如果启用了“**创建完成时打开任务详情**”选项，任务属性窗口将自动打开。在此窗口中，您可以指定常规任务设置，并根据需要更改任务创建期间指定的设置。

    > 您还可以通过单击任务列表中已创建任务的名称来打开任务属性窗口。

    任务被创建、配置并显示在任务列表中。
13. 要运行任务，请在任务列表中选择它，然后单击“**开始**”按钮。
    您还可以在任务属性窗口的**计划**选项卡上设置任务启动计划。
    有关计划启动设置的详细说明，请参阅常规任务设置。

当任务完成时，授权许可密钥将被部署到所选设备。

自动分发授权许可密钥

如果密钥位于管理服务器上的授权许可密钥存储区中，则 Kaspersky Security Center Linux 允许将这些授权许可密钥自动分发至受管理设备。

要将授权许可密钥自动分发至受管理设备，请执行以下操作：

1. 在主菜单中，转到“**操作**” → “**授权许可**” → “**卡巴斯基授权许可**”。
2. 选择您要自动发布到设备的授权许可密钥名称。
3. 在打开的授权许可密钥属性窗口中，选中“**自动分发授权许可密钥到受管理设备**”复选框。
4. 单击“**保存**”按钮。

授权许可密钥将被自动分发到所有兼容设备。

授权许可密钥分发是通过网络代理执行的。没有为应用程序创建授权许可密钥分发任务。

在自动分发授权许可密钥过程中，授权许可对设备数量的限制得到考虑。授权许可限制在授权许可密钥属性中设置。如果达到授权许可限制，对该授权许可密钥的分发自动停止。

请注意，在以下情况下，自动分发的授权许可密钥可能不会显示在虚拟管理服务器存储库中：

- 授权许可密钥对于应用程序无效。
- 虚拟管理服务器没有受管理设备。
- 授权许可密钥已用于由另一个虚拟管理服务器管理的设备，并且已达到设备数量限制。

如果您选择授权许可密钥属性窗口中的**自动分发授权许可密钥到受管理设备**复选框，授权许可密钥会立即分发在您的网络上。如果不选择此选项，您可以稍后手动分发授权许可密钥。

查看使用中授权许可密钥的相关信息

要查看添加到管理服务器存储库的授权许可密钥列表：

在主菜单中，转到“**操作**” → “**授权许可**” → “**卡巴斯基授权许可**”。

显示的列表包含添加到管理服务器存储库的密钥文件和激活码。

要查看关于授权许可密钥的详细信息：

1. 在主菜单中，转到“**操作**” → “**授权许可**” → “**卡巴斯基授权许可**”。
2. 点击所需授权许可密钥的名称。

在打开的授权许可密钥属性窗口，您可以查看：

- 在“**常规**”选项卡上—关于授权许可密钥的主要信息
- 在“**设备**”选项卡上—授权许可密钥用于激活已安装 Kaspersky 应用程序的客户端设备列表

要查看哪些授权许可密钥被部署到特定客户端设备：

1. 在主菜单中，转到 “**资产(设备)**” → “**受管理设备**”。
2. 点击所需设备的名称。
3. 在打开的设备属性窗口中，选择“**应用程序**”选项卡。
4. 点击您要查看其授权许可密钥信息的应用程序名称。
5. 在打开的应用程序属性窗口中，选择“**常规**”选项卡，然后打开“**授权许可**”区域。

将显示有关活动和备用授权许可密钥的主要信息。

为了定义虚拟管理服务器授权许可密钥的最新设置，管理服务器每天至少发送一次请求到 Kaspersky 激活服务器。如果无法使用系统 DNS 访问服务器，应用程序将使用公共 DNS 服务器。

超出了授权许可限制事件

Kaspersky Security Center Linux 允许您获取客户端设备上安装的 Kaspersky 应用程序的授权许可达到限制的事件信息。

授权许可达到限制的此类事件的重要级别根据以下规则定义：

- 如果当前使用单一授权许可的单元的数量达到该授权许可所覆盖的单元总数的 90% 和 100% 之间，事件等级就是**信息**重要级别。
- 如果当前使用单一授权许可的单元的数量达到该授权许可所覆盖的单元总数的 100% 和 110% 之间，事件等级就是**警告**重要级别。
- 如果当前使用单一授权许可的单元的数量超过该授权许可所覆盖的单元总数的 110%，事件等级就是**严重事件**重要级别。

从存储库删除授权许可密钥

当您删除部署到受管理设备上的活动授权许可密钥时，应用程序将继续工作在受管理设备。

要从管理服务器存储库中删除密钥文件或激活码：

1. 检查管理服务器未使用您要删除的密钥文件或激活码。如果管理服务器使用了该密钥，则您无法删除该密钥。要执行检查：
   a. 在主菜单，单击管理服务器旁边的设置图标 ()。
      管理服务器属性窗口将打开。
   b. 在“**常规**”选项卡上，选择“**授权许可密钥**”区域。
   c. 如果所需的密钥文件或激活码显示在打开的区域中，请单击“**删除活动授权许可密钥**”按钮，然后确认操作。之后，管理服务器不再使用删除的授权许可密钥，但该密钥仍保留在管理服务器存储库中。如果所需的密钥文件或激活码未显示，管理服务器不会使用该密钥文件或激活码。
2. 在主菜单中，转到“**操作 → 授权许可 → 卡巴斯基授权许可**”。
3. 选择所需的密钥文件或激活码，然后单击**删除**按钮。

所选密钥文件或激活码即从存储库中删除。

您可以再次添加一个已删除的授权许可密钥或添加一个新授权许可密钥。

Revoking consent with an End User License Agreement

If you decide to stop protecting some of your client devices, you can revoke the End User License Agreement (EULA) for any managed Kaspersky application. You must uninstall the selected application before revoking its EULA.

To revoke a EULA for managed Kaspersky applications:

1. Open the Administration Server properties window and on the 常规 tab select the 最终用户授权许可协议 section.

   A list of EULAs—accepted upon creation of installation packages, at the seamless installation of updates, or upon deployment of Kaspersky Security for Mobile—is displayed.

2. In the list, select the EULA that you want to revoke.

   You can view the following properties of the EULA:

   - Date when the EULA was accepted
   - Name of the user who accepted the EULA

3. Click the acceptance date of any EULA to open its properties window that displays the following data:

   - Name of the user who accepted the EULA
   - Date when the EULA was accepted
   - Unique identifier (UID) of the EULA
   - Full text of the EULA
   - List of objects (installation packages, seamless updates, mobile apps) linked to the EULA, and their respective names and types

4. In the lower part of the EULA properties window, click the 撤回授权许可协议 button.

   > If there exist any objects (installation packages and their respective tasks) that prevent the EULA from being revoked, the corresponding notification is displayed. You cannot proceed with revocation until you delete these objects.

   In the window that opens, you are informed that you must first uninstall the Kaspersky application corresponding to the EULA.

5. Click the button to confirm revocation.

The EULA is revoked. It is no longer displayed in the list of License Agreements in the 最终用户授权许可协议 section. The EULA properties window closes; the application is no longer installed.

Renewing licenses for Kaspersky applications

You can renew a Kaspersky application license that has expired or is about to expire (in less than 30 days).

To renew an expired license or a license that is about to expire:

1. Do either of the following:

   - In the main menu, go to 操作 → 授权许可 → 卡巴斯基授权许可.
   - In the main menu, go to 监控和报告 → 控制板, and then click the **View expiring licenses** link next to a notification.

   The 卡巴斯基授权许可 window opens, where you can view and renew licenses.

2. Click the 续费授权许可 link next to the required license.

   By clicking a license renewal link, you agree to transfer to Kaspersky the following information about Kaspersky Security Center Linux: its version, the localization you are using, the software license ID (that is, the ID of the license you are renewing), and whether you purchased the license via a partner company or not.

3. In the window of the license renewal service that opens follow the instructions to renew a license.

   The license is renewed.

In Kaspersky Security Center Web Console, the notifications are displayed when a license is about to expire, according to the following schedule:

- 30 days before the expiration
- 7 days before the expiration
- 3 days before the expiration
- 24 hours before the expiration
- When a license has expired

使用 Kaspersky Marketplace 选择 Kaspersky 商业解决方案

市场 是主菜单中的一个区域，可让您查看整套 Kaspersky 商业解决方案，选择您需要的解决方案，并在 Kaspersky 网站上进行购买。您可以使用筛选功能，以便仅查看适合您的组织和信息安全系统要求的解决方案。选择解决方案后，Kaspersky Security Center Linux 会将您重定向到 Kaspersky 网站上的相关网页，以了解有关该解决方案的更多信息。每个网页都可让您继续购买或包含有关购买过程的说明。

在"**市场**"区域中，可以使用以下条件筛选 Kaspersky 解决方案：

- 要保护的设备（端点、服务器和其他类型的资产）数量：
  - 50-250
  - 250–1000
  - 大于 1000
- 组织的信息安全团队的成熟度：
  - **基础**

    这是只有一个 IT 团队的企业的典型成熟度。自动阻止最大可能数量的威胁。
  - **最佳**

    这是在 IT 团队内具有特定 IT 安全功能的企业的典型成熟度。在此级别，所需的解决方案使公司能够应对商品威胁以及绕过现有预防机制的威胁。
  - **专家**

这是具有复杂和分布式 IT 环境的企业的典型成熟度。IT 安全团队成熟或者公司拥有 SOC（安全运营中心）团队。所需的解决方案使公司能够应对复杂威胁和针对性攻击。

- 您要保护的资产类型：
  - **端点**：员工的工作站、物理机和虚拟机、嵌入式系统
  - **服务器**：物理和虚拟服务器
  - **云**：公有、私有或混合云环境；云服务
  - **网络**：局域网、IT 基础设施
  - **服务**：Kaspersky 提供的安全相关服务

要查找和购买 Kaspersky 商业解决方案：

1. 在主菜单中，转到“**市场**”。
   默认情况下，该区域显示所有可用的 Kaspersky 商业解决方案。
2. 要仅查看适合您组织的解决方案，请在筛选器中选择所需的值。
3. 点击您要购买或想要了解更多信息的解决方案。

您将被重定向到解决方案网页。您可以按照屏幕上的说明进行购买。

配置卡巴斯基应用程序

本节包含有关手动配置策略和任务、用户角色、构建管理组结构和任务层级的信息。

方案：配置网络保护

快速启动向导使用默认设置创建策略和任务。这些设置可能不是最佳的，甚至是组织不允许的。因此，我们建议您微调这些策略和任务并，然后建其他策略和任务（如果它们对于您的网络而言是必需的）。

先决条件

在您开始之前，确保您已做了如下：

- 安装了 Kaspersky Security Center Linux 管理服务器
- 安装了 Kaspersky Security Center Web Console
- 完成了 Kaspersky Security Center Linux 主安装方案
- 完成了快速启动向导，或在“**受管理设备**”管理组中手动创建了以下策略和任务：
  - Kaspersky Endpoint Security 策略
  - 更新 Kaspersky Endpoint Security 的组任务
  - 网络代理策略

阶段

分阶段配置网络保护：

1. **设置和传播 Kaspersky 应用程序策略和策略配置文件**

   要为安装在受管理设备上的 Kaspersky 应用程序配置和传播设置，您可以使用两种不同的安全管理方法—以设备为中心或以用户为中心。这两种方法可以被合并。

2. **配置任务以远程管理 Kaspersky 应用程序**

   检查使用快速启动向导创建的任务并按需要调整它们。

   使用说明：为 Kaspersky Endpoint Security 设置组任务

   如果必要，创建附加任务以管理安装在客户端设备上的 Kaspersky 应用程序。

3. **评估和限制数据库上的事件负载**

   受管理应用程序运行相关的事件信息将被从客户端设备上传输并记录至管理服务器数据库。要降低管理服务器负载，请评估并限制可以存储在数据库中的最大事件数量。

   使用说明：设置最大事件数。

结果

当您完成该方案时，您将通过配置 Kaspersky 应用程序、任务以及管理服务器接收的事件来保护您的网络：

- Kaspersky 应用程序是根据策略和策略配置文件配置的。
- 应用程序通过一组任务进行管理。
- 设置可以存储在数据库中的最大事件数。

当网络保护配置完成时，您可以继续配置 Kaspersky 数据库和应用程序的常规更新。

关于以设备为中心和以用户为中心的安全管理方法

您可以从设备功能的立场和从用户角色的立场管理安全设置。第一种方法叫做*以设备为中心的安全管理*，第二种叫做*以用户为中心的安全管理*。要应用不同的应用程序设置到不同的设备，您可以使用两种方法的任意或组合。

以设备为中心的安全管理使您可以根据特定于设备的功能将不同的安全应用程序设置应用于受管理设备。例如，您可以将不同的设置应用于分配给不同管理组的设备。

以用户为中心的安全管理使您可以将不同的安全应用程序设置应用于不同的用户角色。您可以创建多个用户角色，为每个用户分配合适的用户角色，并为具有不同角色的用户所拥有的设备定义不同的应用程序设置。例如，您可能要应用不同的应用程序设置到会计和人力资源（HR）人员的设备。结果，当实现了以用户为中心的安全管理时，每个部门—财务部门和人事部门—具有自己的 Kaspersky 应用程序设置配置。设置配置定义了哪些应用程序设置可以被用户更改以及哪些被强制设置并被管理员锁定。

通过使用以用户为中心的安全管理，您可以应用特别应用程序设置到单个用户。这可能用在员工在公司有独一角色或您要监控与个别人的设备相关的安全问题时。取决于该员工在公司的角色，您可以扩展或限制该员工更改应用程序设置的权限。例如，您可能要扩展在本地办公室管理客户端设备的系统管理员的权限。

您也可以组合以设备为中心的安全管理和以用户为中心的安全管理方法。例如，您可以为每个管理组配置特定的应用程序策略，然后为企业的一个或几个用户角色创建策略配置文件。此种情况下，策略和策略配置文件按照以下优先级进行应用：

1. 为以设备为中心的安全管理创建的策略被应用。
2. 它们根据策略配置文件属性被策略配置文件修改。
3. 策略被与用户角色关联的策略配置文件修改。

策略设置和传播：以设备为中心的方法

当您完成该方案后，应用程序将在所有受管理设备上被配置，与您定义的应用程序策略和策略配置文件一致。

先决条件

在开始之前，确保已安装 Kaspersky Security Center Linux 管理服务器和 Kaspersky Security Center Web Console。您也可能要考虑以用户为中心的安全管理作为以设备为中心的方案的附加选项。了解更多两个管理方法的详情。

阶段

以设备为中心的 Kaspersky 应用程序管理方案包含以下步骤：

1. **配置应用程序策略**

   通过为每个应用程序创建策略来配置安装在受管理设备上的 Kaspersky 应用程序设置。策略集将被传播到客户端设备。

   当您在快速启动向导中配置网络保护时，Kaspersky Security Center Linux 为以下应用程序创建默认策略：

   - Kaspersky Endpoint Security for Linux——适用于基于 Linux 的客户端设备
   - Kaspersky Endpoint Security for Windows——适用于基于 Windows 的客户端设备

   如果您通过使用该向导完成了配置过程，您不必为该应用程序创建新策略。

   如果您有几个管理服务器和/或管理组的层级结构，从属管理服务器和子管理组默认从主管理服务器继承策略。您可以强制子组和从属管理服务器的继承以防止上游策略设置的修改。如果您仅要一部分设置被强制继承，您可以在上游策略中锁定它们。剩余未锁定的设置将可以在下流策略中修改。创建的策略层级将允许您有效管理管理组中的设备。

   说明：创建一个策略

2. **创建策略配置文件（可选）**

   如果您想让单一管理组中的设备在不同策略设置下运行，为这些设备创建策略配置文件。策略配置文件是策略设置的命名子集。该子集随带策略在大设备上分发，在特别条件*配置文件激活条件*下将其补充。配置文件仅包含与"基本"策略不同的设置，并在受管理设备上活动。

   通过使用配置文件激活条件，例如，您可以将不同的策略配置文件应用到具有特定硬件配置或标记了特定标签的设备。使用标签筛选满足特别标准的设备。例如，您可以创建名为 *CentOS* 的标签，使用该标签标记所有运行 CentOS 操作系统的设备，然后指定该标签作为策略配置文件激活条件。结果，安装在所有 CentOS 设备上的 Kaspersky 应用程序将被使用它们自己的策略配置文件管理。

   说明：

   - 创建策略配置文件
   - 创建策略配置文件激活规则

3. **传播策略和策略配置文件到受管理设备**

   默认情况下，管理服务器每 15 分钟自动与受管理设备同步一次。同步过程中，新的或更改的策略和策略配置文件被传播到受管理设备。您可以避免自动同步并通过使用强制同步命令手动运行同步。一旦同步完成，策略和策略配置文件被传送和应用到安装的 Kaspersky 应用程序。

   您可以检查策略和策略配置文件是否被传送到了设备。Kaspersky Security Center Linux 在设备属性中指定传送日期和时间。

   说明：强制同步

结果

当以设备为中心的方案完成时，Kaspersky 应用程序根据指定的设置被配置并通过策略层级传播。

配置的应用程序策略和策略配置文件将被自动应用到添加到管理组的新设备。

策略设置和传播：以用户为中心的方法

本节介绍以用户为中心的集中配置安装到受管理设备上的 Kaspersky 应用程序的方案。当您完成该方案后，应用程序将在所有受管理设备上被配置，与您定义的应用程序策略和策略配置文件一致。

先决条件

在开始之前，确保已成功安装 Kaspersky Security Center Linux 管理服务器和 Kaspersky Security Center Web Console，并已完成主要部署方案。您也可能要考虑以设备为中心的安全管理作为以用于为中心的方案的附加选项。了解更多两个管理方法的详情。

过程

以用户为中心的 Kaspersky 应用程序管理方案包含以下步骤：

1. **配置应用程序策略**

   通过为每个应用程序创建策略来配置安装在受管理设备上的 Kaspersky 应用程序设置。策略集将被传播到客户端设备。

   当您在快速启动向导配置您网络的保护时，Kaspersky Security Center Linux 为 Kaspersky Endpoint Security 创建默认策略。如果您通过使用该向导完成了配置过程，您不必为该应用程序创建新策略。

   如果您有几个管理服务器和/或管理组的层级结构，从属管理服务器和子管理组默认从主管理服务器继承策略。您可以强制子组和从属管理服务器的继承以防止上游策略设置的修改。如果您仅要一部分设置被强制继承，您可以在上游策略中锁定它们。剩余未锁定的设置将可以在下流策略中修改。创建的策略层级将允许您有效管理管理组中的设备。

   说明：创建一个策略

2. **指定设备所有者**

   分配受管理设备到对应用户。

   说明：指派用户作为设备所有者

3. **为您的企业定义用户角色**

   联想您企业的员工所做的不同工作。您必须根据他们的角色划分所有员工。例如，您可以按照部门、专业或职位划分他们。然后您将需要为每个组创建用户角色。记住，每个用户角色将拥有其自己的策略配置文件，包含该角色特有的应用程序设置。

4. **创建用户角色**

   为每个员工组创建和配置用户角色或使用预定义用户角色。用户角色将包含到应用程序功能的访问权限组。

   说明：创建一个用户角色

5. **定义每个用户角色范围**

   对于每个创建的用户角色，定义用户和/或安全组以及管理组。与用户角色关联的设置仅应用到属于该角色用户的设备，以及仅在这些设备属于与该角色关联的组（包括子组）时。

   说明：编辑用户角色范围

6. **创建策略配置文件**

   为您企业中的每个用户角色创建策略配置文件。策略配置文件决定了哪些设置将被根据用户角色应用到用户设备上的应用程序。

   说明：创建一个策略配置文件

7. **关联策略配置文件与用户角色**

关联创建的策略配置文件与用户角色。此后：策略配置文件对具有特定角色的用户活动。策略配置文件中配置的设置将被应用到安装于用户设备上的 Kaspersky 应用程序。

说明：关联策略配置文件到角色

8 **传播策略和策略配置文件到受管理设备**

默认下，Kaspersky Security Center Linux 每 15 分钟自动同步管理服务器与受管理设备。同步过程中，新的或更改的策略和策略配置文件被传播到受管理设备。您可以避免自动同步并通过使用强制同步命令手动运行同步。一旦同步完成，策略和策略配置文件被传送和应用到安装的 Kaspersky 应用程序。

您可以检查策略和策略配置文件是否被传送到了设备。Kaspersky Security Center Linux 在设备属性中指定传送日期和时间。

说明：强制同步

结果

当以用户为中心的方案完成时，Kaspersky 应用程序根据指定的设置被配置并通过策略和策略配置文件层级传播。

对于新用户，您将必须创建新账户，分配一个创建的用户角色，并分配设备到用户。配置的应用程序策略和策略配置文件将被自动应用到该用户的新设备。

策略和策略配置文件

在 Kaspersky Security Center Web Console 中，可以为 Kaspersky 应用程序创建策略。该部分描述了策略和策略配置文件，并提供创建和修改它们的说明。

关于策略和策略配置文件

*策略*是应用于一个管理组和其子组的 Kaspersky 应用程序设置集。您可以在管理组的设备上安装多个 Kaspersky 应用程序。Kaspersky Security Center 为管理组中的每个 Kaspersky 应用程序提供一个策略。策略具有以下状态之一：

策略的状态

状态	描述
活动	应用于设备的当前策略。对于每个管理组中的 Kaspersky 应用程序，只能有一个策略处于活动状态。设备对 Kaspersky 应用程序应用活动策略的设置值。
非活动	当前未应用于设备的策略。
漫游	如果选择该选项，策略将在设备离开企业网络时变为活动状态。

策略根据以下规则发挥作用：

- 您可以为单个应用程序配置拥有不同值的多个策略。
- 对于当前应用程序，只能有一个策略处于活动状态。
- 策略可以有子策略。

通常，您可以将策略用作对紧急情况（如病毒攻击）的准备。例如，如果存在通过闪存驱动器进行的攻击，您可以激活相应策略来阻止访问闪存驱动器。在这种情况下，当前的活动策略将自动变为非活动状态。

为了防止维护多个策略，例如，在不同的场合下只是更改几个设置时，可以使用策略配置文件。

*策略配置文件*是策略设置值的命名子集，用于替换策略的设置值。策略配置文件影响受管理设备上有效设置的形成。*有效设置*是当前应用于设备的一组策略设置、策略配置文件设置和本地应用程序设置。

策略配置文件根据以下规则发挥作用：

- 当出现特定的激活情况时，策略配置文件生效。
- 策略配置文件包含的设置值与策略设置不同。
- 激活策略配置文件会更改受管理设备的有效设置。
- 一个策略可以包含最多 100 个策略配置文件。

关于“锁定”和锁定的设置

每个策略设置都有一个锁定按钮图标 (🔒)。下表显示了锁定按钮的状态：

锁定按钮状态

状态	描述
未定义	如果设置旁边显示打开的锁，并且禁用了切换按钮，则策略中未指定该设置。用户可以在受管理应用程序界面中更改这些设置。这些设置的类型称为“*未锁定*”。
强制	如果设置旁边显示关闭的锁，并且启用了切换按钮，则该设置应用于实施策略的设备。用户无法在受管理应用程序界面中修改这些设置的值。这些设置的类型称为“*已锁定*”。

我们强烈建议您关闭要在受管理设备上应用的策略设置的锁定。解锁的策略设置可以由卡巴斯基应用程序设置在受管理设备上重新分配。

您可以使用锁定按钮执行以下操作：

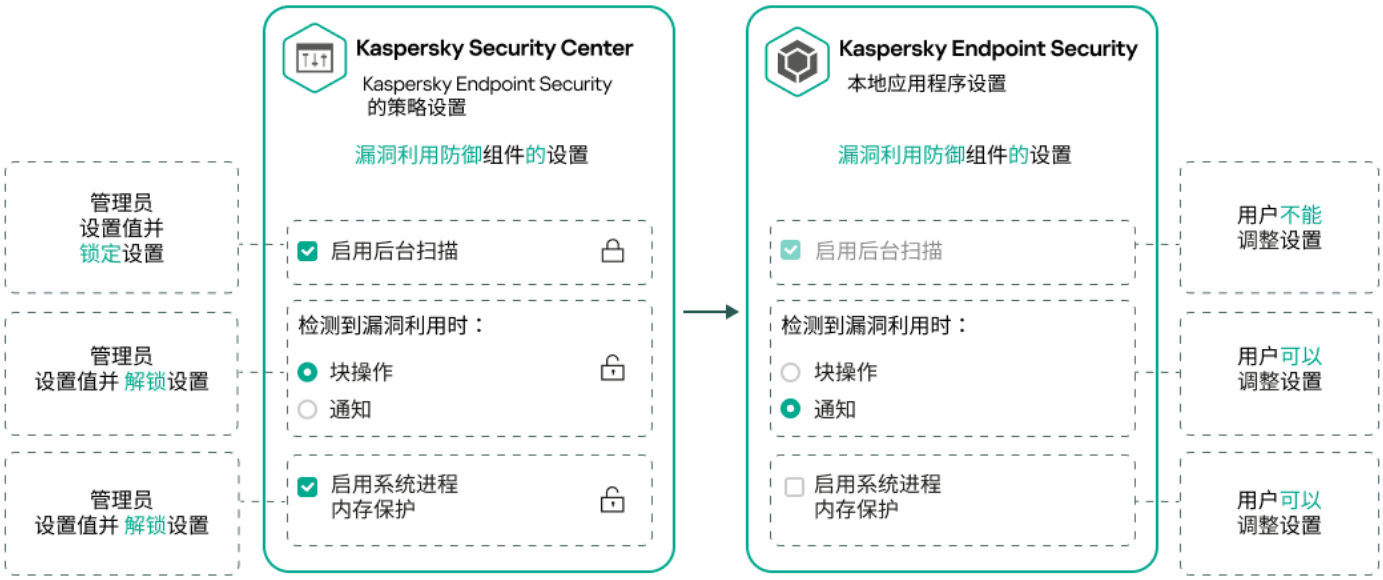
- 锁定管理子组策略的设置
- 在受管理设备上锁定本地 Kaspersky 应用程序的设置

因此，已锁定设置用于在受管理设备上实施有效设置。

有效设置实施的过程包括以下操作：

- 受管理设备将应用 Kaspersky 应用程序的设置值。
- 受管理设备应用策略的锁定设置值。

策略和受管理卡巴斯基应用程序包含相同的一组设置。配置策略设置时，受管理设备上的 Kaspersky 应用程序设置会更改值。您无法调整受管理设备上的已锁定设置（请参见下图）：



锁定和 Kaspersky 应用程序设置

策略继承和策略配置文件

本节提供有关策略和策略配置文件的层级和继承的信息。

策略层级

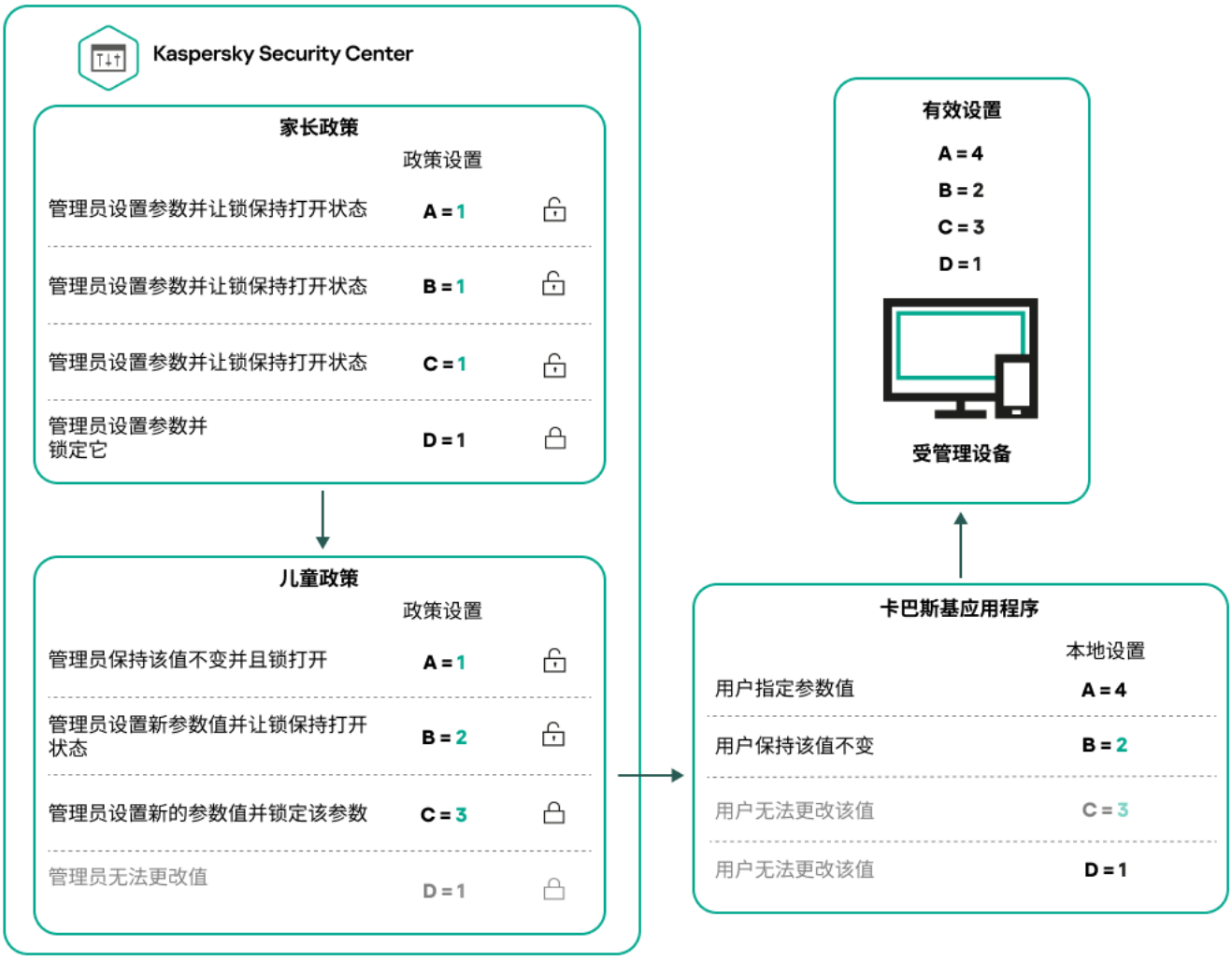
如果不同的设备需要不同的设置，则可以将设备组织到管理组中。

您可以为单个管理组指定策略。策略设置可以被*继承*。继承意味着子组中的策略设置值接收自更高级别的（父）管理组的策略。

因此，父组策略也叫*父策略*。子组策略也称为*子策略*。

默认情况下，管理服务器上存在至少一个受管理设备组。如果要创建自定义组，它们将创建为受管理设备组内的子组。

根据管理组的层级，同一应用程序的策略会互相作用。更高级别（父）管理组的策略中的锁定设置将重新分配子组的策略设置值（请参见下图）。

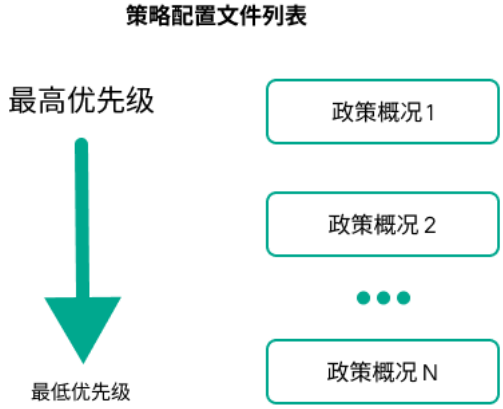


策略层级

策略层级中的策略配置文件

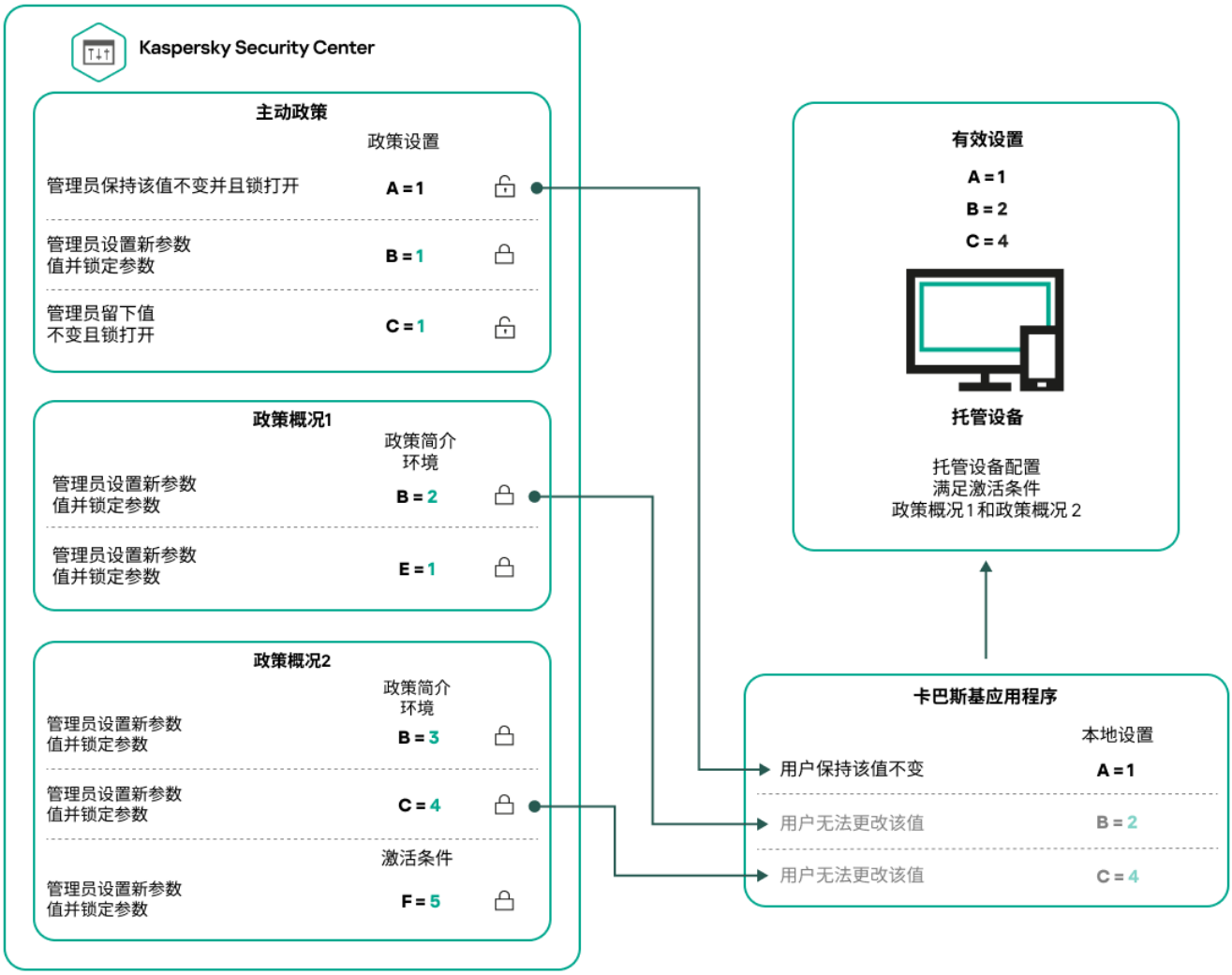
策略配置文件具有以下优先级分配条件：

- 配置文件在策略配置文件列表中的位置指示了其优先级。您可以更改策略配置文件优先级。列表中的最高位置指示最高优先级（请参见下图）。



策略配置文件的优先级定义

- 策略配置文件的激活条件互不依赖。可以同时激活多个策略配置文件。如果多个策略配置文件影响同一设置，则设备将采用策略配置文件中具有最高优先级的设置值（请参见下图）。



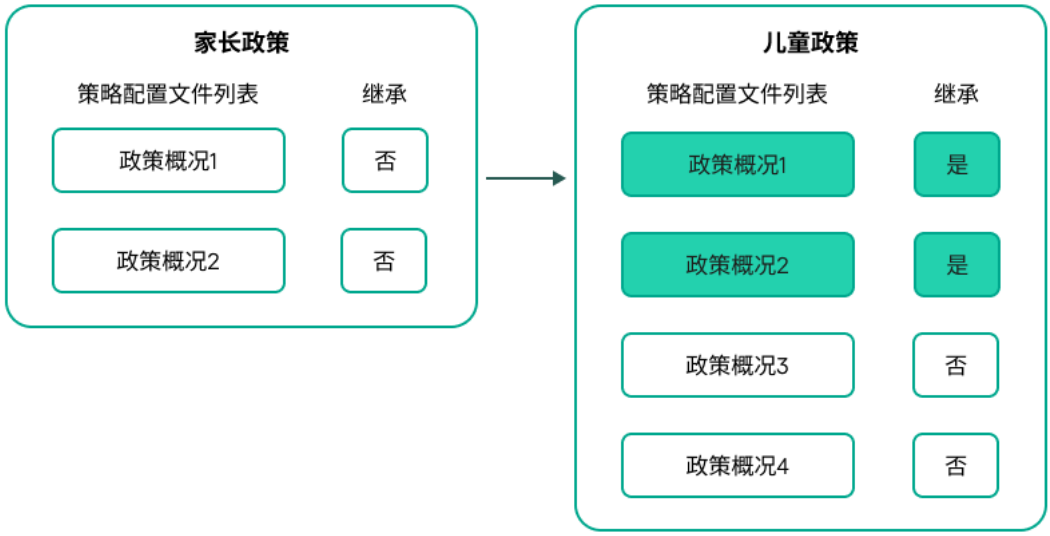
受管理设备配置满足多个策略配置文件的激活条件

继承层级中的策略配置文件

来自不同层次结构级别策略的策略配置文件符合以下条件：

- 较低级别的策略继承较高级别的策略的策略配置文件。从较高级别策略继承的策略配置文件比原始策略配置文件的级别具有更高的优先级。

- 您不能更改继承的策略配置文件的优先级（请参见下图）。

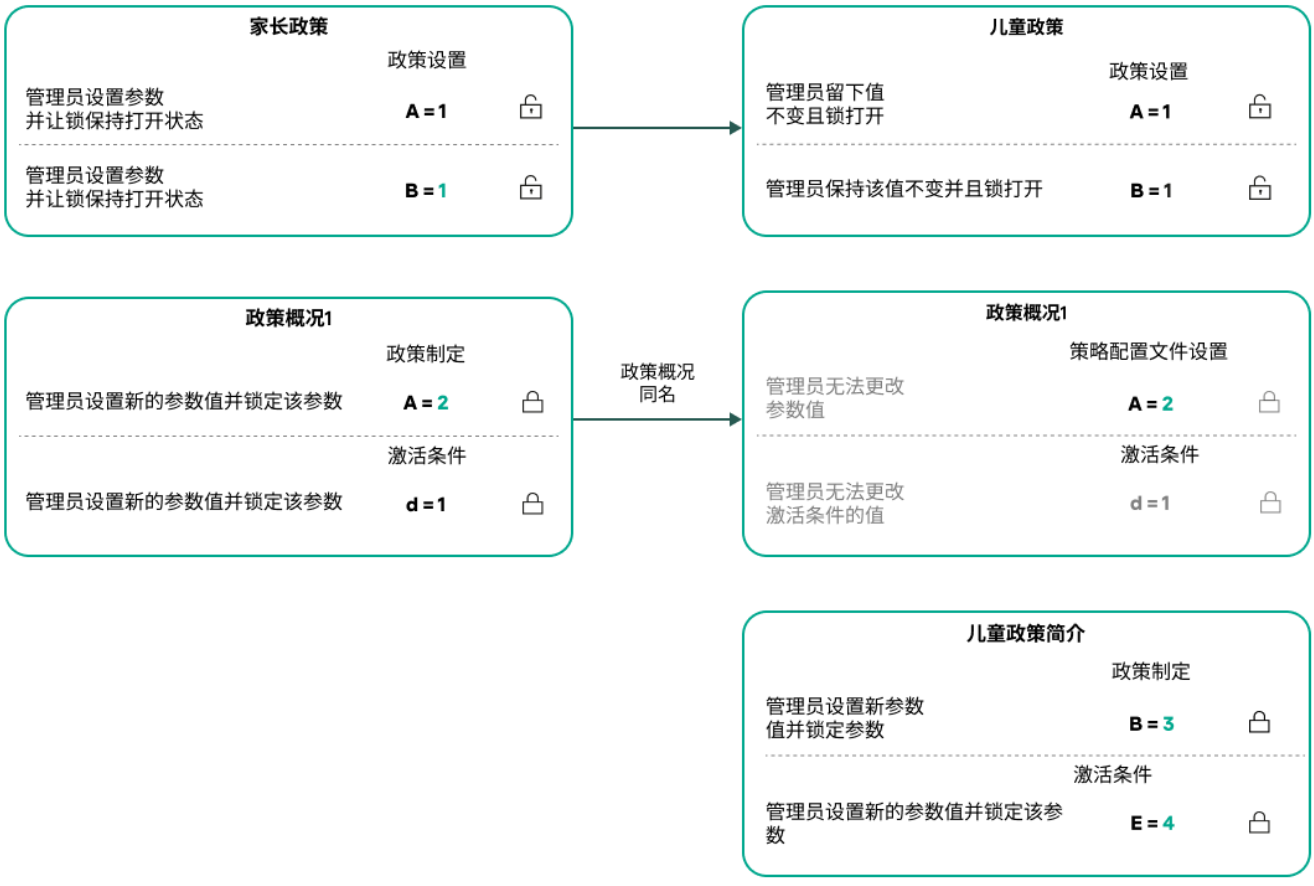


继承策略配置文件

具有相同名称的策略配置文件

如果在不同的层次结构级别中有两个名称相同的策略，则这两个策略按照以下规则起作用：

- 较高级别的策略配置文件的锁定设置和配置文件激活条件将更改较低级别的策略配置文件的设置和配置文件激活条件（请参见下图）。



子配置文件继承父策略配置文件的设置值

- 较高级别的策略配置文件的未锁定设置和配置文件激活条件不会更改较低级别的策略配置文件的设置和配置文件激活条件。

How settings are implemented on a managed device

Implementation of effective settings on a managed device can be described as follows:

- The values of all settings that have not been locked are taken from the policy.
- Then they are overwritten with the values of managed application settings.
- And then the locked settings values from the effective policy are applied. Locked settings values change the values of unlocked effective settings.

Managing policies

This section describes managing policies and provides information about viewing the list of policies, creating a policy, modifying a policy, copying a policy, moving a policy, forced synchronization, viewing the policy distribution status chart, and deleting a policy.

查看策略列表

您可以查看为管理服务器或任何管理组创建的策略列表。

要查看策略列表，请执行以下操作：

1. 在主菜单中，转到“**资产(设备)**” → “**组层级**”。
2. 在管理组结构中，选择您要查看其策略列表的管理组。

   策略列表以表格格式出现。如果没有策略，表格为空。您可以显示或隐藏表格的列，更改它们的顺序，仅查看包含指定值的行，或者使用查找。

创建策略

您可以创建策略；您也可以修改和删除现有策略。

要创建策略：

1. 在主菜单中，转到“**资产(设备)**” → “**策略和配置文件**”。
2. 单击**添加**。
   “**选择应用程序**”窗口将打开。
3. 选择您要为其创建策略的应用程序。
4. 单击“**下一步**”。

新策略设置窗口打开，在其中已选择“**常规**”选项卡。

5. 如果您需要，更改策略的默认名称、默认状态和默认继承设置。

6. 选择“**应用程序设置**”选项卡。
   或者，您可以单击“**保存**”并退出。策略将出现在策略列表，且您可以稍后编辑其设置。

7. 在“**应用程序设置**”选项卡的左侧窗格中选择您需要的类别，并在右侧的结果窗格中编辑策略设置。您可以在每个类别中（区域）编辑策略设置。
   设置集合取决于您为其创建策略的应用程序。有关详细信息，请参阅以下内容：

   - 管理服务器配置
   - 网络代理策略设置
   - Kaspersky Endpoint Security for Linux 帮助
   - Kaspersky Endpoint Security for Windows 帮助

   有关其他安全应用程序设置的详细信息，请参阅相应应用程序的文档。
   当编辑设置时，您可以单击“**取消**”以取消上一次操作。

8. 单击“**保存**”保存策略。

该策略显示在策略列表中。

常规策略设置

常规

在“**常规**”选项卡中，可以修改策略状态并指定策略设置的继承：

- 在“**策略状态**”块，您可以选择策略的模式：
  - 活动

    如果选择该选项，策略将变为活动状态。
    默认情况下已选定该选项。

  - 漫游

    如果选择该选项，策略将在设备离开企业网络时变为活动状态。

  - 不活动

    如果选择该选项，策略将变为不活动状态，但它仍然存储在“**策略**”文件夹中。如果需要，您可以激活该策略。

- 在“**设置继承**”设置组中，您可以配置策略继承：
  - 从父策略继承设置

    如果启用此选项，则策略设置值将从上一级组策略继承，因而被锁定。
    默认情况下已启用该选项。

  - 在子策略中强制继承设置

    如果启用此选项，则在应用策略更改之后，将执行以下操作：
    - 策略设置的值将被传送到管理子组的策略，也就是子策略。
    - 在每个子策略属性窗口**常规**区域的**继承设置**区块，将自动启用**从父策略继承设置**选项。

    如果启用此选项，则子策略设置被锁定。
    默认情况下已禁用该选项。

事件配置

“**事件配置**”区域允许您配置事件记录和事件通知。事件根据重要级别用下面的标签分布：

- **严重**
  “**严重**”区域不显示在网络代理策略属性中。
- **功能失败**
- **警告**
- **信息**

在每个区域，列表显示在管理服务器上事件类型和默认事件存储的期限（天）。点击事件类型允许您指定以下设置：

- **事件注册**
  您可以指定存储事件的天数和选择存储事件的位置：
  - **使用 Syslog 导出到 SIEM 系统**
  - **存储在设备的 OS 事件日志中**
  - **存储在管理服务器的 OS 事件日志中**
- **事件通知**
  您可以选择您是否想由以下方法之一被通知事件：
  - **通过邮件通知**
  - **通过 SMS 通知**
  - **通过运行可执行文件或脚本通知**
  - **通过 SNMP 通知**

默认下，使用在管理服务器属性选项卡中指定的通知设置（例如收件人地址）。如果需要，可以在“**电子邮件**”、“**SMS**”和“**要运行的可执行文件**”选项卡中更改这些设置。

修订历史

“**修订历史**”选项卡允许您查看策略修订列表和回滚策略更改（如有必要）。

修改策略

要修改策略：

1. 在主菜单中，转到“ **资产(设备)** ” → “**策略和配置文件**”。
2. 点击您要修改的策略。
   策略设置窗口打开。
3. 指定“通用设置”和为其创建策略的应用程序的设置。有关详细信息，请参阅以下内容：
   - 管理服务器配置
   - 网络代理策略设置
   - Kaspersky Endpoint Security for Linux 帮助
   - Kaspersky Endpoint Security for Windows 帮助

   有关其他安全应用程序设置的详细信息，请参阅该应用程序的文档。
4. 点击“**保存**”。

对策略所做的更改将保存在策略属性中，并将显示在“**修订历史**”区域中。

Enabling and disabling a policy inheritance option

To enable or disable the inheritance option in a policy:

1. Open the required policy.
2. Open the 常规 tab.
3. Enable or disable policy inheritance:
   - If you enable 从父策略继承设置 in a child policy and an administrator locks some settings in the parent policy, then you cannot change these settings in the child policy.
   - If you disable 从父策略继承设置 in a child policy, then you can change all of the settings in the child policy, even if some settings are locked in the parent policy.
   - If you enable 在子策略中强制继承设置 in the parent group, this enables the 从父策略继承设置 option for each child policy. In this case, you cannot disable this option for any child policy. All of the settings that are

locked in the parent policy are forcibly inherited in the child groups, and you cannot change these settings in the child groups.

4. Click the 保存 button to save changes or click the 取消 button to reject changes.

By default, the 从父策略继承设置 option is enabled for a new policy.

If a policy has profiles, all of the child policies inherit these profiles.

复制策略

您可以从一个管理组复制策略到另一个。

要复制策略到其他管理组：

1. 在主菜单中，转到“ **资产(设备)**” → “**策略和配置文件**”。
2. 选择您要复制的策略旁边的复选框。
3. 单击“**复制**”按钮。
   在屏幕的右侧，管理组树被显示。
4. 在树中，选择目标组，即，要将策略复制到的组。
5. 单击屏幕底部的“**复制**”按钮。
6. 单击“**确定**”以确认操作。

策略将连带其所有配置文件被复制到目标组。目标组中每个复制的策略的状态将是“**不活动**”。您可以随时将状态更改为“**活动**”。

如果目标组中已包含名称与新移动策略的名称一致的策略，那么会在新移动策略的名称后附加一个 （<下一个序列号>） 的索引，例如：（1）。

移动策略

您可以从一个管理组移动策略到另一个。例如，您要删除一个组，但您要为其他组使用其策略。此种情况下，您最好在删除旧组之前将策略从旧组移动到新组。

要移动策略到其他管理组：

1. 在主菜单中，转到“ **资产(设备)**” → “**策略和配置文件**”。
2. 选择您要移动的策略旁边的复选框。
3. 单击“**移动**”按钮。
   在屏幕的右侧，管理组树被显示。
4. 在树中，选择目标组，即，要将策略移动到的组。

5. 单击屏幕底部的“**移动**”按钮。

6. 单击“**确定**”以确认操作。

如果策略不是从资源组继承的，它连带所有配置文件被移动到目标组。目标组中的策略状态为“**不活动**”。您可以随时将状态更改为“**活动**”。

如果策略是从资源组继承的，它保持在资源组。它连带所有其配置文件被复制到目标组。目标组中的策略状态为“**不活动**”。您可以随时将状态更改为“**活动**”。

如果目标组中已包含名称与新移动策略的名称一致的策略，那么会在新移动策略的名称后附加一个 （<下一个序列号>） 的索引，例如：（1）。

导出策略

Kaspersky Security Center Linux 允许您将策略、其设置和策略配置文件保存到 KLP 文件中。您可以使用此 KLP 文件将保存的策略导入到 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux。

要导出策略，请执行以下操作：

1. 在主菜单中，转到“ **资产(设备)**” → “**策略和配置文件**”。

2. 选中要导出的策略旁边的复选框。

   您不能同时导出多个策略。如果您选择了多个策略，**导出**按钮将被禁用。

3. 单击“**导出**”按钮。

4. 在打开的“**另存为**”窗口中，指定策略文件的名称和路径。单击“**保存**”按钮。

   仅当您使用 Google Chrome、Microsoft Edge 或 Opera 时，才会显示“**另存为**”窗口。如果您使用其他浏览器，则策略文件会自动保存在“**下载**”文件夹。

导入策略

Kaspersky Security Center Linux 允许您从 KLP 文件导入策略。KLP 文件包含导出的策略、其设置和策略配置文件。

要导入策略，请执行以下操作：

1. 在主菜单中，转到“ **资产(设备)**” → “**策略和配置文件**”。

2. 单击“**导入**”按钮。

3. 单击**浏览**按钮选择要导入的策略文件。

4. 在打开的窗口中，指定 KLP 策略文件的路径，然后单击“**打开**”按钮。请注意，您仅可选择一个策略文件。

   策略处理启动。

5. 策略成功处理后，选择要向其应用策略的管理组。

6. 单击**完成**按钮以完成策略导入。

出现包含导入结果的通知。如果策略成功导入，可以单击“**详细资料**”链接以查看策略属性。

成功导入后，策略会显示在策略列表中。策略的设置和配置文件也将会导入。无论导出期间选择的策略处于什么状态，导入的策略均处于非活动状态。您可以在策略属性中更改策略状态。

如果新导入的策略与现有策略有相同的名称，则导入的策略在名称后会附加一个（**<下一个序列号>**）索引，例如：**(1)**、**(2)**。

强制同步

尽管 Kaspersky Security Center Linux 自动为受管理设备同步状态、设置、任务和策略，但在某些情况下，管理员必须确切知道在某一给定时刻是否已为指定设备执行同步。

同步单个设备

要强制同步管理服务器和受管理设备：

1. 在主菜单中，转到 “**资产(设备)**” → “**受管理设备**”。
2. 点击要与管理服务器同步的设备名称。
   属性窗口打开，在其中已选择“**常规**”区域。
3. 单击**强制同步**按钮。

应用程序将所选设备与管理服务器同步。

同步多个设备

要在管理服务器和多台受管理设备之间强制同步：

1. 打开管理组的设备列表或设备分类：
   - 在主菜单中，转到**资产(设备)→受管理设备**，单击受管理设备列表上方的**当前路径**字段中的路径链接，然后选择包含要同步的设备的管理组。
   - 运行设备分类以查看设备列表。
2. 选中要与管理服务器同步的设备旁边的复选框。
3. 在受管理设备列表上方，单击省略号按钮 (**...**)，然后单击**强制同步**按钮。
   应用程序将所选设备与管理服务器同步。
4. 在设备列表中，检查所选设备与管理服务器的上次连接时间是否已更改为当前时间。如果时间未更改，则单击“**刷新**”按钮更新页面内容。

所选设备即与管理服务器同步。

查看策略传送时间

在管理服务器上更改 Kaspersky 应用程序策略后，管理员可以检查是否被更改的策略被传输到了特定受管理设备。策略可以在定期同步或者强制同步中传输。

要查看应用程序策略被传输到受管理设备的日期和时间：

1. 在主菜单中，转到 “**资产(设备)**” → “**受管理设备**”。
2. 点击要与管理服务器同步的设备名称。
   属性窗口打开，在其中已选择“**常规**”区域。
3. 选择“**应用程序**”选项卡。
4. 选择您要查看策略同步日期的应用程序。
   应用程序策略窗口打开，在其中已选择“**常规**”区域并显示策略传送日期和时间。

Viewing the policy distribution status chart

In Kaspersky Security Center Linux, you can view the status of policy application on each device in a policy distribution status chart.

To view the policy distribution status on each device:

1. In the main menu, go to 资产(设备) → 策略和配置文件.
2. Select check box next to the name of the policy for which you want to view the distribution status on devices.
3. In the menu that appears, select the 分发 link.
   The **<Policy name> distribution results** window opens.
4. In the **<Policy name> distribution results** window that opens, the **Status description** of the policy is displayed.

You can change number of results displayed in the list with policy distribution. The maximum number of devices is 100000.

To change the number of devices displayed in the list with policy distribution results:

1. In the main menu, go to your account settings, and then select 界面选项.
2. In the **Limit of devices displayed in policy distribution results**, enter the number of devices (up to 100000).
   By default, the number is 5000.
3. Click 保存.
   The settings are saved and applied.

删除策略

如果您不再需要一个策略，您可以删除它。您仅可以删除一个在指定管理组中继承的策略。如果一个策略是继承的，您仅可以在其被创建的上级组删除它。

要删除策略，请执行以下操作：

1. 在主菜单中，转到“**资产(设备)**” → “**策略和配置文件**”。
2. 选中您要删除的策略旁边的复选框，然后单击“**删除**”。
   如果选择继承的策略，“**删除**”按钮变为不可用（变暗）。
3. 单击“**确定**”以确认操作。

策略连带其所有配置文件被删除。

Managing policy profiles

This section describes managing policy profiles and provides information about viewing the profiles of a policy, changing a policy profile priority, creating a policy profile, copying a policy profile, creating a policy profile activation rule, and deleting a policy profile.

查看策略配置文件

要查看策略配置文件：

1. 在主菜单中，转到“**资产(设备)**” → “**策略和配置文件**。
2. 点击您要查看其配置文件的策略名称。
   策略属性窗口打开，在其中已选择“**常规**”选项卡。
3. 打开“**策略配置文件**”选项卡。

策略配置文件列表以表格格式出现。如果策略没有配置文件，将显示空表。

更改策略配置文件优先级

要更改策略配置文件优先级：

1. 转到您要的策略的配置文件列表。
   将出现策略配置文件列表。
2. 在“**策略配置文件**”选项卡上，选中您要更改其优先级的策略配置文件旁边的复选框。
3. 通过单击“**提高优先级**”或“**降低优先级**”来设置策略配置文件在列表中的新位置。
   策略配置文件在列表中的位置越高，其优先级越高。
4. 单击“**保存**”按钮。

所选策略配置文件的优先级被更改并应用。

创建策略配置文件

要创建策略配置文件：

1. 转到您要的策略的配置文件列表。

   将出现策略配置文件列表。如果策略没有配置文件，将显示空表。

2. 单击**添加**。

3. 如果您需要，更改配置文件的默认名称和默认继承设置。

4. 选择“**应用程序设置**”选项卡。

   或者，您可以单击“**保存**”并退出。您创建的配置文件会出现在策略配置文件列表中，您可以稍后编辑其设置。

5. 在“**应用程序设置**”选项卡的左侧窗格中选择您需要的类别，并在右侧的结果窗格中编辑策略设置。您可以在每个类别中（区域）编辑策略配置文件设置。

   当编辑设置时，您可以单击“**取消**”以取消上一次操作。

6. 单击“**保存**”保存配置文件。

该配置文件显示在策略配置文件列表中。

复制策略配置文件

您可以复制策略配置文件到当前策略或其他策略，例如，如果您要对不同策略拥有相同配置文件。您也可以使用复制，如果您想拥有两个或更多仅在少数设置不同的配置文件。

要复制策略配置文件：

1. 转到您要的策略的配置文件列表。

   将出现策略配置文件列表。如果策略没有配置文件，将显示空表。

2. 在“**策略配置文件**”选项卡上，选择要复制的策略配置文件。

3. 单击**复制**。

4. 在打开的窗口中，选择您要复制配置文件的策略。

   您可以复制策略配置文件到相同策略或您指定的策略。

5. 单击**复制**。

策略配置文件被复制到您选择的策略。新复制的配置文件具有最低优先级。如果您复制配置文件到相同策略，新复制的配置文件名称将附加 () 索引，例如：(1)、(2)。

稍后，您可以更改配置文件设置，包括它的名称和属性；原始策略配置文件此种情况下将不被更改。

创建策略配置文件激活规则

要创建策略配置文件激活规则：

1. 转到您要的策略的配置文件列表。
   将出现策略配置文件列表。
2. 在“**策略配置文件**”选项卡上，单击需要为其创建激活规则的策略配置文件。
   如果策略配置文件列表为空，您可以创建策略配置文件。
3. 在“**激活规则**”选项卡上，单击“**添加**”按钮。
   策略配置文件激活规则窗口打开。
4. 指定规则名称。
5. 选择影响您当前创建的策略配置文件的激活的条件的复选框：
   - 策略配置文件激活常规规则

     选择该复选框根据设备离线模式状态设置设备上的策略配置文件激活规则、连接管理服务器规则和分配给设备的标记。

     对于该选项，在下一步指定：
     - 设备状态

       定义设备出现在网络的条件：
       - **在线**—设备在网络中，因此管理服务器可用。
       - **离线**—设备在外部网络，这意味着管理服务器不可用。
       - **N/A**—将不应用标准。
     - 管理服务器连接规则在该设备上活动

       选择策略配置文件激活条件（规则是否被执行）并选择规则名称。
       规则定义设备网络位置以便连接到管理服务器，它的条件必须被满足(或不满足)以便激活策略配置文件。
       用于连接到管理服务器的设备网络位置描述可以在网络代理切换规则中被创建或配置。
   - **特别设备所有者规则**

     对于该选项，在下一步指定：
     - 设备所有者

启用此选项可根据设备所有者在设备上配置和启用配置文件激活规则。在此复选框下的下拉列表中，可以选择配置文件激活标准：

- 设备属于指定的拥有者（"="符号）。
- 设备不属于指定的拥有者（“#”符号）。

  如果启用该选项，配置文件根据配置的标准在设备上激活。启用此选项时，您可以指定设备所有者。如果禁用此选项，配置文件激活标准不起作用。默认情况下已禁用该选项。

- 设备所有者在内部安全组中

  启用此选项可通过所有者在 Kaspersky Security Center Linux 内部安全组中的资格在设备上配置和启用配置文件激活规则。在此复选框下的下拉列表中，可以选择配置文件激活标准：

  - 设备所有者是指定安全组的成员（"="符号）。
  - 设备所有者不是指定安全组的成员（“#”符号）。

    如果启用该选项，配置文件根据配置的标准在设备上激活。您可以指定 Kaspersky Security Center Linux 的安全组。如果禁用此选项，配置文件激活标准不起作用。默认情况下已禁用该选项。

- 硬件说明书规则

  选择该复选框根据内存和逻辑处理器数量设置设备上的策略配置文件激活规则。

  对于该选项，在下一步指定：

  - 内存大小(MB)

    启用此选项可通过设备上可用 RAM 容量在设备上配置和启用配置文件激活规则。在此复选框下的下拉列表中，可以选择配置文件激活标准：

    - 该设备内存大小小于指定值("<" 符号)。
    - 该设备内存大小大于指定值(">" 符号)。

    如果启用该选项，配置文件根据配置的标准在设备上激活。您可以指定设备上的 RAM 卷。如果禁用此选项，配置文件激活标准不起作用。默认情况下已禁用该选项。

  - 逻辑处理器数量

    启用此选项可通过设备上逻辑处理器数量在设备上配置和启用配置文件激活规则。在此复选框下的下拉列表中，可以选择配置文件激活标准：

    - 设备上逻辑处理器数量少于或等于指定值 （"<" 符号）。
    - 设备上逻辑处理器数量大于或等于指定值 （">" 符号）。

    如果启用该选项，配置文件根据配置的标准在设备上激活。您可以指定设备上的逻辑处理器数量。如果禁用此选项，配置文件激活标准不起作用。默认情况下已禁用该选项。

- 角色分配规则

  对于该选项，在下一步指定：

- 由设备所有者特定角色激活策略配置文件

  选择该选项以在设备上根据所有者角色配置和启用配置文件激活规则。从现有角色列表手动添加角色。

  如果启用该选项，配置文件根据配置的标准在设备上激活。

- 标签使用规则

  选择该复选框根据分配到设备的标签设置设备上的策略配置文件激活规则。您可以激活策略配置文件到有或没有所选标签的设备。

  对于该选项，在下一步指定：

  - 标签列表

    在标签列表中，通过选中与相应标签对应的选框，可以指定策略配置文件中的设备包含规则。

    您可以通过列表上方的字段添加新标签到列表，并点击**添加**按钮。

    策略配置文件包含具有选定标签的设备。如果清除选框，则将不应用该标准。默认情况下已清除这些选框。

  - 应用到没有指定标签的设备

    如果必须转换标签分类，则启用此选项。

    如果启用此选项，策略配置文件将包含未带有所选标签的描述的设备。如果禁用此选项，则不应用该标准。

    默认情况下已禁用该选项。

  向导的附加页面数量取决于您在第一步选择的设置。您可以稍后修改策略配置文件激活规则。

6. 检查所配置参数的列表。如果列表正确，请单击“**创建**”。

配置文件将被保存。当触发激活规则时，将在设备上激活该配置文件。

为配置文件创建的策略配置文件激活规则显示在“**激活规则**”选项卡上的策略配置文件属性中。您可以修改或删除任何策略配置文件激活规则。

多个激活规则可以被一起触发。

删除策略配置文件

要删除策略配置文件：

1. 转到您要的策略的配置文件列表。

   将出现策略配置文件列表。

2. 在“**策略配置文件**”选项卡上，选中要删除的策略配置文件旁边的复选框，然后单击“**删除**”。

3. 在打开的窗口中，单击“**删除**”。

策略配置文件即被删除。如果策略从低级别组继承，配置文件会保留在该组，但变成该组的策略配置文件。这可以消除低级别组设备上安装的受管理应用程序的设置的显著修改。

Network Agent policy settings

To configure the Network Agent policy:

1. In the main menu, go to 资产(设备) → 策略和配置文件.
2. Click the name of the Network Agent policy.

   The properties window of the Network Agent policy opens. The properties window contains the tabs and settings described below.

Consider that for Linux and Windows-based devices, various settings are available.

常规

On this tab, you can modify the policy name, policy status and specify the inheritance of policy settings:

- In the 策略状态 block, you can select one of the following policy modes:
  - 活动策略

    If this option is selected, the policy becomes active.

    By default, this option is selected.
  - 非活动策略

    If this option is selected, the policy becomes inactive, but it is still stored in the **Policies** folder. If required, the policy can be activated.
- In the 设置继承 settings group, you can configure the policy inheritance:
  - 从父策略继承设置

    If this option is enabled, the policy setting values are inherited from the upper-level group policy and, therefore, are locked.

    By default, this option is enabled.
  - 在子策略中强制继承设置

If this option is enabled, after policy changes are applied, the following actions will be performed:

- The values of the policy settings will be propagated to the policies of administration subgroups, that is, to the child policies.
- In the **Settings inheritance** block of the **General** section in the properties window of each child policy, the **Inherit settings from parent policy** option will be automatically enabled.

If this option is enabled, the child policies settings are locked.

By default, this option is disabled.

事件配置

On this tab, you can configure event logging and event notification. Events are distributed according to importance level in the following sections:

- 功能失败
- 警告
- 信息

In each section, the list shows the types of events and the default event storage period on the Administration Server (in days). After you click the event type, you can specify the settings of event logging and notifications about events selected in the list. By default, common notification settings specified for the entire Administration Server are used for all event types. However, you can change specific settings for the required event types.

For example, in the 警告 section, you can configure the 发生了安全问题 event type. Such events may happen, for instance, when the free disk space of a distribution point is less than 2 GB (at least 4 GB are required to install applications and download updates remotely). To configure the 发生了安全问题 event, click it and specify where to store the occurred events and how to notify about them.

If Network Agent detected a security issue, you can manage this issue by using the settings of a managed device.

应用程序设置

设置

In the **Settings** section, you can configure the Network Agent policy:

- 仅通过分发点分发文件

If this option is enabled, Network Agents on managed devices retrieve updates from distribution points only.

If this option is disabled, Network Agents on managed devices retrieve updates from distribution points or from Administration Server.

Note that the security applications on managed devices retrieve updates from the source set in the update task for each security application. If you enable the 仅通过分发点分发文件 option, make sure that Kaspersky Security Center Linux is set as an update source in the update tasks.

By default, this option is disabled.

- 事件队列的最大大小(MB)

In this field you can specify the maximum space on the drive that an event queue can occupy.

The default value is 2 megabytes (MB).

- 应用程序被允许在设备上检索策略扩展数据

Network Agent installed on a managed device transfers information about the applied security application policy to the security application (for example, Kaspersky Endpoint Security for Linux). You can view the transferred information in the security application interface.

Network Agent transfers the following information:

- Time of the policy delivery to the managed device
- Name of the active or out-of-office policy at the moment of the policy delivery to the managed device
- Name and full path to the administration group that contained the managed device at the moment of the policy delivery to the managed device
- List of active policy profiles

  You can use the information to ensure the correct policy is applied to the device and for troubleshooting purposes. By default, this option is disabled.

- 保护网络代理服务免遭非授权的卸载或终止，并防止设置更改

When this option is enabled, after Network Agent is installed on a managed device, the component cannot be removed or reconfigured without required privileges. The Network Agent service cannot be stopped. This option has no effect on domain controllers.

Enable this option to protect Network Agent on workstations operated with local administrator rights.

By default, this option is disabled.

- 使用卸载密码

If this option is enabled, by clicking the **Modify** button you can specify the password for the klmover utility and Network Agent remote uninstallation.

By default, this option is disabled.

存储库

In the 存储库 section, you can select the types of objects whose details will be sent from Network Agent to Administration Server. If modification of some settings in this section is prohibited by the Network Agent policy, you cannot modify these settings.

- 已安装应用程序详情

  If this option is enabled, information about applications installed on client devices is sent to the Administration Server.

  By default, this option is enabled.

- 硬件注册表的详细信息

  Network Agent installed on a device sends information about the device hardware to the Administration Server. You can view the hardware details in the device properties.

  Ensure that the lshw utility is installed on Linux devices from which you want to fetch hardware details. Hardware details fetched from virtual machines may be incomplete depending on the hypervisor used.

连接

The 连接 section includes three subsections:

- 网络
- 连接配置文件
- 连接计划

In the 网络 subsection, you can configure the connection to Administration Server, enable the use of a UDP port, and specify the UDP port number.

- In the 连接到管理服务器 settings group, you can configure connection to the Administration Server and specify the time interval for synchronization between client devices and the Administration Server:
  - 同步间隔(分钟)

    Network Agent synchronizes the managed device with the Administration Server. We recommend that you set the synchronization interval (also referred to as the heartbeat) to 15 minutes per 10,000 managed devices.

    If the synchronization interval is set to less than 15 minutes, synchronization is performed every 15 minutes. If synchronization interval is set to 15 minutes or more, synchronization is performed at the specified synchronization interval.

  - 压缩网络流量

If this option is enabled, the speed of data transfer by Network Agent is increased by means of a decrease in the amount of information being transferred and a consequent decreased load on the Administration Server.

The workload on the CPU of the client computer may increase.

By default, this check box is enabled.

- 在 Microsoft Windows 防火墙中打开网络代理端口

  If this option is enabled, a UDP port, necessary for the work of Network Agent, is added to the Microsoft Windows Firewall exclusion list.

  By default, this option is enabled.

- 使用 SSL 连接

  If this option is enabled, connection to the Administration Server is established through a secure port via SSL.

  By default, this option is enabled.

- 以默认连接设置在分发点(如果可用)上使用连接网关

  If this option is enabled, the connection gateway on the distribution point is used under the settings specified in the administration group properties.

  By default, this option is enabled.

- 使用 UDP 端口

  If you need the managed devices to connect to KSN proxy server through a UDP port, enable the **Use UDP port** option and specify a **UDP port number**. By default, this option is enabled. The default UDP port to connect to the KSN proxy server is 15111.

- UDP 端口号

  In this field you can enter the UDP port number. The default port number is 15000.

  The decimal system is used for records.

In the 连接配置文件 subsection, you can specify the network location settings and enable out-of-office mode when Administration Server is not available. The settings in the 连接配置文件 section are available only on devices running Windows:

- 网络位置设置

  Network location settings define the characteristics of the network to which the client device is connected and specify rules for Network Agent switching from one Administration Server connection profile to another when those network characteristics are altered.

- 管理服务器连接配置文件

  Connection profiles are supported only for devices running Windows.

  You can view and add profiles for Network Agent connection to the Administration Server. In this section, you can also create rules for switching Network Agent to different Administration Servers when the following events occur:

  - When the client device connects to a different local network
  - When the device loses connection with the local network of the organization
  - When the connection gateway address is changed or the DNS server address is modified

- 当管理服务器不可用时启用漫游模式

  If this option is enabled, in case of connection through this profile, applications installed on the client device use policy profiles for devices in out-of-office mode, as well as out-of-office policies. If no out-of-office policy has been defined for the application, the active policy will be used.

  If this option is disabled, applications will use active policies.

  By default, this option is disabled.

In the 连接计划 subsection, you can specify the time intervals during which Network Agent sends data to the Administration Server:

- 必要时连接

  If this option is selected, the connection is established when Network Agent has to send data to the Administration Server.

  By default, this option is selected.

- 在指定时间间隔连接

  If this option is selected, Network Agent connects to the Administration Server at a specified time. You can add several connection time periods.

通过分发点的网络轮询

In the 通过分发点的网络轮询 section, you can configure automatic polling of the network. You can use the following options to enable the polling and set its frequency:

- **Zeroconf**

If this option is enabled, the distribution point automatically polls the network with IPv6 devices by using zero-configuration networking (also referred to as *Zeroconf*). In this case, the enabled IP range polling is ignored, because the distribution point polls the whole network.

To start to use Zeroconf, the following conditions must be fulfilled:

- The distribution point must run Linux.
- You must install the avahi-browse utility on the distribution point.

If this option is disabled, the distribution point does not poll networks with IPv6 devices.

By default, this option is disabled.

- IP 范围

  If the option is enabled, the distribution point automatically polls IP ranges according to the schedule that you configured by clicking the 设置轮询计划 button.

  If this option is disabled, the distribution point does not poll IP ranges.

  The frequency of IP range polling for Network Agent versions prior to 10.2 can be configured in the **轮询间隔(分钟)** field. The field is available if the option is enabled.

  By default, this option is disabled.

- 域控制器

  If the option is enabled, the distribution point automatically polls domain controllers according to the schedule that you configured by clicking the 设置轮询计划 button.

  If this option is disabled, the distribution point does not poll domain controllers.

  The frequency of domain controller polling for Network Agent versions prior to 10.2 can be configured in the **轮询间隔(分钟)** field. The field is available if this option is enabled.

  By default, this option is disabled.

分发点网络设置

In the 分发点网络设置 section, you can specify the internet access settings:

- 使用代理服务器
- 地址
- 端口号
- 对本地地址不使用代理服务器

  If this option is enabled, no proxy server is used to connect to devices on the local network.

  By default, this option is disabled.

- 代理服务器身份验证

If this check box is selected, in the entry fields you can specify the credentials for proxy server authentication.

By default, this check box is cleared.

- 用户名
- 密码

KSN 代理(分发点)

In the **KSN 代理(分发点)** section, you can configure the application to use the distribution point to forward Kaspersky Security Network (KSN) requests from the managed devices:

- 在分发点端启用 KSN 代理

  The KSN proxy service is run on the device that is used as a distribution point. Use this feature to redistribute and optimize traffic on the network.

  The distribution point sends the KSN statistics, which are listed in the Kaspersky Security Network statement, to Kaspersky.

  By default, this option is disabled. Enabling this option takes effect only if the 使用管理服务器作为代理服务器 and 我同意使用卡巴斯基安全网络 options are enabled in the Administration Server properties window.

  You can assign a node of an active-passive cluster to a distribution point and enable KSN proxy server on this node.

- 转发 KSN 请求到管理服务器

  The distribution point forwards KSN requests from the managed devices to the Administration Server.

  By default, this option is enabled.

- 通过互联网直接访问 KSN 云/KPSN

  The distribution point forwards KSN requests from managed devices to the KSN Cloud or KPSN. The KSN requests generated on the distribution point itself are also sent directly to the KSN Cloud or KPSN.

- 端口

  The number of the TCP port that the managed devices will use to connect to KSN proxy server. The default port number is 13111.

- UDP 端口

  If you need the managed devices to connect to KSN proxy server through a UDP port, enable the **Use UDP port** option and specify a **UDP port number**. By default, this option is enabled. The default UDP port to connect to the KSN proxy server is 15111.

更新(分发点)

In the 更新(分发点) section, you can enable the downloading diff files feature, so distribution points take updates in the form of diff files from Kaspersky update servers.

重启管理

In the 重启管理 section, you can specify the action to be performed if the operating system of a managed device has to be restarted for correct use, installation, or uninstallation of an application. The settings in the 重启管理 section are available only on devices running Windows:

- 不重启操作系统

  Client devices are not restarted automatically after the operation. To complete the operation, you must restart a device (for example, manually or through a device management task). Information about the required restart is saved in the task results and in the device status. This option is suitable for tasks on servers and other devices where continuous operation is critical.

- 如果必要，自动重启操作系统

  Client devices are always restarted automatically if a restart is required for completion of the operation. This option is useful for tasks on devices that provide for regular pauses in their operation (shutdown or restart).

- 提示用户操作

  The restart reminder is displayed on the screen of the client device, prompting the user to restart it manually. Some advanced settings can be defined for this option: text of the message for the user, the message display frequency, and the time interval after which a restart will be forced (without the user's confirmation). This option is most suitable for workstations where users must be able to select the most convenient time for a restart.

  By default, this option is selected.

  - 重复提示间隔(分钟)

    If this option is enabled, the application prompts the user to restart the operating system with the specified frequency.

    By default, this option is enabled. The default interval is 5 minutes. Available values are between 1 and 1440 minutes.

    If this option is disabled, the prompt is displayed only once.

  - 在该时间后强制重启(分钟)

    After prompting the user, the application forces restart of the operating system upon expiration of the specified time interval.

    By default, this option is enabled. The default delay is 30 minutes. Available values are between 1 and 1440 minutes.

  - 强行关闭锁定会话中的应用程序

Running applications may prevent a restart of the client device. For example, if a document is being edited in a word processing application and is not saved, the application does not allow the device to restart.

If this option is enabled, such applications on a locked device are forced to close before the device restart. As a result, users may lose their unsaved changes.

If this option is disabled, a locked device is not restarted. The task status on this device states that a device restart is required. Users have to manually close all applications running on locked devices and restart these devices.

By default, this option is disabled.

Windows、Linux 和 macOS 网络代理的使用：比较、

网络代理的使用取决于设备的操作系统。网络代理策略和安装包设置也根据操作系统不同而不同。下表比较了适用于 Windows、Linux 和 macOS 操作系统的网络代理的功能和使用方案。

网络代理功能比较

网络代理功能	Windows	Linux	MacOS
安装			
通过使用第三方工具克隆带有操作系统和网络代理的管理员硬盘驱动器镜像进行安装	✓	✓	–
使用用于远程安装应用程序的第三方工具进行安装	✓	✓	✓
通过在设备上运行应用程序安装程序来手动安装	✓	✓	✓
在静默模式下安装网络代理	✓	✓	✓
手动连接客户端设备至管理服务器。klmover 实用程序	✓	✓	✓
自动安装 Kaspersky Security Center 组件的更新和补丁	✓	–	–
自动分发密钥	✓	✓	✓
强制同步	✓	✓	✓
分发点			
用作分发点	✓	✓	✓
自动分配分发点	✓	✓ 不使用网络定位感知 (NLA)。	✓ 不使用网络定位感知 (NLA)。
离线模式更新下载	✓	✓	✓

网络轮询	✓ • IP 范围轮询 • 域控制器轮询	✓ • IP 范围轮询 • Zeroconf 轮询 • 域控制器轮询（Microsoft Active Directory、Samba 4 Active Directory）	–
在分发点端运行 KSN 代理服务	✓	✓	–
通过卡巴斯基更新服务器将更新下载到将更新分发到受管理设备的分发点存储库	✓	✓	– （如果一个或多个运行 Linux 或 macOS 的设备在“将更新下载至分发点存储库”任务范围内，则该任务将以“失败”状态完成，即使该任务在所有 Windows 设备上均已成功完成。）
推送应用程序安装	✓	受限制：无法使用 Linux 分发点在 Windows 设备上执行推送安装。	受限制：无法使用 macOS 分发点在 Windows 设备上执行推送安装。
用作推送服务器	✓	✓	–
处理第三方应用程序			
在设备上远程安装应用程序	✓	✓	✓
在网络代理策略中配置操作系统更新	✓	–	–
查看软件漏洞信息	✓	–	–
扫描应用程序以查找漏洞	✓	–	–
软件更新	✓	–	–
清查设备上所安装的软件	✓	✓	–
虚拟机			
在虚拟机上安装网络代理	✓	✓	✓
虚拟桌面基础架构 (VDI) 的优化设置	✓	✓	✓
对动态虚拟机的支持	✓	✓	✓
其他			
使用 Windows 桌面共享来审核远程客户端设备上的操作	✓	–	–
监控反病毒保护状态	✓	✓	✓
管理设备重启	✓	–	–

支持文件系统回滚	✓	✓	✓
使用网络代理作为连接网关	✓	✓	✓
连接管理器	✓	✓	✓
网络代理从一个管理服务器切换到另一个管理服务器（根据网络位置自动切换）	✓	–	✓
检查客户端设备与管理服务器之间的连接。klnagchk 实用程序	✓	✓	✓
远程连接至客户端设备桌面	✓	–	✓ 通过使用虚拟网络计算 (VNC) 系统。
通过迁移向导下载独立安装包	✓	✓	✓

按操作系统比较网络代理设置

下表显示了可用的网络代理设置，具体取决于安装了网络代理的受管理设备的操作系统。

网络代理设置：按操作系统比较

设置区域	Windows	Linux	MacOS
常规	✓	✓	✓
事件配置	✓	✓	✓
设置	✓	✓ 下列选项可用： • 仅通过分发点分发文件 • 事件队列的最大大小(MB) • 应用程序被允许在设备上检索策略扩展数据	✓
存储库	✓	✓ 下列选项可用： • 已安装应用程序详情 • 硬件注册表的详细信息	–
连接→网络	✓	✓ 除了在 Microsoft Windows 防火墙中打开网络代理端口选项之外。	✓
连接→连接配置文件	✓	–	✓
连接→连接计划	✓	✓	✓
通过分发点的网络	✓	✓	–

轮询	下列选项可用： • Windows 网络 • IP 范围 • 域控制器	下列选项可用： • Zeroconf • IP 范围 • 域控制器	
分发点网络设置	✓	✓	✓
KSN 代理(分发点)	✓	✓	–
更新(分发点)	✓	✓	–
修订历史	✓	✓	✓

Kaspersky Endpoint Security 策略的手动设置

本节提供有关如何配置 Kaspersky Endpoint Security 策略的建议。您可以在策略属性窗口中执行设置。编辑设置时，请单击相关设置组右侧的锁定图标，将指定的值应用到工作站。

配置卡巴斯基安全网络

卡巴斯基安全网络 (KSN) 是云服务的基础设施，包含有关文件、网络资源和软件信誉的信息。卡巴斯基安全网络使 Kaspersky Endpoint Security for Windows 能够更快地响应不同类型的威胁，增强保护组件的性能，并降低误报的可能性。有关卡巴斯基安全网络的更多信息，请参阅 Kaspersky Endpoint Security for Windows 帮助。

要指定推荐的 KSN 设置：

1. 在主菜单中，转到“资产(设备)” → “策略和配置文件”。
2. 单击 Kaspersky Endpoint Security for Windows 策略。

   所选策略的属性窗口打开。
3. 在策略属性中，转到“应用程序设置”→“高级威胁防护”→“卡巴斯基安全网络”。
4. 确保使用 KSN 代理选项被启用。使用此选项有助于重新分发和优化网络流量。

   如果您使用Managed Detection and Response，您必须为分发点启用KSN 代理选项并启用扩展 KSN 模式。
5. [可选]启用对 KSN 服务器的使用，如果 KSN 代理服务不可用。KSN 服务器可能位于 Kaspersky 端（当 KSN 被使用）或第三方端（当 KPSN 被使用）。
6. 单击“确定”。

推荐的 KSN 设置被指定。

检查受防火墙保护的网络列表

确保 Kaspersky Endpoint Security for Windows 防火墙保护您的所有网络。默认情况下，防火墙保护具有以下连接类型的网络：

- **公共网络**。反病毒应用程序、防火墙或过滤器不保护此类网络中的设备。
- **本地网络**。此网络中的设备对文件和打印机的访问受限。
- **可信任网络**。此类网络中的设备受到保护，免受攻击和对文件和数据的未授权访问。

如果您配置了自定义网络，请确保防火墙保护该网络。为此，请检查 Kaspersky Endpoint Security for Windows 策略属性中的网络列表。该列表可能不包含所有网络。

有关防火墙的更多信息，请参阅 Kaspersky Endpoint Security for Windows 帮助。

要查看网络列表：

1. 在主菜单中，转到“**资产(设备)**” → “**策略和配置文件**。
2. 单击 Kaspersky Endpoint Security for Windows 策略。
   所选策略的属性窗口打开。
3. 在策略属性中，转到“**应用程序设置**”→“**关键威胁防护**”→“**防火墙**”。
4. 在“**可用网络**”下，单击“**网络设置**”链接。
   网络连接窗口将打开。该窗口显示网络列表。
5. 如果列表中缺少网络，请添加该网络。

禁用网络设备扫描

当 Kaspersky Endpoint Security for Windows 扫描网络驱动器时，会给它们带来很大的负载。在文件服务器上执行间接扫描更方便。

您可以在 Kaspersky Endpoint Security for Windows 策略属性中禁用网络驱动器扫描。有关这些策略属性的说明，请参阅 Kaspersky Endpoint Security for Windows 帮助。

要禁用网络驱动器扫描：

1. 在主菜单中，转到“**资产(设备)**” → “**策略和配置文件**。
2. 单击 Kaspersky Endpoint Security for Windows 策略。
   所选策略的属性窗口打开。
3. 在策略属性中，转到“**应用程序设置**”→“**关键威胁防护**”→“**文件威胁防护**”。
4. 在**保护范围**下，禁用**所有网络驱动器**选项。
5. 单击“**确定**”。

网络驱动器扫描被禁用。

从管理服务器内存中排除软件详细信息

建议管理服务器不要保存有关在网络设备上启动的软件模块的信息。这样管理服务器内存不会超限。

您可以在 Kaspersky Endpoint Security for Windows 策略属性中禁用保存此信息。

要禁用对已安装软件模块信息的保存：

1. 在主菜单中，转到“**资产(设备)**” → “**策略和配置文件**。
2. 单击 Kaspersky Endpoint Security for Windows 策略。
   所选策略的属性窗口打开。
3. 在策略属性中，转到“**应用程序设置**”→“**常规设置**”→“**报告和存储**”。
4. 在**到管理服务器的数据传输**下，禁用在顶级策略中仍然被启用的**关于启动的应用程序**复选框。
   当选中该复选框时：如果选中此复选框，管理服务器数据库保存网络设备上所有软件模块的所有版本信息。该信息可能需要 Kaspersky Security Center Linux 数据库上的大量磁盘空间(几十 G)。

已安装软件模块的信息不被保存到管理服务器数据库。

配置对工作站上的 Kaspersky Endpoint Security for Windows 界面的访问

如果必须通过 Kaspersky Security Center Linux 在集中模式下管理组织网络上的反病毒保护，请在 Kaspersky Endpoint Security for Windows 策略属性中指定接口设置，如下所述。这样，您将防止未经授权访问工作站上的 Kaspersky Endpoint Security for Windows 以及更改 Kaspersky Endpoint Security for Windows 设置。

有关这些策略属性的说明，请参阅 Kaspersky Endpoint Security for Windows 帮助。

要指定推荐的界面设置：

1. 在主菜单中，转到“**资产(设备)**” → “**策略和配置文件**。
2. 单击 Kaspersky Endpoint Security for Windows 策略。
   所选策略的属性窗口打开。
3. 在策略属性中，转到“**应用程序设置**”→“**常规设置**”→“**界面**”。
4. 在**用户交互**下，选择**没有界面**选项。这禁用了 Kaspersky Endpoint Security for Windows 用户界面在工作站上的显示，这样，其用户将无法更改 Kaspersky Endpoint Security for Windows 的设置。
5. 在**密码保护**下，启用开关按钮。这降低了对工作站上 Kaspersky Endpoint Security for Windows 设置进行未经授权或意外更改的风险。

Kaspersky Endpoint Security for Windows 界面的推荐设置被指定。

在管理服务器数据库中保存重要的策略事件

为了避免管理服务器数据溢出，我们建议您仅保存重要事件到数据库。

要配置注册重要事件到管理服务器数据库：

1. 在主菜单中，转到“**资产(设备)**” → “**策略和配置文件**。
2. 单击 Kaspersky Endpoint Security for Windows 策略。
   所选策略的属性窗口打开。
3. 在策略属性中，打开“**事件配置**”选项卡。
4. 在“**严重**”区域中，单击“**添加事件**”并仅选中以下事件旁边的复选框：
   - *最终用户授权许可协议被违反*
   - *应用程序自动运行被禁用*
   - *激活错误*
   - *检测到活动威胁。高级清除应该被启动*
   - *清除不可能*
   - *检测到先前打开的危险链接*
   - *禁止已终止*
   - *网络活动被阻止*
   - *检测到网络攻击*
   - *应用程序启动被禁止*
   - *访问被拒绝（本地库）*
   - *访问被拒绝 (KSN)*
   - *本地更新错误*
   - *无法同时启动两个任务*
   - *与 Kaspersky Security Center 交互错误*
   - *未更新所有组件*
   - *应用文件加密/解密规则错误*
   - *启用便携模式错误*
   - *禁用便携模式错误*

- *无法加载加密模块*
- *策略无法被应用*
- *更改应用程序组件时出错*

5. 单击“**确定**”。
6. 在“**功能失败**”区域中，单击“**添加事件**”并选中“*任务设置无效。设置未应用。*
7. 单击“**确定**”。
8. 在“**警告**”区域中，单击“**添加事件**”并仅选中以下事件旁边的复选框：
   - *自我保护已禁用*
   - *保护组件已禁用*
   - *备用密钥不正确*
   - *检测到可以被侵入者用于损害您的计算机或个人数据的合法软件（本地库）*
   - *检测到可以被侵入者用于损害您的计算机或个人数据的合法软件 (KSN)*
   - *对象已删除*
   - *对象已清除*
   - *用户已退出加密策略*
   - *文件已由管理员从 卡巴斯基反针对性攻击平台 服务器上的隔离区恢复*
   - *文件被管理员隔离在 Kaspersky Anti Targeted Attack Platform 服务器上*
   - *给管理员的应用程序启动阻止消息*
   - *给管理员的设备访问阻止消息*
   - *给管理员的网页访问阻止消息*
9. 单击“**确定**”。
10. 在“**信息**”区域中，单击“**添加事件**”并仅选中以下事件旁边的复选框：
    - *对象备份副本被创建*
    - *应用程序启动在测试模式中被禁止*
11. 单击“**确定**”。

注册重要事件到管理服务器数据库被配置。

Kaspersky Endpoint Security 更新组任务的手动设置

Kaspersky Endpoint Security 的最优和建议计划选项是“**当新更新下载至存储库时**”（当“**使用任务启动自动随机延迟**”复选框被选中时）。

卡巴斯基安全网络 （KSN）

该区域描述如何使用卡巴斯基安全网络 (KSN) 的在线服务基础架构。该区域提供了关于 KSN 的详细描述,介绍了如何启用 KSN，配置对 KSN 的访问，并查看 KSN 代理服务器的使用统计。

关于 KSN

卡巴斯基安全网络 (KSN) 是一种在线服务的基础架构，可提供对 Kaspersky 在线知识库的访问，其中包含与文件信誉、网络资源和软件相关的信息。使用卡巴斯基安全网络中的数据可确保在遇到新型威胁时 Kaspersky 程序能够做出更快速的响应，提高某些保护组件的效力并降低误报的风险。KSN 允许您使用 Kaspersky 的信誉数据库检索有关安装在受管理设备上的应用程序信息。

一旦加入 KSN，即表示您同意以自动模式将通过 Kaspersky Security Center Linux 管理的客户端设备上安装的 Kaspersky 程序的相关操作信息发送到 Kaspersky。依照当前KSN 访问设置发送信息。

Kaspersky Security Center Linux 支持以下 KSN 基础架构解决方案：

- *全球 KSN* 是一种允许您与 Kaspersky Security Network 交换信息的解决方案。一旦加入 KSN，即表示您同意以自动模式将通过 Kaspersky Security Center Linux 管理的客户端设备上安装的卡巴斯基应用程序的操作相关信息发送到 Kaspersky。依照当前KSN 访问设置发送信息。卡巴斯基分析师还分析收到的信息，并将其包含在卡巴斯基安全网络的信誉数据库和统计数据库中。Kaspersky Security Center Linux 默认使用此解决方案。

- *卡巴斯基私有安全网络 (KPSN)* 是一种解决方案，允许安装了卡巴斯基应用程序的设备用户访问卡巴斯基安全网络的信誉数据库和其他统计数据，而无需从用户自己的计算机向 KSN 发送数据。KPSN 用于由于以下原因无法参与卡巴斯基安全网络的企业客户：

  - 用户设备未连接到互联网。

  - 法律或企业安全策略禁止传输任何数据到国家/地区以外或企业局域网以外。

  您可以在管理服务器属性窗口的 **KSN 代理设置**区域对卡巴斯基私人安全网络设置访问设置。

在运行快速启动向导时，应用程序会提示您加入 KSN。您可以在使用应用程序的任何时间启用或者停止 KSN。

您将根据您在启用 KSN 时阅读并接受的 KSN 声明来使用 KSN。如果 KSN 声明有更新，当您更新或升级管理服务器时会向您显示。您可以接受更新的 KSN 声明，也可以拒绝。如果您拒绝，您将根据之前接受的 KSN 声明的先前版本继续使用 KSN。

启用 KSN 后，Kaspersky Security Center Linux 会检查 KSN 服务器是否可访问。如果无法使用系统 DNS 访问服务器，应用程序将使用公共 DNS 服务器。这对于确保保持受管理设备的安全级别是必要的。

管理服务器管理的客户端设备通过 KSN 代理服务器与 KSN 交互。KSN 代理服务器提供以下功能：

- 即使无法直接访问互联网，客户端设备也可以向 KSN 发送请求以及向 KSN 传送信息。

- KSN 代理可缓存处理后的数据，从而减少发送通道的工作负荷以及为等待客户端设备所请求的信息而花费的时间。

您可以在管理服务器的属性窗口的“**KSN 代理设置**”区域配置 KSN 代理服务器。

Setting up access to KSN

You can set up access to Kaspersky Security Network (KSN) on the Administration Server and on a distribution point.

To set up Administration Server access to KSN:

1. In the main menu, click the settings icon ( ) next to the name of the required Administration Server.

   The Administration Server properties window opens.

2. On the 常规 tab, select the **KSN 代理设置** section.

3. Switch the toggle button to the 在管理服务器上启用 **KSN 代理** 已启用 position.

   Data is sent from client devices to KSN in accordance with the Kaspersky Endpoint Security policy, which is active on those client devices. If this check box is cleared, no data will be sent to KSN from the Administration Server and client devices through Kaspersky Security Center Linux. However, client devices can send data to KSN directly (bypassing Kaspersky Security Center Linux), in accordance with their respective settings. The Kaspersky Endpoint Security policy, which is active on client devices, determines which data will be sent directly (bypassing Kaspersky Security Center Linux) from those devices to KSN.

4. Switch the toggle button to the 使用卡巴斯基安全网络已启用 position.

   If this option is enabled, client devices send patch installation results to Kaspersky. When enabling this option, make sure to read and accept the terms of the KSN Statement.

   If you are using KPSN, switch the toggle button to the 使用卡巴斯基私人安全网络已启用 position and click the 选择 **KSN 代理设置文件** button to download the settings of KPSN (files with the extensions pkcs7 and pem). After the settings are downloaded, the interface displays the provider's name and contacts, as well as the creation date of the file with the settings of KPSN.

   When you switch the toggle button to the 使用卡巴斯基私人安全网络已启用 position, a message appears with details about KPSN.

   The following Kaspersky applications support KPSN:

   - Kaspersky Security Center Linux
   - Kaspersky Endpoint Security for Linux
   - Kaspersky Endpoint Security for Windows

   If you enable KPSN in Kaspersky Security Center Linux, these applications receive information about supporting KPSN. In the settings window of the application, in the **Kaspersky Security Network** subsection of the **Advanced Threat Protection** section, the information about selected KSN provider is displayed — KSN or KPSN.

   > Kaspersky Security Center Linux does not send any statistical data to Kaspersky Security Network if KPSN is configured in the **KSN 代理设置** section of the Administration Server properties window.

5. If you have the proxy server settings configured in the Administration Server properties, but your network architecture requires that you use KPSN directly, enable the 当连接到 **KPSN** 时忽略代理服务器设置 option. Otherwise, requests from the managed applications cannot reach KPSN.

6. Configure the Administration Server connection to the KSN proxy service:

- Under 连接设置, for the **TCP 端口**, specify the number of the TCP port that will be used for connecting to the KSN proxy server. The default port to connect to the KSN proxy server is 13111.

- If you want the Administration Server to connect to the KSN proxy server through a UDP port, enable the **使用 UDP 端口** option and specify a port number for the **UDP 端口**. By default, this option is disabled, and TCP port is used. If this option is enabled, the default UDP port to connect to the KSN proxy server is 15111.

7. Switch the toggle button to the **通过主管理服务器连接从属管理服务器到 KSN 已启用** position.

   If this option is enabled, secondary Administration Servers use the primary Administration Server as the KSN proxy server. If this option is disabled, secondary Administration Servers connect to KSN on their own. In this case, managed devices use secondary Administration Servers as KSN proxy servers.

   > Secondary Administration Servers use the primary Administration Server as a proxy server if in the right pane of the **KSN 代理设置** section, in the properties of secondary Administration Servers the toggle button is switched to the **在管理服务器上启用 KSN 代理 已启用** position.

8. Click the **保存** button.

The KSN access settings will be saved.

You can also set up distribution point access to KSN, for example, if you want to reduce the load on the Administration Server. The distribution point that acts as a KSN proxy server sends KSN requests from managed devices to Kaspersky directly, without using the Administration Server.

To set up distribution point access to Kaspersky Security Network (KSN):

1. Make sure that the distribution point is assigned manually.

2. In the main menu, click the settings icon ( ) next to the name of the required Administration Server.

   The Administration Server properties window opens.

3. On the **常规** tab, select the **分发点** section.

4. Click the name of the distribution point to open its properties window.

5. In the distribution point properties window, in the **KSN 代理** section, enable the **在分发点端启用 KSN 代理** option, and then enable the **通过互联网直接访问 KSN 云/KPSN** option.

6. Click **确定**.

The distribution point will act as a KSN proxy server.

> Please note that the distribution point does not support managed device authentication by using the NTLM protocol.

Enabling and disabling KSN

To enable KSN:

1. In the main menu, click the settings icon ( ) next to the name of the required Administration Server.

   The Administration Server properties window opens.

2. On the 常规 tab, select the **KSN** 代理设置 section.

3. Switch the toggle button to the 在管理服务器上启用 **KSN** 代理 已启用 position.

   The KSN proxy server is enabled.

4. Switch the toggle button to the 使用卡巴斯基安全网络已启用 position.

   KSN will be enabled.

   If the toggle button is enabled, client devices send patch installation results to Kaspersky. When enabling this toggle button, you should read and accept the terms of the KSN Statement.

5. Click the 保存 button.

To disable KSN:

1. In the main menu, click the settings icon ( ) next to the name of the required Administration Server.

   The Administration Server properties window opens.

2. On the 常规 tab, select the **KSN** 代理设置 section.

3. Switch the toggle button to the 在管理服务器上启用 **KSN** 代理 已禁用 position to disable the KSN proxy service, or switch the toggle button to the 使用卡巴斯基安全网络已禁用 position.

   If one of these toggle buttons is disabled, client devices will send no patch installation results to Kaspersky.

   If you are using KPSN, switch the toggle button to the 使用卡巴斯基私人安全网络已禁用 position.

   KSN will be disabled.

4. Click the 保存 button.

Viewing the accepted KSN Statement

When you enable Kaspersky Security Network (KSN), you must read and accept the KSN Statement. You can view the accepted KSN Statement at any time.

To view the accepted KSN Statement:

1. In the main menu, click the settings icon ( ) next to the name of the required Administration Server.

   The Administration Server properties window opens.

2. On the 常规 tab, select the **KSN** 代理设置 section.

3. Click the 查看卡巴斯基安全网络声明 link.

In the window that opens, you can view the text of the accepted KSN Statement.

Accepting an updated KSN Statement

You use KSN in accordance with the KSN Statement that you read and accept when you enable KSN. If the KSN Statement is updated, it is displayed to you when you update or upgrade Administration Server. You can accept the updated KSN Statement or decline it. If you decline it, you will continue using KSN in accordance with the version of the KSN Statement that you previously accepted.

After updating or upgrading Administration Server, the updated KSN Statement is displayed automatically. If you decline the updated KSN Statement, you can still view and accept it later.

To view and then accept or decline an updated KSN Statement:

1. Click the 查看通知 link in the upper-right corner of the main application window.

   The 通知 window opens.

2. Click the 查看更新的 **KSN** 声明 link.

   The 卡巴斯基安全网络声明更新 window opens.

3. Read the KSN Statement, and then make your decision by clicking one of the following buttons:

   - **I accept the updated KSN Statement**
   - **Use KSN under the old Statement**

   Depending on your choice, KSN keeps working in accordance with the terms of the current or updated KSN Statement. You can view the text of the accepted KSN Statement in the properties of Administration Server at any time.

检查分发点是否充当 KSN 代理服务器

在分配为充当分发点的受管理设备上，可以启用 Kaspersky Security Network (KSN) 代理。当 ksnproxy 服务在设备上运行时，受管理设备充当 KSN 代理服务器。您可以在设备上本地检查、打开或关闭此服务。

您可以将基于 Windows 或基于 Linux 的设备分配为分发点。检查分发点的方法取决于该分发点的操作系统。

要检查基于 Linux 的分发点是否充当 KSN 代理服务器：

1. 在分发点设备上，显示正在运行的进程列表。
2. 在正在运行的进程列表中，检查 `/opt/kaspersky/ksc64/sbin/ksnproxy` 进程是否 正在运行。

如果 `/opt/kaspersky/ksc64/sbin/ksnproxy` 进程正在运行，则设备上的网络代理会参与卡巴斯基安全网络，并充当分发点范围内包括的受管理设备的 KSN 代理服务器。

要检查基于 Windows 的分发点是否充当 KSN 代理服务器：

1. 在分发点设备上的 Windows 中，打开“服务”（“所有程序”→“管理工具”→“服务”）。
2. 在服务列表，检查 ksnproxy 服务是否正在运行。

   如果 ksnproxy 服务正在运行，则设备上的网络代理会参与卡巴斯基安全网络，并充当分发点范围内包括的受管理设备的 KSN 代理服务器。

   如果您想，您可以关闭 ksnproxy 服务。在这种情况下，分发点上的网络代理停止参与卡巴斯基安全网络。该需要本地管理员权限。

管理任务

本节介绍 Kaspersky Security Center Linux 使用的任务。

关于任务

Kaspersky Security Center Linux 通过创建和运行*任务*来管理设备上安装的 Kaspersky 应用程序。安装、启用和停用程序、扫描文件、更新数据库和软件模块以及程序的其他操作均需要任务。

特定应用程序的任务可以使用 Kaspersky Security Center Web Console 创建，仅在该应用程序的管理插件安装在 Kaspersky Security Center Web Console 服务器上时。

任务可以在管理服务器和设备上执行。

管理服务器上执行的任务包含以下：

- 自动分发报告
- 将更新下载至存储库
- 备份管理服务器数据
- 数据库维护

以下类型的任务在设备上执行：

- *本地任务* — 在特定设备上执行的任务。

  本地任务可以由管理员使用 Kaspersky Security Center Web Console 修改，或者由远程设备用户修改（例如，通过安全应用程序界面）。如果本地任务同时被管理员和受管理设备用户修改，管理员的修改将生效，因为其具有更高优先级。

- *组任务* — 在特定组的所有设备上执行的任务。

  除非在任务属性中指定了其他项，组任务也影响所选组的所有子组。组任务还影响（可选）已连接到部署在该组或其任意子组中的从属和虚拟管理服务器的设备。

- *全局任务* — 在一组设备上执行的任务，与设备是否包含在某个组中无关。

您可以为每个应用程序创建不管多少个组任务、全局任务或本地任务。

您可以更改任务设置、查看任务进度、复制、导出、导入和删除任务。

仅当为其创建任务的应用程序在运行时，才能在设备上启动任务。

任务执行结果保存在每台设备的操作系统事件日志、管理服务器上的操作系统事件日志和管理服务器数据库中。

不在任务设置中包括私人数据。例如，避免指定域管理员密码。

关于任务范围

*任务范围*是执行任务的设备集合。范围的类型包括以下：

- 对于*本地任务*，范围是设备本身。
- 对于*管理服务器任务*，范围是管理服务器。
- 对于*组任务*，范围是包含在组中的设备列表。

当创建*全局任务*时，您可以使用以下方法指定范围：

- 手动指定特定设备。

  您可以使用 IP 地址（或 IP 范围）或 DNS 名称作为设备地址。

- 从包含有要添加的设备地址的 .txt 文件来导入设备列表（每一个计算机地址必须单独一行）。

  如果通过文件导入设备列表或手动创建设备列表，且如果设备是以名称定义，则列表可以只包含其信息已被输入到管理服务器数据库中的设备。而且，信息必须在设备被连接或设备发现中输入。

- 指定设备分类。

  后续，任务范围随着包含在分类中的设备集的更改而更改。设备分类可以基于设备属性（包含安装在设备上的软件）创建，也可以基于分配到设备的标签来创建。设备分类是指定任务范围的最灵活的方法。

  设备分类的任务总是按管理服务器计划运行。这些任务无法运行在缺少管理服务器连接的设备上。使用其他方法指定范围的任务直接运行在设备上，且因此不取决于到管理服务器的设备连接。

设备分类的任务不会按设备本地时间运行；相反，它们将按照管理服务器本地时间运行。使用其他方法指定范围的任务以设备本地时间运行。

创建任务

要创建任务：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。
2. 单击**添加**。

   “新任务向导”启动。遵循其说明。
3. 如果要修改默认任务设置，请启用“**完成任务创建**”页面上的“**创建完成时打开任务详情**”选项。如果您不启用该选项，任务使用默认设置创建。您可以稍后随时修改默认设置。
4. 单击“**完成**”按钮。

任务被创建并显示在任务列表。

要创建分配给所选设备的新任务：

1. 在主菜单中，转到**资产(设备)** → **受管理设备**。

   将显示受管理设备列表。

2. 在受管理设备列表中，选中设备旁边的复选框以为其运行任务。您可以使用搜索和过滤功能来查找您正在寻找的设备。

3. 单击**运行任务**按钮，然后选择**添加一个新任务**。

   “新任务向导”启动。

   在向导的第一步中，您可以删除被选择包括在任务范围中的设备。按照向导的说明进行操作。

4. 单击“**完成**”按钮。

任务为选定的设备创建。

Starting a task manually

The application starts tasks according to the schedule settings specified in the properties of each task. You can start a task manually at any time from the task list. Alternatively, you can select devices in the **受管理设备** list, and then start an existing task for them.

To start a task manually:

1. In the main menu, go to **资产(设备)** → **任务**.

2. In the task list, select the check box next to the task that you want to start.

3. Click the **开始** button.

   The task starts. You can check the task status in the **状态** column or by clicking the **结果** button.

Viewing the task list

You can view the list of tasks that are created in Kaspersky Security Center Linux.

To view the list of tasks,

In the main menu, go to **资产(设备)** → **任务**.

The list of tasks is displayed. The tasks are grouped by the names of applications to which they are related. For example, the *远程安装应用程序* task is related to the Administration Server, and the *Update* task refers to Kaspersky Endpoint Security.

To view properties of a task,

Click the name of the task.

The task properties window is displayed with several named tabs. For example, the **任务类型** is displayed on the **常规** tab, and the task schedule—on the **计划** tab.

常规任务设置

本节包含您可以查看并为大多数任务配置的设置。可用设置列表取决于您正在配置的任务。

任务创建过程中指定的设置

您可以在创建任务时指定以下设置。一些设置也可以在所创建任务的属性中修改。

- 操作系统重启设置：
  - 不重启设备

    客户端设备在操作后不被自动重启。要完成操作，您必须重启设备(例如，手动或通过设备管理任务)。所需重启的信息被保存在任务结果和设备状态。该选项适用于在需要持续操作的服务器和其他设备上的任务。

  - 重启设备

    如果完成安装需要重启，客户端设备总是被自动重启。该选项适用于允许中断操作(关机或重启)的设备上的任务。

  - 强行关闭锁定会话中的应用程序

    运行应用程序可能会阻止客户端设备重启。例如，如果文档在文档处理应用程序中被编辑且未被保存，则应用程序不允许设备重启。

    如果启用该选项，锁定设备上的此类应用程序在设备重启前被强制关闭。结果，用户可能丢失他们未保存的更改。

    如果禁用该选项，锁定设备不被重启。该设备上的任务状态显示设备需要重启。用户必须手动关闭所有运行在锁定设备上的应用程序并重启这些设备。

    默认情况下已禁用该选项。

- 任务计划设置：
  - **计划开始设置：**
    - 每 N 小时

      任务定期运行，按照指定小时数间隔，从指定的日期和时间开始。

      默认下，任务每六小时运行一次，从当前系统日期和时间开始。

    - 每 N 天

      任务定期运行，按照指定天数间隔。此外，您可以指定第一个任务运行的日期和时间。如果您为其创建任务的应用程序支持这些附加选项，则这些选项可用。

      默认下，任务每天运行一次，从当前系统日期和时间开始。

- 每 N 星期

  任务定期运行，按照指定星期数间隔，从指定的星期和时间开始。

  默认下，任务每星期一于当前系统时间运行一次。

- 每 N 分钟

  任务定期运行，按照指定分钟数间隔，从任务创建日期的指定时间开始。

  默认下，任务每 30 分钟运行一次，从当前系统时间开始。

- 每天(不支持夏令时)

  任务定期运行，按照指定天数间隔。计划不支持夏令时(DST)。这意味着在夏令时开始和结束时当时钟向前或向后拨动一小时时，实际任务启动时间不更改。

  我们不建议您使用该计划。它用于向后兼容 Kaspersky Security Center Linux。

  默认下，任务每天于当前系统时间运行一次。

- 每周

  任务每周在指定星期和指定时间运行。

- 按星期中的天数

  任务定期运行，在指定星期的指定时间。

  默认情况下，任务在每周五 6:00:00 PM 运行。

- 每月

  任务定期运行，在指定月日的指定时间。

  在缺少指定日的月份，任务在最后一天运行。

  默认下，任务在每月的第一天运行，在当前系统时间。

- 手动

  任务不自动运行。您仅可以手动启动。

  默认情况下已启用该选项。

- 每个月在所选周的指定天

  任务定期运行，在指定月日的指定时间。

  默认情况下，不选择任何日期；默认开始时间为 6:00:00 PM。

- 当新更新下载至存储库时

当新更新下载至存储库后任务运行。例如，您可能想要对“*更新*”任务使用该计划。

- 在完成其他任务时

  当前任务在其他任务完成后启动。您可以选择先前任务如何结束(成功或带有错误)以触发当前任务的启动。仅当两个任务被分配给同一设备时，此参数才有效。

- 运行错过的任务

  该选项决定在任务要启动时客户端设备在网络中不可见时任务的行为。

  如果启用该选项，系统将在下一次在客户端设备上运行 Kaspersky 应用程序时尝试启动任务。如果任务计划是“**手动**”、“**一次**”或“**立即**”，则设备在网络中变得可见后或包含在任务范围后，会立即启动任务。

  如果该选项被禁用，则只有已计划的任务将在客户端设备上运行，而对于“**手动**”、“**一次**”和“**立即**”任务，仅会在网络中可见的客户端设备上运行。例如，您可能想为消耗资源的任务禁用该选项，您仅想在业余时间运行该任务。

  默认情况下已启用该选项。

- 使用任务启动自动随机延迟

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动，即*分布式任务启动*。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  当任务被创建时，根据任务中包含客户端设备的数量，分发启动时间被自动计算。然后，任务总是在计算的开始时间启动。然后当任务设置被编辑或者任务被手动启动时，计算的任务启动时间值被更改。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

- 使用任务启动随机延迟间隔(分钟)

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

  默认情况下已禁用该选项。默认时间间隔为一分钟。

- 要分配任务的设备：

  - 选择管理服务器检测到的网络设备

    任务被分配到特定设备。特定设备可以包含管理组的设备和未分配的设备。

    例如，您可能要在安装网络代理到未分配的设备的任务中使用该选项。

  - 手动指定设备地址或从列表导入地址

    您可以指定要为其分配任务的设备的 DNS 名称、IP 地址和 IP 子网。

    您可能要使用该选项以对特定子网执行任务。例如，您可能要安装特定应用程序到会计设备，或者扫描疑似被感染子网中的设备。

- 分配任务到设备分类

  该任务被分配到设备分类中的设备。您可以指定现有分类之一。
  例如，您可能要使用该选项在特定操作系统版本的设备上运行任务。

- 分配任务到管理组

  任务被分配到包含在管理组中的设备。您可以指定现有组之一或者创建新组。
  例如，您可能要使用该选项运行发送消息到用户任务，如果消息针对包含在特定管理组中的设备。

- 账户设置：

  - 默认账户

    在与执行该任务的应用程序相同的账户下运行该任务。
    默认情况下已选定该选项。

  - 指定账户

    填写“**账户**”和“**密码**”字段以指定用于运行任务的账户的详细信息。该账户必须具有足够的权限才能执行此任务。

  - 账户

    运行该任务的账户。

  - 密码

    任务运行时使用的账户的密码。

任务创建后指定的设置

您可以在创建任务后指定以下设置。

- 组任务设置：

  - 分发到子组

    此选项仅在组任务的设置中可用。
    启用此选项后，任务范围包括：
    - 您在创建任务时选择的管理组。
    - 从属于按组层次结构向下的任何级别的选定管理组的管理组。

    禁用此选项后，任务范围仅包括您在创建任务时选择的管理组。
    默认情况下已启用该选项。

- 分发到从属和虚拟管理服务器

  启用此选项后，在主管理服务器上有效的任务也将应用于从属管理服务器（包括虚拟管理服务器）。如果从属管理服务器上已经存在相同类型的任务，则两个任务都将应用于从属管理服务器—现有任务和从主管理服务器继承的任务。

  仅当启用"**分发到子组**"选项时，此选项才可用。

  默认情况下已禁用该选项。

- 高级计划设置：

  - 使用 Wake-On-LAN 功能在任务启动之前开启设备(分钟)

    设备上的操作系统在任务开始之前的指定时间启动。默认时间段为五分钟。

    如果您想要任务在任务范围内的所有客户端设备上运行，包括任务要启动时关闭的设备，则启用该选项。

    如果您希望在任务完成后自动关闭设备，请启用"**任务完成后关闭设备**"选项。可以在同一窗口中找到此选项。

    默认情况下已禁用该选项。

  - 任务完成后关闭设备

    例如，您可能想为每周五工作时间后安装更新到客户端设备的更新安装任务启用该选项，然后在周末关闭这些设备。

    默认情况下已禁用该选项。

  - 如果任务运行超过该时间则停止(分钟)

    在指定时间段过后，任务被自动停止，无论它是否完成。

    如果您想要中断或停止执行时间太长的任务，则启用该选项。

    默认情况下已禁用该选项。默认任务执行时间是 120 分钟。

- 通知设置：

  - 保存任务历史记录块：

    - 存储在管理服务器数据库上(天)

      有关任务范围内所有客户端设备上的任务执行的应用程序事件在指定的天数内被存储在管理服务器。当该时间段过后，信息被从管理服务器删除。

      默认情况下已启用该选项。

    - 存储在设备的 OS 事件日志中

      与任务执行相关的应用程序事件本地存储在每个客户端设备的 Syslog 事件日志中。

      默认情况下已禁用该选项。

- 存储在管理服务器的 OS 事件日志中

  与任务范围内所有客户端设备上的任务执行相关的应用程序事件集中存储在管理服务器操作系统 (OS) 的 Syslog 事件日志中。

  默认情况下已禁用该选项。

- 保存所有事件

  如果选择该选项，所有任务相关事件被保存到事件日志。

- 保存任务进度相关事件

  如果选择该选项，仅任务执行相关事件被保存到事件日志。

- 仅保存任务执行结果

  如果选择该选项，仅任务结果相关事件被保存到事件日志。

- 通知管理员任务执行的结果

  您可以选择管理员接收任务执行通知的方法：通过电子邮件、通过 SMS 和通过运行可执行文件。要配置通知，请点击“**设置**”链接。

  默认下，所有通知方法被禁用。

- 仅通知错误

  如果该选项被启用，管理员仅在任务执行完成但带有错误时被通知。

  如果该选项被禁用，管理员在每次任务执行完成后被通知。

  默认情况下已启用该选项。

- 安全设置。
- 任务范围设置。

  取决于任务范围决定的方式，以下设置被展现：

  - 设备。

    如果任务范围由管理组决定，您可以查看该组。这里不可以更改。然而，您可以设置**任务范围排除项**。

    如果任务范围由设备列表决定，您可以通过添加和删除设备修改该列表。

  - 设备分类

    您可以更改应用程序任务的设备分类。

  - 任务范围排除项

您可以指定应用任务的设备组。要排除的组仅可以是应用任务的管理组的子组。

- 修订历史。

导出任务

Kaspersky Security Center Linux 允许您将任务及其设置保存到 KLT 文件。您可以使用此 KLT 文件将保存的任务导入到 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux。

要导出任务，请执行以下操作：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。
2. 选中要导出的任务旁边的复选框。
   您不能同时导出多个任务。如果您选择了多个任务，**导出**按钮将被禁用。管理服务器任务也将无法导出。
3. 单击“**导出**”按钮。
4. 在打开的“**另存为**”窗口中，指定任务文件的名称和路径。单击“**保存**”按钮。
   仅当您使用 Google Chrome、Microsoft Edge 或 Opera 时，才会显示“**另存为**”窗口。如果您使用其他浏览器，则任务文件会自动保存在“**下载**”文件夹。

导入任务

Kaspersky Security Center Linux 允许您从 KLT 文件导入任务。KLT 文件包含导出的任务及其设置。

要导入任务，请执行以下操作：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。
2. 单击“**导入**”按钮。
3. 单击**浏览**按钮选择要导入的任务文件。
4. 在打开的窗口中，指定 KLT 任务文件的路径，然后单击“**打开**”按钮。请注意，您仅可选择一个任务文件。
   任务处理启动。
5. 任务成功处理后，选择要向其分配任务的设备。为此，请选择以下选项之一：
   - 分配任务到管理组

     任务被分配到包含在管理组中的设备。您可以指定现有组之一或者创建新组。
     例如，您可能要使用该选项运行发送消息到用户任务，如果消息针对包含在特定管理组中的设备。

   - 手动指定设备地址或从列表导入地址

您可以指定要为其分配任务的设备的 DNS 名称、IP 地址和 IP 子网。

您可能要使用该选项以对特定子网执行任务。例如，您可能要安装特定应用程序到会计设备，或者扫描疑似被感染子网中的设备。

- 分配任务到设备分类

  该任务被分配到设备分类中的设备。您可以指定现有分类之一。

  例如，您可能要使用该选项在特定操作系统版本的设备上运行任务。

6. 指定任务范围。

7. 单击**完成**按钮以完成任务导入。

出现包含导入结果的通知。如果任务成功导入，可以单击"**详细资料**"链接以查看任务属性。

成功导入后，任务会显示在任务列表中。任务设置和时间表也会一起导入。任务将根据其时间表启动。

如果新导入的任务与现有任务具有相同的名称，则导入的任务在名称后会附加一个（**<下一个序列号>**）索引，例如：**(1)**、**(2)**。

Starting the Change tasks password wizard

For a non-local task, you can specify an account under which the task must be run. You can specify the account during task creation or in the properties of an existing task. If the specified account is used in accordance with security instructions of the organization, these instructions might require changing the account password from time to time. When the account password expires and you set a new one, the tasks will not start until you specify the new valid password in the task properties.

The Change tasks password wizard enables you to automatically replace the old password with the new one in all tasks in which the account is specified. Alternatively, you can change this password manually in the properties of each task.

To start the Change tasks password wizard:

1. In the main menu, go to 资产**(**设备**)** → 任务.

2. Click 管理启动任务的账户凭证.

   Follow the instructions of the wizard.

Step 1. Specifying credentials

Specify new credentials that are currently valid in your system. When you switch to the next step of the wizard, Kaspersky Security Center Linux checks if the specified account name matches the account name in the properties of each non-local task. If the account names match, the password in the task properties will be automatically replaced with the new one.

To specify the new account, select an option:

- 使用当前账户

  The wizard uses the name of the account under which you are currently signed in to Kaspersky Security Center Web Console. Then manually specify the account password in the 在任务中使用的当前密码 field.

- 指定不同账户

  Specify the name of the account under which the tasks must be started. Then specify the account password in the 在任务中使用的当前密码 field.

If you fill in the 先前密码(可选，如果您要使用当前密码替换它) field, Kaspersky Security Center Linux replaces the password only for those tasks in which both the account name and the old password are found. The replacement is performed automatically. In all other cases you have to choose an action to take in the next step of the wizard.

Step 2. Selecting an action to take

If you did not specify the previous password in the first step of the wizard or if the specified old password has not matched the passwords in the task properties, you must choose an action to take for the tasks found.

To choose an action for a task:

1. Select the check box next to the task for which you want to choose an action.
2. Perform one of the following:
   - To remove the password in the task properties, click 删除凭证.

     The task is switched to run under the default account.
   - To replace the password with a new one, click 即便旧密码错误或未指定也强制密码更改.
   - To cancel the password change, click 未选择操作.

   The chosen actions are applied after you move to the next step of the wizard.

Step 3. Viewing the results

On the last step of the wizard, view the results for each of the found tasks. To complete the wizard, click the **Finish** button.

浏览保存在管理服务器中的任务运行结果

Kaspersky Security Center Linux 允许您查看组任务、特定设备的任务和管理服务器任务的运行结果。但无法浏览本地任务的运行结果。

要查看任务结果：

1. 在任务属性窗口中，选择“**常规**”区域。
2. 点击“**结果**”链接打开**任务结果**窗口。

应用程序标签

该部分描述了应用程序标签，提供了创建和修改它们以及标记第三方应用程序的说明。

关于应用程序标签

Kaspersky Security Center Linux 可让您标记第三方应用程序（非卡巴斯基的软件供应商制作的应用程序）。标签是应用程序标志，可以用于分组或查找应用程序。分配给应用程序的标签可以作为设备分类中的条件。

例如，您可以创建 [浏览器] 标签并分配其到所有浏览器（例如 Microsoft Internet Explorer、Google Chrome、Mozilla Firefox。）

创建应用程序标签

要创建应用程序标签：

1. 在主菜单中，转到“**操作 → 第三方应用程序 → 应用程序标签**“。
2. 单击**添加**。
   新标签窗口打开。
3. 输入标签名称。
4. 单击“**确定**”保存更改。

新标签出现在应用程序标签列表。

重命名应用程序标签

要重命名应用程序标签：

1. 在主菜单中，转到“**操作 → 第三方应用程序 → 应用程序标签**“。
2. 选中要重命名的标签旁边的复选框，然后单击“**编辑**”。
   标签属性窗口打开。
3. 更改标签名称。

4. 单击“**确定**”保存更改。

更新的标签出现在应用程序标签列表。

分配标签到应用程序

要分配一个或多个标签到一个应用程序：

1. 在主菜单中，转到“**操作**” → “**第三方应用程序**” → “**应用程序注册表**”。
2. 点击您要分配标签的应用程序名称。
3. 选择“**标签**”选项卡。

   标签显示所有存在于管理服务器的应用程序标签。对于分配到所选应用程序的标签，“**分配的标签**”列中的复选框处于选中状态。
4. 对于要分配的标签，请选中“**分配的标签**”列中的复选框。
5. 单击“**保存**”保存设置。

标签被分配到应用程序。

从应用程序上删除分配的标签

要从应用程序删除一个或多个标签：

1. 在主菜单中，转到“**操作**” → “**第三方应用程序**” → “**应用程序注册表**”。
2. 点击您要删除标签的应用程序名称。
3. 选择“**标签**”选项卡。

   标签显示所有存在于管理服务器的应用程序标签。对于分配到所选应用程序的标签，“**分配的标签**”列中的复选框处于选中状态。
4. 对于要删除的标签，请清除“**分配的标签**”列中的复选框。
5. 单击“**保存**”保存设置。

标签被从应用程序删除。

> 已卸载应用程序的标签不被删除。如果您想，您可以手动删除它们。

删除应用程序标签

要删除应用程序标签：

1. 在主菜单中，转到“**操作 → 第三方应用程序 → 应用程序标签**“。
2. 在列表中，选择您想要删除的应用程序标签。
3. 单击“**删除**”按钮。
4. 在打开的窗口中，单击“**确定**”。

应用程序标签被删除。删除的标签被从其分配的所有应用程序上自动删除。

Granting offline access to the external device blocked by Device Control

In Device Control component of the Kaspersky Endpoint Security policy, you can manage user access to external devices that are installed on or connected to the client device (for example, hard drives, cameras, or Wi-Fi modules). This lets you protect the client device from infection when such external devices are connected, and prevent loss or leaks of data.

If you need to grant temporary access to the external device blocked by Device Control but it is not possible to add the device to the list of trusted devices, you can grant temporary offline access to the external device. Offline access means that the client device has no access to the network.

You can grant offline access to the external device blocked by Device Control only if the **Allow request for temporary access** option is enabled in the settings of the Kaspersky Endpoint Security policy, in the 应用程序设置 → **Security Controls** → **Device Control** section.

Granting offline access to the external device blocked by Device Control includes the following stages:

1. In the Kaspersky Endpoint Security dialog window, device user who wants to have access to the blocked external device, generates a request access file and sends it to the Kaspersky Security Center Linux administrator.
2. Getting this request, the Kaspersky Security Center Linux administrator creates an access key file and send it to the device user.
3. In the Kaspersky Endpoint Security dialog window, the device user activates the access key file and obtains temporary access to the external device.

To grant temporary access to the external device blocked by Device Control:

1. In the main menu, go to 资产**(**设备**)** → 受管理设备.

   The list of managed devices is displayed.
2. In this list, select the user's device that requests access to the external device blocked by Device Control.

   You can select only one device.
3. Above the list of managed devices, click the ellipsis button (...), and then click the 授予移动模式设备访问权限 button.
4. In the 应用程序设置 window that opens, in the 设备控制 section, click the 浏览 button.

5. Select the request access file that you have received from the user, and then click the 打开 button. The file should have the AKEY format.

   The details of the locked device to which the user has requested access is displayed.

6. Specify the value of the **Access duration** setting.

   This setting defines the length of time for which you grant the user access to the locked device. The default value is the value that was specified by the user when creating the request access file.

7. Specify the value of the **Activation period** setting.

   This setting defines the time period during which the user can activate access to the blocked device by using the provided access key.

8. Click the 保存 button.

9. In the window that opens, select the destination folder in which you want to save the file containing the access key for the blocked device.

10. Click the 保存 button.

As a result, when you send the user the access key file and the user activates it in the Kaspersky Endpoint Security dialog window, the user has temporary access to the blocked device for the specific period.

使用 klscflag 实用程序开放端口 13291

管理服务器上的端口 13291 用于接收来自基于 MMC 的管理控制台的连接。在非 Windows 计算机上，此端口默认关闭。

如果要允许连接到基于 MMC 的管理控制台或使用 klakaut 实用程序，可以使用 klsclag 实用程序开放此端口。请注意，当连接到 Kaspersky Security Center Linux 时，基于 MMC 的管理控制台的功能会降低。我们建议您使用 Kaspersky Security Center Web Console 连接到 Kaspersky Security Center Linux。

klsclag 实用程序会更改 KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN 参数的值。

我们建议您使用 Kaspersky Security Center Web Console 连接到 Kaspersky Security Center Linux。

要开放端口 13291：

1. 在命令行中执行以下命令：

```
$ /opt/kaspersky/ksc64/sbin/klscflag -ssvset -pv klserver -s 87 -n
KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -sv true -svt BOOL_T -ss "|ss_type =
\"SS_SETTINGS\";"
```

2. 通过执行以下命令重新启动 Kaspersky Security Center 管理服务器：

```
$ sudo systemctl restart kladminserver_srv
```

端口 13291 已开放。

要检查端口 13291 是否已成功开放：

在命令行中执行以下命令：

```
$ /opt/kaspersky/ksc64/sbin/klscflag -ssvget -pv klserver -s 87 -n
KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
```

此命令会返回以下结果：

```
+--- (PARAMS_T)
+---KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN = (BOOL_T)true
```

`true` 值表示端口已开放。否则，将显示 `false` 值。

在 Kaspersky Security Center 13.2 Web 控制台中注册 Kaspersky Industrial CyberSecurity for Networks 应用程序

要开始通过 Kaspersky Security Center 13.2 Web Console 使用 Kaspersky Industrial CyberSecurity for Networks Web 应用程序，您必须首先在 Kaspersky Security Center 13.2 Web Console 中注册它。

要注册 Kaspersky Industrial CyberSecurity for Networks 应用程序：

1. 确保完成以下操作：

   - 您已下载并安装 Kaspersky Industrial CyberSecurity for Networks Web 插件。

     您可以稍后在等待 Kaspersky Industrial CyberSecurity for Networks Server 与管理服务器同步时执行此操作。下载并安装插件后，**KICS for Networks**部分将显示在 Kaspersky Security Center Web Console 主菜单中。

   - 在 Kaspersky Industrial CyberSecurity for Networks 网页界面中，配置并启用了与 Kaspersky Security Center 的交互。详情请参阅 Kaspersky Industrial CyberSecurity for Networks 在线帮助。

2. 将安装有 Kaspersky Industrial CyberSecurity for Networks Server 的设备从未分配设备组移动到受管理设备组：

   a. 在主菜单中，转到**发现和部署 → 未分配的设备**。

   b. 选中安装有 Kaspersky Industrial CyberSecurity for Networks Server 的设备旁边的复选框。

   c. 单击**移动到组**按钮。

   d. 在管理组的层次结构中，选中**受管理设备**组旁边的复选框。

   e. 单击“**移动**”按钮。

3. 打开安装了 Kaspersky Industrial CyberSecurity for Networks Server 的设备的属性窗口。

4. 在设备属性页面的 **General** 部分，选择“**不要断开与管理服务器的连接**”选项，然后单击“**保存**”按钮。

5. 在设备属性页面，选择**应用程序**区域。

6. 在**应用程序**区域，选择 Kaspersky Security Center 网络代理。

7. 如果应用程序的当前状态是“*已停止*”，等到它变为“*正在运行*”。

   这最多需要 15 分钟。如果您尚未安装 Kaspersky Industrial CyberSecurity for Networks Web 插件，您可以立即安装。

8. 如果想查看 Kaspersky Industrial CyberSecurity for Networks 的统计信息，您可以在仪表板上添加小部件。要添加小部件，请执行以下操作：

a. 在主菜单中，转到**监控和报告 → 仪表板**。

b. 在仪表板上，单击"**添加或恢复网页小部件**"按钮。

c. 在打开的小部件菜单中，选择"**其它**"。

d. 选择您要添加的小部件：

- KICS for Networks 部署图
- 有关 KICS for Networks Servers 的信息
- KICS for Networks 的最新活动
- KICS for Networks 中存在问题的设备
- KICS for Networks 中的关键事件
- KICS for Networks 中的状态

9. 要继续访问 Kaspersky Industrial CyberSecurity for Networks Web 界面，请执行以下操作：

a. 在主菜单中，转至**KICS for Networks →搜索**。

b. 单击**查找事件或设备**按钮。

c. 在打开的**查询参数**窗口中，单击**服务器**字段。

d. 从与 Kaspersky Security Center 集成的服务器下拉列表中选择 Kaspersky Industrial CyberSecurity for Networks 服务器，然后单击**查找**按钮。

e. 单击 Kaspersky Industrial CyberSecurity for Networks 服务器名称旁边的**转至服务器**链接。

Kaspersky Industrial CyberSecurity for Networks 登录页面将显示。

> 要登录 Kaspersky Industrial CyberSecurity for Networks Web 界面，您需要提供应用程序用户账户凭据。

管理用户和用户角色

该部分描述了用户和用户角色，并提供创建和修改它们、分配角色和组到用户以及关联策略配置文件到角色的说明。

关于用户账户

Kaspersky Security Center Linux 允许您管理用户账户以及安全组。该程序支持两种账户类型：

- 组织员工的账户。在轮询组织网络时，管理服务器检索本地用户账户的数据。
- Kaspersky Security Center Linux 内部用户的账户。您可以在门户上创建内部用户账户。这些账户仅在 Kaspersky Security Center Linux 内使用。

查看用户账户和安全组表：

1. 在主菜单中，转到**用户和角色** → **用户和组**。
2. 选择**用户**或**组**选项卡。

用户或安全组表将打开。如果要查看仅包含内部用户或组或仅包含本地用户或组的表，请将**子类型**过滤条件分别设置为**内部**或**本地**。

关于用于角色

用户角色（也叫*角色*）是包含一组权限集的对象。角色可以与安装在用户设备上的 Kaspersky 应用程序设置关联。您可以分配角色到用户集，或者到管理组层级的任何级别、管理服务器或特定对象级别的安全组集。

如果您通过包含虚拟管理服务器的管理服务器层级来管理设备，请注意，您仅可从物理管理服务器创建、修改或删除用户角色。这样，您可以将用户角色传输到从属管理服务器，包括虚拟服务器。

您可以关联用户角色到策略配置文件。如果用户被分配角色，用户将获得执行工作职能所需的安全设置。

一个用户角色可以与特定管理组中的设备用户关联。

用户角色范围

*用户角色范围*是用户和管理组的组合。与用户角色关联的设置仅应用到属于该角色用户的设备，以及仅在这些设备属于与该角色关联的组（包括子组）时。

使用角色的好处

使用角色的好处之一是您不必为每个受管理设备或用户指定安全设置。公司中的用户和设备数量可能太大，但是需要不同安全设置的不同工作的数量相对较小。

与使用策略配置文件的不同点

策略配置文件是为每个 Kaspersky 应用程序创建的策略的属性。角色与许多为不同应用程序创建的策略配置文件相关联。因此，角色是联合特定用户类型的设置到一处的方法。

Configuring access rights to application features. Role-based access control

Kaspersky Security Center Linux provides facilities for role-based access to the features of Kaspersky Security Center Linux and managed Kaspersky applications.

You can configure access rights to application features for Kaspersky Security Center Linux users in one of the following ways:

- By configuring the rights for each user or group of users individually.
- By creating standard user roles with a predefined set of rights and assigning those roles to users depending on their scope of duties.

Application of user roles is intended to simplify and shorten routine procedures of configuring users' access rights to application features. Access rights within a role are configured in accordance with the standard tasks and the users' scope of duties.

User roles can be assigned names that correspond to their respective purposes. You can create an unlimited number of roles in the application.

You can use the predefined user roles with already configured set of rights, or create new roles and configure the required rights yourself.

Access rights to application features

The table below shows the Kaspersky Security Center Linux features with the access rights to manage the associated tasks, reports, settings, and perform the associated user actions.

To perform the user actions listed in the table, a user has to have the right specified next to the action.

Read, **Write**, and **Execute** rights are applicable to any task, report, or setting. In addition to these rights, a user has to have the **Perform operations on device selections** right to manage tasks, reports, or settings on device selections.

> All tasks, reports, settings, and installation packages that are missing in the table belong to the **General features: Basic functionality** functional area.

Access rights to application features

Functional area	Right	User action: right required to perform the action	Task	Report	Other
General features: Management	**Write**	• Add device to an	None	None	None

of administration groups		administration group: **Write** • Delete device from an administration group: **Write** • Add an administration group to another administration group: **Write** • Delete an administration group from another administration group: **Write**			
General features: **Access objects regardless of their ACLs**	**Read**	Get read access to all objects: **Read**	None	None	None
General features: **Basic functionality**	• **Read** • **Write** • **Execute** • **Perform operations on device selections**	• Device moving rules (create, modify, or delete) for the virtual Server: **Write**, **Perform operations on device selections** • Get Mobile (LWNGT) protocol custom certificate: **Read** • Set Mobile (LWNGT) protocol custom certificate: **Write** • Get NLA-defined network list: **Read**	• "Download updates to the Administration Server repository" • "Deliver reports" • "Distribute installation package" • "Install application on secondary Administration Servers remotely"	• "Report on protection status" • "Report on threats" • "Report on most heavily infected devices" • "Report on status of anti-virus databases" • "Report on errors" • "Report on network attacks" • "Summary report on perimeter defense	None

		• Add, modify, or delete NLA-defined network list: **Write** • View Access Control List of groups: **Read** • View the operating system log: **Read**		applications installed" • "Summary report on types of applications installed" • "Report on users of infected devices" • "安全问题报告" • "Report on events" • "Report on activity of distribution points" • "Report on secondary Administration Servers" • "Report on Device Control events" • "Report on prohibited applications" • "Report on Web Control" • "受管理设备加密状态报告" • "大容量存储设备加密状态报告" • "加密驱动器访问权限报告" • "文件加密错误报告" • "加密文件访问被阻止报告"

				• "Report on effective user permissions" • "Report on rights"	
General features: **Deleted objects**	• **Read** • **Write**	• View deleted objects in the Recycle Bin: **Read** • Delete objects from the Recycle Bin: **Write**	None	None	None
General features: **Event processing**	• **Delete events** • **Edit event notification settings** • **Edit event logging settings** • **Write**	• Change events registration settings: **Edit event logging settings** • Change events notification settings: **Edit event notification settings** • Delete events: **Delete events**	None	None	Settings: • The maximu numbe of events stored the databa • Period time fo storing events from th delete device
General features: **Operations on Administration Server**	• **Read** • **Write** • **Execute** • **Modify object ACLs** • **Perform operations on device selections**	• Specify ports of Administration Server for the network agent connection: **Write** • Specify ports of Activation Proxy launched on the Administration Server: **Write** • Specify ports of Activation Proxy for Mobile launched on the	• "Backup of Administration Server data" • "Databases maintenance"	None	None

		Administration Server: **Write** • Specify ports of the Web Server for distribution of standalone packages: **Write** • Specify ports of the Web Server for distribution of MDM profiles: **Write** • Specify SSL-ports of the Administration Server for connection via Web Console: **Write** • Specify ports of the Administration Server for mobile connection: **Write** • Specify the maximum number of events stored in the Administration Server database: **Write** • Specify the maximum number of events that can be sent by the Administration Server: **Write** • Specify time period during which events can be sent by the		

		Administration Server: **Write**			
General features: Kaspersky software deployment	• **Manage Kaspersky patches** • **Read** • **Write** • **Execute** • **Perform operations on device selections**	Approve or decline installation of the patch: **Manage Kaspersky patches**	None	• "Report on license key usage by virtual Administration Server" • "Report on Kaspersky software versions" • "Report on incompatible applications" • "Report on versions of Kaspersky software module updates" • "Report on protection deployment"	Installatio package: "Kaspersk
General features: Key management	• **Export key file** • **Write**	• Export key file: **Export key file** • Modify Administration Server license key settings: **Write**	None	None	None
General features: Enforced report management	• **Read** • **Write**	• Create reports regardless of their ACLs: **Write** • Execute reports regardless of their ACLs: **Read**	None	None	None
General features: Hierarchy of Administration Servers	**Configure hierarchy of Administration Servers**	• Register, update, or delete secondary	None	None	None

		Administration Servers: **Configure hierarchy of Administration Servers**			
General features: **User permissions**	**Modify object ACLs**	• Change Security properties of any object: **Modify object ACLs** • Manage user roles: **Modify object ACLs** • Manage internal users: **Modify object ACLs** • Manage security groups: **Modify object ACLs** • Manage aliases: **Modify object ACLs**	None	None	None
General features: **Virtual Administration Servers**	• **Manage virtual Administration Servers** • **Read** • **Write** • **Execute** • **Perform operations on device selections**	• Get list of virtual Administration Servers: **Read** • Get information on the virtual Administration Server: **Read** • Create, update, or delete a virtual Administration Server: **Manage virtual Administration Servers** • Move a virtual Administration Server to	None	None	None

		another group: **Manage virtual Administration Servers** • Set administration virtual Server permissions: **Manage virtual Administration Servers**			
General features: **Encryption Key Management**	**Write**	Import the encryption keys: **Write**	None	None	None
System management: **Vulnerability and patch management**	• **Read** • **Write** • **Execute** • **Perform operations on device selections**	• View third-party patch properties: **Read** • Change third-party patch properties: **Write**	• "Fix vulnerabilities" • "Install required updates and fix vulnerabilities"	"Report on software updates"	None

Predefined user roles

User roles assigned to Kaspersky Security Center Linux users provide them with sets of access rights to application features.

Users created on a virtual Server cannot be assigned a role on the Administration Server.

You can use the predefined user roles with already configured set of rights, or create new roles and configure the required rights yourself. Some of the predefined user roles available in Kaspersky Security Center Linux can be associated with specific job positions, for example, **Auditor**, **Security Officer**, **Supervisor**. Access rights of these roles are pre-configured in accordance with the standard tasks and scope of duties of the associated positions. The table below shows how roles can be associated with specific job positions.

Examples of roles for specific job positions

Role	Comment
Auditor	Permits all operations with all types of reports, all viewing operations, including viewing deleted objects (grants the **Read** and **Write** permissions in the **Deleted objects** area). Does not permit other operations. You can assign this role to a person who performs the audit of your organization.
Supervisor	Permits all viewing operations; does not permit other operations. You can assign this role to a

	security officer and other managers in charge of the IT security in your organization.
Security Officer	Permits all viewing operations, permits reports management; grants limited permissions in the **System management**: **Connectivity** area. You can assign this role to an officer in charge of the IT security in your organization.

The table below shows the access rights assigned to each predefined user role.

Features of the functional areas **Mobile Device Management: General** and **System management** are not available in Kaspersky Security Center Linux. A user with the roles **Vulnerability and patch management administrator/operator** or **Mobile Device Management Administrator/Operator** has access only for rights from the **General features**: **Basic functionality** area.

Access rights of predefined user roles

Role	Description
Administration Server Administrator	Permits all operations in the following functional areas, in **General features**: • **Basic functionality** • **Event processing** • **Hierarchy of Administration Servers** • **Virtual Administration Servers** Grants the **Read** and **Write** rights in the **General features: Encryption key management** functional area.
Administration Server Operator	Grants the **Read** and **Execute** rights in all of the following functional areas, in **General features**: • **Basic functionality** • **Virtual Administration Servers**
Auditor	Permits all operations in the following functional areas, in **General features**: • **Access objects regardless of their ACLs** • **Deleted objects** • **Enforced report management** You can assign this role to a person who performs the audit of your organization.
Installation Administrator	Permits all operations in the following functional areas, in **General features**: • **Basic functionality** • **Kaspersky software deployment** • **License key management** Grants **Read** and **Execute** rights in the **General features: Virtual Administration Servers** functional area.
Installation Operator	Grants the **Read** and **Execute** rights in all of the following functional areas, in **General features**:

	• **Basic functionality** • **Kaspersky software deployment** (also grants the **Manage Kaspersky Lab patches** right in this area) • **Virtual Administration Servers**
Kaspersky Endpoint Security Administrator	Permits all operations in the following functional areas: • **General features: Basic functionality** • Kaspersky Endpoint Security area, including all features Grants the **Read** and **Write** rights in the **General features: Encryption key management** functional area.
Kaspersky Endpoint Security Operator	Grants the **Read** and **Execute** rights in all of the following functional areas: • **General features: Basic functionality** • Kaspersky Endpoint Security area, including all features
Main Administrator	Permits all operations in functional areas, *except* for the following areas, in **General features**: • **Access objects regardless of their ACLs** • **Enforced report management** Grants the **Read** and **Write** rights in the **General features: Encryption key management** functional area.
Main Operator	Grants the **Read** and **Execute** (where applicable) rights in all of the following functional areas: • **General features**: • **Basic functionality** • **Deleted objects** • **Operations on Administration Server** • **Kaspersky Lab software deployment** • **Virtual Administration Servers** • Kaspersky Endpoint Security area, including all features
Mobile Device Management Administrator	Permits all operations in the **General features: Basic functionality** functional area.
Security Officer	Permits all operations in the following functional areas, in **General features**: • **Access objects regardless of their ACLs** • **Enforced report management**

	Grants the **Read**, **Write**, **Execute**, **Save files from devices to the administrator's workstation**, and **Perform operations on device selections** rights in the **System management: Connectivity** functional area. You can assign this role to an officer in charge of the IT security in your organization.
Self Service Portal User	Permits all operations in the **Mobile Device Management: Self Service Portal** functional area. This feature is not supported in Kaspersky Security Center 11 and later version.
Supervisor	Grants the **Read** right in the **General features**: **Access objects regardless of their ACLs** and **General features**: **Enforced report management** functional areas. You can assign this role to a security officer and other managers in charge of the IT security in your organization.

分配对特定对象的访问权限

除了分配服务器级别的访问权限，您还可以配置对特定对象的访问，例如对特定任务的访问。该应用程序允许您指定对以下对象类型的访问权限：

- 管理组
- 任务
- 报告
- 设备分类
- 事件分类

要分配对特定对象的访问权限：

1. 根据对象类型，在主菜单中转到相应区域：
   - **资产(设备)** → **组层级**
   - **资产(设备)**→**任务**
   - **监控和报告** → **报告**
   - **资产(设备)**→**设备分类**
   - **监控和报告** → **事件分类**
2. 打开要为其配置访问权限的对象的属性。

   要打开管理组或任务的属性窗口，单击对象名称。其他对象的属性可以使用工具栏上的按钮打开。
3. 在属性窗口中，打开**访问权限**部分。

   用户列表将打开。列出的用户和安全组具有对象的访问权限。默认情况下，如果您使用管理组或服务器的层级，则列表和访问权限是从父管理组或主服务器继承的。
4. 为了能够修改列表，启用**使用自定义权限**选项。
5. 配置访问权限：

- 使用**添加**和**删除**按钮修改列表。
- 指定用户或安全组的访问权限。执行以下操作之一：
  - 如果要手动指定访问权限，请选择用户或安全组，单击“**访问权限**”按钮，然后指定访问权限。
  - 如果要分配一个用户角色到用户或安全组，请选择用户或安全组，单击“**角色**”按钮，然后选择要分配的角色。

6. 单击“**保存**”按钮。

配置对象的访问权限。

分配访问权限到用户和组

您可以给予用户和用户组访问权限以使用管理服务器和您拥有管理插件的 Kaspersky 程序（例如，Kaspersky Endpoint Security for Linux）的不同功能。

将访问权限分配给用户或用户组：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ()。
   管理服务器属性窗口将打开。
2. 在**“访问权限”**选项卡上，选中要分配权限的用户或安全组名称旁边的复选框，然后单击**“访问权限”**按钮。
   您不能同时选择多个用户或安全组。如果您选择了多个条目，**访问权限**按钮将被禁用。
3. 配置用户或组的权限集：
   a. 使用管理服务器或其他卡巴斯基应用程序的功能扩展节点。
   b. 选择所需功能或访问权限旁边的**允许**或**拒绝**复选框。
      *示例 1：*选中**应用程序集成**节点旁边的**允许**复选框，向用户或组授予对应用程序集成功能（**读取**、**写入**和**执行**）的所有可用访问权限。
      *示例 2：*展开**加密密钥管理**节点，然后选中写入权限旁边**的允许**复选框，以授予用户或组对加密密钥管理功能的**写入**访问权限。
4. 配置访问权限集后，单击**确定**。

用户或用户组的权限集将被配置。

管理服务器（或管理组）的权限被分成以下部分：

- 常规功能：
  - 管理组的管理（仅适用于 Kaspersky Security Center Linux 11 或更新）
  - 访问对象而不考虑它们的 ACLs（仅对 Kaspersky Security Center Linux 11 或更新）
  - 基本功能
  - 已删除对象（仅适用于 Kaspersky Security Center Linux 11 或更新）

    - 加密密钥管理
    - 事件处理
    - 管理服务器操作（仅在管理服务器的属性窗口）
    - Kaspersky 软件部署
    - 授权许可密钥管理
    - 应用程序整合
    - 强制报告管理
    - 管理服务器层级
    - 用户权限
    - 虚拟管理服务器
- 移动设备管理：
    - 常规
    - Self Service Portal
- 系统管理：
    - 连接
    - 硬件清单
    - 网络访问控制
    - 操作系统部署
    - 远程安装
    - 软件清查

如果没有为访问权限选择“**允许**”或“**拒绝**”，则该访问权限被认为*未定义*：它将被拒绝，直到被用户明确拒绝或允许为止。

用户权限是以下各项的集合：

- 用户自己的权限
- 分配给该用户的所有角色的权限
- 用户所属的所有安全组的权限
- 分配到用户所属安全组的所有角色的权限

如果至少一个权限集对权限“**拒绝**”，那么用户被拒绝该权限，即便其他集允许它或保持未定义。

添加内部用户账户

要向 Kaspersky Security Center Linux 添加新的内部用户账户：

1. 在主菜单中，转至**用户和角色** → **用户和组**，然后选择**用户**选项卡。
2. 单击**添加**。
3. 在打开的“**添加用户**”窗口中，指定新用户账户设置：
   - **名称**。
   - 连接到 Kaspersky Security Center Linux 的用户的**密码**。
     密码必须符合以下规则：
     - 密码必须是8 到 16 位字符长度。
     - 密码必须包含以下组中三组的字符：
       - 大写字母 (A-Z)
       - 小写字母 (a-z)
       - 数字 (0-9)
       - 特殊字符 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - 密码不可以包含任何空格、Unicode 字符以及“.”和“@”按先后顺序的组合。

     要查看您输入的字符，请单击并按住“**显示**”按钮。

     > 输入密码的尝试次数有限。默认下，允许的最大密码输入尝试次数是 10。您可以管理允许的密码输入尝试次数，描述在“更改允许的密码输入尝试次数”。

     > 如果用户输入无效的密码指定次数，用户账户被锁定一小时。您仅可以通过更改密码解除阻止用户账户。
4. 单击“**保存**”保存设置。

新的用户账户将被添加到用户列表中。

创建安全组

要创建安全组：

1. 在主菜单中，转至**用户和角色** → **用户和组**，然后选择**组**选项卡。

2. 单击**添加**。

3. 在打开的**创建安全组**窗口中，为新安全组指定以下设置：

   - **组名称**
   - **描述**

4. 单击“**保存**”保存设置。

新的安全组已被添加到组列表中。

编辑内部用户账户

要编辑 Kaspersky Security Center Linux 的内部用户账户：

1. 在主菜单中，转至**用户和角色** → **用户和组**，然后选择**用户**选项卡。
2. 点击您要编辑的用户账户名称。
3. 在打开的用户设置窗口中的“**常规**”选项卡上，更改用户账户设置：

   - **描述**
   - **完整名称**
   - **邮件地址**
   - **主电话**
   - 为连线到 Kaspersky Security Center Linux 的用户的**设置新密码**。
     密码必须符合以下规则：
     - 密码必须是8 到 16 位字符长度。
     - 密码必须包含以下组中三组的字符：
       - 大写字母 (A-Z)
       - 小写字母 (a-z)
       - 数字 (0-9)
       - 特殊字符 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - 密码不可以包含任何空格、Unicode 字符以及“.”和“@”按先后顺序的组合。

     要查看输入的密码，单击并按住“**显示**”按钮。

输入密码的尝试次数有限。默认下，允许的最大密码输入尝试次数是 10。您可以更改允许的尝试次数；但是，出于安全原因，我们不建议您减少此数字。如果用户输入无效的密码指定次数，用户账户被锁定一小时。您仅可以通过更改密码解除阻止用户账户。

- 如果必要，将切换按钮切换到“**已禁用**”以禁止用户连接到应用程序。您可以禁用账户，例如，在员工离职后。

4. 在“**身份验证安全**”选项卡上，可以指定此账户的安全设置。
5. 在“**组**”选项卡上，可以添加用户到安全组。
6. 在“**设备**”选项卡上，可以分配设备到用户。
7. 在“**角色**”选项卡上，可以分配角色到用户。
8. 单击“**保存**”保存设置。

更新的用户账户出现在用户列表中。

编辑安全组

要编辑安全组：

1. 在主菜单中，转至**用户和角色** → **用户和组**，然后选择**组**选项卡。
2. 点击您要编辑的安全组名称。
3. 在打开的组设置窗口中，更改安全组设置：
   - 在**常规**选项卡上，您可以更改**名称**和**描述**设置。这些设置仅适用于内部安全组。
   - 在“**用户**”选项卡上，可以添加用户到安全组。此设置仅适用于内部用户和内部安全组。
   - 在“**角色**”选项卡上，可以分配角色到安全组。
4. 单击“**保存**”保存设置。

更改将应用于安全组。

为用户或安全组分配角色

为用户或安全组分配角色：

1. 在主菜单中，转至**用户和角色**→**用户和组**，然后选择**用户**或**组**选项卡。
2. 选择要向其分配角色的用户或安全组的名称。
   您可以选择多个名称。

3. 在菜单项目上，单击“**分配角色**”按钮。

   角色分配向导启动。

4. 按照向导的说明进行操作：选择要分配给所选用户或安全组的角色，然后选择角色的范围。

   *用户角色范围*是用户和管理组的组合。与用户角色关联的设置仅应用到属于该角色用户的设备，以及仅在这些设备属于与该角色关联的组（包括子组）时。

拥有一组管理服务器使用权限的角色将被指派给用户（或多个用户，或安全组）。在用户或安全组列表中，**已分配角色**列中会出现一个复选框。

添加用户账户到内部安全组

您仅可以添加内部用户账户到内部安全组。

要添加用户账户到内部安全组：

1. 在主菜单中，转至**用户和角色** → **用户和组**，然后选择**用户**选项卡。
2. 选择您要添加到安全组的用户账户旁边的复选框。
3. 单击“**分配组**”按钮。
4. 在打开的“**分配组**”窗口中，选择要将用户账户添加到的安全组。
5. 单击“**保存**”按钮。

用户账户被添加到安全组。您还可以使用组设置将内部用户添加到安全组。

指派用户作为设备所有者

有关将用户指定为移动设备所有者的信息，请参阅 Kaspersky Security for Mobile 帮助。

要指派用户作为设备所有者：

1. 如果要分配连接到虚拟管理服务器的设备的所有者，请先切换到虚拟管理服务器：
   a. 在主菜单中，单击当前管理服务器名称右侧的 V 形图标 ()。
   b. 选择所需的管理服务器。
2. 在主菜单中，转至**用户和角色** → **用户和组**，然后选择**用户**选项卡。

   系统打开一个用户列表。如果您当前连接到虚拟管理服务器，则该列表包括来自当前虚拟管理服务器和主管理服务器的用户。
3. 点击您要分配为设备所有者的用户账户名称。
4. 在打开的用户设置窗口中，选择“**设备**”选项卡。

5. 单击**添加**。

6. 从设备列表中，选择您要分配给用户的设备。

7. 单击**"确定"**。

所选的设备被添加到分配给用户的设备列表。

您可以在**"资产(设备)"**→**"受管理设备"**中执行相同操作，方法是单击要分配的设备名称，然后单击**"管理设备所有者"**链接。

Enabling account protection from unauthorized modification

You can enable an additional option to protect a user account from unauthorized modification. If this option is enabled, modifying user account settings requires authorization of the user with the rights for modification.

To enable or disable account protection from unauthorized modification:

1. In the main menu, go to 用户和角色 → 用户和组, and then select the 用户 tab.
2. Click the name of the internal user account for which you want to specify account protection from unauthorized modification.
3. In the user settings window that opens, select the 身份验证安全 tab.
4. On the 身份验证安全 tab, select the 请求身份验证以检查修改此账户的权限 option if you want to request credentials every time when account settings are changed or modified. Otherwise, select the 允许用户修改该账户而不需要附加身份验证 option.
5. Click the **Save** button.

Two-step verification

This section describes how you can use two-step verification to reduce the risk of unauthorized access to Kaspersky Security Center Web Console.

Scenario: configuring two-step verification for all users

This scenario describes how to enable two-step verification for all users and how to exclude user accounts from two-step verification. If you did not enable two-step verification for your account before you enable it for other users, the application opens the window for enabling two-step verification for your account, first. This scenario also describes how to enable two-step verification for your own account.

If you enabled two-step verification for your account, you may proceed to the stage of enabling of two-step verification for all users.

Prerequisites

Before you start:

- Make sure that your user account has the Modify object ACLs right of the **General features: User permissions** functional area for modifying security settings for other users' accounts.
- Make sure that the other users of Administration Server install an authenticator application on their devices.

Stages

Enabling two-step verification for all users proceeds in stages:

1. **Installing an authenticator application on a device**

   You can install any application that supports the Time-based One-time Password algorithm (TOTP), such as:

   - Google Authenticator
   - Microsoft Authenticator
   - Bitrix24 OTP
   - Yandex Key
   - Avanpost Authenticator
   - Aladdin 2FA

   To check if Kaspersky Security Center Linux supports the authenticator application that you want to use, enable two-step verification for all users or for a particular user.

   One of the steps suggests that you specify the security code generated by the authenticator application. If it succeeds, then Kaspersky Security Center Linux supports the selected authenticator.

2. **Synchronizing the authenticator application time with the time of the device on which Administration Server is installed**

   Ensure that the time on the device with the authenticator application and the time on the device with the Administration Server are synchronized to UTC, by using external time sources. Otherwise, failures may occur during the authentication and activation of two-step verification.

3. **Enabling two-step verification for your account and receiving the secret key for your account**

   After you enable two-step verification for your account, you can enable two-step verification for all users.

4. **Enabling two-step verification for all users**

   Users with two-step verification enabled must use it to log in to Administration Server.

5. **Prohibit new users from setting up two-step verification for themselves**

   In order to further improve Kaspersky Security Center Web Console access security, you can prohibit new users from setting up two-step verification for themselves.

6. **Editing the name of a security code issuer**

   If you have several Administration Servers with similar names, you may have to change the security code issuer names for better recognition of different Administration Servers.

7. **Excluding user accounts for which you do not need to enable two-step verification**

   If required, you can exclude users from two-step verification. Users with excluded accounts do not have to use two-step verification to log in to Administration Server.

8. **Configuring two-step verification for your own account**

   If the users are not excluded from two-step verification and two-step verification is not yet configured for their accounts, they need to configure it in the window that opens when they sign-in to Kaspersky Security Center Web Console. Otherwise, they will not be able to access the Administration Server in accordance with their rights.

Results

Upon completion of this scenario:

- Two-step verification is enabled for your account.
- Two-step verification is enabled for all user accounts of the Administration Server, except for user accounts that were excluded.

About two-step verification for an account

Kaspersky Security Center Linux provides two-step verification for users of Kaspersky Security Center Web Console. When two-step verification is enabled for your own account, every time you log in to Kaspersky Security Center Web Console, you enter your user name, password, and an additional single-use security code. To receive a single-use security code, you must have an authenticator app on your computer or your mobile device.

A security code has an identifier referred to as *issuer name*. The security code issuer name is used as an identifier of the Administration Server in the authenticator app. You can change the name of the security code issuer name. The security code issuer name has a default value that is the same as the name of the Administration Server. The issuer name is used as an identifier of the Administration Server in the authenticator app. If you change the security code issuer name, you must issue a new secret key and pass it to the authenticator app. A security code is single-use and valid for up to 90 seconds (the exact time may vary).

Any user for whom two-step verification is enabled can reissue his or her own secret key. When a user authenticates with the reissued secret key and uses it for logging in, Administration Server saves the new secret key for the user account. If the user enters the new secret key incorrectly, Administration Server does not save the new secret key and leaves the current secret key valid for the further authentication.

> Any authentication software that supports the Time-based One-time Password algorithm (TOTP) can be used as an authenticator app, for example, Google Authenticator. In order to generate the security code, you must synchronize the time set in the authenticator app with the time set for Administration Server.

To check if Kaspersky Security Center Linux supports the authenticator app that you want to use, enable two-step verification for all users or for a particular user.

One of the steps suggests that you specify the security code generated by the authenticator app. If it succeeds, then Kaspersky Security Center Linux supports the selected authenticator.

An authenticator app generates the security code as follows:

1. Administration Server generates a special secret key and QR code.

2. You pass the generated secret key or QR code to the authenticator app.

3. The authenticator app generates a single-use security code that you pass to the authentication window of Administration Server.

We highly recommend that you install an authenticator app on more than one device. Save the secret key (or QR code) and keep it in a safe place. This will help you to restore access to Kaspersky Security Center Web Console in case you lose access to your mobile device.

To secure the usage of Kaspersky Security Center Linux, you can enable two-step verification for your own account and enable two-step verification for all users.

You can exclude accounts from two-step verification. This can be necessary for service accounts that cannot receive a security code for authentication.

Two-step verification works according to the following rules:

- Only a user account that has the Modify object ACLs right in the **General features: User permissions** functional area can enable two-step verification for all users.
- Only a user that enabled two-step verification for his or her own account can enable the option of two-step verification for all users.
- Only a user that enabled two-step verification for his or her own account can exclude other user accounts from the list of two-step verification enabled for all users.
- A user can enable two-step verification only for his or her own account.
- A user account that has the Modify object ACLs right in the **General features: User permissions** functional area and is logged in to Kaspersky Security Center Web Console by using two-step verification can disable two-step verification: for any other user only if two-step verification for all users is disabled, for a user excluded from the list of two-step verification that is enabled for all users.
- Any user that logged in to Kaspersky Security Center Web Console by using two-step verification can reissue his or her own secret key.
- You can enable the two-step verification for all users option for the Administration Server you are currently working with. If you enable this option on the Administration Server, you also enable this option for the user accounts of its virtual Administration Servers and do not enable two-step verification for the user accounts of the secondary Administration Servers.

Enabling two-step verification for your own account

You can enable two-step verification only for your own account.

Before you start enabling two-step verification for your account, ensure that an authenticator application is installed on your mobile device. Ensure that the time set in the authenticator application is synchronized with the time set of the device on which Administration Server is installed.

To enable two-step verification for a user account:

1. In the main menu, go to 用户和角色 → 用户和组, and then select the 用户 tab.
2. Click the name of your account.
3. In the user settings window that opens, select the 身份验证安全 tab:
   a. Select the 请求用户名、密码和安全码(两步验证) option. Click the **Save** button.
   b. In the two-step verification window that opens, click 查看如何建立两步验证.
      Enter the secret key in the authenticator application or click 查看二维码 and scan the QR code by the authenticator application on your mobile device to receive one-time security code.
   c. In the two-step verification window, specify the security code generated by the authenticator application, and then click the 检查和应用 button.
4. Click the **Save** button.

Two-step verification is enabled for your account.

Enabling two-step verification for all users

You can enable two-step verification for all users of Administration Server if your account has the Modify object ACLs right in the **General features: User permissions** functional area and if you are authenticated by using two-step verification.

To enable two-step verification for all users:

1. In the main menu, click the settings icon ( ) next to the name of the required Administration Server.
   The Administration Server properties window opens.
2. On the 身份验证安全 tab of the properties window, switch the toggle button of the **two-step verification for all users** option to the enabled position.
3. If you did not enable two-step verification for your account, the application opens the window for enabling two-step verification for your own account.
   a. In the two-step verification window, click 查看如何建立两步验证.
   b. Enter the secret key in the authenticator application manually or click 查看二维码 and scan the QR code by the authenticator application on your mobile device to receive one-time security code.
   c. In the two-step verification window, specify the security code generated by the authenticator application, and then click the 检查和应用 button.

Two-step verification is enabled for all users. From now on, users of the Administration Server, including the users that were added after enabling two-step verification for all users, have to configure two-step verification for their accounts, except for users that are excluded from two-step verification.

Disabling two-step verification for a user account

You can disable two-step verification for your own account, as well as for an account of any other user.

> You can disable two-step verification of another user's account if your account has the Modify object ACLs right in the **General features: User permissions** functional area.

To disable two-step verification for a user account:

1. In the main menu, go to 用户和角色 → 用户和组, and then select the 用户 tab.
2. Click the name of the internal user account for whom you want to disable two-step verification. This may be your own account or an account of any other user.
3. In the user settings window that opens, select the 身份验证安全 tab.
4. Select the 仅请求用户名和密码 option if you want to disable two-step verification for a user account.
5. Click the **Save** button.

Two-step verification is disabled for the user account.

Disabling two-step verification for all users

You can disable two-step verification for all users if two-step verification is enabled for your account and your account has the Modify object ACLs right in the **General features: User permissions** functional area. If two-step verification is not enabled for your account, you must enable two-step verification for your account before disabling it for all users.

To disable two-step verification for all users:

1. In the main menu, click the settings icon ( ) next to the name of the required Administration Server.

   The Administration Server properties window opens.
2. On the 身份验证安全 tab of the properties window, switch the toggle button of the **two-step verification for all users** option to disabled position.
3. Enter the credentials of your account in the authentication window.

Two-step verification is disabled for all users.

Excluding accounts from two-step verification

You can exclude user accounts from two-step verification if you have the Modify object ACLs right in the **General features: User permissions** functional area.

If a user account is excluded from the list of two-step verification for all users, this user does not have to use two-step verification.

Excluding accounts from two-step verification can be necessary for service accounts that cannot pass the security code during authentication.

If you want to exclude some user accounts from two-step verification:

1. In the main menu, click the settings icon ( ) next to the name of the required Administration Server.

   The Administration Server properties window opens.

2. On the 身份验证安全 tab of the properties window, in the two-step verification exclusions table click the 添加 button.

3. In the window that opens:

   a. Select the user accounts that you want to exclude.

   b. Click the 确定 button.

The selected user accounts are excluded from two-step verification.

为您自己的账户配置两步验证

启用两步验证后首次登录 Kaspersky Security Center Linux 时，为您自己的账户配置两步验证的窗口将打开。

在为账户配置两步验证之前，请确保移动设备上安装了认证应用程序。通过使用外部时间源，确保具有身份验证器应用程序的设备上的时间和具有管理服务器的设备上的时间与 UTC 同步。

要为账户配置两步验证：

1. 使用移动设备上的身份验证器应用程序生成一次性安全代码。为此，请执行以下操作之一：

   - 在身份验证器应用程序中手动输入密钥。
   - 单击**查看二维码**并使用身份验证器应用程序扫描二维码。

   您的移动设备上将显示安全代码。

2. 在两步验证配置窗口中，指定由认证应用程序生成的安全代码，然后单击**"检查和应用"**按钮。

   您的账户已配置两步验证。您可以根据您的权限访问管理服务器。

禁止新用户为自己设置两步验证

为了进一步提高 Kaspersky Security Center Web Console 访问安全性，您可以禁止新用户为自己设置两步验证。

如果启用此选项，则被禁用两步验证的用户（例如新域管理员）无法为自己配置两步验证。因此，未经已启用两步验证的另一位 Kaspersky Security Center Linux 管理员的批准，此类用户无法在管理服务器上进行身份验证，也无法登录 Kaspersky Security Center Web Console。

如果为所有用户启用了两步验证，则此选项可用。

要禁止新用户为自己设置两步验证：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ()。
   管理服务器属性窗口将打开。
2. 在属性窗口的**身份验证安全**选项卡上，将切换按钮**禁止新用户为自己设置两步验证**切换到启用位置。

此选项不会影响添加到两步验证排除的用户账户。

要向被禁用两步验证的用户授予 Kaspersky Security Center Web Console 访问权限，请暂时关闭**禁止新用户为自己设置两步验证**选项，要求用户启用两步验证，然后重新打开该选项。

Generating a new secret key

You can generate a new secret key for a two-step verification for your account only if you are authorized by using two-step verification.

To generate a new secret key for a user account:

1. In the main menu, go to 用户和角色 → 用户和组, and then select the 用户 tab.
2. Click the name of the user account for whom you want to generate a new secret key for two-step verification.
3. In the user settings window that opens, select the 身份验证安全 tab.
4. On the 身份验证安全 tab, click the 生成新的私密密钥 link.
5. In the two-step verification window that opens, specify a new security key generated by the authenticator application.
6. Click the 检查和应用 button.

A new secret key is generated for the user.

If you lose your mobile device, you can install an authenticator application on another mobile device and generate a new secret key to restore access to Kaspersky Security Center Web Console.

Editing the name of a security code issuer

You can have several identifiers (they are called issuers) for different Administration Servers. You can change the name of a security code issuer in case, for example, if the Administration Server already uses a similar name of security code issuer for another Administration Server. By default, the name of a security code issuer is the same as the name of the Administration Server.

After you change the security code issuer name you have to reissue a new secret key and pass it to the authenticator application.

To specify a new name of security code issuer:

1. In the main menu, click the settings icon () next to the name of the required Administration Server.
   The Administration Server properties window opens.

2. In the user settings window that opens, select the 身份验证安全 tab.
3. On the 身份验证安全 tab, click the 编辑 link.
   The 编辑安全码发布者 section opens.
4. Specify a new security code issuer name.
5. Click the **OK** button.

A new security code issuer name is specified for the Administration Server.

更改允许的密码输入尝试次数

Kaspersky Security Center Linux 用户可以输入无效密码的次数有限。达到限制后，用户账户被锁定一小时。

默认下，允许的最大密码输入尝试次数是 10。您可以更改允许的密码输入尝试次数，描述在该部分。

要更改允许的密码输入尝试次数：

1. 在管理服务器设备上，运行 Linux 命令行。
2. 从 klscflag 实用程序运行以下命令：

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

   其中 N 是输入密码的尝试次数。
3. 要应用更改，请重新启动管理服务器服务。

允许的最大密码输入尝试次数被更改。

删除用户或安全组

您仅可以删除内部用户或内部安全组。

要删除用户或安全组：

1. 在主菜单中，转至**用户和角色→用户和组**，然后选择**用户**或**组**选项卡。
2. 选择您要删除的用户或安全组旁边的复选框。
3. 单击**删除**。
4. 在打开的窗口中，单击“**正常**”。

用户或安全组被删除。

创建用户角色

要创建用户角色：

1. 在主菜单中，转到“**用户和角色**” → “**角色**”。
2. 单击**添加**。
3. 在打开的“**新角色名称**”窗口中，输入新角色名称。
4. 单击“**正常**”应用更改。
5. 在打开的角色属性窗口中，更改角色设置：
   - 在“**常规**”选项卡上，编辑角色名称。
     您无法编辑预定义角色名称。
   - 在“**设置**”选项卡上，编辑角色范围和策略以及与角色关联的配置文件。
   - 在“**访问权限**”选项卡上，编辑 Kaspersky 应用程序的访问权限。
6. 单击“**保存**”保存设置。

新角色出现在用户角色列表。

编辑用户角色

要编辑用户角色：

1. 在主菜单中，转到“**用户和角色**” → “**角色**”。
2. 点击您要编辑的角色名称。
3. 在打开的角色属性窗口中，更改角色设置：
   - 在“**常规**”选项卡上，编辑角色名称。
     您无法编辑预定义角色名称。
   - 在“**设置**”选项卡上，编辑角色范围和策略以及与角色关联的配置文件。
   - 在“**访问权限**”选项卡上，编辑 Kaspersky 应用程序的访问权限。
4. 单击“**保存**”保存设置。

更新的角色出现在用户角色列表。

编辑用户角色范围

*用户角色范围*是用户和管理组的组合。与用户角色关联的设置仅应用到属于该角色用户的设备，以及仅在这些设备属于与该角色关联的组（包括子组）时。

要添加用户、安全组和管理组到用户角色范围，您可以使用以下方法之一：

方法 1：

1. 在主菜单中，转至**用户和角色→用户和组**，然后选择**用户**或**组**选项卡。
2. 选择您要添加到用户角色范围的用户或安全组旁边的复选框。
3. 单击“**分配角色**”按钮。
   角色分配向导启动。使用**下一步**按钮进行向导。
4. 在向导的“**选择角色**”页面上，选择要分配的用户角色。
5. 在向导的“**定义范围**”页面上，选择要添加到用户角色范围的管理组。
6. 单击“**分配角色**”按钮关闭窗口。

所选用户或安全组和所选管理组被添加到用户角色范围。

方法 2：

1. 在主菜单中，转到**用户和角色 → 角色**。
2. 点击您要定义范围的角色名称。
3. 在打开的角色属性窗口中，选择“**设置**”选项卡。
4. 在“**角色范围**”区域中，单击“**添加**”。
   角色分配向导启动。使用**下一步**按钮进行向导。
5. 在向导的“**定义范围**”页面上，选择要添加到用户角色范围的管理组。
6. 在向导的“**选择用户**”页面上，选择要添加到用户角色范围的用户和安全组。
7. 单击“**分配角色**”按钮关闭窗口。
8. 点击**关闭**按钮（×）以关闭角色属性窗口。

所选用户或安全组和所选管理组被添加到用户角色范围。

删除用户角色

要删除用户角色：

1. 在主菜单中，转到“**用户和角色**” → “**角色**”。

2. 选择您要删除的角色旁边的复选框。

3. 单击**删除**。

4. 在打开的窗口中，单击“**正常**”。

   用户角色被删除。

关联策略配置文件到角色

您可以关联用户角色到策略配置文件。此种情况下，该策略配置文件的激活规则基于角色：策略配置文件对具有指定角色的用户可用。

例如，策略禁止在管理组的所有设备上运行 GPS 导航软件。GPS 导航软件仅在“用户”管理组中的单个设备上是必须的——该设备属于导游。此种情况下，您可以分配“导游”角色给其所有者，然后创建一个策略配置文件，允许 GPS 导航软件仅在分配了“导游”角色的用户的设备上运行。所有其他策略设置被保留。仅带有“导游”角色的用户将被允许运行 GPS 导航软件。然后，如果其他员工被分配了“导游”角色，该新员工也在组织的设备上运行导航软件。运行 GPS 导航软件在相同管理组的其他设备上仍将被禁止。

要关联角色到策略配置文件：

1. 在主菜单中，转到“**用户和角色**” → “**角色**”。

2. 选择您要关联策略配置文件的角色名称。

   角色属性窗口打开，在其中已选择“**常规**”选项卡。

3. 选择“**设置**”选项卡并向下滚动至“**策略和配置文件**”区域。

4. 单击**编辑**。

5. 要关联角色到：

   - **现有策略配置文件**—点击所学策略名称旁边的臂章图标(>)，然后选择您要关联角色的配置文件旁边的复选框。

   - **新策略配置文件**：

     a. 选择您要创建配置文件的策略旁边的复选框。

     b. 单击**新策略配置文件**。

     c. 为新配置文件指定名称并配置配置文件设置。

     d. 单击“**保存**”按钮。

     e. 选择新配置文件旁边的复选框。

6. 单击**分配到角色**。

   配置文件被关联到角色并显示在角色属性中。配置文件自动应用到分配了该角色的用户的任意设备。

API Reference Guide

This Kaspersky Security Center OpenAPI reference guide is designed to assist in the following tasks:

- Automation and customization. You can automate tasks that you might not want to handle manually. For example, as an administrator, you can use Kaspersky Security Center OpenAPI to create and run scripts that will facilitate developing the structure of administration groups and keep that structure up-to-date.
- Custom development. Using OpenAPI, you can develop a client application.

You can use the search field in the right part of the screen to locate the information you need in the OpenAPI reference guide.

OPENAPI REFERENCE GUIDE

Samples of scripts

The OpenAPI reference guide contains samples of the Python scripts listed in the table below. The samples show how you can call OpenAPI methods and automatically accomplish various tasks for protecting your network, for instance, create a "primary/secondary" hierarchy, run tasks in Kaspersky Security Center Linux, or assign distribution points. You can run the samples as is or create your own scripts based on the samples.

To call the OpenAPI methods and run scripts:

1. Download the KlAkOAPI.tar.gz archive. This archive includes the KlAkOAPI package and samples (you can copy them from the archive or the OpenAPI reference guide). The KlAkOAPI.tar.gz archive is also located in the Kaspersky Security Center Linux installation folder.
2. Install the KlAkOAPI package from the KlAkOAPI.tar.gz archive on a device where Administration Server is installed.

   You can call the OpenAPI methods, run the samples and your own scripts only on devices where Administration Server and the KlAkOAPI package are installed.

Matching between user scenarios and samples of Kaspersky Security Center OpenAPI methods

Sample	Purpose of the sample	Scenario
Log KlAkParams	You can extract and process data by using the `KlAkParams` data structure. The sample shows how to work with this data structure. The sample output may be present in different ways. You can get the data to send an HTTP method or to use it in your code.	Monitoring and reporting
Create and delete a "primary/secondary" hierarchy	You can add a secondary Administration Server and establish a "primary/secondary" hierarchy. Alternately, you can disconnect the secondary Administration Server from the hierarchy.	Creating a hierarchy of Administration Servers, adding a secondary Administration Server, and deleting a hierarchy of Administration Servers
Download network list files via connection gateway to the specified host	You can connect to Network Agent on the needed device by using a connection gateway, and then download a file with the network list to your device.	Adjustment of distribution points and connection gateways
Install a license key	You can connect to the primary Administration	Licensing of managed

stored in the primary Administration Server repository onto the secondary Administration Servers	Server, download a required license key from it, and transmit this key to all the secondary Administration Servers included in a hierarchy.	applications
Create a report of effective user rights	You can create different reports. For instance, you can generate the report of effective user rights by using this sample. This report describes the rights that a user has, depending on his or her group and role. You can download the report in the HTML, PDF, or Excel format.	Generating and viewing a report
Start the device task	You can connect to Network Agent on the needed device by using a connection gateway, and then run the necessary task.	Starting a task manually
Register distribution points for devices in a group	You can assign managed devices as distribution points (previously known as update agents).	Updating Kaspersky databases and applications
Enumerate all groups	You can perform various actions with administration groups. The sample shows how to do the following: • Get an identifier of the "Managed devices" root group • Move through the group hierarchy • Retrieve the full, expanded hierarchy of groups, along with their names and nesting	Configuring Administration Server
Enumerate tasks, query task statistics, and run a task	You can find out the following information: • Task progress history • Current task status • Number of tasks in different statuses You can also run a task. By default, the sample runs a task after it outputs statistics.	Monitoring task execution
Create and run a task	You can create a task. Specify the following task parameters in the sample: • Type • Method of run • Name • Device group for which the task will be used	Creating a task

	By default, the sample creates a task with the "Show message" type. You can run this task for all managed devices of Administration Server. If necessary, you can specify your own task parameters.	
Enumerate license keys	You can get a list of all the active license keys for Kaspersky applications installed on managed devices of Administration Server. The list contains detailed data about every license key, such as a name, type, or expiration date.	Viewing information about license keys in use
Create and find an internal user	You can create an account for further work.	Selecting the account to start Administration Server
Create a custom category	You can create the application category with the needed parameters.	Creating an application category with content added manually
Enumerate users by using SrvView	You can use the SrvView class to request detailed information from the Administration Server. For instance, you can get a list of users by using this sample.	Managing user accounts

Applications interacting with Kaspersky Security Center Linux via OpenAPI

Some applications interact with Kaspersky Security Center Linux via OpenAPI. Such applications include, for example, Kaspersky Anti Targeted Attack Platform or Kaspersky Security for Virtualization. This can also be a custom client application developed by you based on OpenAPI.

Applications interacting with Kaspersky Security Center Linux via OpenAPI connect to Administration Server. If you have configured an allowlist of IP addresses for connecting to the Administration Server, add IP addresses of devices where applications using Kaspersky Security Center Linux OpenAPI are installed. To find out whether the application that you use works by OpenAPI, see Help of this application.

更新 Kaspersky 数据库和应用程序

该部分描述了定期更新以下内容必须采取的步骤：

- Kaspersky 数据库和软件模块
- 已安装的 Kaspersky 应用程序，包括 Kaspersky Security Center Linux 组件和安全应用程序

方案：定期更新 Kaspersky 数据库和应用程序

本节提供定期更新 Kaspersky 数据库、软件模块和应用程序的方案。在您完成配置网络保护方案后，您必须维持保护系统的可靠性以确保管理服务器和受管理设备保持受保护状态以防范各种威胁，包括病毒、网络攻击和钓鱼攻击。

网络保护通过更新以下内容保持最新：

- Kaspersky 数据库和软件模块
- 已安装的 Kaspersky 应用程序，包括 Kaspersky Security Center Linux 组件和安全应用程序

当您完成方案时，您可以确保：

- 您的网络被最新的卡巴斯基软件保护，包括 Kaspersky Security Center Linux 组件和安全应用程序。
- 对网络安全至关重要的反病毒数据库和其他 Kaspersky 数据库始终保持最新。

先决条件

受管理设备必须连接到管理服务器。如果未建立连接，请考虑手动更新 Kaspersky 数据库和软件模块，或者直接从 Kaspersky 更新服务器更新。

管理服务器必须连接到互联网。

在您开始之前，确保您已做了如下：

1. 根据通过 Kaspersky Security Center Web Console 部署 Kaspersky 应用程序的方案将 Kaspersky 安全应用程序部署到受管理设备。
2. 创建了配置了所有所需策略、策略配置文件和任务，根据网络保护配置方案。
3. 分配了适当数量的分发点，与受管理设备和网路拓扑一致。

更新 Kaspersky 数据库和应用程序分阶段进行：

1. **选择更新 scheme**

   您可以使用多种方案来安装安全应用程序的更新。选择一个或多个满足您网络需求的 scheme。

2. **创建管理服务器的“将更新下载至存储库”任务**

   该任务由 Kaspersky Security Center 快速启动向导自动创建。如果您未运行向导，立即创建任务。

此任务需要从 Kaspersky 更新服务器下载更新到管理服务器的存储库，以及为 Kaspersky Security Center Linux 更新 Kaspersky 数据库和软件模块。更新被下载后，它们可以被传播到受管理设备。

如果您的网络被分配了分发点，更新被从管理服务器存储库自动下载到分发点存储库。此种情况下，分发点所在范围的受管理设备从分发点存储库下载更新，而不是从管理服务器存储库。

使用说明：创建管理服务器的“将更新下载至存储库”任务

3. **创建“将更新下载至分发点存储库”任务（可选）**

   默认下，更新被从管理服务器下载到分发点。您可以配置 Kaspersky Security Center Linux 直接从 Kaspersky 更新服务器下载更新到分发点。您可以下载到分发点存储库，例如，如果管理服务器和分发点之间的流量比分发点和 Kaspersky 更新服务器之间的流量贵，或者如果您的管理服务器没有互联网访问。

   当您的网络已分配分发点并已创建“*将更新下载至分发点存储库*”任务时，分发点从 Kaspersky 更新服务器下载更新，而不是从管理服务器存储库下载。

   操作说明：创建将更新下载至分发点存储库的任务

4. **配置分发点**

   当您的网络已分配分发点时，确保在所有所需分发点的属性中启用“**部署更新**”选项。当该选项对分发点禁用时，包含在分发点范围中的设备从管理服务器存储库下载更新。

5. **通过使用差异文件优化更新过程（可选）**

   您可以使用差异文件优化管理服务器和受管理设备之间的流量。启用此功能后，管理服务器或分发点将下载差异文件，而不是整个 Kaspersky 数据库或软件模块文件。diff 文件描述了数据库或软件模块的文件的两个版本之间的差异。因此，diff 文件比整个文件占用更少的空间。这导致降低管理服务器之间或分发点和受管理设备之间的流量。要使用此功能，请在“*将更新下载至管理服务器存储库*”任务和/或“*将更新下载至分发点存储库*”任务的属性中启用“**下载差异文件**”选项。

   使用说明：使用差异文件更新 Kaspersky 数据库和软件模块

6. **为安全应用程序配置更新的自动安装**

   为受管理应用程序创建“*更新*”任务，以提供对软件模块和 Kaspersky 数据库（包括反病毒数据库）的及时更新。要确保定期更新，我们建议您在配置任务计划时选择“**当新更新下载至存储库时**”选项。

   如果您的网络包括仅支持 IPv6 的设备，并且您想要定期更新这些设备上安装的安全应用程序，请确保受管理设备上已安装管理服务器版本 13.2 和网络代理版本 13.2。

   如果更新需要查看和接受最终用户授权许可协议的条款，您需要先接受它们。此后，更新可以被传播到受管理设备。

结果

方案完成后，Kaspersky Security Center Linux 配置为在更新下载到管理服务器的存储库后更新卡巴斯基数据库。您然后可以继续监控网络状态。

关于更新 Kaspersky 数据库、软件模块和应用程序

为了确保管理服务器和受管理设备的保护是最新的，您必须提供以下内容的定期更新：

- Kaspersky 数据库和软件模块

  在下载卡巴斯基数据库和软件模块之前，Kaspersky Security Center Linux 会检查卡巴斯基服务器是否可访问。如果无法使用系统 DNS 访问服务器，应用程序将使用公共 DNS 服务器。这对于确保更新反病毒数据库并保持受管理设备的安全级别是必要的。

- 已安装的 Kaspersky 应用程序，包括 Kaspersky Security Center Linux 组件和安全应用程序

  Kaspersky Security Center Linux 不能自动更新 Kaspersky 应用程序。要更新应用程序，请从 Kaspersky 网站下载最新的应用程序版本，然后手动安装它们：

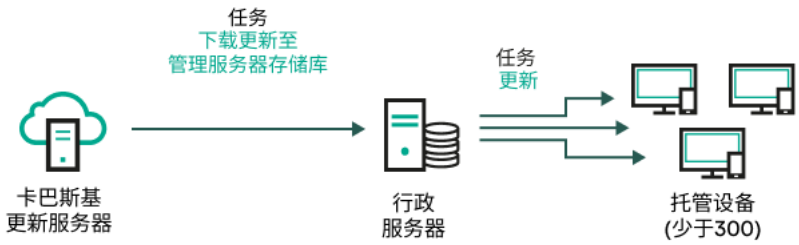
  - Kaspersky Security Center Linux 管理服务器、Kaspersky Security Center Web Console
  - 网络代理、Kaspersky Endpoint Security、管理 Web 插件

取决于您网络的配置，您可以使用以下方案来下载和分发所需更新到受管理设备：

- 通过使用单个任务：*将更新下载至管理服务器存储库*
- 通过使用两个任务：
  - "*将更新下载至管理服务器存储库*"任务
  - 创建"*将更新下载至分发点存储库*"任务
- 通过本地文件夹、共享文件夹或 FTP 服务器手动
- 直接从卡巴斯基更新服务器到受管理设备上的 Kaspersky Endpoint Security
- 如果管理服务器没有互联网连接，则通过本地或网络文件夹

使用"将更新下载至管理服务器存储库"任务

在此方案中，Kaspersky Security Center Linux 通过"*将更新下载至管理服务器存储库*"任务来下载更新。在单一网段包含少于 300 台受管理设备或每个网段包含少于 10 台受管理设备的小网络中，更新直接从管理服务器存储库被分发到受管理设备（参见下图）。



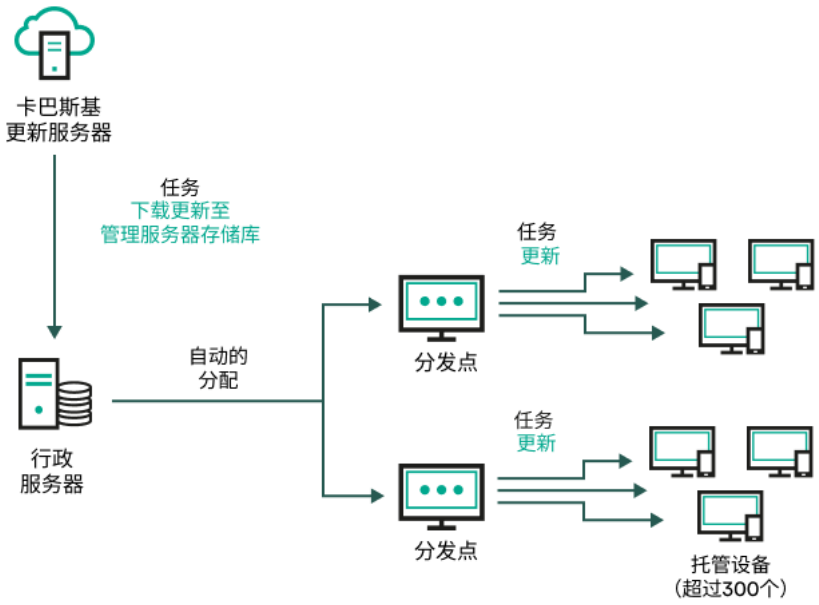
通过使用"*将更新下载至管理服务器存储库*"任务更新，而不使用分发点

更新源不仅可以是 Kaspersky 更新服务器，还可以是本地或网络文件夹。

默认下，管理服务器与 Kaspersky 更新服务器通信并使用 HTTPS 协议下载更新。您可以配置管理服务器使用 HTTP 协议，而不是 HTTPS。

如果您的网络中的单一网段包含 300 台或更多受管理设备，或者每个网段包含多于 9 台受管理设备，我们建议您使用分发点传播更新到受管理设备（参见下图）。分发点降低管理服务器负载并优化管理服务器和受管理设备之间的流量。您可以计算数字并配置您网络所需的分发点。

此种方案中，更新被从管理服务器存储库自动下载到分发点存储库。分发点所在范围的受管理设备从分发点存储库下载更新，而不是从管理服务器存储库。



通过使用"*将更新下载至管理服务器存储库*"任务更新，并使用分发点

"*将更新下载至管理服务器存储库*"任务完成后，Kaspersky Endpoint Security 的 Kaspersky 数据库和软件模块的更新即下载到管理服务器存储库。这些更新通过Kaspersky Endpoint Security *更新*任务安装。

"*将更新下载至管理服务器存储库*"任务在虚拟管理服务器上不可用。虚拟管理服务器的存储库将显示已下载至主管理服务器的更新。

您可以配置在测试设备集上进行更新的操作和错误验证。如果验证成功，更新被分发到其他受管理设备。

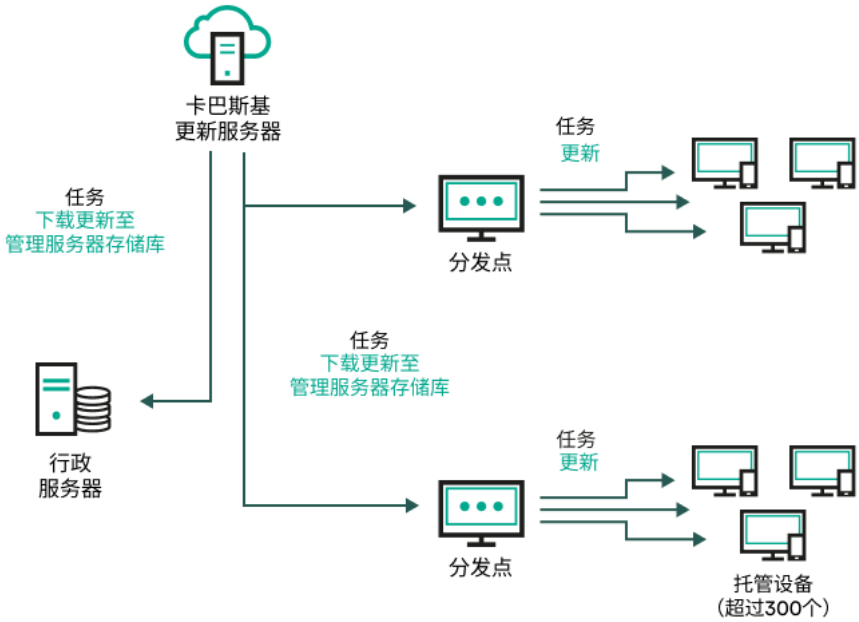
每个 Kaspersky 应用程序都从管理服务器请求所需更新。管理服务器集合这些更新并仅下载应用程序请求的更新。这确保了相同更新不被下载多次，且不必要更新不被下载。当运行"*将更新下载至管理服务器存储库*"任务时，管理服务器自动发送以下信息到 Kaspersky 更新服务器以便确保相关版本的 Kaspersky 数据库和软件模块的下载：

- 应用程序 ID 和版本
- 应用程序启动 ID
- 活动密钥 ID
- "*将更新下载至管理服务器存储库*"任务运行 ID

传输的信息都不包含个人数据或其他机密数据。AO Kaspersky Lab 依照法律需求保护信息。

使用两个任务："将更新下载至管理服务器存储库"任务和"将更新下载至分发点存储库"任务

您可以直接从 Kaspersky 更新服务器下载更新到分发点存储库，而不是从管理服务器存储库，然后分发更新到受管理设备（参见下图）。您可以下载到分发点存储库，例如，如果管理服务器和分发点之间的流量比分发点和 Kaspersky 更新服务器之间的流量贵，或者如果您的管理服务器没有互联网访问。



通过使用"*将更新下载至管理服务器存储库*"任务和"*将更新下载至分发点存储库*"任务更新

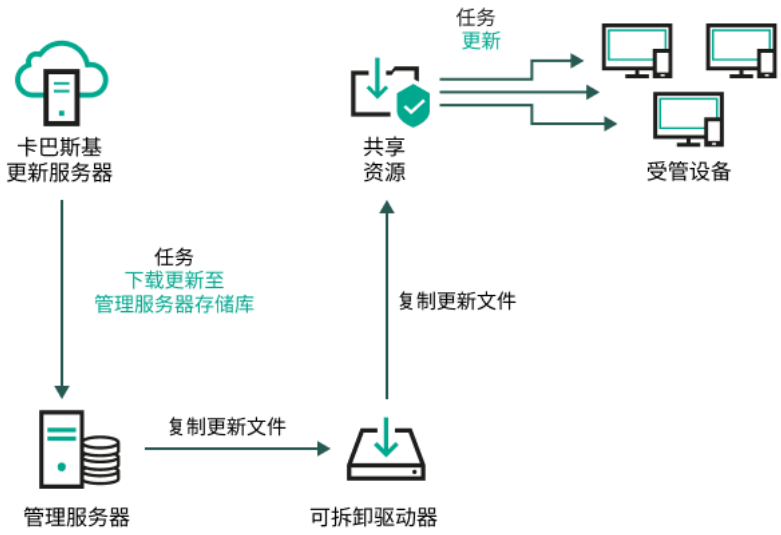
默认下，管理服务器和分发点与 Kaspersky 更新服务器通信并使用 HTTPS 协议下载更新。您可以配置管理服务器和/或分发点使用 HTTP 协议，而不是 HTTPS。

要实施此方案，除了"*将更新下载至管理服务器存储库*"任务外，请创建"*将更新下载至分发点存储库*"任务。此后，分发点将从 Kaspersky 更新服务器下载更新，而不是从管理服务器存储库。

此方案也需要"*将更新下载至管理服务器存储库*"任务，因为该任务被用于下载 Kaspersky 数据库和 Kaspersky Security Center Linux 软件模块。

通过本地文件夹、共享文件夹或 FTP 服务器手动

如果客户端设备未连接到管理服务器，您可以使用本地文件夹或共享资源作为 Kaspersky 数据库、软件模块和应用程序的更新源。在此方案中，您需要从管理服务器存储库复制所需更新到可移动驱动器，然后复制更新到在 Kaspersky Endpoint Security 设置中指定为更新源的本地文件夹或共享资源（参见下图）。



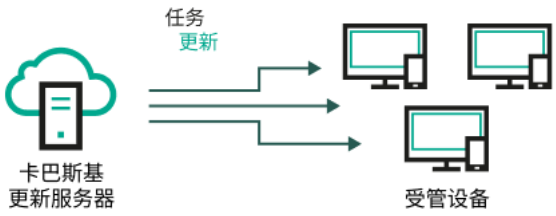
通过本地文件夹、共享文件夹或 FTP 服务器更新

有关 Kaspersky Endpoint Security 中更新源的更多信息，请参见以下帮助文档：

- Kaspersky Endpoint Security for Linux 帮助
- Kaspersky Endpoint Security for Windows 帮助

直接从卡巴斯基更新服务器到受管理设备上的 Kaspersky Endpoint Security

在受管理设备上，您可以配置 Kaspersky Endpoint Security 直接从 Kaspersky 更新服务器接收更新（参见下图）。



直接从 Kaspersky 更新服务器更新安全应用程序

在此方案中，安全应用程序不使用 Kaspersky Security Center Linux 提供的存储库。要直接从 Kaspersky 更新服务器接收更新，请在安全应用程序中指定 Kaspersky 更新服务器作为更新源。有关这些设置的详细信息，请参见以下帮助文档：

- Kaspersky Endpoint Security for Linux 帮助
- Kaspersky Endpoint Security for Windows 帮助

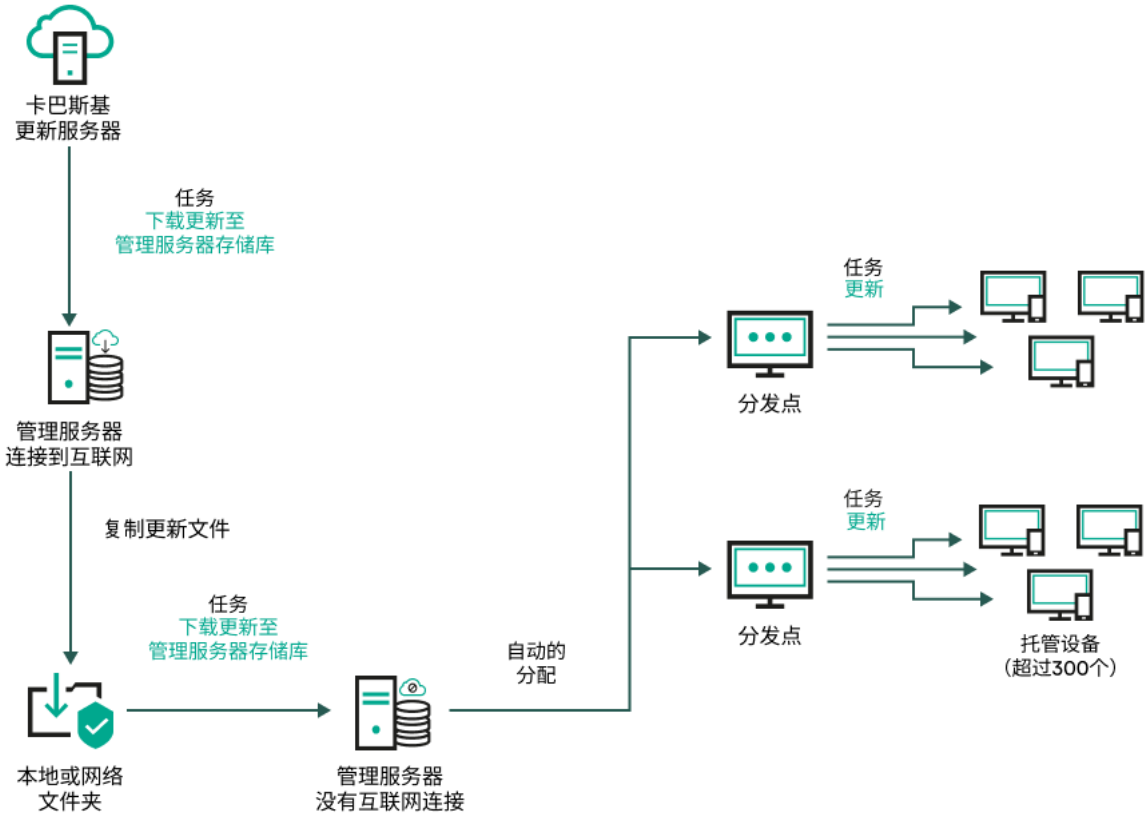
如果管理服务器没有互联网连接，则通过本地或网络文件夹

如果管理服务器没有互联网连接，您可以配置“*将更新下载至管理服务器存储库*”任务以从本地或网络文件夹下载更新。在这种情况下，必须不时地将所需的更新文件复制到指定文件夹。例如，您可以从以下来源之一复制所需的更新文件：

- 具有互联网连接的管理服务器（请参见下图）

  由于管理服务器只下载安全应用程序请求的更新，管理服务器管理的安全应用程序集（有互联网连接的应用程序和没有互联网连接的应用程序）必须匹配。

  如果用于下载更新的管理服务器版本为 13.2 或更早，请打开“*将更新下载至管理服务器存储库*”任务的属性，然后启用“**使用旧方案下载更新**”选项。



如果管理服务器没有互联网连接，则通过本地或网络文件夹更新

- 卡巴斯基更新实用程序

  由于此实用程序使用旧方案下载更新，请打开“*将更新下载至管理服务器存储库*”任务，然后启用“*使用旧方案下载更新*”选项。

创建“将更新下载至管理服务器存储库”任务

“*将更新下载至管理服务器存储库*”任务允许您将卡巴斯基安全应用程序的数据库和软件模块的更新从卡巴斯基更新服务器下载到管理服务器存储库。

Kaspersky Security Center 快速启动向导会自动创建管理服务器的“*将更新下载至管理服务器存储库*”任务。任务列表中只能有一个“*将更新下载至管理服务器存储库*”任务。如果该任务已从管理服务器的任务列表中删除，您可以再次创建该任务。

完成“*将更新下载至管理服务器存储库*”任务并下载更新后，可以将它们传播到受管理设备。

在向受管理设备分发更新之前，可以运行“*更新验证*”任务。这样可以确保管理服务器将正确安装下载的更新，并且安全级别不会由于更新而降低。要在分发更新之前对其进行验证，请配置“*将更新下载至管理服务器存储库*”任务设置中的“**运行更新验证**”选项。

要创建“将更新下载至管理服务器存储库”任务：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。
2. 单击**添加**。

"新任务向导"启动。遵照向导的说明。

3. 对于 Kaspersky Security Center 应用程序，选择"**将更新下载至管理服务器存储库**"任务类型。

4. 指定您正创建的任务的名称。任务名称不能包含多于 100 个字符并且不能包括任何特殊字符（*<>-_?:\"|）。

5. 在**完成任务创建**页面上，您可以启用**创建完成时打开任务详情**选项以打开任务属性窗口并修改默认任务设置。否则，您可以稍后随时配置任务设置。

6. 单击"**完成**"按钮。

   任务即被创建并显示在任务列表中。

7. 单击创建的任务名称以打开任务属性窗口。

8. 在任务属性窗口中的"**应用程序设置**"选项卡上，指定以下设置：

   - 更新源

     作为更新来源，您可以使用卡巴斯基更新服务器、本地或网络文件夹或者主管理服务器。

     在"*将更新下载至管理服务器存储库*"任务和"*将更新下载至分发点存储库*"任务中，如果选择受密码保护的本地或网络文件夹作为更新源，则用户身份验证不起作用。要解决此问题，首先挂载受密码保护的文件夹，然后指定所需的凭据，例如，通过操作系统。之后，您可以选择此文件夹作为更新下载任务中的更新源。Kaspersky Security Center Linux 不会要求您输入凭据。

   - 更新存储文件夹

     用于存储已保存更新的指定文件夹的路径。您可以将指定的文件夹路径复制到剪贴板。您不能更改组任务的指定文件夹的路径。

   - 强制从属管理服务器更新

     如果启用该选项，当新更新下载后管理服务器立刻在从属管理服务器上启动更新任务。否则，从属管理服务器上的更新任务根据计划启动。

     默认情况下已禁用该选项。

   - 复制下载的更新到附加文件夹

     管理服务器接收更新后，它复制它们到指定文件夹。如果您想要在您的网络上手动管理更新的分发，则使用该选项。

     例如，您可能要在以下情况下使用该选项：您组织的网络包含几个独立子网，且每个子网的设备不能访问其他子网。然而，所有子网中的设备都可以访问通用网络共享。此种情况下，您在子网之一设置管理服务器从 Kaspersky 更新服务器下载更新，启用该选项，然后指定该网络共享。对于其他管理服务器的"将更新下载至存储库"任务中，指定与更新源相同的网络共享。

     默认情况下已禁用该选项。

   - 下载差异文件

该选项启用下载 diff 文件功能。

默认情况下已禁用该选项。

- 使用旧方案下载更新

  从版本 14 开始，Kaspersky Security Center Linux 使用新方案下载数据库和软件模块的更新。要使应用程序使用新方案下载更新，更新源包含的更新文件必须具有与新方案兼容的元数据。如果更新源包含的更新文件的元数据仅与旧方案兼容，请启用“**使用旧方案下载更新**”选项。否则，更新下载任务将失败。

  例如，当指定本地或网络文件夹为更新源，并且此文件夹中的更新文件已被以下应用程序之一下载时，您必须启用此选项：

  - 卡巴斯基更新实用程序

    此实用程序使用旧方案下载更新。

  - Kaspersky Security Center 13 Linux

    例如，您的管理服务器 1 没有互联网连接。在这种情况下，您可以使用具有互联网连接的管理服务器 2 下载更新，然后将更新放置到本地或网络文件夹以将其用作管理服务器 1 的更新源。如果管理服务器 2 的版本为 13 或更低，请在管理服务器 1 的任务中启用“**使用旧方案下载更新**”选项。

  默认情况下已禁用该选项。

- 运行更新验证

  管理服务器从源下载更新并将其保存到临时存储库，然后运行“**更新验证任务**”字段中定义的任务。如果任务成功完成，则将更新从临时存储库复制到管理服务器上的共享文件夹，然后分发到所有将管理服务器作为更新源的设备（启动具有“**当新更新下载至存储库时**”计划类型的任务）。只有在执行“*更新验证*”任务之后，将更新下载至存储库的任务才完成。

  默认情况下已禁用该选项。

9. 在任务属性窗口中的“**计划**”选项卡上，创建任务启动计划。如果必要，指定以下设置：

- 计划开始：

  - 手动（默认选择）

    任务不自动运行。您仅可以手动启动。

    默认情况下已启用该选项。

  - 每 N 分钟

    任务定期运行，按照指定分钟数间隔，从任务创建日期的指定时间开始。

    默认下，任务每 30 分钟运行一次，从当前系统时间开始。

  - 每 N 小时

    任务定期运行，按照指定小时数间隔，从指定的日期和时间开始。

    默认下，任务每六小时运行一次，从当前系统日期和时间开始。

- 每 N 天

  任务定期运行，按照指定天数间隔。此外，您可以指定第一个任务运行的日期和时间。如果您为其创建任务的应用程序支持这些附加选项，则这些选项可用。

  默认下，任务每天运行一次，从当前系统日期和时间开始。

- 每 N 星期

  任务定期运行，按照指定星期数间隔，从指定的星期和时间开始。

  默认下，任务每星期一于当前系统时间运行一次。

- 每天(不支持夏令时)

  任务定期运行，按照指定天数间隔。计划不支持夏令时(DST)。这意味着在夏令时开始和结束时当时钟向前或向后拨动一小时时，实际任务启动时间不更改。

  我们不建议您使用该计划。它用于向后兼容 Kaspersky Security Center Linux。

  默认下，任务每天于当前系统时间运行一次。

- 每周

  任务每周在指定星期和指定时间运行。

- 按星期中的天数

  任务定期运行，在指定星期的指定时间。

  默认情况下，任务在每周五 6:00:00 PM 运行。

- 每月

  任务定期运行，在指定月日的指定时间。

  在缺少指定日的月份，任务在最后一天运行。

  默认下，任务在每月的第一天运行，在当前系统时间。

- 每个月在所选周的指定天

  任务定期运行，在指定月日的指定时间。

  默认情况下，不选择任何日期；默认开始时间为 6:00:00 PM。

- 在完成其他任务时

  当前任务在其他任务完成后启动。您可以选择先前任务如何结束(成功或带有错误)以触发当前任务的启动。仅当两个任务被分配给同一设备时，此参数才有效。

- 其他任务设置：

  - 运行错过的任务

该选项决定在任务要启动时客户端设备在网络中不可见时任务的行为。

如果启用该选项，系统将在下一次在客户端设备上运行 Kaspersky 应用程序时尝试启动任务。如果任务计划是“手动”、“一次”或“立即”，则设备在网络中变得可见后或包含在任务范围后，会立即启动任务。

如果该选项被禁用，则只有已计划的任务将在客户端设备上运行，而对于“手动”、“一次”和“立即”任务，仅会在网络中可见的客户端设备上运行。例如，您可能想为消耗资源的任务禁用该选项，您仅想在业余时间运行该任务。

默认情况下已启用该选项。

- 使用任务启动自动随机延迟

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动，即*分布式任务启动*。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  当任务被创建时，根据任务中包含客户端设备的数量，分发启动时间被自动计算。然后，任务总是在计算的开始时间启动。然后当任务设置被编辑或者任务被手动启动时，计算的任务启动时间值被更改。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

- 使用任务启动随机延迟间隔(分钟)

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

  默认情况下已禁用该选项。默认时间间隔为一分钟。

- 如果任务运行超过该时间则停止(分钟)

  在指定时间段过后，任务被自动停止，无论它是否完成。

  如果您想要中断或停止执行时间太长的任务，则启用该选项。

  默认情况下已禁用该选项。默认任务执行时间是 120 分钟。

10. 单击“保存”按钮。

任务被创建和配置。

当管理服务器执行“*将更新下载至管理服务器存储库*”任务时，数据库和软件模块的更新将从更新源下载并存储在管理服务器的共享文件夹中。如果您为管理组创建此任务，它将仅被应用到包含在指定管理组中的网络代理。

这些更新将从管理服务器共享文件夹分发至客户端设备和从属管理服务器。

验证已下载的更新

安装更新到受管理设备之前，您可以先通过“*更新验证*”任务检查更新。作为“*将更新下载至管理服务器存储库*”任务的一部分，“*更新验证*”任务会自动执行。管理服务器从更新源下载更新，将其保存在临时存储库并执行“*更新验证*”任务。如果任务成功完成，更新将从临时存储库复制到管理服务器共享文件夹。它们被分发到所有以该管理服务器为更新源的客户端设备。

如果“*更新验证*”任务的结果显示位于临时存储库中的更新是错误的，或“*更新验证*”任务发生错误，这些更新不会被复制到共享文件夹。管理服务器保留之前的更新集。此外，计划类型为“**当新更新下载至存储库时**”的任务也不会启动。如果新更新扫描成功完成，在下次启动“*将更新下载至管理服务器存储库*”任务时将执行这些操作。

如果在一台或多台测试设备上出现以下情况，那么更新集合就被认为是无效的：

- 发生了更新任务错误。
- 安全应用程序的实时保护状态在应用更新后更改。
- 运行按需扫描任务过程中发现了一个被感染的对象。
- Kaspersky 程序出现运行时错误。

如果在任何测试设备上未出现以上情况，该更新集就被认为是有效的，“*更新验证*”任务被认为已成功完成。

在开始创建“*更新验证*”任务之前，请执行先决条件：

1. 创建包含多台测试设备的管理组。您将需要此组来验证更新。

   建议使用网络中具有最可靠的保护和最常用的应用程序配置的设备。这种方法可提高扫描期间病毒检测的质量和可能性，并将误报的风险降至最低。如果在测试设备上检测到病毒，“*更新验证*”任务将被视为不成功。

2. 为 Kaspersky Security Center 支持的应用程序（例如 Kaspersky Endpoint Security for Linux）创建更新和病毒软件扫描任务。创建更新和恶意软件扫描任务时，请指定具有测试设备的管理组。

   “*更新验证*”任务会在测试设备上依次运行更新和恶意软件扫描任务，以检查所有更新是否有效。此外，在创建“*更新验证*”任务时，您需要指定更新和恶意软件扫描任务。

3. 创建“*将更新下载至管理服务器存储库*”任务。

要让 Kaspersky Security Center Linux 将更新分发至客户端设备前对下载的更新进行验证，请执行以下操作：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。
2. 单击“**将更新下载至管理服务器存储库**”任务。
3. 在打开的任务属性窗口中，转到“**应用程序设置**”选项卡，然后启用“**运行更新验证**”选项。
4. 如果“*更新验证*”任务存在，请单击“**选择任务**”按钮。在打开的窗口中，在具有测试设备的管理组中选择“*更新验证*”任务。
5. 如果您先前未创建“*更新验证*”任务，请执行以下操作：

   a. 单击“**新任务**”按钮。

   b. 如果要更改预设名称，则在打开的“新任务向导”中指定任务名称。

   c. 选择您先前创建的具有测试设备的管理组。

   d. 首先，选择 Kaspersky Security Center Linux 支持的所需应用程序的更新任务，然后选择恶意软件扫描任务。

   之后，会出现以下选项。我们建议将这些选项保持启用状态：

   - 在数据库更新后重启设备

在设备上更新反病毒数据库后，建议重新启动设备。

默认情况下已启用该选项。

- 在数据库更新和设备重启后检查实时保护状态

  如果启用此选项，则“*更新验证*”任务将检查下载到管理服务器存储库的更新是否有效，以及在反病毒数据库更新和设备重启后保护级别是否降低。

  默认情况下已启用该选项。

e. 指定运行“*更新验证*”任务将使用的账户。您可以使用您的账户并保持“**默认账户**”选项为启用状态。或者，您可以指定另一个用于运行该任务并具有必要访问权限的账户。为此，请选择“**指定账户**”选项，然后输入该账户的凭据。

6. 单击“**保存**”关闭“*将更新下载至管理服务器存储库*”任务的属性窗口。

自动更新验证被启用。现在，您可以运行“*将更新下载至管理服务器存储库*”任务，它将从更新验证开始。

创建“将更新下载至分发点存储库”任务

您可以为管理组创建“*将更新下载至分发点存储库*”任务。该任务将为包含在指定管理组中的分发点运行。

您可以使用该任务，例如，如果管理服务器和分发点之间的流量比分发点和 Kaspersky 更新服务器之间的流量贵，或者如果您的管理服务器没有互联网访问。

此任务需要从 Kaspersky 更新服务器下载更新到分发点的存储库。更新列表包含：

- Kaspersky 安全应用程序的数据库和软件模块的更新
- Kaspersky Security Center 组件更新
- Kaspersky 安全应用程序更新

更新被下载后，它们可以被传播到受管理设备。

*要创建“**将更新下载至分发点存储库**”任务，对于选定的管理组：*

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。
2. 单击“**添加**”按钮。

   “新任务向导”启动。遵照向导的说明。
3. 对于 Kaspersky Security Center 应用程序，在“**任务类型**”字段中选择“**将更新下载至分发点存储库**”。
4. 指定您正创建的任务的名称。任务名称不能包含多于 100 个字符并且不能包括任何特殊字符（*<>-_?:\"|）。
5. 选择一个选项按钮以指定管理组、设备分类或应用程序任务的设备。
6. 在“**完成任务创建**”步骤，如果要修改默认任务设置，请启用“**创建完成时打开任务详情**” 选项。如果您不启用该选项，任务使用默认设置创建。您可以稍后随时修改默认设置。

7. 单击“**创建**”按钮。

   任务被创建并显示在任务列表。

8. 点击创建的任务的名称以打开任务属性窗口。

9. 在任务属性窗口的“**应用程序设置**”选项卡上，指定以下设置：

- 更新源

  以下资源可以用作分发点的更新源：

  - Kaspersky 更新服务器

    Kaspersky 程序可以从 Kaspersky 的 HTTP(S) 服务器下载数据库和应用程序模块更新。

    默认情况下已选中该选项。

  - 主管理服务器

    此资源适用于为从属或虚拟管理服务器创建的任务。

  - 本地或网络文件夹

    包含最新更新的本地或网络文件夹。只有已安装的 SMB 共享才能用作网络文件夹。在选择本地文件夹时，您必须在安装了管理服务器的设备上指定一个文件夹。

    > 在“*将更新下载至管理服务器存储库*”任务和“*将更新下载至分发点存储库*”任务中，如果选择受密码保护的本地或网络文件夹作为更新源，则用户身份验证不起作用。要解决此问题，首先挂载受密码保护的文件夹，然后指定所需的凭据，例如，通过操作系统。之后，您可以选择此文件夹作为更新下载任务中的更新源。Kaspersky Security Center Linux 不会要求您输入凭据。

- 更新存储文件夹

  用于存储已保存更新的指定文件夹的路径。您可以将指定的文件夹路径复制到剪贴板。您不能更改组任务的指定文件夹的路径。

- 下载差异文件

  该选项启用下载 diff 文件功能。

  默认情况下已禁用该选项。

- 使用旧方案下载更新

从版本 14 开始，Kaspersky Security Center Linux 使用新方案下载数据库和软件模块的更新。要使应用程序使用新方案下载更新，更新源包含的更新文件必须具有与新方案兼容的元数据。如果更新源包含的更新文件的元数据仅与旧方案兼容，请启用“**使用旧方案下载更新**”选项。否则，更新下载任务将失败。

例如，当指定本地或网络文件夹为更新源，并且此文件夹中的更新文件已被以下应用程序之一下载时，您必须启用此选项：

- 卡巴斯基更新实用程序

  此实用程序使用旧方案下载更新。

- Kaspersky Security Center 13 Linux

  例如，分发点配置为从本地或网络文件夹获取更新。在这种情况下，您可以使用具有互联网连接的管理服务器下载更新，然后将更新放置到分发点的本地或网络文件夹。如果管理服务器的版本为 13 或更低，请在“*将更新下载至分发点存储库*”任务中启用“**使用旧方案下载更新**”选项。

默认情况下已禁用该选项。

10. 为任务启动创建计划。如果必要，指定以下设置：

- 计划开始：
  - 手动（默认选择）

    任务不自动运行。您仅可以手动启动。

    默认情况下已启用该选项。

  - 每 N 分钟

    任务定期运行，按照指定分钟数间隔，从任务创建日期的指定时间开始。

    默认下，任务每 30 分钟运行一次，从当前系统时间开始。

  - 每 N 小时

    任务定期运行，按照指定小时数间隔，从指定的日期和时间开始。

    默认下，任务每六小时运行一次，从当前系统日期和时间开始。

  - 每 N 天

    任务定期运行，按照指定天数间隔。此外，您可以指定第一个任务运行的日期和时间。如果您为其创建任务的应用程序支持这些附加选项，则这些选项可用。

    默认下，任务每天运行一次，从当前系统日期和时间开始。

  - 每 N 星期

    任务定期运行，按照指定星期数间隔，从指定的星期和时间开始。

    默认下，任务每星期一于当前系统时间运行一次。

  - 每天(不支持夏令时)

任务定期运行，按照指定天数间隔。计划不支持夏令时(DST)。这意味着在夏令时开始和结束时当时钟向前或向后拨动一小时时，实际任务启动时间不更改。

我们不建议您使用该计划。它用于向后兼容 Kaspersky Security Center Linux。

默认下，任务每天于当前系统时间运行一次。

- 每周

  任务每周在指定星期和指定时间运行。

- 按星期中的天数

  任务定期运行，在指定星期的指定时间。

  默认情况下，任务在每周五 6:00:00 PM 运行。

- 每月

  任务定期运行，在指定月日的指定时间。

  在缺少指定日的月份，任务在最后一天运行。

  默认下，任务在每月的第一天运行，在当前系统时间。

- 每个月在所选周的指定天

  任务定期运行，在指定月日的指定时间。

  默认情况下，不选择任何日期；默认开始时间为 6:00:00 PM。

- 在检测到病毒爆发时

  任务在“*病毒爆发*”事件发生后运行。选择将监控病毒爆发的应用程序类型。有下列应用程序类型可用：

  - 用于工作站和文件服务器的反病毒
  - 用于周边防护的反病毒
  - 用于邮件系统的反病毒

  默认情况下选定所有应用程序类型。

  您可能想根据报告病毒爆发的反病毒应用程序类型运行不同的任务。此种情况下，删除您不需要的应用程序类型分类。

- 在完成其他任务时

  当前任务在其他任务完成后启动。您可以选择先前任务如何结束(成功或带有错误)以触发当前任务的启动。仅当两个任务被分配给同一设备时，此参数才有效。

- 运行错过的任务

该选项决定在任务要启动时客户端设备在网络中不可见时任务的行为。

如果启用该选项，系统将在下一次在客户端设备上运行 Kaspersky 应用程序时尝试启动任务。如果任务计划是“手动”、“一次”或“立即”，则设备在网络中变得可见后或包含在任务范围后，会立即启动任务。

如果该选项被禁用，则只有已计划的任务将在客户端设备上运行，而对于“手动”、“一次”和“立即”任务，仅会在网络中可见的客户端设备上运行。例如，您可能想为消耗资源的任务禁用该选项，您仅想在业余时间运行该任务。

默认情况下已启用该选项。

- 使用任务启动自动随机延迟

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动，即*分布式任务启动*。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  当任务被创建时，根据任务中包含客户端设备的数量，分发启动时间被自动计算。然后，任务总是在计算的开始时间启动。然后当任务设置被编辑或者任务被手动启动时，计算的任务启动时间值被更改。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

- 使用任务启动随机延迟间隔(分钟)

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

  默认情况下已禁用该选项。默认时间间隔为一分钟。

11. 单击“保存”按钮。

    任务被创建和配置。

除了您在任务创建过程中指定的设置，您还可以更改所创建任务的其他属性。

执行“*将更新下载至分发点存储库*”任务时，数据库和软件模块的更新从更新源下载并存储在共享文件夹。下载的更新将仅被包含在指定管理组的分发点和没有更新下载任务的更新代理使用。

添加“将更新下载至管理服务器存储库”任务的更新源

在创建或使用“将更新下载至管理服务器存储库”任务时，可以选择以下更新源：

- Kaspersky 更新服务器
- 主管理服务器

  此资源适用于为从属或虚拟管理服务器创建的任务。
- 本地或网络文件夹

在“*将更新下载至管理服务器存储库*”任务和“*将更新下载至分发点存储库*”任务中，如果选择受密码保护的本地或网络文件夹作为更新源，则用户身份验证不起作用。要解决此问题，首先挂载受密码保护的文件夹，然后指定所需的凭据，例如，通过操作系统。之后，您可以选择此文件夹作为更新下载任务中的更新源。Kaspersky Security Center Linux 不会要求您输入凭据。

默认使用 Kaspersky 更新服务器，但您也可以从本地或网络文件夹下载更新。如果您的网络没有互联网访问权限，您可能希望使用文件夹。在这种情况下，您可以从 Kaspersky 更新服务器手动下载更新并将下载的文件放在所需的文件夹中。

您只能指定一个本地或网络文件夹路径。作为本地文件夹，您必须在安装了管理服务器的设备上指定一个文件夹。作为网络文件夹，您可以使用 FTP 或 HTTP 服务器，或者 SMB 共享。如果 SMB 共享需要身份验证，则必须提前使用所需的凭据将其安装在系统中。我们建议不要使用 SMB1 协议，因为它不安全。

如果同时添加 Kaspersky 更新服务器和本地或网络文件夹，将首先从文件夹下载更新。如果下载时出错，将使用 Kaspersky 更新服务器。

如果包含更新的共享文件夹受密码保护，请启用“**指定账户以访问更新源的共享文件夹(如果有)**”选项并输入访问所需的账户凭据。

要添加更新源：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。
2. 单击**将更新下载至管理服务器存储库**。
3. 转到“**应用程序设置**”选项卡。
4. 在“**更新源**”行，单击“**配置**”按钮。
5. 在打开的窗口中，单击“**添加**”按钮。
6. 在更新源列表中，添加所需的源。如果选中“**本地或网络文件夹**”复选框，则指定文件夹的路径。
7. 单击“**确定**”，然后关闭更新源属性窗口。
8. 在更新源窗口中，单击“**确定**”。
9. 单击任务窗口中的“**保存**”按钮。

现在更新将从指定的源下载到管理服务器存储库。

关于使用 diff 文件更新 Kaspersky 数据库和软件模块

当 Kaspersky Security Center Linux 从卡巴斯基更新服务器下载更新时，它通过使用差异文件来优化流量。您也可以对从网络中其他设备（管理服务器、分发点和客户端设备）获取更新的设备启用对 diff 文件的使用。

关于下载 diff 文件功能

diff 文件描述了数据库或软件模块的文件的两个版本之间的差异。使用 diff 文件节省您公司网络内的流量，因为 diff 文件相比数据库和软件模块的完整文件占据更少的空间。如果对管理服务器或分发点启用 *下载 diff 文件*功能，diff 文件被保存到该管理服务器或分发点。结果，从该管理服务器或分发点获取更新的设备可以使用保存的 diff 文件更新它们的数据库和软件模块。

要优化对 diff 文件的使用，我们建议您根据管理服务器或分发点的更新计划同步从管理服务器或更新代理获取更新的的设备的更新计划。然而，即便设备更新频率小于从其获取更新的管理服务器或分发点，流量也被节省。

分发点不对 diff 文件的自动分发使用 IP 多点传送。

Enabling the Downloading diff files feature: scenario

Stages

1. **Enabling the feature on Administration Server**

   Enable the feature in the settings of a *Download updates to the repository of the Administration Server* task.

2. **Enabling the feature for a distribution point**

   Enable the feature for a distribution point that receives updates by means of a *Download updates to the repositories of distribution points* task.

   Then enable the feature in the Network Agent policy settings for a distribution point that receives updates from Administration Server.

   Then enable the feature for a distribution point that receives updates from Administration Server.

   The feature is enabled in the Network Agent policy settings and—if the distribution points are assigned manually and if you want to override policy settings—in the 分发点 section of the Administration Server properties.

To check that the Downloading diff files feature is successfully enabled, you can measure the internal traffic before and after you perform the scenario.

通过分发点下载更新

Kaspersky Security Center Linux 允许分发点从管理服务器、Kaspersky 服务器或本地网络文件夹接收更新。

要为分发点配置更新下载：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ()。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**分发点**”区域。
3. 单击将用于将更新传送到组中的客户端设备的分发点的名称。
4. 在分发点属性窗口中选择“**更新源**”区域。
5. 为分发点选择更新源：

- 更新源

  选择分发点的更新源：

  - 要允许分发点从管理服务器接收更新，请选择“**从管理服务器检索**”。
  - 要允许分发点使用任务接收更新，请选择“**使用更新下载任务**”，然后指定“*将更新下载至分发点存储库*”任务：
    - 如果设备上已存在此类任务，请在列表中选择该任务。
    - 如果设备上尚不存在此类任务，请单击“**创建任务**”链接创建任务。“新任务向导”启动。遵照向导的说明操作。

- 下载差异文件

  该选项启用下载 diff 文件功能。

  默认情况下已启用该选项。

分发点将从指定的更新源接收更新。

更新离线设备上的 Kaspersky 数据库和软件模块

更新受管理设备上的 Kaspersky 数据库和软件模块对于保持设备对病毒和其他威胁的防护是非常重要的任务。管理员通常通过使用管理服务器存储库来配置定期更新。

当您需要在未连接到管理服务器（主或从）、分发点或互联网的设备（或设备组）上更新数据库和软件模块时，您必须使用其他更新源，例如 FTP 服务器或本地文件夹。此种情况下，您必须使用大容量设备传送所需更新的文件，例如闪存驱动器或外部硬盘驱动器。

您可以从这里复制所需更新：

- 管理服务器。

  为确保管理服务器存储库包含所需的安装在离线设备上的安全应用程序的更新，至少一台受管理的在线设备必须安装了相同的安全应用程序。该应用程序必须配置为通过“*将更新下载至管理服务器存储库*”任务从管理服务器存储库接收更新。

- 任何安装了相同安全应用程序，并配置为从管理服务器存储库、分发点存储库或直接从 Kaspersky 更新服务器接收更新的设备。

以下是通过从管理服务器存储库复制而更新数据库和软件模块的例子。

要更新离线设备上的 Kaspersky 数据库和软件模块：

1. 连接可移动驱动器到管理服务器所在设备。
2. 复制更新文件到可移动驱动器。

   默认下，更新位于：\\<server name>\KLSHARE\Updates。

或者，您可以配置 Kaspersky Security Center Linux 定期复制更新到您选择的文件夹。为此，请使用“*将更新下载至管理服务器存储库*”任务的属性中的“**复制下载的更新到附加文件夹**”选项。如果您指定闪存驱动器或外部硬盘驱动器上的文件夹作为该选项的目标文件夹，该大容量存储设备将总是包含更新的最新版本。

3. 在离线设备上，配置 Kaspersky Endpoint Security 以从本地文件夹或共享文件夹接收更新，例如 FTP 服务器或共享文件夹。

   说明：

   - Kaspersky Endpoint Security for Linux 帮助
   - Kaspersky Endpoint Security for Windows 帮助

4. 从可移动驱动器复制更新到您想用作更新源的本地文件夹或共享资源。

5. 在需要安装更新的离线设备上，启动 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Windows 的*更新*任务，具体取决于离线设备的操作系统。

更新任务完成后，设备上的 Kaspersky 数据库和软件模块为最新。

备份和恢复 Web 插件

Kaspersky Security Center 13.2 Web 控制台允许您备份 Web 插件的当前状态，以便以后能够恢复保存的状态。例如，您可以在将 Web 插件更新到较新版本之前对其进行备份。更新后，如果较新的版本不符合您的要求或期望，您可以从备份中恢复以前版本的 Web 插件。

要备份 Web 插件：

1. 在主菜单中，转到**设置 → Web 插件**。
2. 在“**Web 插件**”区域中，选择要备份的 Web 插件，然后单击“**创建备份副本**”按钮。

选定的 Web 插件得到备份。您可以在“**备份**”区域中查看创建的备份。

要从备份中恢复 Web 插件：

1. 在主菜单中，转到“**设置 → 备份**”。
2. 在“**备份**”区域中，选择要恢复的 Web 插件的备份，然后单击“**从备份恢复**”按钮。

Web 插件将从选定的备份中恢复。

监控、报告和审计

本节介绍 Kaspersky Security Center Linux 的监控和报告功能。这些功能给您一个基础架构、保护状态和统计信息的总览。

在 Kaspersky Security Center Linux 部署之后或操作过程中，您可以配置监控和报告功能以适应您的需要。

方案：监控和报告

本节提供在 Kaspersky Security Center Linux 中配置监控和报告功能的方案。

先决条件

在您部署 Kaspersky Security Center Linux 到组织网络中后，您可以开始监控它并生成其功能报告。

组织网络中的监控和报告分步骤进行：

1. **配置设备状态切换**

   熟悉取决于特定条件的设备状态设置。通过更改这些设置，您可以更改带有*严重*或*警告*重要级别的设备数量。当配置设备状态切换时，确保以下：

   - 新设置不与您组织的安全策略信息冲突。
   - 您可以及时对您组织网络中的重要安全事件做出反应。

2. **配置客户端设备上的事件通知**

   说明：

   配置客户端设备上的事件通知（通过邮件、SMS 或运行可执行文件）。

3. **对严重、警告、信息通知执行推荐的操作**

   说明：

   对您的组织网络执行推荐的操作

4. **查看您组织网络的安全状态**

   说明：

   - 查看“保护状态”小组件
   - 生成并查看保护状态报告
   - 生成并查看错误报告

5. **定位不被保护的客户端设备**

   说明：

   - 查看新设备小组件
   - 生成并查看保护部署报告

6. **检查客户端设备保护**

说明：

- 根据保护状态和威胁统计类别生成并查看报告
- 启动并查看“严重”事件分类

7. **评估和限制数据库上的事件负载**

   受管理应用程序操作相关的事件信息将被从客户端设备上传输并记录至管理服务器数据库。要降低管理服务器负载，请评估并限制可以存储在数据库中的最大事件数量。

   说明：

   - 限制最大事件数量

8. **查看授权许可信息**

   说明：

   - 将“授权许可密钥使用”小组件添加到控制板并查看
   - 生成并查看授权许可密钥使用报告

结果

完成方案后，您被通知您组织网络的保护，因此可以为进一步保护计划操作。

关于监控和报告的类型

组织网络的安全事件信息存储在管理服务器数据库。基于事件，Kaspersky Security Center Web Console 提供对于您组织网络的以下类型的监控和报告：

- 控制板
- 报告
- 事件分类
- 通知

控制板

控制板通过对信息进行图形显示来允许您监控您组织网络的安全趋势。

报告

报告功能允许您获取您组织网络的详细安全数字信息、保存该信息到文件、通过邮件发送它和打印它。

事件分类

事件分类提供了从管理服务器数据库中选择的指定事件集合的屏幕视图。这些事件集根据以下类别进行分组：

- 按重要级别—**严重事件**、**功能失败**、**警告**和**信息事件**
- 按时间—**最近事件**
- 按类型—**用户请求**和**审计事件**

您可以基于 Kaspersky Security Center Web Console 界面上可以配置的设置创建和查看用户定义的事件分类。

通知

通知提醒您事件并帮助您通过执行推荐操作或您认为适当的操作来加速您对这些事件的响应。

仪表板和小部件

本节包含有关仪表板和仪表板提供的小部件的信息。本节包括有关如何管理小部件和配置小部件设置的说明。

使用控制板

控制板通过对信息进行图形显示来允许您监控您组织网络的安全趋势。

在 Kaspersky Security Center Web Console 的"**监控和报告**"区域中单击"**控制板**"可打开控制板。

控制板提供可以自定义的部件。您可以选择大量不同的部件，显示为饼图、表格、图表和列表。部件中显示的信息会自动更新，更新周期为一到两分钟。更新间隔根据不同部件而不同。您可以在任意时刻通过设置菜单在部件上手动刷新数据。

默认下，部件包含存储在管理服务器数据库中的所有事件的信息。

Kaspersky Security Center Web Console 具有以下类别的默认部件集：

- **保护状态**
- **部署**
- **更新**
- **威胁统计**
- **其他**

一些部件具有带链接的文本信息。您可以通过点击链接查看详细信息。

当配置控制板时，您可以添加您需要的部件或隐藏您不需要的部件，更改部件的大小或外观，移动部件以及更改它们的设置。

添加工具到控制板

要添加工具到控制板：

1. 在主菜单中，转到“**监控和报告 → 控制板**”。
2. 单击“**添加或还原 Web 小部件**”按钮。
3. 在可用工具列表，选择您要添加到控制板的工具。
   工具按类别分组。要查看包含在类别中的工具列表，点击类别名称旁边的臂章图标(>)。
4. 单击“**添加**”按钮。

所选的工具被添加到控制板结尾。

您现在可以编辑所添加工具的展示和参数。

从控制板隐藏工具

要从控制板隐藏工具：

1. 在主菜单中，转到“**监控和报告**” → “**控制板**”。
2. 点击您要隐藏的工具旁边的设置图标（⚙）。
3. 选择**隐藏 Web 小部件**。
4. 在打开的“**警告**”窗口中，单击“**确定**”。

所选工具被隐藏。稍后，您可以再次添加该工具到控制板。

移动工具到控制板

要移动工具到控制板：

1. 在主菜单中，转到“**监控和报告**” → “**控制板**”。
2. 点击您要移动的工具旁边的设置图标（⚙）。
3. 选择**移动**。
4. 点击您要移动工具的地方。您仅可以选择其他工具。

所选工具的地方被清扫。

更改部件尺寸或样子

对于显示图表的工具，您可以更改其展示–线条图或线形图。对于一些工具，您可以更改其大小：最小、中度或最大。

要更改工具展示：

1. 在主菜单中，转到“**监控和报告**” → “**控制板**”。
2. 点击您要编辑的小组件旁边的设置图标（⚙）。
3. 执行以下操作之一：
   - 要显示条形图形式的小组件，请选择“**图表类型：线条**”。
   - 要显示折线图形式的小组件，请选择“**图表类型：线形**”。
   - 要更改小组件占用的区域，请选择以下值之一：
     - **最小**
     - **最小 (仅线条)**
     - **中度 (饼图)**
     - **中度 (线条图)**
     - **最大**

所选工具的展示被更改。

更改部件设置

要更改工具设置：

1. 在主菜单中，转到“**监控和报告 → 控制板**”。
2. 点击您要更改的小组件旁边的“设置”图标 (⚙)。
3. 选择**显示设置**。
4. 在打开的工具设置窗口，更改所需的工具设置。
5. 单击“**保存**”保存设置。

所选工具的设置被更改。

设置集合取决于特定工具。以下是一些通用设置：

- **Web 小部件范围**（小组件显示其信息的对象集）—例如，管理组或设备分类。
- **选择任务**（小组件显示其信息的任务）。
- **时间间隔**（在小组件中显示信息的时间间隔）—两个指定日期之间；从指定日期到当前日期；或从当前日期减去指定天数。

- **设置状态为“严重”，如果这些被指定**和**设置状态为“警告”，如果这些被指定**（确定交通信号灯颜色的规则）。

更改小部件设置后，您可以手动刷新小部件上的数据。

要刷新小部件上的数据：

1. 在主菜单中，转到“**监控和报告**” → “**控制板**”。
2. 点击您要移动的工具旁边的设置图标（⚙）。
3. 选择**刷新**。

小部件上的数据得到刷新。

关于仅仪表板模式

您可以为不管理网络但希望在 Kaspersky Security Center Linux 中查看网络保护统计信息的员工（例如高层管理人员）配置“仅仪表板模式”。当用户启用此模式后，只会向用户显示带有一组预定义小部件的仪表板。因此，用户可以监视小部件中指定的统计信息，例如，所有受管理设备的保护状态、最近检测到的威胁数量或网络中最常见的威胁列表。

当用户在仅仪表板模式下工作时，将应用以下限制：

- 主菜单不向用户显示，因此用户无法更改网络保护设置。
- 用户不能对小部件执行任何操作，例如，添加或隐藏小部件。因此，您需要将用户需要的所有小部件都放在仪表板上并进行配置，例如，设置对象计数规则或指定时间间隔。

您不能为自己分配仅仪表板模式。如果要在此模式下工作，请联系系统管理员、受管理服务提供商 (MSP) 或在“**常规功能：用户权限**”功能区域中拥有“修改对象 ACL”权限的用户。

配置仅仪表板模式

在开始配置仅仪表板模式之前，确保满足以下先决条件：

- 您在“**常规功能：用户权限**”功能区域中拥有“修改对象 ACL”权限。如果您没有此权限，则用于配置模式的选项卡将缺失。
- 您在“**常规功能：基本功能**”功能区域中拥有“读取”权限。

如果您的网络中安排了管理服务器层级，若要配置仅仪表板模式，请转到在**用户和角色 → 用户和组** 区域中**用户**选项卡上提供了用户账户的服务器。可以是主服务器或物理从属服务器。无法在虚拟服务器上调整模式。

要配置仅仪表板模式：

1. 在主菜单中，转至**用户和角色 → 用户和组**，然后选择**用户**选项卡。

2. 单击要使用小部件调整仪表板的用户账户名。

3. 在打开的账户设置窗口中，选择“**仪表板**”选项卡。

   在打开的选项卡上，您和用户将看到相同的仪表板。

4. 如果启用了“**在仅仪表板模式下显示控制台**”选项，则对切换按钮进行切换以将其禁用。

   启用此选项后，您也无法更改仪表板。禁用该选项后，您可以管理小部件。

5. 配置仪表板外观。“**仪表板**”选项卡上准备的小部件级供具有可自定义账户的用户使用。用户不能更改小部件的任何设置或大小，也不能从仪表板添加或删除任何小部件。因此，请为用户调整好，以便用户可以查看网络保护统计信息。为此，在“**仪表板**”选项卡上，可以对小部件执行与在“**监控和报告**”→“**控制板**”区域中相同的操作：

   - 向仪表板添加新的小部件。
   - 隐藏用户不需要的小部件。
   - 移动小部件到特定文件夹。
   - 更改小部件的大小或外观。
   - 更改小部件设置。

6. 对切换按钮进行切换以启用“**在仅仪表板模式下显示控制台**”选项。

   之后，只有仪表板可供用户使用。用户可以监视统计信息，但不能更改网络保护设置和仪表板外观。由于为您显示的仪表板与为用户显示的仪表板相同，您也无法更改仪表板。

   如果禁用该选项，则会为用户显示主菜单，因此用户可以在 Kaspersky Security Center Linux 中执行各种操作，包括更改安全设置和小部件。

7. 完成配置仅仪表板模式后，单击“**保存**”按钮。只有这样，准备好的仪表板才会显示给用户。

8. 如果用户想要查看支持的卡巴斯基应用程序的统计信息并需要访问权限来执行此操作，请为用户配置权限。之后，卡巴斯基应用程序数据将在这些应用程序的小部件中显示给用户。

现在用户可以在自定义账户下登录 Kaspersky Security Center Linux 并在仅仪表板模式下监视网络保护统计信息。

报告

本节介绍如何使用报告、管理自定义报告模板、使用报告模板生成新报告以及创建报告交付任务。

使用报告

报告功能允许您获取您组织网络的详细安全数字信息、保存该信息到文件、通过邮件发送它和打印它。

在 Kaspersky Security Center Web Console 的“**监控和报告**”区域中单击“**报告**”可打开报告。

默认下，报告包含 30 天内的信息。

Kaspersky Security Center Linux 具有一组默认的以下类别的报告：

- 保护状态
- 部署
- 更新
- 威胁统计
- 其他

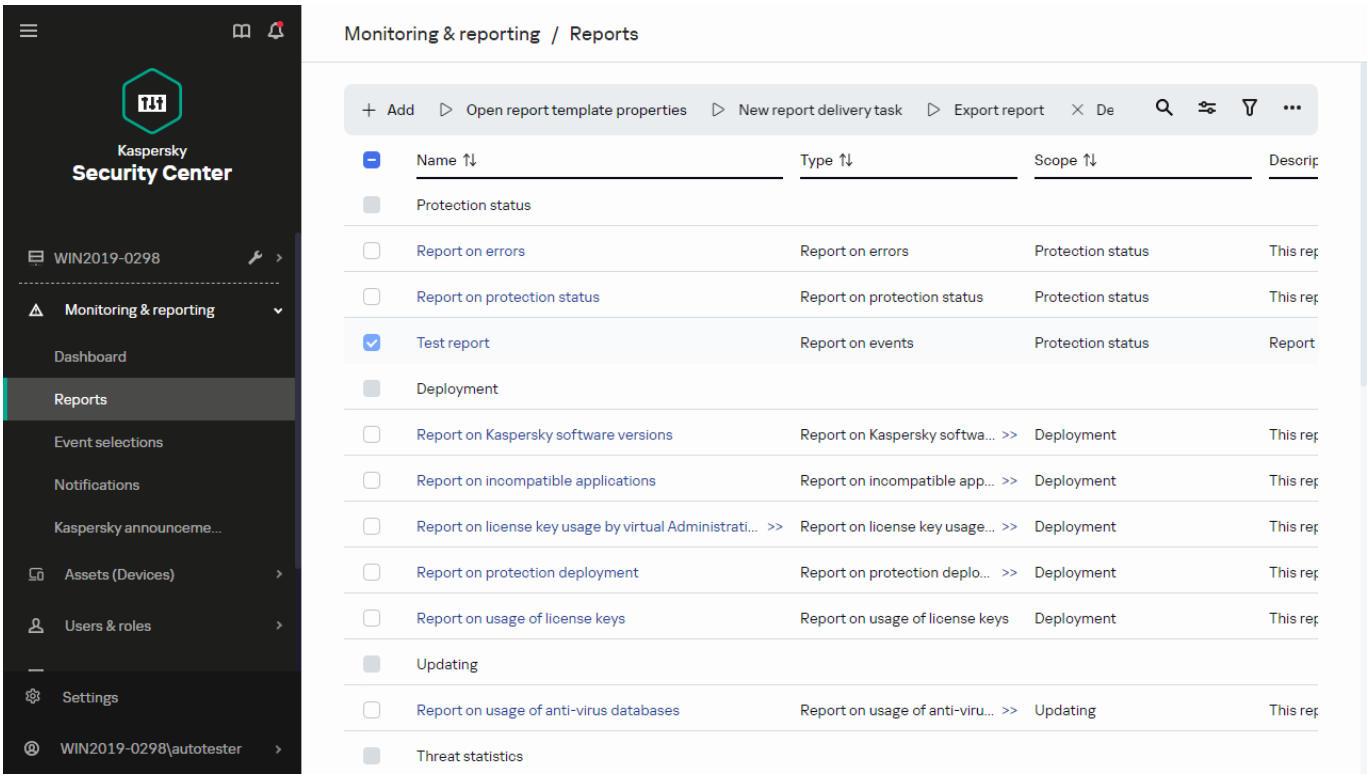
您可以创建自定义报告模板、编辑报告模板和删除它们。

您可以基于现有模板创建报告、导出报告到文件和创建报告传送任务。

创建报告模板

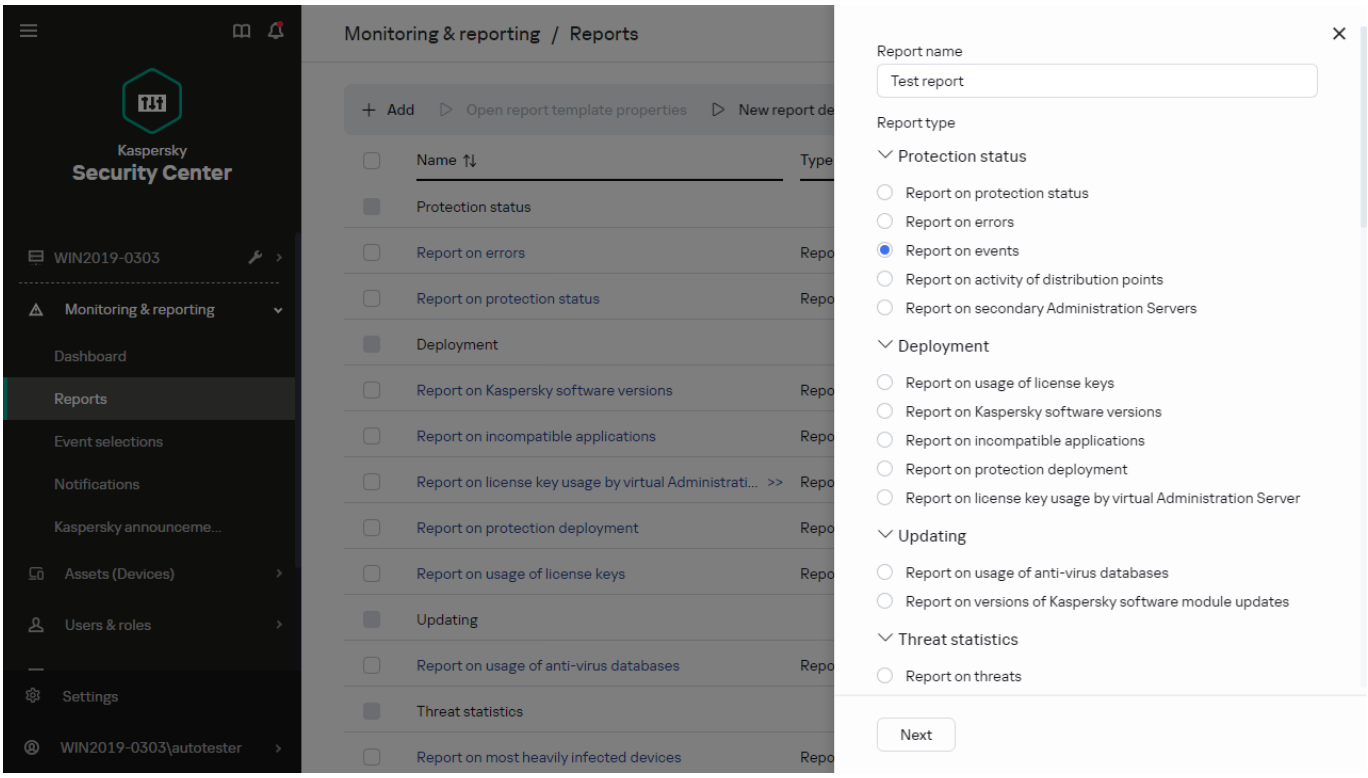
要创建报告模板：

1. 在主菜单中，转到“监控和报告” → “报告”。



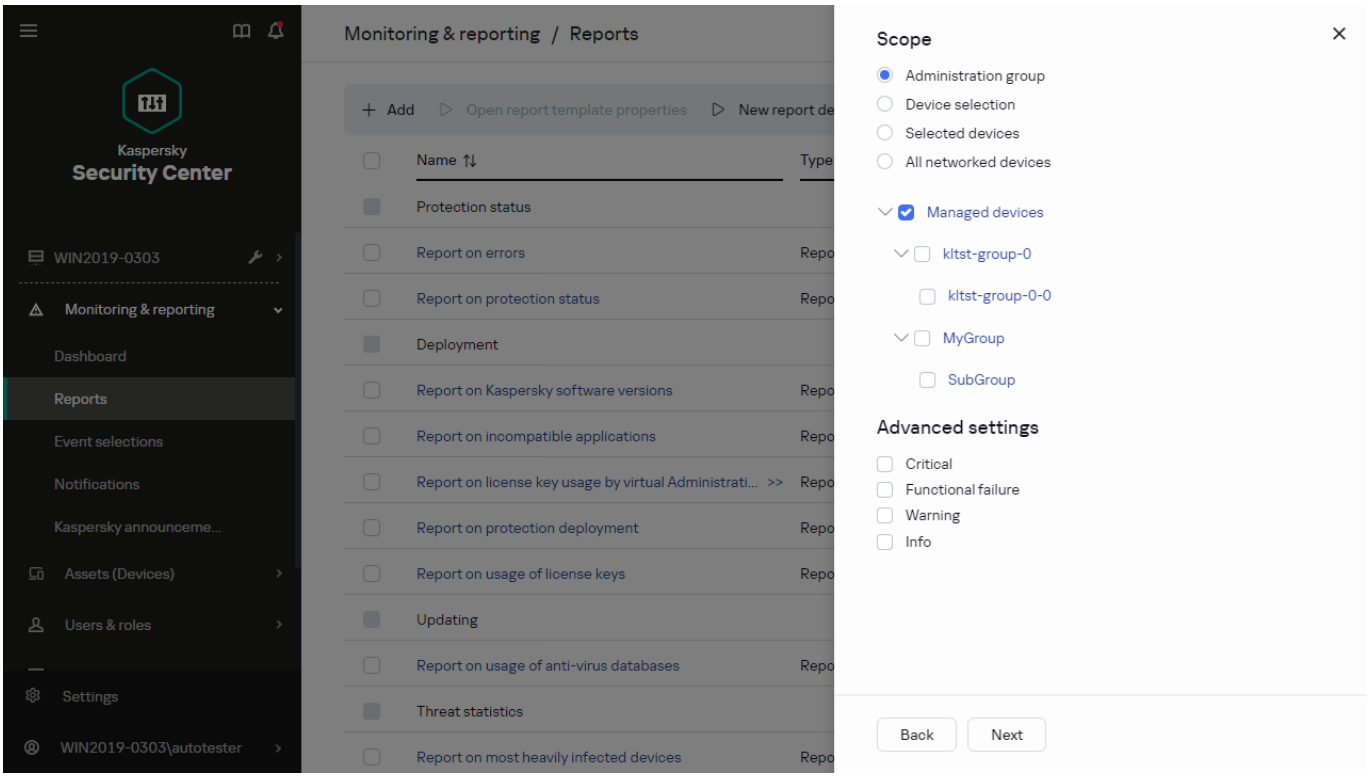
报告子区域中的报告模板列表

2. 单击添加。
   程序将启动“新报告模板向导”。使用下一步按钮进行向导。
3. 在向导的第一页，输入报告名称并选择报告类型。



新报告模板向导。指定报告模板的名称和类型

4. 在向导的"**范围**"页面上，选择要基于该报告模板显示其数据到报告的客户端设备集合（管理组、设备分类、所选设备或所有网络设备）。

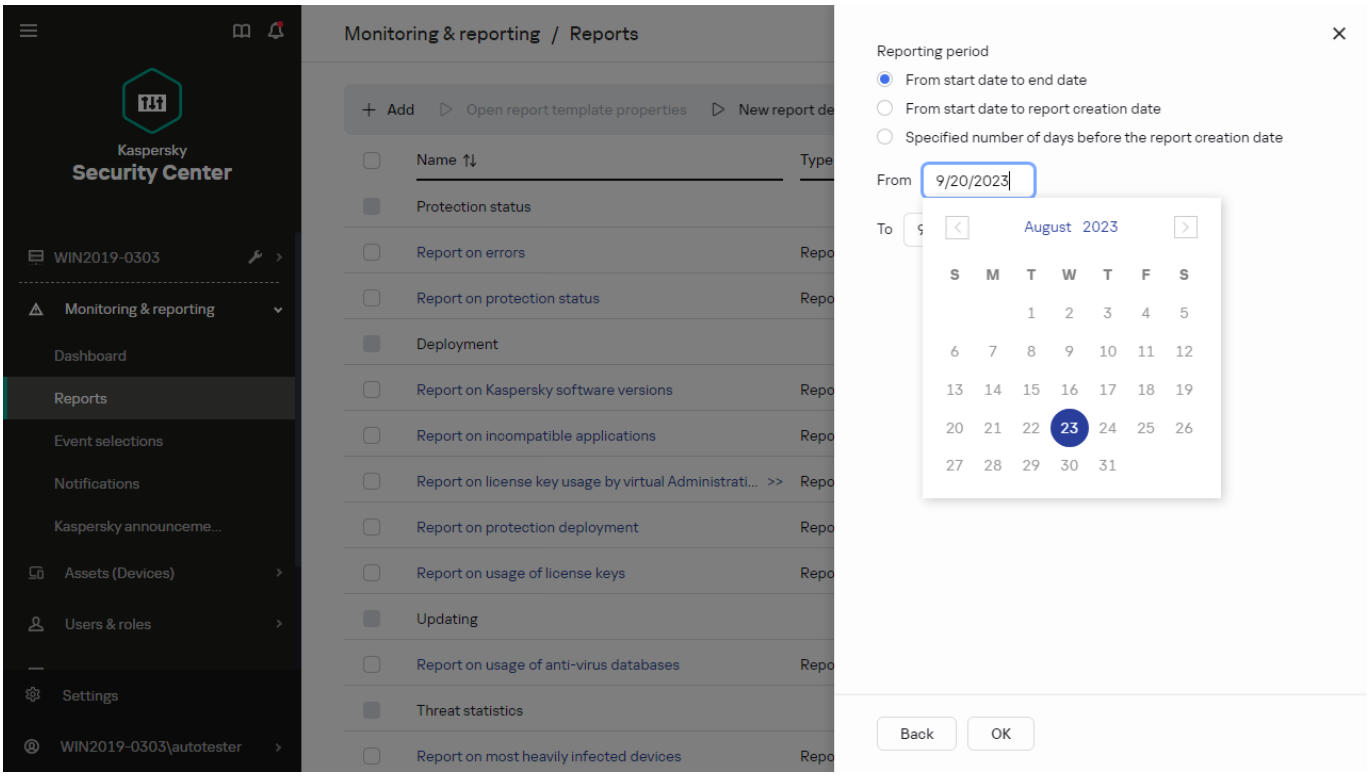


新报告模板向导。指定报告模板范围

5. 在向导的"**报告周期**"页面上，指定报告周期。有以下可用值：

- 在两个指定日期之间
- 从指定日期到报告创建日期
- 从报告创建日期减去指定天数，到报告创建日期

该页对一些报告可能不显示。



新报告模板向导。指定报告期间

6. 单击“**确定**”关闭向导。

7. 执行以下操作之一：

   - 单击“**保存和运行**”按钮以保存新报告模板并基于其运行报告。
     报告模板被保存。报告被生成。
   - 单击“**保存**”按钮保存新报告模板。
     报告模板被保存。

您可以使用新模板来生成和查看报告。

查看和编辑报告模板属性

您可以查看和编辑报告模板的基本属性，例如，报告模板名称或显示在报告中的字段。

要查看和编辑报告模板属性：

1. 在主菜单中，转到“**监控和报告**” → “**报告**”。

2. 选中您要查看和编辑其属性的报告模板旁边的复选框。
   另外，您可以先生成报告，然后单击“**编辑**”按钮。

3. 单击**打开报告模板属性**按钮。
   “**编辑报告 <报告名称>**”窗口打开，其中已选择“**常规**”选项卡。

4. 编辑报告模板属性：

- “常规”选项卡：
  - 报告模板名称
  - 显示条目的最大数量

    如果启用该选项，显示在表格中的带有详细报告数据的条目数量不超过指定值。请注意，此选项不会影响将报告导出到文件时可包含在报告中的最大事件数。

    报告条目首先根据报告模板属性的**字段 → 详细资料字段**区域中指定的规则进行排序，然后仅保存第一个结果条目。带有详细报告数据的表头展示显示的条目数量和匹配其他报告模板设置的可用条目总数。

    如果禁用该选项，带有详细报告数据的表显示所有可用条目。我们不建议您禁用该选项。限制显示的报告条目数量降低数据库管理系统 (DBMS) 负载，也降低生成和导出报告的所需时间。一些报告包含太多条目。如果是这样，您可能难于阅读和分析所有。而且，您的设备可能在生成此报告时内存不够，进而您将无法查看报告。

    默认情况下已启用该选项。默认值是 1000。

  - 组

    单击“**设置**”按钮以更改为其创建报告的客户端设备集合。对于一些报告类型，按钮可能不可用。实际设置取决于创建报告模板时指定的设置。

  - 时间间隔

    单击“**设置**”按钮以修改报告周期。对于一些报告类型，按钮可能不可用。有以下可用值：

    - 在两个指定日期之间
    - 从指定日期到报告创建日期
    - 从报告创建日期减去指定天数，到报告创建日期

  - 包含来自从属和虚拟管理服务器的数据

    如果启用该选项，报告包含属于创建模板的管理服务器的从属和虚拟管理服务器的信息。

    如果您要仅从当前管理服务器查看数据，禁用该选项。

    默认情况下已启用该选项。

  - 嵌套级别

    报告包含位于当前管理服务器下小于或等于指定嵌套级别的从属和虚拟管理服务器的数据。

    默认值是 1。如果您必须从树中位于低级别的从属管理服务器接收信息，您可能要更改该值。

  - 数据等待间隔(分钟)

    在生成报告之前，创建报告模板的管理服务器等待从属管理服务器的数据指定分钟数。如果在该时间段后未从从属管理服务器接收到数据，报告依然运行。除了实际数据，报告还显示从缓存获取的数据（如果启用了“**缓存从属管理服务器数据**”选项），否则为 **N/A**（不可用）。

    默认值是 5 分钟。

  - 缓存从属管理服务器数据

从属管理服务器定期传输数据到创建报告模板的管理服务器。传输的数据存储在缓存。

如果在生成报告时当前管理服务器无法从从属管理服务器接收数据，报告显示从缓存接收的数据。数据传输到缓存的日期也被显示。

启用该选项允许您查看从属管理服务器信息，即便实时数据无法被获取。然而，所显示数据可能过期。

默认情况下已禁用该选项。

- 缓存更新频率(小时)

  从属管理服务器定期传输数据到创建报告模板的管理服务器。您可以指定此时间段（以小时为单位）。如果指定 0 小时，则仅在生成报告时传输数据。

  默认值是 0。

- 从从属管理服务器传输详细信息

  在生成的报告中，带有详细报告数据的表格包含创建报告模板的管理服务器的从属管理服务器的数据。

  启用该选项减慢报告生成并增加管理服务器之间的流量。然而，您可以在一个报告中查看所有数据。

  除了启用该选项，您可能想分析详细报告数据以检测故障从属管理服务器，然后仅为该故障管理服务器生成相同报告。

  默认情况下已禁用该选项。

- **字段**选项卡

  选择要显示在报告中的字段，使用“**上移**”按钮和“**下移**”按钮更改这些字段的顺序。使用“**添加**”按钮或“**编辑**”按钮指定是否报告中的信息必须排序并按照每个字段进行筛选。

  在“**详细字段过滤器**”区域中，还可以单击“**转换过滤器**”按钮以开始使用扩展筛选格式。通过这种格式可以使用逻辑或运算来组合各个字段中指定的筛选条件。单击该按钮后，“**转换过滤器**”面板在右侧打开。单击“**转换过滤器**”按钮以确认转换。您现在可以使用“**详细资料字段**”区域中的条件来定义转换的筛选器，这些条件通过逻辑或运算进行应用。

  将报告转换为支持复杂筛选条件的格式将使该报告与 Kaspersky Security Center 的早期版本（11 及更早版本）不兼容。此外，转换后的报告将不包含运行此类不兼容版本的从属管理服务器的任何数据。

5. 单击“**保存**”保存设置。
6. 关闭**编辑报告<Report name>**窗口。

更新的报告模板显示在报告模板列表。

导出报告到文件

您可以将一份或多份报告保存为 XML、HTML 或 PDF。Kaspersky Security Center Linux 允许您同时将最多 10 个报告导出为指定格式的文件。

要导出报告到文件：

1. 在主菜单中，转到“**监控和报告**” → “**报告**”。
2. 选择您要导出的报告。

   如果您选择超过 10 个报告，**导出报告**按钮将被禁用。
3. 单击“**导出报告**”按钮。
4. 在打开的窗口中，指定以下导出参数：

   - **文件名**。

     如果您选择导出一份报告，请指定报告文件名。

     如果您选择多个报告，报告文件名将与所选报告模板的名称一致。
   - **最大条目数**。

     指定报告文件中包含的最大条目数。默认值是 10,000。

     您可以导出包含无限数量条目的报告。请注意，如果您的报告包含大量条目，则生成和导出报告所需的时间会增加。
   - **文件格式**。

     选择报告文件类型：XML、HTML 或 PDF。如果导出多个报告，所有选定的报告都会以指定格式保存为单独文件。

     > 将报告转换为 PDF 需要 wkhtmltopdf 工具。选择 PDF 选项后，管理服务器会检查设备上是否安装了 wkhtmltopdf 工具。如果未安装该工具，应用程序将显示一条消息，提示必须在管理服务器设备上安装该工具。手动安装该工具，然后继续下一步。
5. 单击“**导出报告**”按钮。

报告以指定格式保存到文件。

生成和浏览报告

要创建和查看报告，请执行以下操作：

1. 在主菜单中，转到“**监控和报告**” → “**报告**”。
2. 单击要用于创建报告的报告模板的名称。

   将生成并显示使用所选模板的报告。

> 将根据为管理服务器设置的本地化集显示报告数据。

> 在生成的报告中，某些字体可能无法正确显示在图表上。要解决此问题，请安装 fontconfig 库。另外，请检查操作系统中是否安装了与您的操作系统区域设置相对应的字体。

该报告将显示下列数据：

- 在“**概要**”选项卡上：
  - 报告名称和类型、简要描述和报告时间段，以及为哪个设备组生成该报告的相关信息。
  - 图表显示最有代表性的报告数据。
  - 带有计算好的报告指示器的加固表格。
- 在“**详细资料**”选项卡上，显示一个包含详细报告数据的表格。

创建报告发送任务

您可以创建传送所选报告的任务。

要创建报告传送任务：

1. 在主菜单中，转到“**监控和报告**” → “**报告**”。
2. 【可选】选择您要创建报告传送任务的报告模板旁边的复选框。
3. 单击“**新报告传送任务**”按钮。
4. “新任务向导”启动。使用**下一步**按钮进行向导。
5. 在向导的第一页，输入任务名称。默认名称是“**传送报告 (<N>)**”，其中 <N> 是任务序号。
6. 在向导的任务设置页面，指定以下设置：
   a. 要使用任务传送的报告模板。如果您在步骤 2 选择了它们，跳过该步骤。
   b. 报告格式：HTML、XLS 或 PDF。
      将报告转换为 PDF 需要 wkhtmltopdf 工具。选择 PDF 选项后，管理服务器会检查设备上是否安装了 wkhtmltopdf 工具。如果未安装该工具，应用程序将显示一条消息，提示必须在管理服务器设备上安装该工具。手动安装该工具，然后继续下一步。
   c. 报告是否使用电子邮件连同邮件通知设置一起发送。
   d. 报告是否被保存到文件夹，先前在该文件夹中保存的报告是否被覆盖，以及是否使用特定账户访问文件夹（对于共享文件夹）。
7. 如果要在创建任务后修改其他任务设置，请在向导的“**完成任务创建**”页面上启用“**创建完成时打开任务详情**”选项。
8. 单击“**创建**”按钮创建任务并关闭向导。
   报告传送任务被创建。如果启用了“**创建完成时打开任务详情**”选项，将打开任务设置窗口。

删除报告模板

要删除一个或几个报告模板：

1. 在主菜单中，转到“**监控和报告**” → “**报告**”。
2. 选择您要删除的报告模板旁边的复选框。
3. 单击“**删除**”按钮。
4. 在打开的窗口中，单击“**确定**”以确认您的选择。

所选报告模板被删除。如果这些报告模板被包含在报告传送任务中，它们也被从任务删除。

事件和事件分类

本节提供有关事件和事件分类、Kaspersky Security Center Linux 组件中发生的事件类型以及管理频繁事件阻止的信息。

关于 Kaspersky Security Center Linux 中的事件

Kaspersky Security Center Linux 允许您接收受管理设备上安装的管理服务器和 Kaspersky 应用程序在操作期间发生的事件信息。事件信息保存在管理服务器数据库。

按类型划分的事件

Kaspersky Security Center Linux 中有以下类型的事件：

- 常规事件。这些事件发生在所有受管理 Kaspersky 应用程序中。常规事件的一个示例是病毒爆发常规事件具有严格定义的语法和语义。常规事件用于报告和控制板等方面。
- 受管理 Kaspersky 应用程序特定事件。每个受管理 Kaspersky 应用程序都拥有自己的事件集。

按来源划分的事件

您可以在应用程序策略的“**事件配置**”选项卡上查看应用程序可以生成的事件的完整列表。对于管理服务器，您还可以在管理服务器属性中查看事件列表。

以下应用程序可以生成事件：

- Kaspersky Security Center Linux 组件：
  - 管理服务器
  - 网络代理
- 受管理的卡巴斯基应用程序

  有关受管理的卡巴斯基应用程序生成的事件的详细信息，请参阅相应应用程序的文档。

按重要性级别划分的事件

每个事件都有自己的重要级别。取决于发生的条件，一个事件可以被分配不同的重要级别。四个事件重要级别如下：

- *严重事件*指示发生了可能导致数据丢失、操作系统异常或严重错误的严重问题。
- *功能失败*指示在应用程序操作中或执行过程中发生了严重问题、错误或功能异常。
- *警告*是不严重的事件，但是也指示了今后可能发生的潜在问题。如果在事件发生后应用程序可以被恢复而不丢失数据或功能，则这些事件是警告级别。
- *信息*事件用于提示成功完成操作、应用程序的正常功能或完成了某过程。

每个事件都有一个存储期限，在这时间内您可以在 Kaspersky Security Center Linux 中查看或修改。一些事件默认下不保存在管理服务器数据库，因为它们的存储期限是零。仅可以在管理服务器数据库中保存至少一天的事件可以被导出到外部系统。

Kaspersky Security Center Linux 组件事件

每个 Kaspersky Security Center Linux 组件都拥有自己的事件类型集。本节列出了 Kaspersky Security Center 管理服务器和网络代理中发生的事件类型。Kaspersky 应用程序中发生的事件类型不在此区域列出。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。对于管理服务器，您还可以在管理服务器属性中查看和配置事件列表。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

事件类型描述的数据结构

对于每个事件类型，它的显示名称、ID、字母码、描述和默认存储期限被提供。

- **事件类型显示名称**。该文本当您配置事件时和它们发生时被显示在 Kaspersky Security Center Linux 中。
- **事件类型 ID**。该数码在您使用第三方工具分析事件时使用。
- **事件类型**（字母码）。该代码用于您使用 Kaspersky Security Center Linux 数据库中提供的公共视图浏览和处理事件时以及事件被导出到 SIEM 系统时。
- **描述**。该文本包含事件发生的情况以及此种情况下您可以做的事。
- **默认存储期限**。这是事件存储在管理服务器数据库的天数，显示在管理服务器事件列表中。该时间段之后，事件被删除。如果事件存储期限值是 0，此类事件被检测但不显示在管理服务器事件列表。如果您配置了保存此类事件到操作系统事件日志，您可以在那里找到它们。

  您可以更改事件存储期限：设置事件存储期限

Administration Server events

This section contains information about the events related to the Administration Server.

管理服务器严重事件

该表显示具有“**严重**”重要性级别的 Kaspersky Security Center 管理服务器事件。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。对于管理服务器，您还可以在管理服务器属性中查看和配置事件列表。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

管理服务器严重事件

事件类型显示名称	事件类型 ID	事件类型	描述	默认存储期限
已超过授权许可数量限制	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	每天，Kaspersky Security Center Linux 检查是否超过授权许可限制。 当管理服务器发现安装在客户端设备上的 Kaspersky 应用程序超过了授权许可限制，以及由单一授权许可覆盖的当前使用的授权许可单元数量超过了该授权许可覆盖的单元总数的 110%，则该类型的事件发生。 即便当该事件发生时，客户端设备是被保护的。 您可以通过以下方式响应事件： • 查看受管理设备列表。删除不在使用的设备。 • 为更多设备提供授权许可（添加有效的激活码或密钥文件到管理服务器）。 Kaspersky Security Center Linux 决定当授权许可限制被超过时生成事件的规则。	180 天
设备已失去管理	4111	KLSRV_HOST_OUT_CONTROL	如果受管理设备在网络中可见，但一定时间未连接到管理服务器，则该类型的事件发生。 找到什么阻止了设备上网络代理的正常功能。可能的原因包括网络问题和从设备卸载网络代理。	180 天
设备状态是“严重”	4113	KLSRV_HOST_STATUS_CRITICAL	当受管理设备被分配*严重*状态时，该类型的事件发生。您可以配置设备状态被更改到*严重*的条件。	180 天
密钥文件已被添加到拒绝列表	4124	KLSRV_LICENSE_BLACKLISTED	当 Kaspersky 已将您使用的激活码或密钥文件添加到拒绝列表时，会发生该类型事件。 联系技术支持获得更多详情。	180 天
授权许可	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	当商业授权许可的失效日期即将到来时，会发生此类事件。	180 天

即将过期			Kaspersky Security Center Linux 每天检查一次授权许可到期日期是否临近。此类型的事件在授权许可到期之前 30 天、15 天、5 天 和 1 天发布。该天数无法被更改。如果管理服务器在授权许可到期日之前的指定日期被关闭，则事件直到第二天才发布。 当商业授权许可到期后，Kaspersky Security Center Linux 仅提供基本功能。 您可以通过以下方式响应事件： • 请确保将备用授权许可密钥添加到管理服务器中。 • 如果您使用订阅，请确保续订。如果无限制订阅已在到期日前预付费给服务提供商，则该订阅会自动续订。	
证书已过期	4132	KLSRV_CERTIFICATE_EXPIRED	当移动设备管理的管理服务器证书过期时，会发生此类事件。 您需要更新过期的证书。 您可以通过选中证书发行设置中的“**如果可能，自动重新发布证书**”复选框来配置证书自动更新。	180 天

管理服务器功能失败事件

该表显示具有“**功能失败**”重要性级别的 Kaspersky Security Center 管理服务器事件。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。对于管理服务器，您还可以在管理服务器属性中查看和配置事件列表。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

管理服务器功能失败事件

事件类型显示名称	事件类型 ID	事件类型	描述	默认存储期限
运行时错误	4125	KLSRV_RUNTIME_ERROR	由于未知问题，该类型的事件发生。 多数情况下，这些是 DBMS 问题、网络问题和其他软件和硬件问题。 事件详情可以在事件描述中找到。	180 天
已授权应用程序组之一的安装已超过限制	4126	KLSRV_INVLICPROD_EXCEDED	管理服务器定期生成该类型的事件（每小时）。如果您在 Kaspersky Security Center Linux 中管理第三方应用程序的授权许可密钥，并且安装数量超过了第三方应用程序授权许可密钥所设置的限制，则会发生该类型事件。	180 天

			您可以通过以下方式响应事件： • 查看受管理设备列表。从未使用第三方应用程序的设备上删除该应用程序。 • 为更多设备使用第三方授权许可。 您可以使用已授权应用程序组的功能管理第三方应用程序的授权许可密钥。这是一组由满足您所设标准的第三方应用程序组成的授权应用程序群组。	
将更新复制到指定文件夹失败	4123	KLSRV_UPD_REPL_FAIL	当软件更新被复制到附加共享文件夹时，该类型的事件发生。 您可以通过以下方式响应事件： • 检查用于获取文件夹访问的用户账户是否具有写权限。 • 检查文件夹的用户名和/或密码是否被更改。 • 检查互联网连接，因为它可能是事件原因。遵照指示更新数据库和软件模块。	180天
没有剩余硬盘空间	4107	KLSRV_DISK_FULL	当安装管理服务器的设备的硬盘空间不足时，会发生此类事件。 释放设备上的磁盘空间。	180天
共享文件夹不可用	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	如果管理服务器共享文件夹不可用，则该类型的事件发生。 您可以通过以下方式响应事件： • 检查管理服务器(共享文件夹所在位置)是否已开启并可用。 • 检查文件夹的用户名和/或密码是否被更改。 • 检查网络连接。	180天
管理服务器数据库不可用	4109	KLSRV_DATABASE_UNAVAILABLE	如果管理服务器数据库不可用则该类型的事件发生。 您可以通过以下方式响应事件： • 检查安装了 SQL Server 的远程服务器是否可用。 • 查看 DBMS 日志以发现管理服务器数据库不可用的原因。例如，因为维护，安装了 SQL Server 的远程服务器可能不可用。	180天

管理服务器数据库空间不足	4110	KLSRV_DATABASE_FULL	当管理服务器数据库没有剩余空间时，该类型的事件发生。
			当管理服务器的数据库达到其容量，以及当不可能再往数据库记录时，管理服务器不工作。
			以下是根据您使用的 DBMS，该事件的原因，以及到该事件的正确响应：
			• 您使用 SQL Server Express 版本 DBMS：
			  • 在 SQL Server Express 文档中，查看所用版本的数据库大小限制。可能您的管理服务器数据库已超过了数据库大小限制。
			  • 限制存储在管理服务器数据库的事件数量。
			  • 在管理服务器数据库中有太多由应用程序控制组件发送的事件。您可以更改与管理服务器数据库中的应用程序控制事件存储有关的 Kaspersky Endpoint Security 策略的设置。
			• 您使用 DBMS 而不是 SQL Server Express Edition：
			  • 不限制存储在管理服务器数据库的事件数量。
			  • 降低存储在管理服务器数据库的事件数量。
			在 DBMS 选项处查看信息。
				180 天

管理服务器警告事件

下表显示了具有“**警告**”重要级别的 Kaspersky Security Center 管理服务器事件。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。对于管理服务器，您还可以在管理服务器属性中查看和配置事件列表。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

管理服务器警告事件

事件类型显示名称	事件类型 ID	事件类型	描述	默认存储期限
已检测到频繁事件		KLSRV_EVENT_SPAM_EVENTS_DETECTED	当管理服务器在受管理设备上检测到频繁发生的事件时，会发生这种类型的事件。请参阅	90 天

			以下部分了解详情：阻止频繁事件。	
已超过授权许可数量限制	4098	KLSRV_EV_LICENSE_CHECK_100_110	每天，Kaspersky Security Center Linux 检查是否超过授权许可限制。 当管理服务器发现安装在客户端设备上的 Kaspersky 应用程序超过了授权许可限制，以及由单一授权许可覆盖的当前使用的授权许可单元数量达到了该授权许可覆盖的单元总数的 100% 到 110%，则该类型的事件发生。 即便当该事件发生时，客户端设备是被保护的。 您可以通过以下方式响应事件： • 查看受管理设备列表。删除不在使用的设备。 • 为更多设备提供授权许可（添加有效的激活码或密钥文件到管理服务器）。 Kaspersky Security Center Linux 决定当授权许可限制被超过时生成事件的规则。	90 天
设备在网络上已长时间没有活动	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	当受管理设备在一段时间内显示出不活动状态时，会发生此类事件。 这种情况通常发生在受管理设备已解除授权时。 您可以通过以下方式响应事件： • 要从受管理设备列表中手动删除该设备。 指定时间间隔，经过该间隔后，使用 Kaspersky Security Center 14 Web Console 创建“**设备在网络上已长时间没有活动**”事件。 • 指定时间间隔，在该间隔后，使用 Kaspersky Security Center Web Console 自动将设备自动从组中删除。	90 天
设备名称冲突	4102	KLSRV_EVENT_HOSTS_CONFLICT	当管理服务器将两台或更多受管理设备视为单台设备时，会发生此类事件。	90 天

			在受管理设备上使用克隆的硬盘驱动器进行软件部署，而没有将参考设备上的网络代理切换到专用磁盘克隆模式时，通常会发生这种情况。 为避免此问题，请在克隆此设备的硬盘驱动器之前将参考设备上的网络代理切换到磁盘克隆模式。	
设备状态是“警告”	4114	KLSRV_HOST_STATUS_WARNING	当受管理设备被分配*警告*状态时，该类型的事件发生。您可以配置设备状态被更改到*警告*的条件。	90 天
已授权应用程序组之一的安装即将超过限制	4127	KLSRV_INVLICPROD_FILLED	当已授权应用程序组中包含的第三方应用程序安装数量达到授权许可密钥属性中指定的最大允许值的 90% 时，将发生此类事件。 您可以通过以下方式响应事件： • 如果某些受管理设备上未使用第三方应用程序，请从这些设备中删除该应用程序。 • 如果您预计第三方应用程序安装数量将在不久的将来超过允许的最大值，请考虑预先获取更多设备的第三方授权许可。 您可以使用已授权应用程序组的功能管理第三方应用程序的授权许可密钥。	90 天
证书已被请求	4133	KLSRV_CERTIFICATE_REQUESTED	当自动重新颁发移动设备管理证书失败时，将发生此类事件。 以下是事件的可能原因和对事件的适当响应： • 对禁用了“**如果可能，自动重新发布证书**”选项的证书启动自动重新发布。这可能是由于在证书创建过程中发生的错误所致。可能需要手动重新颁发证书。 • 如果使用与公钥基础结构的集成，则原因可能是用于与 PKI 集成和用于颁发证书的账户缺少 SAM-Account-Name 属性。查看账户属性。	90 天
证书已删除	4134	KLSRV_CERTIFICATE_REMOVED	当管理员删除了移动设备管理的任何类型的证书（通用、邮	90 天

			件、VPN）时，会发生此类事件。 删除证书后，通过此证书连接的移动设备将无法连接到管理服务器。 在调查与移动设备管理相关的故障时，此事件可能会有所帮助。	
APNs 证书已过期	4135	KLSRV_APN_CERTIFICATE_EXPIRED	当 APNs 证书过期时，会发生此类事件。 您需要手动续订 APNs 证书并将其安装在 iOS MDM 服务器上。	未存储
APNs 证书即将过期	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	当 APNs 证书距离过期不到 14 天时，会发生此类事件。 当 APNs 证书过期时，您需要手动续订 APNs 证书并将其安装在 iOS MDM 服务器上。 我们建议您在过期日期前安排 APNs 证书续订。	未存储
发送 **FCM** 消息到移动设备失败	4138	KLSRV_GCM_DEVICE_ERROR	当移动设备管理配置为使用 Google Firebase Messaging (FCM) 连接到具有 Android 操作系统的受管理移动设备，并且 FCM 服务器无法处理从管理服务器收到的某些请求时，会发生此类事件。这意味着某些受管理移动设备不会收到推送通知。 读取事件描述详细信息中的 HTTP 代码，并相应做出响应。有关从 FMC 服务器收到的 HTTP 代码以及相关错误的更多信息，请参阅 Google Firebase 服务文档（参见“下游消息错误响应代码”一章）。	90 天
发送 **FCM** 消息到 **FCM** 服务器时发生 **HTTP** 错误	4139	KLSRV_GCM_HTTP_ERROR	当移动设备管理配置为使用 Google Firebase Messaging (FCM) 连接到具有 Android 操作系统的受管理移动设备，并且 FCM 服务器回复管理服务器请求的 HTTP 代码不是 200（正常）时，会发生此类事件。 以下是事件的可能原因和对事件的适当响应： • FMC 服务器端出现问题。读取事件描述详细信息中的 HTTP 代码，并相应做出响应。有关从 FMC 服务器收到的 HTTP 代码以及相关错误的更多信息，请参阅 Google Firebase 服务文档	90 天

			（参见“下游消息错误响应代码”一章）。 • 代理服务器端出现问题（如果使用代理服务器）。读取事件详细信息中的 HTTP 代码，并相应做出响应。	
发送 FCM 消息到 FCM 服务器失败	4140	KLSRV_GCM_GENERAL_ERROR	使用 Google Firebase Cloud Messaging HTTP 协议时，由于管理服务器端发生意外错误，而发生此类事件。 读取事件描述中的详细信息，并相应做出响应。 如果您自己找不到问题的解决方案，建议与 Kaspersky 技术支持联系。	90 天
硬盘驱动器剩余空间少	4105	KLSRV_NO_SPACE_ON_VOLUMES	当安装管理服务器的设备的硬盘空间不足时，会发生此类事件。 释放设备上的磁盘空间。	90 天
管理服务器数据库的剩余空间少	4106	KLSRV_NO_SPACE_IN_DATABASE	如果管理服务器数据库受限制则该类型的事件发生。如果您不纠正情况，管理服务器数据库就将达到其容量且管理服务器将不工作。 以下是根据您使用的 DBMS，该事件的原因，以及到该事件的正确响应。 您使用 SQL Server Express 版本 DBMS： • 在 SQL Server Express 文档中，查看所用版本的数据库大小限制。可能您的管理服务器数据库即将超过数据库大小限制。 • 限制存储在管理服务器数据库的事件数量。 • 在管理服务器数据库中有太多由应用程序控制组件发送的事件。您可以更改与管理服务器数据库中的应用程序控制事件存储有关的 Kaspersky Endpoint Security 策略的设置。 您使用 DBMS 而不是 SQL Server Express Edition： • 不限制存储在管理服务器数据库的事件数量 • 降低存储在管理服务器数据库的事件数量	90 天

			在 DBMS 选项处查看信息。	
到从属管理服务器的连接已中断	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	当与从属管理服务器的连接中断时，会发生此类事件。 读取安装了从属管理服务器的设备上的操作系统日志，并相应做出响应。	90 天
到主管理服务器的连接已中断	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	当与主管理服务器的连接中断时，会发生此类事件。 读取安装了主管理服务器的设备上的操作系统日志，并相应做出响应。	90 天
已注册卡巴斯基软件模块的新更新	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	当管理服务器为需要批准安装的受管理设备上安装的 Kaspersky 软件注册新更新时，会发生此类事件。 使用 Kaspersky Security Center Web Console 批准或拒绝更新。	90 天
超过了数据库中事件数的限制，已开始删除事件	4145	KLSRV_EVP_DB_TRUNCATING	当从管理服务器数据库删除旧事件在管理服务器数据库达到容量后开始时，该类型的事件发生。 您可以通过以下方式响应事件： • 更改存储在管理服务器数据库的事件最大数量 • 降低存储在管理服务器数据库的事件数量	未存储
超过了数据库中事件数的限制，事件已被删除	4146	KLSRV_EVP_DB_TRUNCATED	当从管理服务器数据库删除旧事件在管理服务器数据库达到容量后完成时，该类型的事件发生。 您可以通过以下方式响应事件： • 更改允许存储在管理服务器数据库的事件最大数量 • 降低存储在管理服务器数据库的事件数量	未存储

管理服务器信息事件

下表显示了具有“**信息**”重要级别的 Kaspersky Security Center 管理服务器事件。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。对于管理服务器，您还可以在管理服务器属性中查看和配置事件列表。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

事件类型显示名称	事件类型ID	事件类型	默认存储期限	评论
授权许可密钥的 **90%** 已经使用	4097	KLSRV_EV_LICENSE_CHECK_90	30天	
已检测到新设备	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30天	
设备已被自动添加到组	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30天	
设备已从组中删除：长时间在网络中不活动	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30天	
已授权应用程序组之一的安装即将超过限制(已经使用 **95%** 以上)	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30天	
找到了要发送至卡巴斯基以分析的文件	4131	KLSRV_APS_FILE_APPEARED	30天	
此移动设备上的 **FCM** 实例 **ID** 已被更改	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30天	
更新已被成功复制到指定文件夹	4122	KLSRV_UPD_REPL_OK	30天	
到从属管理服务器的连接已建立	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30天	
到主管理服务器的连接已建立	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30天	
数据库已更新	4144	KLSRV_UPD_BASES_UPDATED	30天	
审计：到管理服务器的连接已建立	4147	KLAUD_EV_SERVERCONNECT	30天	
审计：对象已修改	4148	KLAUD_EV_OBJECTMODIFY	30天	该事件追踪以下对象中的更改： • 管理组 • 安全组 • 用户 • 任务

				• 任务 • 策略 • 服务器 • 虚拟服务器
审计：对象状态已修改	4150	KLAUD_EV_TASK_STATE_CHANGED	30天	例如，当任务以错误失败时会发生该事件。
审计：组设置已修改	4149	KLAUD_EV_ADMGROUP_CHANGED	30天	
审计：到管理服务器的连接已终止	4151	KLAUD_EV_SERVERDISCONNECT	30天	
审计：对象属性已被修改	4152	KLAUD_EV_OBJECTPROPMODIFIED	30天	该事件追踪以下属性中的更改： • 用户 • 授权许可 • 服务器 • 虚拟服务器

审计：用户许可已被修改	4153	KLAUD_EV_OBJECTACLMODIFIED	30 天	
审计：已从管理服务器导入或导出加密密钥	5100	KLAUD_EV_DPEKEYSEXPORT	30 天	

Network Agent events

This section contains information about the events related to Network Agent.

网络代理警告事件

下表显示具有“**警告**”严重级别的网络代理事件。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

网络代理警告事件

事件类型显示名称	事件类型 ID	事件类型	默认存储期限
发生了安全问题	549	GNRL_EV_APP_INCIDENT_OCCURED	30 天
KSN 代理已启动。检查 **KSN** 可用性失败	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 天

网络代理信息事件

下表显示具有“**信息**”严重级别的网络代理事件。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

网络代理信息事件

事件类型显示名称	事件类型 ID	事件类型	默认存储期限
应用程序已安装	7703	KLNAG_EV_INV_APP_INSTALLED	30 天
应用程序已卸载	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 天
已安装监控的应用程序	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 天
已卸载监控的应用程序	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 天
已添加新设备	7708	KLNAG_EV_DEVICE_ARRIVAL	30 天
设备已被删除	7709	KLNAG_EV_DEVICE_REMOVE	30 天
已检测到新设备	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 天
设备已被授权	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 天

KSN 代理已启动。KSN 可用性检查已成功完成	7719	KSNPROXY_STARTED_CON_CHK_OK	30 天
KSN 代理已停止	7720	KSNPROXY_STOPPED	30 天

使用事件分类

事件分类提供了从管理服务器数据库中选择的指定事件集合的屏幕视图。这些事件集根据以下类别进行分组：

- 按重要级别—**严重事件**、**功能失败**、**警告**和**信息事件**
- 按时间—**最近事件**
- 按类型—**用户请求**和**审计事件**

您可以基于 Kaspersky Security Center Web Console 界面上可以配置的设置创建和查看用户定义的事件分类。

在 Kaspersky Security Center Web Console 的"**监控和报告**"区域中单击"**事件分类**"可使用事件分类。

默认下，事件分类包含 7 天内的信息。

Kaspersky Security Center Linux 具有一组默认的事件（预定义）选择：

- 不同重要级别的事件：
  - **严重事件**
  - **功能失败**
  - **警告**
  - **信息消息**
- **用户请求**（受管理应用程序事件）
- **最近事件**（上周）
- 审计事件。

您也可以创建和配置附加用户定义分类。在用户定义分类中，您可以根据设备属性（设备名称、IP 范围和管理组）、根据事件类型和严重级别、根据应用程序和组件名称、以及根据时间间隔来筛选事件。也可以包含任务结果到搜索范围。您也可以单一搜索字段，可以输入一个词或几个词。所有属性（例如事件名称、描述、组件名称）中包含任意所输入词的事件被显示。

对于预定义和用户定义的分类，您可以限制显示事件的数量或者要搜索的记录的数量。两个选项都影响 Kaspersky Security Center Linux 显示事件所花费的时间。数据库越大，过程越耗时。

您可以执行以下操作：

- 编辑事件分类的属性
- 生成事件分类
- 查看事件分类的详细信息

- 删除事件分类
- 从管理服务器数据库中删除事件

创建事件分类

要创建事件分类，请执行以下操作：

1. 在主菜单中，转到“**监控和报告**” → “**事件分类**”。
2. 单击**添加**。
3. 在打开的“**新事件分类**”窗口中，指定新事件分类的设置。在窗口中重复此操作。
4. 单击“**保存**”保存设置。
   确认窗口打开。
5. 要查看事件分类结果，请保持“**转到分类结果**”复选框为选中状态。
6. 单击“**保存**”确认事件分类创建。

如果将“**转到分类结果**”复选框保持选中状态，将显示事件分类结果。否则，新事件分类出现在事件分类列表。

编辑事件分类

要编辑事件分类：

1. 在主菜单中，转到“**监控和报告**” → “**事件分类**”。
2. 选中您要编辑的事件分类旁边的复选框。
3. 单击“**属性**”按钮。
   事件分类设置窗口打开。
4. 编辑事件分类属性。

   > 对于预定义的事件分类，只能编辑以下选项卡上的属性：**常规**（除了分类名称）、**时间**和**访问权限**。

   对于用户定义分类，您可以编辑所有属性。
5. 单击“**保存**”保存设置。

编辑的事件分类显示在列表。

查看事件分类列表

要查看事件分类：

1. 在主菜单中，转到“**监控和报告**” → “**事件分类**”。
2. 选择您要启动的事件分类旁边的复选框。
3. 执行以下操作之一：
   - 如果您要在事件分类结果中配置排序，做以下：
     a. 单击**重新配置排序并开始**按钮。
     b. 在显示的“**重新配置事件分类排序**”窗口中，指定排序设置。
     c. 单击分类的名称。
   - 否则，如果想要以事件在管理服务器上的顺序查看事件列表，请单击分类名称。

事件分类结果被显示。

导出事件分类

Kaspersky Security Center Linux 允许您将事件分类及其设置保存到 KLT 文件。您可以使用此 KLO 文件将保存的事件分类导入到 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux。

请注意，您只能导出用户定义的事件分类。Kaspersky Security Center Linux 默认集中的事件分类（预定义分类）无法保存到文件。

要导出事件分类：

1. 在主菜单中，转到**监控和报告** → **事件分类**。
2. 选中您要导出的事件分类旁边的复选框。
   您不能同时导出多个事件分类。如果您选择了多个分类，**导出**按钮将被禁用。
3. 单击“**导出**”按钮。
4. 在打开的**“另存为”**窗口中，指定事件分类文件名和路径，然后单击**保存**按钮。
   仅当您使用 Google Chrome、Microsoft Edge 或 Opera 时，才会显示“**另存为**”窗口。如果您使用其他浏览器，则事件分类文件会自动保存在“**下载**”文件夹。

导入事件分类

Kaspersky Security Center Linux 允许您从 KLO 文件导入事件分类。KLO 文件包含导出的事件分类及其设置。

要导入事件分类：

1. 在主菜单中，转到**监控和报告** → **事件分类**。

2. 单击**导入**按钮，然后选择要导入的事件分类文件。

3. 在打开的窗口中，指定 KLO 文件的路径，然后单击“**打开**”按钮。请注意，您仅可选择一个事件分类文件。
   事件分类处理开始。

出现包含导入结果的通知。如果事件分类导入成功，您可以单击**查看导入详细信息**链接来查看事件分类属性。

成功导入后，事件分类会显示在分类列表中。事件分类的设置也会被导入。

> 如果新导入的事件分类与现有事件分类有相同的名称，则导入的分类在名称后会附加一个（**<下一个序列号>**）索引，例如：**(1)**、**(2)**。

查看事件详情

要查看事件详情：

1. 启动事件分类。

2. 点击所需事件的时间。
   “**事件属性**”窗口打开。

3. 在显示的窗口中，您可以做以下：

   - 查看关于所选事件的信息
   - 在事件分类结果中转到上一个事件和下一个事件
   - 转到发生事件的设备
   - 转到包含发生事件的设备的管理组
   - 对于任务相关事件，转到任务属性

导出事件到文件

要导出事件到文件：

1. 启动事件分类。

2. 选择所需事件旁边的复选框。

3. 单击“**导出到文件**”按钮。

   所选事件被导出到文件。

从事件查看对象历史

从创建或修改支持修订管理的对象的事件，您可以切换到对象的修订历史。

要从事件查看对象历史：

1. 启动事件分类。
2. 选择所需事件旁边的复选框。
3. 单击**修订历史**按钮。

   对象修订历史被打开。

删除事件

要删除一个或几个事件：

1. 启动事件分类。
2. 选择所需事件旁边的复选框。
3. 单击“**删除**”按钮。

   所选事件被删除且无法恢复。

删除事件分类

> 您仅可以删除用户定义的事件分类。预定义事件分类无法被删除。

要删除一个或几个事件分类：

1. 在主菜单中，转到“**监控和报告**” → “**事件分类**”。
2. 选择您要删除的事件分类旁边的复选框。
3. 单击**删除**。
4. 在打开的窗口中，单击“**确定**”。

   事件分类被删除。

设置事件存储期限

Kaspersky Security Center Linux 允许您接收受管理设备上安装的管理服务器和 Kaspersky 应用程序在操作期间发生的事件信息。事件信息保存在管理服务器数据库。您可能需要将某些事件存储比默认值指定的时间更长或更短的时间。您可以更改事件存储期限的默认设置。

如果您无意将某些事件存储在管理服务器的数据库中，则可以在管理服务器策略和 Kaspersky 应用程序策略或在管理服务器属性（仅对于管理服务器事件）中禁用相应设置。这将降低数据库中的事件类型数量。

事件的存储期限越长，数据库达到最大值速度越快。但是，事件的存储期限越长，执行监控和报告任务的时间就越长。

要为管理服务器中的事件设置存储期限：

1. 在主菜单中，转到“**资产(设备)**” → “**策略和配置文件**“。
2. 执行以下操作之一：
   - 要配置网络代理或受管理 Kaspersky 应用程序的事件存储期限，请单击相应策略的名称。
     策略属性页面将打开。
   - 要配置管理服务器事件，请在主菜单中单击所需管理服务器名称旁边的“设置”图标 ( )。
     如果有管理服务器的策略，则可以改为单击该策略的名称。
     将打开管理服务器属性页面（或管理服务器策略属性页面）。
3. 选择**事件配置**选项卡。
   将显示与“**严重**”区域有关的事件类型列表。
4. 选择“**功能失败**”、“**警告**”或“**信息**”区域。
5. 在右侧面板中的事件类型列表中，点击您要更改其存储期限的事件的链接。
   在打开的窗口的“**事件注册**”区域中，启用“**存储在管理服务器数据库上(天)**”选项。
6. 在该开关按钮下面的编辑框中，输入存储事件的天数。
7. 如果您不希望在管理服务器数据库中存储事件，请禁用“**存储在管理服务器数据库上(天)**”选项。

   如果您在管理服务器属性窗口中配置管理服务器事件，并且在 Kaspersky Security Center 管理服务器策略中锁定了事件设置，则无法重新定义事件的存储期限值。

8. 单击“**确定**”。
   策略的属性窗口关闭。

从现在开始，当管理服务器接收并存储选定类型的事件时，它们将具有更改的存储期限。管理服务器不会更改以前接收的事件的存储期限。

Blocking frequent events

This section provides information about managing frequent events blocking and about removing blocking of frequent events.

About blocking frequent events

A managed application, for example, Kaspersky Endpoint Security for Linux, installed on a single or several managed devices can send a lot of events of the same type to the Administration Server. Receiving frequent events may overload the Administration Server database and overwrite other events. Administration Server starts blocking the most frequent events when the number of all the received events exceeds the specified limit for the database.

Administration Server blocks the frequent events from receiving automatically. You cannot block the frequent events yourself, or choose which events to block.

If you want to find out if an event is blocked, you can view the notification list or you can check if this event is present in the 阻止频繁事件 section of the Administration Server properties. If the event is blocked, you can do the following:

- If you want to prevent overwriting the database, you can continue blocking such type of events from receiving.
- If you want, for example, to find the reason of sending the frequent events to the Administration Server, you can unblock frequent events and continue receiving the events of this type anyway.
- If you want to continue receiving the frequent events until they become blocked again, you can remove from blocking the frequent events.

Managing frequent events blocking

Administration Server blocks the automatic receiving of frequent events, but you can unblock and continue to receive frequent events. You can also block receiving frequent events that you unblocked before.

To manage frequent events blocking:

1. In the main menu, click the settings icon ( ) next to the name of the required Administration Server.

   The Administration Server properties window opens.

2. On the 常规 tab, select the **Blocking frequent events** section.
3. In the **Blocking frequent events** section:
   - If you want to unblock the receiving of frequent events:
     a. Select the frequent events you want to unblock, and then click the **Exclude** button.
     b. Click the **Save** button.
   - If you want to block receiving frequent events:
     a. Select the frequent events you want to block, and then click the **Block** button.

b. Click the **Save** button.

Administration Server receives the unblocked frequent events and does not receive the blocked frequent events.

Removing blocking of frequent events

You can remove blocking for frequent events and start receiving them until Administration Server blocks these frequent events again.

To remove blocking for frequent events:

1. In the main menu, click the settings icon ( ) next to the name of the required Administration Server.

   The Administration Server properties window opens.

2. On the 常规 tab, select the **Blocking frequent events** section.

3. In the **Blocking frequent events** section, select the frequent event types for which you want to remove blocking.

4. Click the **Remove from blocking** button.

The frequent event is removed from the list of frequent events. Administration Server will receive events of this type.

在管理服务器上的事件处理和存储

关于程序和受管理设备的操作事件信息保存在管理服务器数据库。每个事件都归属于特定类型和严重级别（*严重事件*、*功能失败*、*警告*或*信息*）。基于事件发生的条件，程序可以分配不同的严重级别到相同类型的事件。

您可以在管理服务器属性窗口的 **事件配置** 区域查看分配给事件的类型和严重级别。在**事件配置**区域，您也可以配置管理服务器对每个事件的处理：

- 在管理服务器、设备 OS 事件日志和管理服务器计算机 OS 事件日志中注册事件。
- 通知管理员事件的方法（例如，SMS 或者邮件消息）。

在管理服务器属性窗口的**事件存储库**区域，您可以通过限制事件记录数和存储期限来编辑管理服务器数据库的事件存储设置。当您指定事件最大数时，应用程序计算用于指定数目的存储空间的大概大小。您可以使用该大概计算来评估您在磁盘上是否具有足够空间以避免数据库溢出。管理服务器数据库的默认容量是 400,000 个事件。最大建议的数据库容量是 45,000,000 个事件。

应用程序每 10 分钟检查一次数据库。如果事件数达到指定的最大值加 10,000，应用程序将删除最旧的事件，以便仅保留指定的最大事件数。

当管理服务器删除旧事件后，它无法保存新事件到数据库。在此时间段内，拒绝事件的信息被写入操作系统日志。新事件被列队，然后在删除操作后被保存到数据库。

通知和设备状态

本节包含有关如何查看通知、配置通知传送、使用设备状态和启用更改设备状态的信息。

使用通知

通知提醒您事件并帮助您通过执行推荐操作或您认为适当的操作来加速您对这些事件的响应。

根据选择的通知方法，有以下类型的通知可用：

- 屏幕通知
- 通过 SMS 通知
- 通过电子邮件通知
- 通过可执行文件或脚本通知

屏幕通知

屏幕通知提醒您按照重要级别分组的事件(*严重*、*警告*和*信息*)。

屏幕通知可以有两种状态之一：

- *已查看*。您已对通知执行了推荐操作或您已手动为通知分配了该状态。
- *未查看*。您未对通知执行了推荐操作或您未手动为通知分配了该状态。

默认下，通知列表包含*未查看*状态的通知。

您可以通过查看屏幕通知和实时响应它们来监控您的组织网络。

通过电子邮件、SMS 和可执行文件或脚本通知

Kaspersky Security Center Linux 提供通过发送您认为重要的事件的通知来监控您的组织网络。对任意事件，您可以配置通过电子邮件、SMS 或运行可执行文件或脚本进行通知。

在通过电子邮件或 SMS 接收通知时，您可以决定您对事件的响应。此响应应该最适合您组织的网络。通过运行可执行文件或脚本，您预定义对事件的响应。您也可以认为运行可执行文件或脚本是对事件的首选响应。可执行文件运行后，您可以采取其他步骤响应事件。

查看屏幕通知

您可以通过三种方式查看屏幕上的通知：

- 在“**监控和报告**”→“**通知**”区域中。这里，您可以查看预定义类别的通知。
- 您可以打开单独的窗口。此种情况下，您可以标记通知为已查看。
- 在“**监控和报告**”→“**控制板**”区域上的“**所选严重级别的通知**”小组件中。在小组件中，可以仅查看处于“*严重*”和“*警告*”重要级别的事件通知。

您可以执行操作，例如，可以响应事件。

要查看预定义类别的通知：

1. 在主菜单中，转到“**监控和报告**” → “**通知**”。
   在左侧面板选择“**所有通知**”类别，在右侧面板显示所有通知。
2. 在左侧面板，选择类别之一：
   - **部署**
   - **设备**
   - **保护**
   - **更新**（这包括有关可下载的 Kaspersky 应用程序的通知和有关已下载的反病毒数据库更新的通知）
   - **漏洞利用防御**
   - **管理服务器**（这仅包含管理服务器相关事件）
   - **有用链接**（这包括 Kaspersky 资源的链接，例如 Kaspersky 技术支持、Kaspersky 论坛、授权许可续费页面或 Kaspersky IT 百科全书）
   - **卡巴斯基新闻**（这包括 Kaspersky 应用程序发布信息）

   所选类别的通知列表被显示。列表包含以下：

- 与通知主题相关的图标：部署 ()、保护 ()、更新 ()、设备管理 ()、漏洞利用防御 ()、管理服务器 ()。
- “通知”重要级别。显示以下重要级别的通知：**关键通知** ()、**警告通知** ()、**信息通知**。列表中的通知按重要级别分组。
- **通知**。这包含通知描述。
- **操作**。这包含建议您执行的快速操作链接。例如，通知点击该链接，您可以转到存储库并安装安全应用程序到设备，或查看设备列表或事件列表。您为通知执行推荐操作之后，该通知被分配*已查看*状态。
- **注册的状态**。这包含从通知被注册到管理服务器到现在为止过去的天数或小时数。

要在单独的窗口中按重要级别查看屏幕通知：

1. 在 Kaspersky Security Center Web Console 的右上角，点击旗帜图标()。

   如果旗帜图标具有红点，表示有未查看的通知。

   列出通知的窗口被打开。默认情况下，将选择“**所有通知**”选项卡，并且通知按重要级别分组：“*严重*”、“*警告*”和“*信息*”。
2. 选择“**系统**”选项卡。
   将显示“*严重*”() 和“*警告*”() 重要级别通知的列表。通知列表包含以下：
   - 颜色标记。严重通知标记为红色。警告通知标记为黄色。
   - 指示通知主题的图标：部署 ()、保护 ()、更新 ()、设备管理 ()、漏洞利用防御 ()、管理服务器 ()。

- 通知描述。
- 旗帜图标。旗帜图标是灰色的，如果通知被分配了*未查看*状态。当您选择灰色旗帜图标并分配*已查看*状态到通知时，图标更改颜色到白色。
- 推荐操作的链接。单击该链接后执行推荐操作时，通知的状态为*已查看*。
- 从通知被注册到管理服务器到现在为止过去的天数。

3. 选择“**更多**”选项卡。

   将显示“*信息*”重要级别通知的列表。

   该列表的组织与“**系统**”选项卡上的列表相同（请参见上面说明）。仅有的不同是没有颜色标记。

您可以通过注册在管理服务器上的日期间隔来筛选通知。使用“**显示过滤器**”复选框来管理筛选器。

要在部件上查看屏幕通知：

1. 在“**控制板**”区域中，选择“**添加或还原 Web 小部件**”。
2. 在打开的窗口中，单击“**其他**”类别，选择“**所选严重级别的通知**”小组件，然后单击“添加”。

   该小组件现在显示在“**控制板**”选项卡上。默认情况下，小组件上显示“*严重*”重要级别的通知。

   您可以点击小组件上的“**设置**”按钮并更改小组件设置以查看“*警告*”重要级别的通知。或者，您可以添加另一个小组件：**所选严重级别的通知**，带有“*警告*”重要级别。

   部件上的通知列表由尺寸限制并包含两个通知。这两个通知是关于最近事件的。

部件上的通知列表包含以下：

- 与通知主题相关的图标：部署 ()、保护 ()、更新 ()、设备管理 ()、漏洞利用防御 ()、管理服务器 ()。
- 通知描述和推荐操作的链接。单击该链接后执行推荐操作时，通知的状态为*已查看*。
- 从通知被注册到管理服务器到现在为止过去的天数或小时数。
- 到其他通知的链接。单击该链接后，您将转到“**监控和报告**”区域的“**通知**”区域中的通知视图。

About device statuses

Kaspersky Security Center Linux assigns a status to each managed device. The particular status depends on whether the conditions defined by the user are met. In some cases, when assigning a status to a device, Kaspersky Security Center Linux takes into consideration the device's visibility flag on the network (see the table below). If Kaspersky Security Center Linux does not find a device on the network within two hours, the visibility flag of the device is set to *Not Visible*.

The statuses are the following:

- *Critical* or *Critical/Visible*
- *Warning* or *Warning/Visible*
- *OK* or *OK/Visible*

The table below lists the default conditions that must be met to assign the *Critical* or *Warning* status to a device, with all possible values.

Conditions for assigning a status to a device

Condition	Condition description	Available values
安全应用程序未安装	Network Agent is installed on the device, but a security application is not installed.	• Toggle button is on. • Toggle button is off.
检测到太多病毒	Some viruses have been found on the device by a task for virus detection, for example, the Malware scan task, and the number of viruses found exceeds the specified value.	More than 0.
实时保护级别与管理员设置的级别不同	The device is visible on the network, but the real-time protection level differs from the level set (in the condition) by the administrator for the device status.	• Stopped. • Paused. • Running.
恶意软件扫描已长时间未执行	The device is visible on the network and a security application is installed on the device, but neither the *Malware scan* task nor a local scan task has been run within the specified time interval. The condition is applicable only to devices that were added to the Administration Server database 7 days ago or earlier.	More than 1 day.
数据库已过期	The device is visible on the network and a security application is installed on the device, but the anti-virus databases have not been updated on this device within the specified time interval. The condition is applicable only to devices that were added to the Administration Server database 1 day ago or earlier.	More than 1 day.
长时间没有连接	Network Agent is installed on the device, but the device has not connected to an Administration Server within the specified time interval, because the device was turned off.	More than 1 day.
检测到活动威胁	The number of unprocessed objects in the 活动威胁 folder exceeds the specified value.	More than 0 items.
需要重新启动	The device is visible on the network, but an application requires the device restart longer than the specified time interval and for one of the selected reasons.	More than 0 minutes.
安装了不兼容的应用程序	The device is visible on the network, but software inventory performed through Network Agent has detected incompatible applications installed on the device.	• Toggle button is off. • Toggle button is on.
授权许可已过期	The device is visible on the network, but the license has expired.	• Toggle button is off. • Toggle button is on.

授权许可即将过期	The device is visible on the network, but the license will expire on the device in less than the specified number of days.	More than 0 days.
无效的加密状态	Network Agent is installed on the device, but the device encryption result is equal to the specified value.	• Does not comply with the policy due to the user's refusal (for external devices only). • Does not comply with the policy due to an error. • Restart is required when applying the policy. • No encryption policy is specified. • Not supported. • When applying the policy.
检测到未处理的安全问题	Some unprocessed security issues have been found on the device. Security issues can be created either automatically, through managed Kaspersky applications installed on the client device, or manually by the administrator.	• Toggle button is off. • Toggle button is on.
应用程序定义的设备状态	The status of the device is defined by the managed application.	• Toggle button is off. • Toggle button is on.
设备磁盘空间不足	Free disk space on the device is less than the specified value or the device could not be synchronized with the Administration Server. The *Critical* or *Warning* status is changed to the *OK* status when the device is successfully synchronized with the Administration Server and free space on the device is greater than or equal to the specified value.	More than 0 MB.
设备已失去管理	During device discovery, the device was recognized as visible on the network, but more than three attempts to synchronize with the Administration Server	• Toggle

	failed.	button is off. • Toggle button is on.
保护已禁用	The device is visible on the network, but the security application on the device has been disabled for longer than the specified time interval. In this case, the state of the security application is *stopped* or *failure*, and differs from the following: *starting*, *running*, or *suspended*.	More than 0 minutes.
安全应用程序没有运行	The device is visible on the network and a security application is installed on the device but is not running.	• Toggle button is off. • Toggle button is on.

Kaspersky Security Center Linux allows you to set up automatic switching of the status of a device in an administration group when specified conditions are met. When the specified conditions are met, the client device is assigned one of the following statuses: *Critical* or *Warning*. When the specified conditions are not met, the client device is assigned the *OK* status.

Different statuses may correspond to different values of one condition. For example, by default, if the 数据库已过期 condition has the **More than 3 days** value, the client device is assigned the *Warning* status; if the value is **More than 7 days**, the *Critical* status is assigned.

If you upgrade Kaspersky Security Center Linux from the previous version, the values of the 数据库已过期 condition for assigning the status to *Critical* or *Warning* do not change.

When Kaspersky Security Center Linux assigns a status to a device, for some conditions (see the Condition description column) the visibility flag is taken into consideration. For example, if a managed device was assigned the *Critical* status because the 数据库已过期 condition was met, and later the visibility flag was set for the device, then the device is assigned the *OK* status.

配置设备状态切换

您可以更改条件以将*严重*或*警告*状态分配给设备。

要启用更改设备状态到严重：

1. 在主菜单中，转到“**资产(设备)**” → “**组层级**”。
2. 在打开的组列表中，单击包含您要更改其设备状态的组名称的链接。
3. 在打开的属性窗口中，选择“**设备状态**”选项卡。
4. 在左侧窗格中，选择“**严重**”。
5. 在右侧窗格的“**设置状态为“严重”，如果这些被指定**”区域中，启用将设备切换为“*严重*”状态的条件。

您只能更改未在在父策略中锁定的设置。

6. 在列表中选中条件旁边的单选按钮。
7. 在列表的左上角，单击“**编辑**”按钮。
8. 为所选条件设置所需的值。
   可以不为每个条件设置值。
9. 单击“**确定**”。

满足指定条件时，受管理设备被分配*严重*状态。

要启用更改设备状态到警告：

1. 在主菜单中，转到“**资产(设备)**” → “**组层级**”。
2. 在打开的组列表中，单击包含您要更改其设备状态的组名称的链接。
3. 在打开的属性窗口中，选择“**设备状态**”选项卡。
4. 在左侧窗格中，选择“**警告**”。
5. 在右侧窗格的“**设置状态为“警告”，如果这些被指定**”区域中，启用将设备切换为“*警告*”状态的条件。

   您只能更改未在在父策略中锁定的设置。

6. 在列表中选中条件旁边的单选按钮。
7. 在列表的左上角，单击“**编辑**”按钮。
8. 为所选条件设置所需的值。
   可以不为每个条件设置值。
9. 单击“**确定**”。

满足指定条件时，受管理设备被分配*警告*状态。

配置通知传送

您可以配置发生在 Kaspersky Security Center Linux 中的事件的通知。根据选择的通知方法，有以下类型的通知可用：

- 电子邮件—当发生事件时，Kaspersky Security Center Linux 向指定的电子邮件地址发送通知。
- SMS—当发生事件时，Kaspersky Security Center Linux 向指定的电话号码发送通知。
- 可执行文件—当事件发生时，可执行文件被运行在管理服务器。

要配置发生在 Kaspersky Security Center Linux 中的事件的通知传送：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ()。
   管理服务器属性窗口打开，**常规**选项卡被选中。
2. 单击“**通知**”区域，在右侧窗格中选择所需通知方法的选项卡：
   - 电子邮件

“**电子邮件**”选项卡允许您配置通过电子邮件发送的事件通知。

在“**SMTP 服务器**”字段中，指定邮件服务器地址，以分号分隔。您可以使用下列值：

- IPv4 或 IPv6 地址
- SMTP 服务器的 DNS 名称

在“**SMTP 服务器端口**”字段中，指定 SMTP 服务器通信端口号。默认端口号是 25。

如果启用“**使用 DNS MX 查找**”选项，则可以将多个 IP 地址 MX 记录用于同一个 SMTP 服务器 DNS 名称。同一 DNS 名称可能有多个 MX 记录，这些记录具有不同的电子邮件接收优先级。管理服务器将尝试按 MX 记录优先级的升序向 SMTP 服务器发送电子邮件通知。

如果启用“**使用 DNS MX 查找**”选项但不启用 TLS 设置，建议您将服务器设备上的 DNSSEC 设置用作发送电子邮件通知的额外保护措施。

如果启用“**使用 ESMTP 身份验证**”选项，则可以在“**用户名**”和“**密码**”字段中指定 ESMTP 身份验证设置。默认情况下，该选项被禁用，ESMTP 身份验证设置不可用。

您可以指定 SMTP 服务器连接的 TLS 设置：

- **不使用 TLS**

如果要禁用电子邮件加密，则可以选择此选项。

- **如果 SMTP 服务器支持则使用 TLS**

如果要使用 TLS 连接到 SMTP 服务器，则可以选择此选项。如果 SMTP 服务器不支持 TLS，则管理服务器不使用 TLS 连接 SMTP 服务器。

- **始终使用 TLS，检查服务器证书的有效性**

如果要使用 TLS 身份验证设置，则可以选择此选项。如果 SMTP 服务器不支持 TLS，则管理服务器无法连接 SMTP 服务器。

建议使用此选项以更好地保护与 SMTP 服务器的连接。如果选择此选项，则可以设置 TLS 连接的身份验证设置。

如果您选择“**始终使用 TLS，检查服务器证书的有效性**”值，则可以指定用于 SMTP 服务器身份验证的证书，并选择要允许通过任意版本的 TLS 还是仅允许通过 TLS 1.2 或更高版本进行通信。此外，还可以指定用于 SMTP 服务器上客户端身份验证的证书。

您可以单击“**指定证书**”链接来指定用于 TLS 连接的证书：

- 浏览 SMTP 服务器证书文件：

您可以接收含有受信任证书颁发机构的证书列表的文件，并将该文件上传到管理服务器。Kaspersky Security Center Linux 会检查 SMTP 服务器的证书是否也具有受信任证书颁发机构的签名。如果 SMTP 服务器的证书不是从受信任证书颁发机构接收的，Kaspersky Security Center Linux 将无法连接到 SMTP 服务器。

- 浏览客户端证书文件：

您可以使用从任何来源（例如，从任何受信任证书颁发机构）收到的证书。您必须指定以下证书类型之一的证书及其私钥：

- X-509 证书：

您必须指定一个证书文件和一个私钥文件。这两个文件不相互依赖，文件的加载顺序也不重要。加载这两个文件时，必须指定用于解码私钥的密码。如果私钥未编码，则密码可以为空值。

- pkcs12 容器：

您必须上传包含证书及其私钥的单个文件。加载该文件时，必须指定用于解码私钥的密码。如果私钥未编码，则密码可以为空值。

单击“**发送测试消息**”按钮允许您检查是否正确配置了通知：应用程序发送测试通知到您指定的电子邮件地址。

在“**收件人(电子邮件地址)**”字段中，指定应用程序将通知发送到的电子邮件地址。您可以在该字段指定多个地址，以分号分隔。

在“**主题**”字段中，指定电子邮件主题。您可以置此字段为空。

在“**主题模板**”下拉列表中，选择主题的模板。由所选模板确定的变量自动放置在“**主题**”字段中。您可以选择几个邮件模板构建邮件主题。

在“**发件人邮件地址：如果未指定该设置，收件人地址将被使用。 警告：我们不建议您使用虚假邮件地址**”字段中，指定发件人电子邮件地址。如果您将该字段置空，收件人地址被使用。不建议使用虚假邮件地址。

“**通知消息**”字段包含事件发生时应用程序发送的事件信息标准文本。该文本包含代替参数，例如事件名称、设备名称和域名。您可以通过添加其他带有更新事件详情的替代参数编辑消息文本。

> 如果通知文本包含百分号（%）字符，您必须指定两次以允许消息发送。例如，“CPU 负载是 100%%”。

单击“**配置通知限制数**”链接允许您指定应用程序在指定时间段可以发送的最大通知数量。

- SMS

“**SMS**”选项卡允许您配置将各种事件的 SMS 通知传输到手机。SMS 消息通过邮件网关发送。

在“**SMTP 服务器**”字段中，指定邮件服务器地址，以分号分隔。您可以使用下列值：

- IPv4 或 IPv6 地址
- SMTP 服务器的 DNS 名称

在“**SMTP 服务器端口**”字段中，指定 SMTP 服务器通信端口号。默认端口号是 25。

如果启用“**使用 ESMTP 身份验证**”选项，则可以在“**用户名**”和“**密码**”字段中指定 ESMTP 身份验证设置。默认情况下，该选项被禁用，ESMTP 身份验证设置不可用。

您可以指定 SMTP 服务器连接的 TLS 设置：

- **不使用 TLS**

如果要禁用电子邮件加密，则可以选择此选项。

- **如果 SMTP 服务器支持则使用 TLS**

如果要使用 TLS 连接到 SMTP 服务器，则可以选择此选项。如果 SMTP 服务器不支持 TLS，则管理服务器不使用 TLS 连接 SMTP 服务器。

- **始终使用 TLS，检查服务器证书的有效性**

如果要使用 TLS 身份验证设置，则可以选择此选项。如果 SMTP 服务器不支持 TLS，则管理服务器无法连接 SMTP 服务器。

建议使用此选项以更好地保护与 SMTP 服务器的连接。如果选择此选项，则可以设置 TLS 连接的身份验证设置。

如果您选择“**始终使用 TLS，检查服务器证书的有效性**”值，则可以指定用于 SMTP 服务器身份验证的证书，并选择要允许通过任意版本的 TLS 还是仅允许通过 TLS 1.2 或更高版本进行通信。此外，还可以指定用于 SMTP 服务器上客户端身份验证的证书。

您可以单击“**指定证书**”链接来指定 SMTP 服务器证书文件。您可以接收含有受信任证书颁发机构的证书列表的文件，并将该文件上传到管理服务器。Kaspersky Security Center Linux 会检查 SMTP 服务器的证书是否也具有受信任证书颁发机构的签名。如果 SMTP 服务器的证书不是从受信任证书颁发机构接收的，Kaspersky Security Center Linux 将无法连接到 SMTP 服务器。

在“**收件人(电子邮件地址)**”字段中，指定应用程序将通知发送到的电子邮件地址。您可以在该字段指定多个地址，以分号分隔。通知将被传送到指定邮件地址关联的电话号码。

在“**主题**”字段中，指定电子邮件主题。

在“**主题模板**”下拉列表中，选择主题的模板。取决于所选模板的变量放置在“**主题**”字段中。您可以选择几个邮件模板构建邮件主题。

在“**发件人邮件地址：如果未指定该设置，收件人地址将被使用。 警告：我们不建议您使用虚假邮件地址**”字段中，指定发件人电子邮件地址。如果您将该字段置空，收件人地址被使用。不建议使用虚假邮件地址。

在“**SMS 消息收件人电话号码**”字段中，指定短信通知收件人的手机号码。

在“**通知消息**”字段中，指定事件发生时应用程序发送的事件信息文本。该文本可以包含替代参数，例如事件名称、设备名称和域名。

如果通知文本包含百分号（%）字符，您必须指定两次以允许消息发送。例如，“CPU 负载是 100%%”。

单击“**发送测试消息**”可检查是否正确配置了通知：应用程序发送测试通知到您指定的收件人。

单击“**配置通知限制数**”链接可指定应用程序在指定时间段可以发送的最大通知数量。

- 要运行的可执行文件

  如果选择该通知方法，您可以在输入字段指定事件发生时要启动的应用程序。

  在“**当事件发生时要在管理服务器上运行的可执行文件**”字段中指定要运行的文件的文件夹和名称。在指定文件之前，准备文件并指定定义了要在通知消息中发送的事件详细信息的占位符。您指定的文件夹和文件必须位于管理服务器上。

  单击“**配置通知限制数**”链接允许您指定应用程序在指定时间段可以发送的最大通知数量。

3. 在选项卡上，定义通知设置。
4. 单击“**确定**”按钮以关闭管理服务器属性窗口。

保存的通知传送设置被应用到在 Kaspersky Security Center Linux 中发生的所有事件。

您可以在管理服务器设置、策略设置或应用程序设置的“**事件配置**“区域中覆盖某些事件的通知传送设置。

测试通知

为了检查事件通知是否可以发送，程序将在客户端设备上使用 Eicar 测试病毒检测通知。

要验证事件通知的发送，请执行以下操作：

1. 停止客户端设备上的实时文件系统保护任务，将 EICAR 测试病毒复制到客户端设备。然后，重新启用文件系统的实时保护。
2. 为管理组中的客户端设备或特定设备运行扫描任务，包括带有 EICAR病毒的设备。

   如果扫描任务配置正确，程序会检测到测试病毒。如果通知配置正确，您将收到检测到病毒的通知。

要打开测试病毒检测记录：

1. 在主菜单中，转到“**监控和报告**” → “**事件分类**”。
2. 单击“**最近事件**”选择项名称。

   在打开的窗口中，将显示有关测试病毒的通知。

EICAR 测试病毒不包含任何危害您设备的代码。不过，多数厂商的安全应用程序都将该文件视为病毒。您可以从 EICAR 官方网站上下载该测试病毒。

通过运行可执行文件显示的事件通知

Kaspersky Security Center Linux 可通过运行可执行文件将客户端设备上的事件通知管理员。可执行文件必须包含另外一个可执行文件，而后者具有要转发给管理员的事件的占位符。

描述事件的占位符

占位符	占位符描述
%SEVERITY%	事件重要性级别

%COMPUTER%	发生事件的设备的名称
%DOMAIN%	域
%EVENT%	事件
%DESCR%	事件描述
%RISE_TIME%	创建时间
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	任务名称
%KL_PRODUCT%	网络代理
%KL_VERSION%	网络代理版本号
%HOST_IP%	IP 地址
%HOST_CONN_IP%	计算机 IP 地址

例如：
事件通知由某个可执行文件（例如，script1.bat）发出，在该可执行文件中，将启动具有 %COMPUTER% 占位符的另一个可执行文件（例如，script2.bat）。当发生事件时，将在管理员的设备上运行 script1.bat 文件，而该文件随后运行具有 %COMPUTER% 占位符的 script2.bat 文件。管理员将接收到发生事件的设备的名称。

卡巴斯基公告

本节介绍如何使用、配置和禁用卡巴斯基公告。

About Kaspersky announcements

The Kaspersky announcements section (监控和报告 → **Kaspersky announcements**) keeps you informed by providing information related to your version of Kaspersky Security Center Linux and the managed applications installed on the managed devices. Kaspersky Security Center Linux periodically updates the information in the section by removing outdated announcements and adding new information.

Kaspersky Security Center Linux shows only those Kaspersky announcements that relate to the currently connected Administration Server and the Kaspersky applications installed on the managed devices of this Administration Server. The announcements are shown individually for any type of Administration Server—primary, secondary, or virtual.

Administration Server must have an internet connection to receive Kaspersky announcements.

The announcements include information of the following types:

- Security-related announcements

  Security-related announcements are intended to keep the Kaspersky applications installed in your network up-to-date and fully functional. The announcements may include information about critical updates for Kaspersky applications, fixes for found vulnerabilities, and ways to fix other issues in Kaspersky applications. By default, security-related announcements are enabled. If you do not want to receive the announcements, you can disable this feature.

To show you the information that corresponds to your network protection configuration, Kaspersky Security Center Linux sends data to Kaspersky cloud servers and receives only those announcements that relate to the Kaspersky applications installed in your network. The data set that can be sent to the servers is described in the End User License Agreement that you accept when you install Kaspersky Security Center Administration Server.

- Marketing announcements

  Marketing announcements include information about special offers for your Kaspersky applications, advertisements, and news from Kaspersky. Marketing announcements are disabled by default. You receive this type of announcements only if you enabled Kaspersky Security Network (KSN). You can disable marketing announcements by disabling KSN.

  To show you only relevant information that might be helpful in protecting your network devices and in your everyday tasks, Kaspersky Security Center Linux sends data to Kaspersky cloud servers and receives the appropriate announcements. The data set that can be sent to the servers is described in the Processed Data section of the KSN Statement.

New information is divided into the following categories, according to importance:

1. Critical info
2. Important news
3. Warning
4. Info

When new information appears in the Kaspersky announcements section, Kaspersky Security Center Web Console displays a notification label that corresponds to the importance level of the announcements. You can click the label to view this announcement in the Kaspersky announcements section.

You can specify the Kaspersky announcements settings, including the announcement categories that you want to view and where to display the notification label. If you do not want to receive announcements, you can disable this feature.

Specifying Kaspersky announcements settings

In the Kaspersky announcements section, you can specify the Kaspersky announcements settings, including the categories of the announcements that you want to view and where to display the notification label.

To configure Kaspersky announcements:

1. In the main menu, go to 监控和报告 → 卡巴斯基通告.
2. Click the **Settings** link.

   The Kaspersky announcement settings window opens.
3. Specify the following settings:

   - Select the importance level of the announcements that you want to view. The announcements of other categories will not be displayed.
   - Select where you want to see the notification label. The label can be displayed in all console sections, or in the 监控和报告 section and its subsections.

4. Click the **OK** button.

   The Kaspersky announcement settings are specified.

Disabling Kaspersky announcements

The Kaspersky announcements section (监控和报告 → **Kaspersky announcements**) keeps you informed by providing information related to your version of Kaspersky Security Center Linux and managed applications installed on the managed devices. If you do not want to receive Kaspersky announcements, you can disable this feature.

The Kaspersky announcements include two types of information: security-related announcements and marketing announcements. You can disable the announcements of each type separately.

To disable security-related announcements:

1. In the main menu, click the settings icon ( ) next to the name of the required Administration Server.

   The Administration Server properties window opens.

2. On the 常规 tab, select the **Kaspersky announcements** section.

3. Switch the toggle button to the **Security-related announcements are disabled** position.

4. Click the 保存 button.

   Kaspersky announcements are disabled.

Marketing announcements are disabled by default. You receive marketing announcements only if you enabled Kaspersky Security Network (KSN). You can disable this type of announcement by disabling KSN.

To disable marketing announcements:

1. In the main menu, click the settings icon ( ) next to the name of the required Administration Server.

   The Administration Server properties window opens.

2. On the 常规 tab, select the **KSN 代理设置** section.

3. Disable the 使用卡巴斯基安全网络已启用 option.

4. Click the 保存 button.

   Marketing announcements are disabled.

Exporting events to SIEM systems

This section describes how to configure export of events to the SIEM systems.

方案：配置导出事件到 SIEM 系统

Kaspersky Security Center Linux 允许配置通过以下方法之一导出事件到 SIEM 系统：导出到任何使用 Syslog 格式的 SIEM 系统或直接从 Kaspersky Security Center 数据库导出事件到 SIEM 系统。完成此方案后，管理服务器会自动将事件发送到 SIEM 系统。

先决条件

在开始配置 Kaspersky Security Center Linux 中的事件导出之前：

- 了解有关事件导出方法的更多信息。
- 确保拥有系统设置的值。

> 您可以按任意顺序执行此方案的步骤。

将事件导出到 SIEM 系统的过程包括以下步骤：

- **配置 SIEM 系统以接收来自 Kaspersky Security Center Linux 的事件。**

  说明：配置 SIEM 系统中的事件导出

- **选择要导出到 SIEM 系统的事件**

  标记要导出到 SIEM 系统的事件。首先，标记所有受管理卡巴斯基应用程序中发生的常规事件。然后，可以标记特定受管理卡巴斯基应用程序的事件。

- **配置导出事件到 SIEM 系统**

  您可以使用以下方法之一导出事件：

  - 使用 TCP/IP、UDP 或 TLS over TCP 协议
  - 使用直接从 Kaspersky Security Center 数据库导出事件（Kaspersky Security Center 数据库中提供了一组公共视图；您可以在 klakdb.chm 文档中找到这些公共视图的描述。）

结果

配置导出事件到 SIEM 系统后，如果您选择了要导出的事件，可以查看导出结果。

在您开始之前

当设置在 Kaspersky Security Center Linux 中自动导出事件时，必须指定一些 SIEM 系统设置。建议您提前检查这些设置，以便准备设置 Kaspersky Security Center Linux。

要成功配置自动发送事件到 SIEM 系统，您必须知道以下设置：

- **SIEM 系统服务器地址**

  > 安装了当前使用的 SIEM 系统的服务器的 IP 地址。在您的 SIEM 系统设置中检查此值。

- **SIEM 系统服务器端口**

用于在 Kaspersky Security Center Linux 和 SIEM 系统服务器之间建立连接的端口号。在 Kaspersky Security Center Linux 设置和 SIEM 系统的接收设置中指定该值。

- 协议

  用于从 Kaspersky Security Center Linux 传输消息到您的 SIEM 系统的协议。在 Kaspersky Security Center Linux 设置和 SIEM 系统的接收设置中指定该值。

关于事件导出

Kaspersky Security Center Linux 允许您接收受管理设备上安装的管理服务器和 Kaspersky 应用程序在操作期间发生的事件信息。事件信息保存在管理服务器数据库。

您可以在处理组织和技术级别的安全问题的集中式系统内使用事件导出，提供安全监控服务，以及合并来自不同解决方案的信息。即是提供对网络硬件和应用程序生成的安全警告的实时分析的 SIEM 系统，或者安全操作中心 (SOC)。

这些系统可以从许多源接收数据，包括网络、安全、服务器、数据库和应用程序。SIEM 系统也提供功能以集成监控的数据，以便帮助您避免丢失关键事件。而且，系统执行相关事件和警告的自动分析以通知管理员安全问题。警告可以通过仪表盘实现，或可以通过第三方渠道发送，例如邮件。

从 Kaspersky Security Center Linux 导出事件到外部 SIEM 系统的进程设计两部分：事件发送者，Kaspersky Security Center 和事件接收者，SIEM 系统。要成功导出事件，您必须在 SIEM 系统和 Kaspersky Security Center Linux 中进行配置。您可以先配置任意一端。您可以配置 Kaspersky Security Center Linux 中的事件传输，然后配置 SIEM 系统对事件的接收，或者相反。

事件导出的 Syslog 格式

您可以将 Syslog 格式的事件发送到任何 SIEM 系统。使用 Syslog 格式，您可以转发在管理服务器上和在受管理设备上安装的卡巴斯基应用程序中发生的任意事件。导出 Syslog 格式的事件时，您可以准确选择将转发到 SIEM 系统的事件类型。

通过 SIEM 系统接收事件

SIEM 系统必须接收和正确解析来自 Kaspersky Security Center Linux 的事件。因为这些目的，您必须正确配置 SIEM 系统。配置取决于特定的 SIEM 系统。然而，有一些配置所有 SIEM 系统的通用步骤，例如配置接收器和解析器。

关于配置 SIEM 系统中的事件导出

从 Kaspersky Security Center Linux 导出事件到外部 SIEM 系统的进程设计两部分：事件发送者，Kaspersky Security Center 和事件接收者，SIEM 系统。必须在 SIEM 系统和 Kaspersky Security Center Linux 中配置事件导出。

您在 SIEM 系统中指定的设置取决于您使用的系统。通常，对于所有 SIEM 系统，您必须设置接收器和消息解析器（可选）以解析接收的事件。

设置接收器

为了接收 Kaspersky Security Center Linux 发送的事件，您必须在您的 SIEM 系统中设置接收器。通常，必须在 SIEM 系统指定以下设置：

- **导出协议**

  消息传输协议，UDP、TCP 或 TLS over TCP。该协议必须与您在 Kaspersky Security Center Linux 中指定的协议相同。

- **端口**

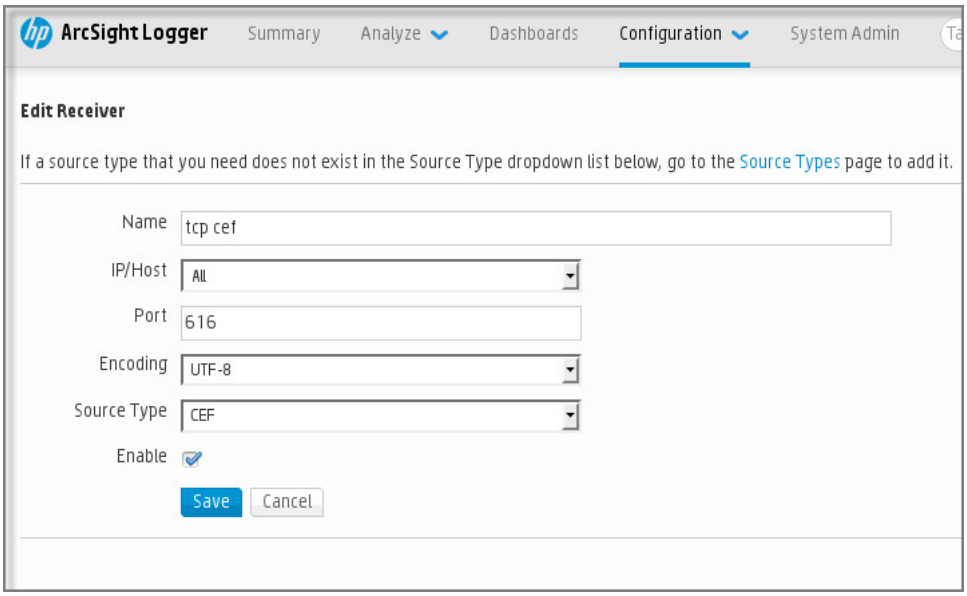
  指定用于连接到 Kaspersky Security Center Linux 的端口号。该端口必须与您在配置 SIEM 系统期间在 Kaspersky Security Center Linux 中指定的端口相同。

- **数据格式**

  指定 Syslog 格式。

根据所使用的 SIEM 系统，您可能需要指定一些附加接收器设置。

下图显示了 ArcSight 的接收器设置截图。



ArcSight 的接收器设置

消息解析器

导出的事件作为消息被传递到 SIEM 系统。这些消息必须正确解析，以便事件信息可以被 SIEM 系统使用。消息解析器是 SIEM 系统的一部分，它们用于拆分消息内容到相关字段，例如事件 ID、严重级别、描述、参数等等。这将启用 SIEM 系统以处理从 Kaspersky Security Center Linux 接收的事件，以便它们可以被存储在 SIEM 系统数据库。

Marking of events for export to SIEM systems in Syslog format

This section describes how to mark events for further export to SIEM systems in Syslog format.

关于标记要以 Syslog 格式导出到 SIEM 系统的事件

在启用自动导出事件后，您必须选择将被导出到外部 SIEM 系统的事件。

您可以配置基于以下条件之一导出 Syslog 格式的事件到外部系统：

- 标记常规事件。如果在事件设置或管理服务器设置中标记要在策略中导出的事件，SIEM 系统将接收由特定策略管理的所有应用程序中发生的所标记事件。如果导出的事件在策略中被选中，您将不能为由该策略管理的个别应用程序重新定义所选事件。
- 为受管理应用程序标记事件。如果为受管理设备上安装的受管理应用程序选择要导出的事件，SIEM 系统将仅接收该应用程序中发生的事件。

Marking events of a Kaspersky application for export in the Syslog format

If you want to export events that occurred in a specific managed application installed on the managed devices, mark the events for export in the application policy. In this case, the marked events are exported from all of the devices included in the policy scope.

To mark events for export for a specific managed application:

1. In the main menu, go to 资产(设备) → 策略和配置文件.
2. Click the policy of the application for which you want to mark events.

   The policy settings window opens.
3. Go to the 事件配置 section.
4. Select the check boxes next to the events that you want to export to a SIEM system.
5. Click the 使用 **Syslog** 标记以导出到 **SIEM** 系统 button.

   You can also mark an event for export to a SIEM system in the 事件注册 section, which opens by clicking the link of the event.
6. A check mark (✓) appears in the **Syslog** column of the event or events that you marked for export to the SIEM system.
7. Click the 保存 button.

The marked events from the managed application are ready to be exported to a SIEM system.

You can mark which events to export to a SIEM system for a specific managed device. If previously exported events were marked in an application policy, you will not be able to redefine the marked events for a managed device.

To mark events for export for a managed device:

1. In the main menu, go to 资产(设备) → 受管理设备.

The list of managed devices is displayed.

2. Click the link with the name of the required device in the list of managed devices.

   The properties window of the selected device is displayed.

3. Go to the 应用程序 section.

4. Click the link with the name of the required application in the list of applications.

5. Go to the 事件配置 section.

6. Select the check boxes next to the events that you want to export to SIEM.

7. Click the 使用 **Syslog** 标记以导出到 **SIEM** 系统 button.

   Also, you can mark an event for export to a SIEM system in the 事件注册 section, that opens by clicking the link of the event.

8. A check mark (✓) appears in the **Syslog** column of the event or events that you marked for export to the SIEM system.

From now on, Administration Server sends the marked events to the SIEM system if export to the SIEM system is configured.

Marking general events for export in Syslog format

You can mark general events that Administration Server will export to SIEM systems by using the Syslog format.

To mark general events for export to a SIEM system:

1. Do one of the following:

   - In the main menu, click the settings icon (⚙) next to the name of the required Administration Server.
   - In the main menu, go to 资产**(**设备**)** → 策略和配置文件, and then click a link of a policy.

2. In the window that opens, go to the 事件配置 tab.

3. Click 使用 **Syslog** 标记以导出到 **SIEM** 系统.

   Also, you can mark an event for export to SIEM system in the 事件注册 section, that opens by clicking the link of the event.

4. A check mark (✓) appears in the **Syslog** column of the event or events that you marked for export to the SIEM system.

From now on, Administration Server sends the marked events to the SIEM system if export to the SIEM system is configured.

关于使用 Syslog 格式导出事件

您可以使用 Syslog 格式将管理服务器和受管理设备上安装的其他 Kaspersky 应用程序中发生的事件导出到 SIEM 系统。

Syslog 是消息记录协议的标准。它允许分离生成消息的软件、存储消息的系统和报告和分析消息的软件。每个消息都带有设备代码标签，指示生成消息的软件类型，并被分配严重级别。

Syslog 格式由 Request for Comments (RFC) 文档定义，该文档由 Internet Engineering Task Force（互联网标准）发布。RFC 5424 标准用于从 Kaspersky Security Center Linux 导出事件到外部系统。

在 Kaspersky Security Center Linux 中，您可以配置使用 Syslog 格式导出事件到外部系统。

导出过程包含两个步骤：

1. 启用自动事件导出。在该步骤，Kaspersky Security Center Linux 被配置，以便能发送事件到 SIEM 系统。Kaspersky Security Center Linux 在您启用自动导出后立即开始发送事件。
2. 选择事件以导出到外部系统。在该步骤，您可以选择导出哪些事件到 SIEM 系统。

Configuring Kaspersky Security Center Linux for export of events to a SIEM system

To export events to a SIEM system, you have to configure the process of export in Kaspersky Security Center Linux.

To configure export to SIEM systems in the Kaspersky Security Center Web Console:

1. In the main menu, click the settings icon ( ) next to the name of the required Administration Server.

   The Administration Server properties window opens.

2. On the 常规 tab, select the **SIEM** section.
3. Click the 设置 link.

   The 导出设置 section opens.

4. Specify the settings in the 导出设置 section:

   - SIEM 系统服务器地址

     The IP address of the server on which the currently used SIEM system is installed. Check this value in your SIEM system settings.

   - SIEM 系统端口

     Port number used to establish a connection between Kaspersky Security Center Linux and your SIEM system server. You specify this value in the Kaspersky Security Center Linux settings and in the receiver settings of your SIEM system.

- 协议

Select the protocol to be used for transferring messages to the SIEM system. You can select either the TCP/IP, UDP, or TLS over TCP protocol.

Specify the following TLS settings if you select the TLS over TCP protocol:

- 服务器身份验证

  In the 服务器身份验证 field, you can select the **Trusted certificates** or **SHA fingerprints** values:

  - **Trusted certificates**. You can receive a file with the list of certificates from a trusted certification authority (CA) and upload the file to Kaspersky Security Center Linux. Kaspersky Security Center Linux checks whether the certificate of the SIEM system server is also signed by a trusted CA or not.

    To add a trusted certificate, click the **Browse for CA certificates file** button, and then upload the certificate.

  - **SHA fingerprints**. You can specify SHA-1 thumbprints of the SIEM system certificates in Kaspersky Security Center Linux. To add a SHA-1 thumbprint, enter it in the 指纹 field, and then click the 添加 button.

  By using the 添加客户端身份验证 setting, you can generate a certificate to authenticate Kaspersky Security Center Linux. Thus, you will use a self-signed certificate issued by Kaspersky Security Center Linux. In this case, you can use both a trusted certificate and a SHA fingerprint to authenticate the SIEM system server.

- 添加主题名称/主题备选名称

  Subject name is a domain name for which the certificate is received. Kaspersky Security Center Linux cannot connect to the SIEM system server if the domain name of the SIEM system server does not match the subject name of the SIEM system server certificate. However, the SIEM system server can change its domain name if the name has changed in the certificate. In this case, you can specify subject names in the 添加主题名称/主题备选名称 field. If any of the specified subject names matches the subject name of the SIEM system certificate, Kaspersky Security Center Linux validates the SIEM system server certificate.

- 添加客户端身份验证

  For client authentication, you can insert your certificate or generate it in Kaspersky Security Center Linux.

  - 插入证书. You can use a certificate that you received from any source, for example, from any trusted CA. You must specify the certificate and its private key by using one of the following certificate types:

    - **X.509** 证书 **PEM**. Upload a file with a certificate in the 证书文件 field, and a file with a private key in the 密钥文件 field. Both files do not depend on each other and the order of loading the files is not significant. When both files are uploaded, specify the password for decoding the private key in the 密码或证书验证 field. The password can have an empty value if the private key is not encoded.

    - **X.509** 证书 **PKCS12**. Upload a single file that contains a certificate and its private key in the 证书文件 field. When the file is uploaded, specify the password for decoding the private key in the 密码或证书验证 field. The password can have an empty value if the private key is not encoded.

  - 生成密钥. You can generate a self-signed certificate in Kaspersky Security Center Linux. As a result, Kaspersky Security Center Linux stores the generated self-signed certificate, and you can

pass the public part of the certificate or SHA1-fingerprint to the SIEM system.

5. If you want, you can export archived events from the Administration Server database and set the start date from which you want to start the export of archived events:

   a. Click the 设置导出起始日期 link.

   b. In the section that opens, specify the start date in the 导出的起始日期 field.

   c. Click the 确定 button.

6. Switch the option to the 自动导出事件至 **SIEM** 系统数据库已启用 position.

7. Click the 保存 button.

Export to a SIEM system is configured. From now on, if you configured the receiving of events in a SIEM system, Administration Server exports the marked events to a SIEM system. If you set the start date of export, Administration Server also exports the marked events stored in the Administration Server database from the specified date.

直接从数据库导出事件

您可以直接从 Kaspersky Security Center Linux 数据库接收事件，而不必使用 Kaspersky Security Center Linux 界面。您可以直接查询公共视图并接收事件数据或基于现有公共视图创建您自己的视图并定位它们以获取所需数据。

公共视图

为了您的方便，在 Kaspersky Security Center Linux 数据库中提供了公共视图集。您可以在 klakdb.chm 文档中找到这些公共视图的描述。

v_akpub_ev_event 公共视图包含一组展示数据库中事件参数的字段集。在 klakdb.chm 文档中您也可以查找对应于其他 Kaspersky Security Center Linux 实体的公共视图信息，例如，设备、应用程序或用户。您可以在您的查询中使用该信息。

该部分包含了使用 klsql2 实用工具创建 SQL 查询的说明以及查询例子。

要创建 SQL 查询或数据库视图，您也可以使用其他程序以操作数据库。有关如何查看连接到 Kaspersky Security Center Linux 数据库的参数（例如实例名称和数据库名称）的信息，请参阅相应部分。

使用 klsql2 实用工具创建 SQL 查询

该部分描述了如何使用 klsql2 实用工具，以及如何使用该实用工具创建 SQL 查询。使用安装的 Kaspersky Security Center Linux 版本中包含的 klsql2 实用程序版本。

要使用 klsql2 实用程序：

1. 转到安装了 Kaspersky Security Center 管理服务器的设备上的 /opt/kaspersky/ksc64/sbin/klsql2 目录。

2. 在此目录中，创建 src.sql 空白文件。

3. 在任意文本编辑器中打开 src.sql。

4. 在 src.sql 文件中，键入所需的 SQL 查询，然后保存该文件。

5. 在 Kaspersky Security Center 管理服务器设备上，在命令行，输入以下命令以从 src.sql 文件运行 SQL 查询并保存结果到 result.xml 文件：
   `sudo ./klsql2 -i src.sql -u <用户名> -p <密码> -o result.xml`
   其中 `<username>` 和 `<password>` 是有权访问数据库的用户账户的凭据。

6. 如果需要，输入有权访问数据库的用户账户的登录名和密码。

7. 打开新创建的 result.xml 文件以查看查询结果。

您可以编辑 src.sql 文件并创建到公共视图的任意查询。然后，从命令行，执行您的查询并保存结果到文件。

klsql2 实用工具中的 SQL 查询例子

该部分显示 SQL 查询的例子，通过 klsql2 实用工具创建。

以下例子阐述了对过去七天发生在设备上的事件的获取，并根据事件发生时间显示事件，最近的事件最先显示。

例如：

```
SELECT
e.nId, /* 事件标识 */
e.tmRiseTime, /* 事件发生的时间 */
e.strEventType, /* 事件类型的内部名称 */
e.wstrEventTypeDisplayName, /* 事件的显示名称 */
e.wstrDescription, /* 事件的显示描述 */
e.wstrGroupName, /* 事件所在的组名称 */
h.wstrDisplayName, /* 发生事件的设备的显示名称 */
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 /* 发生事件的设备的 IP 地址 */
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
```

查看 Kaspersky Security Center Linux 数据库名称

如果您要通过 SQL Server、MySQL 或 MariaDB 数据库管理工具访问 Kaspersky Security Center Linux 数据库，您必须知道数据库的名称以便从您的 SQL 脚本编辑器连接。

要查看 Kaspersky Security Center Linux 数据库名称：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ( )。
   管理服务器属性窗口将打开。

2. 在“**常规**”选项卡上，选择“**当前数据库详情**”区域。

数据库名称在“**数据库名称**”字段中指定。使用数据库名称在您的 SQL 查询中定位数据库。

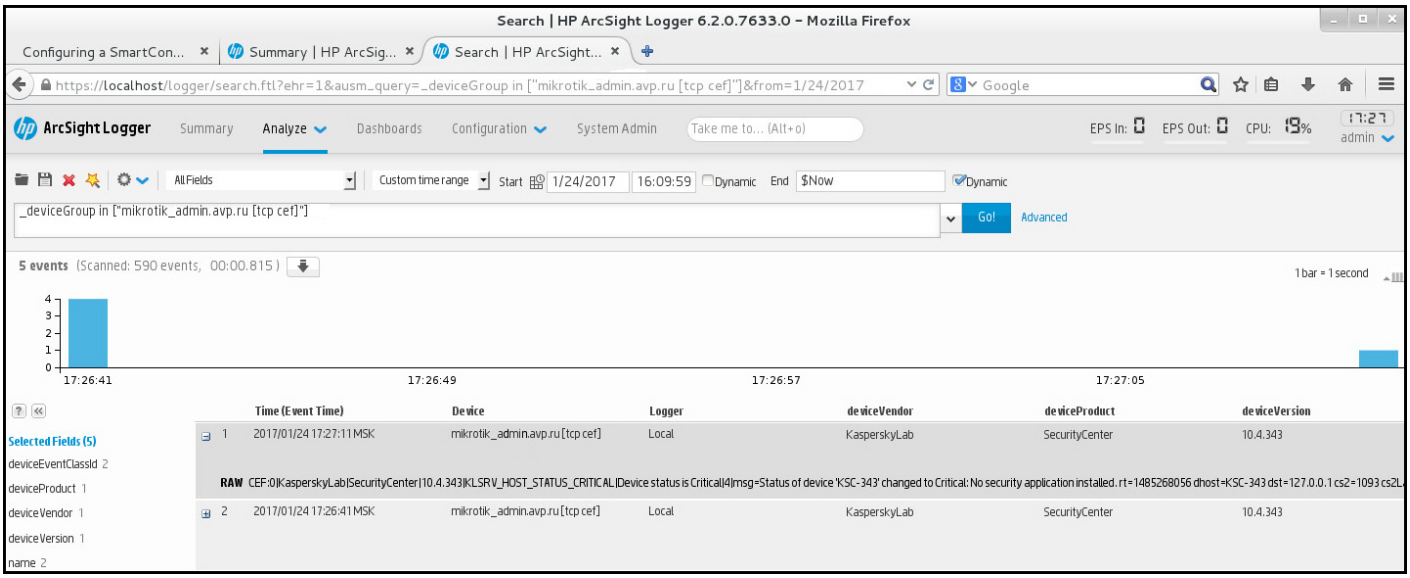
查看导出结果

您可以控制事件导出过程的成功完成。为此，检查带有导出事件的邮件是否被您的 SIEM 系统接收。

如果从 Kaspersky Security Center Linux 发送的事件被接收并被您的 SIEM 系统正确解析，两端的配置被正确完成。否则，检查您在 Kaspersky Security Center Linux 中指定的设置是否与您的 SIEM 系统中的设置一致。

下图显示导出到 ArcSight 的事件。例如，第一个事件是严重的管理服务器事件：“*设备状态为严重*”。

导出事件在您 SIEM 系统中的显示随您使用的 SIEM 系统而不同。



事件例子

管理对象修订

该区域包含了对象修订管理的信息。Kaspersky Security Center Linux 允许跟踪对象修改。您每次保存更改到对象时，*修订*被创建。每个修订都有一个数字。

支持修订管理的应用程序对象包括：

- 管理服务器
- 策略
- 任务
- 管理组
- 用户账户

- 安装包

您可以对对象修订采取以下操作：

- 将所选修订与当前进行比较
- 比较所选的修订
- 将对象与相同类型的其他对象的所选修订进行比较
- 查看所选修订
- 回滚对对象所做的更改到所选的修订
- 保存修订到 .txt 文件

在任何支持修订管理的对象的属性窗口，“**修订历史**”区域显示了包含以下详情的对象修订列表：

- 对象修订版本
- 对象修改的日期和时间
- 修改对象的用户的名称
- 运行在对象上的操作
- 与对象设置更改相关的修订描述

  默认下，对象修订描述为空。要添加描述到修订，请选择相关修订并单击“**描述**”按钮。在“**对象修订描述**”窗口，输入修订描述的文本。

关于对象修订

您可以对对象修订采取以下操作：

- 将所选修订与当前进行比较
- 比较所选的修订
- 将对象与相同类型的其他对象的所选修订进行比较
- 查看所选修订
- 回滚对对象所做的更改到所选的修订
- 保存修订到 .txt 文件

在任何支持修订管理的对象的属性窗口，“**修订历史**”区域显示了包含以下详情的对象修订列表：

- 对象修订版本
- 对象修改的日期和时间
- 修改对象的用户的名称

- 运行在对象上的操作
- 与对象设置更改相关的修订描述

回滚对象到先前修订

如果必要，您可以回滚对对象所做的更改。例如，您可能必须转换策略设置到特定日期的状态。

要回滚对对象所做的更改：

1. 在对象属性窗口中，打开“**修订历史**”选项卡。
2. 在对象修订列表中，选择要回滚更改的修订。
3. 单击**回滚**按钮。
4. 单击“**确定**”以确认操作。

   该对象被回滚到所选修订。对象修订列表显示所做的操作记录。修订描述显示了您转换对象所到的修订号的信息。

回滚操作仅适用于策略和任务对象。

对象删除

该部分提供了关于删除对象和查看已删除对象的信息。

您可以删除对象，包括以下：

- 策略
- 任务
- 安装包
- 虚拟管理服务器
- 用户
- 安全组
- 管理组

当您删除对象时，其信息保留在数据库。已删除对象的信息的存储期限与对象修订的存储期限一致（推荐期限是 90 天）。您仅在权限的**已删除对象**区域具有**修改**权限时才能更改存储期限。

关于删除客户端设备

当您从管理组中删除受管理设备时，应用程序会将设备移至未分配的设备组。删除设备后，已安装的卡巴斯基应用程序——网络代理和安全应用程序（例如 Kaspersky Endpoint Security）——将保留在设备上。

Kaspersky Security Center Linux 根据以下规则处理未分配设备组中的设备：

- 如果您配置了设备移动规则，并且设备符合移动规则的条件，则该设备会根据规则被自动移动到管理组。
- 设备会被存储在未分配的设备组中，并根据设备保留规则自动从组中删除。

  设备保留规则不会影响具有一个或多个使用完整磁盘加密进行加密的驱动器的设备。此类设备不会被自动删除——您只能手动删除它们。如果您需要删除带有加密驱动器的设备，请先解密驱动器，然后再删除该设备。

  当您删除带有加密驱动器的设备时，解密驱动器所需的数据也会被删除。在这种情况下，要解密驱动器，必须满足以下条件：

  - 设备被重新连接到管理服务器以恢复解密驱动器所需的数据。
  - 设备用户记住解密密码。
  - 用于加密驱动器的安全应用程序（例如 Kaspersky Endpoint Security for Windows）仍安装在设备上。

  如果驱动器由卡巴斯基磁盘加密技术加密，您还可以尝试使用 FDERT Restore Utility 恢复数据。

当您从未分配的设备组中手动删除设备时，应用程序会从列表中删除该设备。删除设备后，已安装的卡巴斯基应用程序（如果有）将保留在设备上。然后，如果该设备对管理服务器仍然可见并且您配置了常规网络轮询，Kaspersky Security Center Linux 会在网络轮询期间发现该设备并将其添加回未分配的设备组。因此，最好仅当设备对管理服务器不可见时再手动删除设备。

从隔离区和备份区中下载和删除文件

本节提供有关如何从 Kaspersky Security Center 13.2 Web 控制台的隔离区和备份区中下载和删除文件的信息。

从隔离区和备份区中下载文件

只有满足以下两个条件之一，您才能下载隔离区和备份区中的文件：在设备的设置中启用了**"不断开与管理服务器的连接"**选项，或者正在使用连接网关。否则，下载无法进行。

要将隔离区或备份区中的文件的副本保存到硬盘驱动器，请执行以下操作：

1. 执行以下操作之一：
   - 如果要从隔离区保存文件副本，请在主菜单中转到**操作 → 存储库 → 隔离**。
   - 如果要从备份区保存文件副本，请在主菜单中转到**操作 → 存储库 → 备份**。
2. 在打开的窗口中，选择要下载的文件并单击 **下载**。

下载开始。已放置在客户端设备上隔离区中的文件的副本将被保存到指定的文件夹中。

关于从隔离、备份或活动威胁存储库中删除对象

当客户端设备上安装的卡巴斯基安全应用程序将对象放置到隔离、备份或活动威胁存储库时，它们会将添加对象的信息发送到 Kaspersky Security Center Linux 中的**隔离**、**备份**或者**活动威胁**区域。当您打开其中一个区域时，从列表中选择一个对象并单击“**移除**”按钮，Kaspersky Security Center Linux 将执行以下操作之一或两个操作：

- 从列表中移除选定对象
- 从存储库中删除选定对象

要执行的操作由将选定对象放置到存储库的卡巴斯基应用程序定义。卡巴斯基应用程序在“**条目添加者**”字段中予以指定。有关要执行的操作的详细信息，请参阅卡巴斯基应用程序的文档。

Remote diagnostics of client devices

You can use remote diagnostics for remote execution of the following operations on Windows-based and Linux-based client devices:

- Enabling and disabling tracing, changing the tracing level, and downloading the trace file
- Downloading system information and application settings
- Downloading event logs
- Generating a dump file for an application
- Starting diagnostics and downloading diagnostics reports
- Starting, stopping, and restarting applications

You can use event logs and diagnostics reports downloaded from a client device to troubleshoot problems on your own. Also, if you contact Kaspersky Technical Support, a Technical Support specialist might ask you to download trace files, dump files, event logs, and diagnostics reports from a client device for further analysis at Kaspersky.

Opening the remote diagnostics window

To perform remote diagnostics on Windows-based and Linux-based client devices, you first have to open the remote diagnostics window.

To open the remote diagnostics window:

1. To select the device for which you want to open the remote diagnostics window, perform one of the following:
   - If the device belongs to an administration group, in the main menu, go to 资产(设备) → 受管理设备.
   - If the device belongs to the Unassigned devices group, in the main menu, go to 发现和部署 → 未分配的设备.
2. Click the name of the required device.
3. In the device properties window that opens, select the 高级 tab.
4. In the window that opens, click 远程诊断.

   This opens the 远程诊断 window of a client device. If connection between Administration Server and the client device is not established, the error message displays.

Alternatively, if you need to obtain all diagnostic information about a Linux-based client device at once, you can run the collect.sh script on this device.

Enabling and disabling tracing for applications

You can enable and disable tracing for applications, including Xperf tracing.

Enabling and disabling tracing

To enable or disable tracing on a remote device:

1. Open the remote diagnostics window of a client device.
2. In the remote diagnostics window, select the 卡巴斯基应用程序 tab.
   In the 应用程序管理 section, the list of Kaspersky applications installed on the device displays.
3. In the list of applications, select the application for which you want to enable or disable tracing.
   The list of remote diagnostics options opens.
4. If you want to enable tracing:
   a. In the 跟踪 section, click 启用跟踪.
   b. In the 修改跟踪级别 window that opens, we recommend that you keep the default values of the settings. When required, a Technical Support specialist will guide you through the configuration process. The following settings are available:
      - 跟踪级别
        The tracing level defines the amount of detail that the trace file contains.
      - 基于循环的跟踪
        The application overwrites the tracing information to prevent excessive increase in the size of the trace file. Specify the maximum number of files to be used to store the tracing information, and the maximum size of each file. If the maximum number of trace files of the maximum size are written, the oldest trace file is deleted so that a new trace file can be written.

        This setting is available for Kaspersky Endpoint Security only.
   c. Click 保存.

   The tracing is enabled for the selected application. In some cases, the security application and its task must be restarted in order to enable tracing.

   On Linux-based client devices, tracing for the Updater of Network Agent component is regulated by the Network Agent settings. Therefore, the 启用跟踪 and 修改跟踪级别 options are disabled for this component on client devices running Linux.
5. If you want to disable tracing for the selected application, click the 禁用跟踪 button.
   The tracing is disabled for the selected application.

Enabling Xperf tracing

For Kaspersky Endpoint Security, a Technical Support specialist may ask you to enable Xperf tracing for information about the system performance.

To enable and configure Xperf tracing or disable it:

1. Open the remote diagnostics window of a client device.
2. In the remote diagnostics window, select the 卡巴斯基应用程序 tab.

   In the 应用程序管理 section, the list of Kaspersky applications installed on the device displays.
3. In the list of applications, select Kaspersky Endpoint Security for Windows.

   The list of remote diagnostics options for Kaspersky Endpoint Security for Windows displays.
4. In the **Xpref 跟踪** section, click 启用 **Xperf 跟踪**.

   If Xperf tracing is already enabled, the 禁用 **Xperf 跟踪** button is displayed instead. Click this button if you want to disable Xperf tracing for Kaspersky Endpoint Security for Windows.
5. In the 更改 **Xperf 跟踪级别** window that opens, depending on the request from the Technical Support specialist, do the following:

   a. Select one of the following tracing levels:

   - 轻度级别

     A trace file of this type contains the minimum amount of information about the system.

     By default, this option is selected.

   - 深度级别

     A trace file of this type contains more detailed information than trace files of the *Light* type and may be requested by Technical Support specialists when a trace file of the *Light* type is not enough for the performance evaluation. A *Deep* trace file contains technical information about the system including information about hardware, operating system, list of started and finished processes and applications, events used for performance evaluation, and events from Windows System Assessment Tool.

   b. Select one of the following Xperf tracing types:

   - 基本类型

     The tracing information is received during operation of the Kaspersky Endpoint Security application.

     By default, this option is selected.

   - 重启时类型

     The tracing information is received when the operating system starts on the managed device. This tracing type is effective when the issue that affects the system performance occurs after the device is turned on and before Kaspersky Endpoint Security starts.

   You may also be asked to enable the 循环文件大小**(MB)** option to prevent excessive increase in the size of the trace file. Then specify the maximum size of the trace file. When the file reaches the maximum size, the oldest tracing information is overwritten with new information.

   c. Define the rotation file size.

   d. Click 保存.

Xperf tracing is enabled and configured.

6. If you want to disable Xperf tracing for Kaspersky Endpoint Security for Windows, click 禁用 **Xperf** 跟踪 in the **Xpref** 跟踪 section.

   Xperf tracing is disabled.

Downloading trace files of an application

To download a trace file of an application:

1. Open the remote diagnostics window of a client device.
2. In the remote diagnostics window, select the 卡巴斯基应用程序 tab.

   In the 应用程序管理 section, the list of Kaspersky applications installed on the device displays.
3. In the list of applications, select the application for which you want to download a trace file.
4. In the 跟踪 section, click the 跟踪文件 button.

   This opens the 设备跟踪日志 window, where a list of trace files is displayed.
5. In the list of trace files, select the file that you want to download.
6. Do one of the following:

   - Download the selected file by clicking 下载. You can select one or several files for downloading.
   - Download a portion of the selected file:

     a. Click 下载一部分.

        You cannot download portions of several files at the same time. If you select more than one trace file, the 下载一部分 button will be disabled.

     b. In the window that opens, specify the name and the file portion to download, according to your needs.

        For Linux-based devices, editing the file portion name is not available.

     c. Click 下载.

The selected file, or its portion, is downloaded to the location that you specify.

Deleting trace files

You can delete trace files that are no longer needed.

To delete a trace file:

1. Open the remote diagnostics window of a client device.
2. In the remote diagnostics window that opens, select the 事件日志 tab.

3. In the 跟踪文件 section, click **Windows Update** 日志 or 远程安装日志, depending on which trace files you want to delete.

   The **Windows Update** 日志 link is available only for Windows-based client devices.

   This opens the 设备跟踪日志 window, where a list of trace files is displayed.

4. In the list of trace files, select one or several files that you want to delete.

5. Click the 删除 button.

The selected trace files are deleted.

Downloading application settings

To download application settings from a client device:

1. Open the remote diagnostics window of a client device.

2. In the remote diagnostics window, select the 卡巴斯基应用程序 tab.

3. In the 应用程序设置 section, click the 下载 button to download information about the settings of the applications installed on the client device.

The ZIP archive with information is downloaded to the specified location.

从客户端设备下载系统信息

要从客户端设备下载系统信息：

1. 打开客户端设备的远程诊断窗口。

2. 在远程诊断窗口中，选择**系统信息**选项卡。

3. 单击**下载**按钮可下载有关客户端设备的系统信息。

   如果您获取有关 Linux 设备的系统信息，紧急终止应用程序的转储文件将被添加到结果文件中。

包含信息的文件将被下载到指定位置。

Downloading event logs

To download an event log from a remote device:

1. Open the remote diagnostics window of a client device.

2. In the remote diagnostics window, on the 事件日志 tab, click 所有设备日志.

3. In the 所有设备日志 window, select one or several relevant logs.

4. Do one of the following:

   - Download the selected log by clicking 下载整个文件.
   - Download a portion of the selected log:

     a. Click 下载一部分.

     You cannot download portions of several logs at the same time. If you select more than one event log, the 下载一部分 button will be disabled.

     b. In the window that opens, specify the name and the log portion to download, according to your needs.

     For Linux-based devices, editing the log portion name is not available.

     c. Click 下载.

The selected event log, or a portion of it, is downloaded to the specified location.

Starting, stopping, restarting the application

You can start, stop, and restart applications on a client device.

To start, stop, or restart an application:

1. Open the remote diagnostics window of a client device.
2. In the remote diagnostics window, select the 卡巴斯基应用程序 tab.
   In the 应用程序管理 section, the list of Kaspersky applications installed on the device displays.
3. In the list of applications, select the application that you want to start, stop, or restart.
4. Select an action by clicking one of the following buttons:

   - 停止应用程序

     This button is available only if the application is currently running.

   - 重启应用程序

     This button is available only if the application is currently running.

   - 启动应用程序

     This button is available only if the application is not currently running.

   Depending on the action that you have selected, the required application is started, stopped, or restarted on the client device.

If you restart the Network Agent, a message is displayed stating that the current connection of the device to the Administration Server will be lost.

Running the remote diagnostics of Kaspersky Security Center Linux Network Agent and downloading the results

To start diagnostics for Kaspersky Security Center Linux Network Agent on a remote device and download the results:

1. Open the remote diagnostics window of a client device.
2. In the remote diagnostics window, select the 卡巴斯基应用程序 tab.

   In the 应用程序管理 section, the list of Kaspersky applications installed on the device displays.
3. In the list of applications, select **Kaspersky Security Center Linux Network Agent**.

   The list of remote diagnostics options opens.
4. In the 诊断报告 section, click the 运行诊断 button.

   This starts the remote diagnostics process and generates a diagnostics report. When the diagnostics process is complete, the 下载诊断报告 button becomes available.
5. Click the 下载诊断报告 button to download the report.

The report is downloaded to the specified location.

Running an application on a client device

You may have to run an application on the client device, if a Kaspersky support specialist requests it. You do not have to install the application on that device.

To run an application on the client device:

1. Open the remote diagnostics window of a client device.
2. In the remote diagnostics window, select the 运行远程应用程序 tab.
3. In the 应用程序文件 section, click the 浏览 button to select a ZIP archive containing the application that you want to run on the client device.

   > The ZIP archive must include the utility folder. This folder contains the executable file to be run on a remote device.

   You can specify the executable file name and the command-line arguments, if necessary. To do this, fill in the **Executable file in an archive to be run on a remote device** and 命令行参数 fields.
4. Click the 上传和运行 button to run the specified application on a client device.
5. Follow the instructions of the Kaspersky support specialist.

为应用程序创建内存转储文件

应用程序转储文件允许您查看某个时间点在客户端设备上运行的应用程序的参数。该文件还包含有关为应用程序加载的模块的信息。

生成转储文件仅适用于在 Windows 客户端设备上运行的 32 位进程。对于运行 Linux 的客户端设备和 64 位进程，此功能不受支持。

要为应用程序创建转储文件：

1. 打开客户端设备的远程诊断窗口。
2. 在远程诊断窗口中，选择单击**运行远程应用程序**选项卡。
3. 在**生成进程内存转储文件**区域中，指定要为其生成转储文件的应用程序的可执行文件。
4. 单击**下载**按钮以保存指定应用程序的转储文件。

   如果指定的应用程序未在客户端设备上运行，则会显示错误消息。

在基于 Linux 的客户端设备上运行远程诊断

Kaspersky Security Center Linux 允许您从客户端设备下载基本诊断信息。或者，您可以使用卡巴斯基的 collect.sh 脚本获取有关基于Linux 的设备的诊断信息。该脚本在需要诊断的 Linux 客户端设备上运行，然后生成一个文件，其中包含诊断信息、该设备的系统信息、应用程序的跟踪文件、设备日志以及被紧急终止的应用程序的转储文件。

我们建议您使用 collect.sh 脚本一次性获取有关 Linux 客户端设备的所有诊断信息。如果通过 Kaspersky Security Center Linux 远程下载诊断信息，您将需要浏览远程诊断界面的所有部分。此外，可能无法完全获得 Linux 设备的诊断信息。

如果您需要将生成的包含诊断信息的文件发送给卡巴斯基技术支持，请在发送文件之前删除所有机密信息。

要使用 collect.sh 脚本从 Linux 客户端设备下载诊断信息：

1. 下载 collect.sh 脚本，它在collect.tar.gz 存档中。
2. 将下载的压缩包复制到需要诊断的 Linux 客户端设备上。
3. 运行以下命令解压 collect.tar.gz 存档：

   ```
   # tar -xzf collect.tar.gz
   ```

4. 执行以下命令指定脚本执行权限：

   ```
   # chmod +x collect.sh
   ```

5. 使用具有管理员权限的账户运行 collect.sh 脚本：

   ```
   # ./collect.sh
   ```

一个包含诊断信息的文件将生成并被保存到 /tmp/$HOST_NAME-collect.tar.gz 文件夹中。

在客户端设备上管理第三方应用程序

本节介绍与管理客户端设备上安装的第三方应用程序有关的 Kaspersky Security Center Linux 功能。

方案：应用程序管理

您可以管理用户设备上的应用程序启动。您可以允许或阻止应用程序在受管理设备上运行。此功能由“应用程序控制”组件实现。您可以管理 Windows 或 Linux 设备上安装的应用程序。

对于基于 Linux 的操作系统，从 Kaspersky Endpoint Security 11.2 for Linux 开始，均提供应用程序控制组件。

先决条件

- Kaspersky Security Center Linux已部署在您的组织中。
- Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Windows 的策略已创建并处于活动状态。

阶段

“应用程序控制”使用方案分阶段进行：

1. **形成并查看客户端设备上的应用程序列表**

   此阶段帮助您了解受管理设备上安装了哪些应用程序。您可以查看应用程序列表，并根据组织的安全策略确定要允许和禁止哪些应用程序。限制可能与组织中的信息安全策略有关。如果您非常清楚受管理设备上安装了哪些应用程序，则可以跳过此阶段。

   使用说明：获取并查看客户端设备上安装的应用程序列表

2. **形成并查看客户端设备上的可执行文件列表**

   此阶段帮助您了解在受管理设备上发现了哪些可执行文件。查看可执行文件列表，并将其与允许和禁止的可执行文件列表进行比较。对可执行文件的使用限制可能与组织中的信息安全策略有关。如果您非常清楚受管理设备上安装了哪些可执行文件，则可以跳过此阶段。

   使用说明：获取并查看客户端设备上存储的可执行文件列表

3. **为组织中使用的应用程序创建应用程序类别**

   分析受管理设备上存储的应用程序和可执行文件的列表。在分析基础上，创建应用程序类别。建议创建一个“工作应用程序”类别，以覆盖组织中使用的标准应用程序集。如果不同的安全组在工作中使用不同的应用程序集，则可以为每个安全组创建单独的应用程序类别。

   根据创建应用程序类别的条件集，可以创建两种类型的应用程序类别。

   操作说明：用手动添加的内容创建应用程序类别，创建包含来自选定设备的可执行文件的应用程序类别

4. **在 Kaspersky Endpoint Security 策略中配置“应用程序控制”**

   使用您在上一阶段创建的应用程序类别，在 Kaspersky Endpoint Security for Linux 策略中配置“应用程序控制”组件。

   操作说明：在 Kaspersky Endpoint Security for Windows 策略中配置“应用程序控制”

5. **在测试模式下开启“应用程序控制”组件**

   为确保应用程序控制规则不会阻止用户工作所需的应用程序，建议在创建新规则后启用应用程序控制规则测试并分析其操作。启用测试后，Kaspersky Endpoint Security for Windows 将不会阻止被应用程序控制规则禁止启动的应用程序，而是将有关其启动的通知发送到管理服务器。

   测试应用程序控制规则时，建议执行以下操作：

   - 确定测试周期。测试周期从几天到两个月不等。
   - 检查由测试“应用程序控制”操作生成的事件。

   Kaspersky Security Center Web Console 操作说明：在 Kaspersky Endpoint Security for Windows 策略中配置“应用程序控制”组件。遵循此说明并在配置过程中启用“**测试模式**”选项。

6. **更改“应用程序控制”组件的应用程序类别设置**

   如有必要，请更改“应用程序控制”设置。根据测试结果，您可以将与“应用程序控制”组件事件相关的可执行文件添加到含有手动添加内容的应用程序类别中。

   操作说明：Kaspersky Security Center Web Console：添加事件相关的可执行文件到应用程序类别

7. **在操作模式下应用“应用程序控制”的规则**

   测试应用程序控制规则并完成应用程序类别的配置后，您可以在操作模式下应用“应用程序控制”的规则。

   Kaspersky Security Center Web Console 操作说明：在 Kaspersky Endpoint Security for Windows 策略中配置“应用程序控制”组件。遵循此说明并在配置过程中禁用“**测试模式**”选项。

8. **验证“应用程序控制”配置**

   确保已完成以下操作：

   - 已创建应用程序类别。
   - 已使用应用程序类别配置“应用程序控制”。
   - 已在操作模式下应用“应用程序控制”的规则。

结果

方案完成后，将控制受管理设备上的应用程序启动。用户只能启动组织中允许的应用程序，而不能启动组织中禁止的应用程序。

有关“应用程序控制”的详细信息，请参阅 Kaspersky Endpoint Security for Linux 帮助 和 Kaspersky Security for Windows 帮助 。

About Application Control

The Application Control component monitors users' attempts to start applications and regulates the startup of applications by using Application Control rules.

> Application Control component is available for Kaspersky Endpoint Security 11.2 for Linux and later versions.

Startup of applications whose settings do not match any of the Application Control rules is regulated by the selected operating mode of the component:

- *Denylist*. The mode is used if you want to allow the startup of all applications except the applications specified in block rules. This mode is selected by default.

- *Allowlist*. The mode is used if you want to block the startup of all applications except the applications specified in allow rules.

The Application Control rules are implemented through application categories. You create application categories defining specific criteria. In Kaspersky Security Center Linux there are three types of application categories:

- Category with content added manually. You define conditions, for example, file metadata, file hashcode, file certificate, file path, to include executable files in the category.

- Category that includes executable files from selected devices. You specify a device whose executable files are automatically included in the category.

- Category that includes executable files from selected folder. You specify a folder from which executable files are automatically included in the category.

For detailed information about Application Control, refer to the Kaspersky Endpoint Security for Linux Help and Kaspersky Endpoint Security for Windows Help.

Obtaining and viewing a list of applications installed on client devices

Kaspersky Security Center Linux inventories all software installed on managed client devices running Linux and Windows.

Network Agent compiles a list of applications installed on a device, and then transmits this list to Administration Server. It takes about 10-15 minutes for the Network Agent to update the application list.

For Windows-based client devices, Network Agent receives most of the information about installed applications from the Windows registry. For Linux-based client devices, package managers provide information about installed applications to Network Agent.

To view the list of applications installed on managed devices:

1. In the main menu, go to 操作 → 第三方应用程序 → 应用程序注册表.

   The page displays a table with the applications that are installed on managed devices. Select the application to view its properties, for example, vendor name, version number, list of executable files, list of devices on which the application is installed.

2. You can group and filter the data of the table with installed applications as follows:

   - Click the settings icon ( ) in the upper-right corner of the table.

     In the invoked 列设置 menu, select the columns to be displayed in the table. To view the operating system type of the client devices on which the application is installed, select the 操作系统类型 column.

   - Click the filter icon ( ) in the upper-right corner of the table, and then specify and apply the filter criterion in the invoked menu.

     The filtered table of installed applications is displayed.

To view the list of applications installed on a specific managed device,

In the main menu, go to 设备 → 受管理设备 → **<device name>** → 高级 → 应用程序注册表. In this menu, you can export the list of applications to a CSV file or TXT file.

For detailed information about Application Control, refer to the Kaspersky Endpoint Security for Linux Help and Kaspersky Endpoint Security for Windows Help.

Obtaining and viewing a list of executable files stored on client devices

You can obtain a list of executable files stored on managed devices. To inventory executable files, you must create an inventory task.

For Kaspersky Endpoint Security for Linux, the feature of inventorying executable files is available since no earlier that version 11.2.

To create an inventory task for executable files on client devices:

1. In the main menu, go to 资产(设备) → 任务.

   The list of tasks is displayed.

2. Click the 添加 button.

   The New task wizard starts. Follow the steps of the wizard.

3. On the 新任务 page, from the 应用程序 drop-down list, select Kaspersky Endpoint Security for Linux or Kaspersky Endpoint Security for Windows, depending on the operating system of the client devices.

4. From the 任务类型 drop-down list, select 清单.

5. On the 完成任务创建 page, click the 完成 button.

   After the New task wizard has finished, the 清单 task is created and configured. If you want, you can change the settings for the created task. The newly created task is displayed in the list of tasks.

For a detailed description of the inventory task, see the Kaspersky Endpoint Security for Linux Help and the Kaspersky Endpoint Security for Windows Help.

After the 清单 task is performed, the list of executable files stored on managed devices is formed, and you can view the list.

During inventory, executable files in the following formats are detected: MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR, and HTML.

To view the list of executable files stored on client devices:

In the main menu, go to 操作 → 第三方应用程序 → 可执行文件.

The page displays the list of executable files stored on client devices.

Creating an application category with content added manually

You can specify a set of criteria as a template of executable files for which you want to allow or block a start in your organization. On the basis of executable files corresponding to the criteria, you can create an application category and use it in the Application Control component configuration.

To create an application category with content added manually:

1. In the main menu, go to 操作 → 第三方应用程序 → 应用程序类别.

   The page with a list of application categories is displayed.

2. Click the 添加 button.

   The New category wizard starts. Follow the steps of the wizard.

3. On the 选择策略创建方法 page of the wizard, specify the application category name and select the 含有手动添加内容的类别。可执行文件的数据被手动添加到该类别中 option.

4. On the 条件 page of the wizard, click the **Add** button to add a condition criterion to include files in the creating category.

5. On the 条件标准 page, select a rule type for the creation of category from the list:

   - 从 KL 类别

     If this option is selected, you can specify a Kaspersky application category as the condition of adding applications to the user category. The applications from the specified Kaspersky category will be added to the user application category.

   - 从存储库选择证书

     If this option is selected, you can specify certificates from the storage. Executable files that have been signed in accordance with the specified certificates will be added to the user category.

   - 指定应用程序路径 (支持掩码)

     If this option is selected, you can specify the path to the folder on the client device containing the executable files that are to be added to the user application category.

   - 可移动驱动器

     If this option is selected, you can specify the type of the medium (any drive or removable drive) on which the application is run. Applications that have been run on the selected drive type are added to the user application category.

   - 哈希、元数据或证书:

     - 从可执行文件列表选择

       If this option is selected, you can use the list of executable files on the client device to select and add applications to the category.

     - 从应用程序注册表选择

If this option is selected, application registry is displayed. You can select an application from the registry and specify the following file metadata:

- File name.
- File version. You can specify precise value of the version or describe a condition, for example "greater than 5.0".
- Application name.
- Application version. You can specify precise value of the version or describe a condition, for example "greater than 5.0".
- Vendor.

- 手动指定

If this option is selected, you must specify file hash, or metadata, or certificate as the condition of adding applications to the user category.

文件哈希

Depending on the version of the security application installed on devices on your network, you should select an algorithm for hash value computing by Kaspersky Security Center Linux for files in this category. Information about computed hash values is stored in the Administration Server database. Storage of hash values does not increase the database size significantly.

SHA-256 is a cryptographic hash function: no vulnerabilities have been found in its algorithm, and so it is considered the most reliable cryptographic function nowadays. Kaspersky Endpoint Security for Linux supports SHA-256 computing.

Select either of the options of hash value computing by Kaspersky Security Center Linux for files in the category:

- If all instances of security applications installed on your network are Kaspersky Endpoint Security for Linux, select the **SHA-256** check box.
- Select the **MD5** 哈希 check box only if you use Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux does not support the MD5 hash function.

元数据

If this option is selected, you can specify file metadata as file name, file version, vendor. The metadata will be sent to Administration Server. Executable files that contain the same metadata will be added to the application category.

证书

If this option is selected, you can specify certificates from the storage. Executable files that have been signed in accordance with the specified certificates will be added to the user category.

- From archived folder

If this option is selected, you can specify a file of an archived folder, and then select which condition you want to use to add applications to the user category. The archived folder is unpacked and the conditions that you select are applied to the files in the folder. As a condition, you can select one of the following criteria:

- 文件哈希

  You select which hash function (MD5 or SHA-256) you want to use to calculate hash values. The applications that have the same hash value as the files in the archived folder are added to the user application category.

  Select an MD5 hash function only if you use Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux does not support the MD5 hash function.

- 元数据

  You select which metadata you want to use as criteria. Executable files that contain the same metadata will be added to the user application category.

- 证书

  You select which certificate properties (certificate subject, fingerprint, or issuer) you want to use as criteria. Executable files that have been signed with the certificates that have the same properties will be added to the user category.

If this option is selected, you can specify a file of an archived folder, and then select which condition you want to use to add applications to the user category. The archived folder is unpacked and the conditions that you select are applied to the files in the folder. As a condition, you can select one of the following criteria:

- 文件哈希

  You select which hash function (MD5 or SHA-256) you want to use to calculate hash values. The applications that have the same hash value as the files in the archived folder are added to the user application category.

  Select an MD5 hash function only if you use Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux does not support the MD5 hash function.

- 元数据

  You select which metadata you want to use as criteria. Executable files that contain the same metadata will be added to the user application category.

- 证书

  You select which certificate properties (certificate subject, fingerprint, or issuer) you want to use as criteria. Executable files that have been signed with the certificates that have the same properties will be added to the user category.

The selected criterion is added to the list of conditions.

You can add as many criteria for the creating application category as you need.

6. On the 排除项 page of the wizard, click the **Add** button to add an exclusive condition criterion to exclude files from the category that is being created.

7. On the 条件标准 page, select a rule type from the list, in the same way that you selected a rule type for category creation.

When the wizard finishes, the application category is created. It is displayed in the list of application categories. You can use the created application category when you configure Application Control.

For detailed information about Application Control, refer to the Kaspersky Endpoint Security for Linux Help and Kaspersky Endpoint Security for Windows Help.

Creating an application category that includes executable files from selected devices

You can use executable files from selected devices as a template of executable files that you want to allow or block. Based on executable files from selected devices, you can create an application category and use it in the Application Control component configuration.

To create application category that includes executable files from selected devices:

1. In the main menu, go to 操作 → 第三方应用程序 → 应用程序类别.

   The page with a list of application categories is displayed.

2. Click the 添加 button.

   The New category wizard starts. Follow the steps of the wizard.

3. On the 选择策略创建方法 page of the wizard, specify the category name and select the 包含所选设备上可执行文件的类别。这些可执行文件被自动处理，它们的度量数据被添加到类别中 option.

4. Click 添加.

5. In the window that opens, select a device or devices whose executable files will be used to create the application category.

6. Specify the following settings:

   - Hash value computing algorithm

     Depending on the version of the security application installed on devices on your network, you should select an algorithm for hash value computing by Kaspersky Security Center Linux for files in this category. Information about computed hash values is stored in the Administration Server database. Storage of hash values does not increase the database size significantly.

     SHA-256 is a cryptographic hash function: no vulnerabilities have been found in its algorithm, and so it is considered the most reliable cryptographic function nowadays. Kaspersky Endpoint Security for Linux supports SHA-256 computing.

     Select either of the options of hash value computing by Kaspersky Security Center Linux for files in the category:

     - If all instances of security applications installed on your network are Kaspersky Endpoint Security for Linux, select the **SHA-256** check box.

     Select the **MD5** 哈希 check box only if you use Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux does not support the MD5 hash function.

     The **Calculate SHA-256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and any later versions)** check box is selected by default.

     The **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** is cleared by default.

- 与管理服务器存储库同步数据

  Select this option if you want that Administration Server periodically to check changes in the specified folder (or folders).

  By default, this option is disabled.

  If you enable this option, specify the period (in hours) to check changes in the specified folder (folders). By default, scan interval is 24 hours.

- 文件类型

  In this section, you can specify file type that is used to create the application category.

  所有文件. All files are taken into consideration when creating the category. By default, this option is selected.

  仅应用程序类别之外的文件. Only files outside the application categories are taken into consideration when creating the category.

- 文件夹

  In this section you can specify which folders from the selected device (devices) contain files that are used to create the application category.

  所有文件夹. All folders are taken into consideration for the creating category. By default, this option is selected.

  指定文件夹. Only specified folder is taken into consideration for the creating category. If you select this option you must specify path to the folder.

When the wizard finishes, the application category is created. It is displayed in the list of application categories. You can use the created application category when you configure Application Control.

Creating an application category that includes executable files from selected folder

You can use executable files from a selected folder as a standard of executable files that you want to allow or block in your organization. On the basis of executable files from the selected folder, you can create an application category and use it in the Application Control component configuration.

To create an application category that includes executable files from the selected folder:

1. In the main menu, go to 操作 → 第三方应用程序 → 应用程序类别.

   The page with a list of application categories is displayed.

2. Click the 添加 button.

   The New category wizard starts. Proceed through the wizard by using the **Next** button.

3. On the 选择策略创建方法 page of the wizard, specify the category name and select the 包含指定文件夹内可执行文件的类别。复制到指定文件夹的应用程序可执行文件被自动处理，它们的度量数据被添加到类别中 option.

4. Specify the folder whose executable files will be used to create the application category.

5. Define the following settings:

- 包含动态链接库 (DLL) 到该类别

  The application category includes dynamic-link libraries (files in DLL format), and the Application Control component logs the actions of such libraries running in the system. Including DLL files in the category may lower the performance of Kaspersky Security Center.

  By default, this check box is cleared.

- 包含脚本数据到该类别

  The application category includes data on scripts, and scripts are not blocked by Web Threat Protection. Including the script data in the category may lower the performance of Kaspersky Security Center.

  By default, this check box is cleared.

- Hash value computing algorithm: 为该类别中的文件计算 **SHA-256(在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更新版本中支持)** / 为该类别中的文件计算 **MD5(在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 更早版本中支持)**

  Depending on the version of the security application installed on devices on your network, you should select an algorithm for hash value computing by Kaspersky Security Center Linux for files in this category. Information about computed hash values is stored in the Administration Server database. Storage of hash values does not increase the database size significantly.

  SHA-256 is a cryptographic hash function: no vulnerabilities have been found in its algorithm, and so it is considered the most reliable cryptographic function nowadays. Kaspersky Endpoint Security for Linux supports SHA-256 computing.

  Select either of the options of hash value computing by Kaspersky Security Center Linux for files in the category:

  - If all instances of security applications installed on your network are Kaspersky Endpoint Security for Linux, select the **SHA-256** check box.

  Select the **MD5 哈希** check box only if you use Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux does not support the MD5 hash function.

  The **Calculate SHA-256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and any later versions)** check box is selected by default.

  The **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** is cleared by default.

- 强制扫描文件夹以查找更改

  If this option is enabled, the application regularly checks the folder of category content addition for changes. You can specify the frequency of checks (in hours) in the entry field next to the check box. By default, the time interval between forced checks is 24 hours.

  If this option is disabled, the application does not force any checks of the folder. The Server attempts to access files if they have been modified, added, or deleted.

  By default, this option is disabled.

When the wizard finishes, the application category is created. It is displayed in the list of application categories. You can use the application category at Application Control configuration.

For detailed information about Application Control, refer to the Kaspersky Endpoint Security for Linux Help and Kaspersky Endpoint Security for Windows Help.

Viewing the list of application categories

You can view the list of configured application categories and the settings of each application category.

To view the list of application categories,

In the main menu, go to 操作 → 第三方应用程序 → 应用程序类别.

The page with a list of application categories is displayed.

To view properties of an application category,

Click the name of the application category.

The properties window of the application category is displayed. The properties are grouped on several tabs.

Configuring Application Control in the Kaspersky Endpoint Security for Windows policy

After you create Application Control categories, you can use them for configuring Application Control in Kaspersky Endpoint Security for Windows policies.

To configure Application Control in the Kaspersky Endpoint Security for Windows policy:

1. In the main menu, go to 资产(设备) → 策略和配置文件.

   A page with a list of policies is displayed.

2. Click the **Kaspersky Endpoint Security for Windows** policy.

   The policy settings window opens.

3. Go to 应用程序设置 → **Security Controls** → **Application Control**.

   The **Application Control** window with Application Control settings is displayed.

4. The **Application Control** option is enabled by default. Switch the toggle button **Application Control DISABLED** to disable the option.

5. In the **Application Control Settings** block settings, enable the operation mode to apply the Application Control rules and allow Kaspersky Endpoint Security for Windows to block startup of applications.

   If you want to test the Application Control rules, in the **Application Control Settings** section, enable the test mode. In the test mode, Kaspersky Endpoint Security for Windows does not block startup of applications, but logs information about triggered rules in the report. Click the 查看报告 link to view this information.

6. Enable the **Control DLL modules load** option if you want Kaspersky Endpoint Security for Windows to monitor the loading of DLL modules when applications are started by users.

   Information about the module and the application that loaded the module will be saved to a report.

   Kaspersky Endpoint Security for Windows monitors only the DLL modules and drivers loaded after the **Control DLL modules load** option is selected. Restart the computer after selecting the **Control DLL modules load** option if you want Kaspersky Endpoint Security for Windows to monitor all DLL modules and drivers, including those loaded before Kaspersky Endpoint Security for Windows is started.

7. (Optional) In the **Message templates** block, change the template of the message that is displayed when an application is blocked from starting and the template of the email message that is sent to you.

8. In the **Application Control Mode** block settings, select the **Denylist** or **Allowlist** mode.

   By default, the **Denylist** mode is selected.

9. Click the **Rules Lists Settings** link.

   The **Denylists and allowlists** window opens to let you add an application category. By default, the **Denylist** tab is selected if the **Denylist** mode is selected, and the **Allowlist** tab is selected if the **Allowlist** mode is selected.

10. In the **Denylists and allowlists** window, click the 添加 button.

    The **Application Control rule** window opens.

11. Click the **Please choose a category** link.

    The **Application Category** window opens.

12. Add the application category (or categories) that you created earlier.

    You can edit the settings of a created category by clicking the **Edit** button.

    You can create a new category by clicking the **Add** button.

    You can delete a category from the list by clicking the **Delete** button.

13. After the list of application categories is complete, click the 确定 button.

    The **Application Category** window closes.

14. In the **Application Control** rule window, in the **Subjects and their rights** section, create a list of users and groups of users to apply the Application Control rule.

15. Click the 确定 button to save the settings and to close the **Application Control rule** window.

16. Click the 确定 button to save the settings and to close the **Denylists and allowlists** window.

17. Click the 确定 button to save the settings and to close the **Application Control** window.

18. Close the window with the Kaspersky Endpoint Security for Windows policy settings.

Application Control is configured. After the policy is propagated to the client devices, the startup of executable files is managed.

For detailed information about Application Control, refer to the Kaspersky Endpoint Security for Linux Help and Kaspersky Endpoint Security for Windows Help.

Adding event-related executable files to the application category

After you configure Application Control in the Kaspersky Endpoint Security policies, the following events will be displayed in the list of events:

- **Application startup prohibited** (*Critical* event). This event is displayed if you have configured Application Control to apply rules.
- **Application startup prohibited in test mode** (*Info* event). This event is displayed if you have configured Application Control to test rules.
- **Message to administrator about application startup prohibition** (*Warning* event). This event is displayed if you have configured Application Control to apply rules and a user has requested access to the application that is blocked at startup.

It is recommended to create event selections to view events related to Application Control operation.

You can add executable files related to Application Control events to an existing application category or to a new application category. You can add executable files only to an application category with content added manually.

To add executable files related to Application Control events to an application category:

1. In the main menu, go to 监控和报告 → 事件分类.

   The list of event selections is displayed.

2. Select the event selection to view events related to Application Control and start this event selection.

   If you have not created event selection related to Application Control, you can select and start a predefined selection, for example, **Recent events**.

   The list of events is displayed.

3. Select the events whose associated executable files you want to add to the application category, and then click the 分配到类别 button.

   The New category wizard starts. Proceed through the wizard by using the **Next** button.

4. On the wizard page, specify the relevant settings:

   - In the 对事件相关可执行文件所采取的操作 section, select one of the following options:

     - 添加到新的应用程序类别

       Select this option if you want to create a new application category based on event-related executable files.

       By default, this option is selected.

       If you have selected this option, specify a new category name.

     - 添加到现有应用程序类别

       Select this option if you want to add event-related executable files to an existing application category.

       By default, this option is not selected.

       If you have selected this option, select the application category with content added manually to which you want to add executable files.

   - In the 规则类型 section, select one of the following options:

- 添加到包含的规则
- 添加到排除的规则

- In the 用作条件的参数 section, select one of the following options:
  - 证书详情(或没有证书的文件的 SHA-256 哈希)

    Files may be signed with a certificate. Multiple files may be signed with the same certificate. For example, different versions of the same application may be signed with the same certificate, or several different applications from the same vendor may be signed with the same certificate. When you select a certificate, several versions of an application or several applications from the same vendor may end up in the category.

    Each file has its own unique SHA256 hash function. When you select an SHA256 hash function, only one corresponding file, for example, the defined application version, ends up in the category.

    Select this option if you want to add to the category rules the certificate details of an executable file (or the SHA256 hash function for files without a certificate).

    By default, this option is selected.

  - 证书详情(没有证书的文件将被跳过)

    Files may be signed with a certificate. Multiple files may be signed with the same certificate. For example, different versions of the same application may be signed with the same certificate, or several different applications from the same vendor may be signed with the same certificate. When you select a certificate, several versions of an application or several applications from the same vendor may end up in the category.

    Select this option if you want to add the certificate details of an executable file to the category rules. If the executable file has no certificate, this file will be skipped. No information about this file will be added to the category.

  - 仅 SHA-256 (没有哈希的文件将被跳过)

    Each file has its own unique SHA256 hash function. When you select an SHA256 hash function, only one corresponding file, for example, the defined application version, ends up in the category.

    Select this option if you want to add only the details of the SHA256 hash function of the executable file.

  - 仅 MD5 (停产模式，仅对 Kaspersky Endpoint Security 10 Service Pack 1 版本)

    Select this option only if you use Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux does not support an MD5 hash function.

    Each file has its own unique MD5 hash function. When you select an MD5 hash function, only one corresponding file, for example, the defined application version, ends up in the category.

5. Click **OK**.

When the wizard finishes, executable files related to the Application Control events are added to the existing application category or to a new application category. You can view settings of the application category that you have modified or created.

For detailed information about Application Control, refer to the Kaspersky Endpoint Security for Linux Help and Kaspersky Endpoint Security for Windows Help.

层级指南

该部分提供了 Kaspersky Security Center Linux 尺寸信息。

关于本指南

Kaspersky Security Center Linux（也称为 Kaspersky Security Center）层级指南专为安装管理 Kaspersky Security Center 的专业人员，以及为使用 Kaspersky Security Center 的企业提供技术支持的人员而设计。

所有建议和计算的前提是，在网络上 Kaspersky Security Center 管理安装了 Kaspersky 软件的设备的保护。

要在不同的操作条件下获取和维持优化运行，您必须考虑网络设备数量、网络拓扑和您需要的 Kaspersky Security Center 功能集。

此指南提供下列信息：

- Kaspersky Security Center 的限制
- Kaspersky Security Center 关键节点的限制（管理服务器和分发点）：
  - 管理服务器和分发点的硬件需求
  - 管理服务器数量和层级限制
  - 计算分发点的数量和配置
- 数据库中的事件记录配置取决于网络设备的数量
- 特定任务的配置旨在优化 Kaspersky Security Center 的性能
- Kaspersky Security Center 管理服务器和每个受保护设备间的流量率(网络负载)

以下情况下建议参考该文档：

- 当在安装 Kaspersky Security Center 前计划资源时
- 当向部署了 Kaspersky Security Center 的网络计划显著更改时
- 从在受限制网段（测试环境）使用 Kaspersky Security Center 切换到在企业网络上全面部署 Kaspersky Security Center 时
- 当对使用的 Kaspersky Security Center 功能集做更改时

管理服务器计算

该部分提供了管理服务器设备的软件和硬件需求。也提供了根据组织网络配置计算管理服务器数量和层级的建议。

管理服务器的硬件资源计算

该部分包含为计划管理服务器的硬件资源提供向导的计算。

DBMS 和管理服务器的硬件需求

下表提供了测试得出的 DBMS 和管理服务器建议最低硬件要求。对于支持的操作系统和 DBMS 的完整列表，请参考硬件和软件需求列表。

管理服务器、DBMS 和 Web 控制台均位于单独的设备上，网络包括 50,000 台设备

安装了管理服务器的设备的配置

硬件	参数值
CPU	8 核，2500 MHz
RAM	16 GB
硬盘驱动器	300 GB，推荐 RAID 10
网卡	1 Gbit

安装了 DBMS 服务器的设备的配置

硬件	参数值
CPU	16 核，2500 MHz
RAM	32 GB
硬盘驱动器	300 GB，推荐 RAID 10
网卡	1 Gbit

安装了 Web 控制台的设备的配置

硬件	参数值
CPU	4 核，2500 MHz
RAM	8 GB
硬盘驱动器	40 GB
网卡	1 Gbit

管理服务器和 Web 控制台位于同一设备上，DBMS 位于单独的设备上，网络包括 50,000 台设备

安装了管理服务器和 Web 控制台的设备的配置

硬件	参数值
CPU	12 核，2500 MHz
RAM	24 GB

硬盘	340 GB，推荐 RAID 10
网卡	1 Gbit

安装了 DBMS 服务器的设备的配置

硬件	参数值
CPU	16 核，2500 MHz
RAM	32 GB
硬盘驱动器	300 GB，推荐 RAID 10
网卡	1 Gbit

测试在以下系统上运行：

- 自动分配分发点在管理服务器上启用，或者分发点根据建议的表格被手动指定。
- 备份任务保存备份副本到位于专用服务器的文件资源。

数据库空间计算

必须在数据库中保留的大约空间可以使用以下公式计算：

(600 * C + 2.3 * E + 2.5 * A + 1.2 * N * F), KB

其中：

- C 是设备数量。
- E 要存储的事件的数量。
- A 是活动目录对象的总数：
  - 设备账户
  - 用户账户
  - 安全组账户
  - 活动目录组织单元

  如果活动目录扫描被禁用，A 等效于 0。
- N 是端点设备上已清查可执行文件的平均数量。
- F 是端点设备的数量，其中可执行文件已清查。

如果您计划在 Kaspersky Endpoint Security 策略设置中启用通知管理服务器您运行的应用程序，您将需要额外空间(0.03 * C GB)在数据库中存储您运行的应用程序信息。

操作期间，一定的*未占用空间*总是出现在数据库。因此，数据库文件的实际尺寸（默认下，如果您使用 SQL Server 做为 DBMS 的话，是 KAV.MDF 文件）经常是两倍于数据库中被占用空间的尺寸。

不建议明确限制透明日志（默认下，文件 KAV_log.LDF，如果您使用 SQL Server 作为 DBMS）的大小。建议保留 MAXSIZE 参数的默认值。然而，如果您必须限制该文件的大小，请考虑对于 KAV_log.LDF，参数 MAXSIZE 的典型必要值是 20480 MB。

磁盘空间计算

文件夹 /var/opt/kaspersky/klnagent_srv/ 需要的管理服务器磁盘空间可以使用以下公式估算：

(724 * C + 0.15 * E + 0.17 * A), KB

其中：

- C 是设备数量。
- E 要存储的事件的数量。
- A 是活动目录对象的总数：
  - 设备账户
  - 用户账户
  - 安全组账户
  - 活动目录组织单元

如果活动目录扫描被禁用，A 等效于 0。

计算管理服务器的数量和配置

要减少主管理服务器负载，您可以分配另外的管理服务器到每个管理组。每个主管理服务器的从属管理服务器的数量不能超过 500。

我们建议您基于您组织网络的配置来创建管理服务器配置。

有关将动态虚拟机连接到 Kaspersky Security Center 的建议

动态虚拟机（也简称为“动态 VM”）比静态虚拟机消耗更多资源。

有关动态虚拟机的更多信息，请参阅对动态虚拟机的支持。

连接新的动态 VM 时，Kaspersky Security Center Linux 在 Kaspersky Security Center Web Console 中为此动态 VM 创建一个记录并将该动态 VM 移至管理组。此后，动态 VM 被添加到管理服务器数据库中。管理服务器与安装在此动态 VM 上的网络代理完全同步。

在组织的网络中，网络代理为每个动态 VM 创建以下网络列表：

- 硬件

- 安装的软件
- 检测到的漏洞
- 应用程序控制组件的事件和可执行文件列表

网络代理将这些网络列表传输到管理服务器。网络列表的大小取决于安装在动态 VM 上的组件，并且可能会影响 Kaspersky Security Center Linux 和数据库管理系统的 (DBMS) 性能。注意，负载可能呈非线性增长。

在用户使用完动态 VM 并将其关闭后，该虚拟机将从虚拟基础架构中删除，且有关该虚拟机的条目也将从管理服务器数据库中删除。

所有这些操作都会消耗大量的 Kaspersky Security Center Linux 和管理服务器数据库资源，并会降低 Kaspersky Security Center Linux 和 DBMS 的性能。建议您最多将 20,000 个动态 VM 连接到 Kaspersky Security Center Linux。

如果连接的动态 VM 执行标准操作（例如，数据库更新）并且消耗不超过 80% 的内存和 75-80% 的可用内核，您可以将超过 20,000 个动态 VM 连接到 Kaspersky Security Center Linux。

更改动态 VM 上的策略设置、软件或操作系统可能减少或增加资源消耗。最优资源消耗占比为 80-95%。

分发点和连接网关的计算

该部分提供了用作分发点的设备的硬件需求，以及根据企业网络配置计算分发点和连接网关数量的建议。

分发点需求

要处理多达 10,000 台客户端设备，分发点必须至少满足以下要求（提供了测试台配置）：

- CPU：Intel Core™ i7-7700 CPU 3.60 GHz 4 核。
- RAM：8 GB。
- 可用存储空间：120 GB。

如果管理服务器上有任何远程安装任务等待，带有分发点的设备也会请求一定的剩余磁盘空间，这些空间与要安装的安装包大小相当。

如果管理服务器上有一个或多个更新（补丁）安装和漏洞修复任务实例，带有分发点的设备也会请求一定的剩余磁盘空间，相当于两倍的补丁总大小。

计算分发点的数量和配置

网络包含越多的客户端设备，就需要越多的分发点。我们建议您禁用分发点的自动分配。当分发点的自动分配被启用时，如果客户端设备数量很大，管理服务器就分配分发点并定义其配置。

使用单独分配的分发点

如果您计划使用特定设备作为分发点(就是，单独分配的服务器)，您可以不使用分发点的自动分配。此种情况下，确保您要分配为分发点的设备具有足够的剩余磁盘空间卷，不定期关闭，且禁用了睡眠模式。

网络中基于网络设备数量被专门分配的包含单一网段的分发点的数量

网段中的客户端设备的数量	分发点数量
少于 300	0（不分配分发点）
大于 300	可接受：(N/10,000 + 1)，建议：(N/5,000 + 2)，N 是网络设备数量

网络中基于网络设备数量被专门分配的包含多个网段的分发点的数量

每个网段中的客户端设备的数量	分发点数量
少于 10	0（不分配分发点）
10–100	1
大于 100	可接受：(N/10,000 + 1)，建议：(N/5,000 + 2)，N 是网络设备数量

使用标准客户端设备（工作站）作为分发点

如果您计划使用标准客户端设备（就是，工作站）作为分发点，我们建议您按照所示分配分发点（参见下表），以便避免通信渠道和管理服务器过载。

网络中基于网络设备数量作为分发点工作的包含单一网段的工作站的数量

网段中的客户端设备的数量	分发点数量
少于 300	0（不分配分发点）
大于 300	(N/300 + 1)，N 是网络设备数量；至少有三台分发点

网络中基于网络设备数量作为分发点工作的包含多个网段的工作站的数量

每个网段中的客户端设备的数量	分发点数量
少于 10	0（不分配分发点）
10–30	1
31–300	2
大于 300	(N/300 + 1)，N 是网络设备数量；至少有三台分发点

如果分发点被关闭(或由于某些原因不可用)，其范围内的受管理设备可以访问管理服务器以更新。

连接网关数量计算

如果您计划使用连接网关，我们建议您为该功能指定特别的设备。

一个连接网关可以覆盖最多 10,000 台受管理设备。

任务和策略事件信息的记录

该部分提供了管理服务器数据库中的事件存储计算，并提供如何最小化事件数量的建议，从而降低管理服务器负载。

默认情况下，每个任务和策略的属性可以用于存储所有任务执行和策略强制执行的相关事件。

然而，如果任务运行过于频繁（例如，每周多于一次）且在大量设备间（例如，多于 10,000 台），事件数量可能过大且事件可能溢出数据库。此种情况下，建议选择任务设置的两个选项中的一个：

- **保存任务进度相关事件**。此种情况下，数据库仅从运行任务的每个设备接收任务启动、进程和完成信息（成功、带有警告或错误）。
- **仅保存任务执行结果**。此种情况下，数据库仅从运行任务的每个设备接收任务完成信息（成功、带有警告或错误）。

如果策略为大数量设备定义（例如，多于 10,000 台），事件数量可能很大且事件可能溢出数据库。此种情况下，建议在策略设置中仅选择最关键的事件并启用它们的记录。建议您禁用所有其他事件的记录。

为此，您将降低数据库中的事件数量，提高与数据库中事件表分析相关的场景的执行速度，并降低严重事件被大数量事件覆盖的风险。

您也可以降低任务或策略相关事件的存储期限。任务相关事件和策略相关事件的默认期限分别是 7 天和 30 天。当更改事件存储期限时，请考虑您的组织采用的工作程序以及系统管理员用以分析每个事件的时间。

建议在以下情况修改事件存储设置：

- 有关组任务中间状态变化的事件和有关应用策略的事件在 Kaspersky Security Center Linux 数据库的所有事件中占据很高比例。
- 操作系统日志开始显示事件超过存储限制时的自动删除。

基于每天来自每个设备的事件数量不超过 20 的假设来选择事件记录选项。如果必要，您可以稍微增加该限制，但仅是在您网络中的设备数量相对小时（少于 10,000 台）。

特别考虑和特定任务的优化设置

特定任务受制于基于网络设备数量的特别考虑。该部分提供了此类任务设置的优化配置建议。

设备发现、数据备份任务、数据库维护任务和更新 Kaspersky Endpoint Security 的组任务是 Kaspersky Security Center Linux 的基本功能部分。

清查任务是漏洞和补丁管理功能的一部分，且在该功能未激活时不可用。

设备发现频率

不建议增加设备发现的默认频率，因为这可以增加域控制器负载。相反，建议使用您组织需要的最小频率计划轮询。计算最优计划的建议提供在下表。

设备发现计划

网络设备数量	建议的设备发现频率
少于 10,000	默认频率或更低
10,000 或更多	每天一次或更低

管理服务器数据备份任务和数据库维护任务

当以下任务运行时管理服务器停止工作：

- 备份管理服务器数据
- 数据库维护

当这些任务运行时，数据库无法接收任何数据。

您可能必须重新计划这些任务以便它们和其他管理服务器任务不同时执行。

更新 Kaspersky Endpoint Security 的组任务

如果管理服务器作为更新源，Kaspersky Endpoint Security 10 和后续版本的组更新任务的建议计划选项是“**当新更新下载至存储库时**”，其中“**使用任务启动自动随机延迟**”复选框被选中。

如果从 Kaspersky 服务器下载更新到存储库的本地任务已在每个分发点上创建，时段性计划将被建议给 Kaspersky Endpoint Security 组更新任务。随机时段值必须是一小时。

软件清查任务

您可以在获取已安装应用程序相关信息的同时减少数据库的负载。为此，我们建议您在安装了一组标准软件的参考设备上运行清单任务。

管理服务器从单个设备接收的可执行文件数量不能超过 150,000。当 Kaspersky Security Center Linux 达到了该限制，它无法接收任何新文件。

通常，常规客户端设备上的文件数量不超过 60,000。文件服务器上的可执行文件数量可能更大甚至超过 150,000 阈值。

管理服务器和受保护设备间的网络负载详情

该部分提供了一定条件下的网络流量测试度量结果。当您计划网络基础架构和您组织网络中（或管理服务器和其他要保护其设备的组织间）吞吐量时，可以参考该信息。知道了网络吞吐量，您也可以估算不同数据传输操作将花费的时间。

不同方案下的流量消耗

下表显示不同方案下管理服务器和受管理设备之间流量度量测试的结果。

默认下，设备每 15 分钟或更长间隔与管理服务器同步一次。然而，如果您在管理服务器上修改策略或任务的设置，该策略（或任务）所适用的设备会提前进行同步，从而将新设置传输到设备上。

方案	从管理服务器到每个受管理设备的流量	从每个受管理设备到管理服务器的流量
安装带有更新数据库的 Kaspersky Endpoint Security for Linux	390 MB	3.3 MB
网络代理安装	75 MB	397 KB
网络代理和 Kaspersky Endpoint Security for Linux 同时安装	459 MB	3.6 MB
反病毒数据库初始更新，不更新软件包中的数据库（如果参与卡巴斯基安全网络被禁用）	113 MB	1.8 MB
反病毒数据库每日更新（如果参与卡巴斯基安全网络被启用）	22 MB	373 MB
设备数据库更新之前的初始化同步（策略和任务传输）	382 KB	446 KB
在设备上更新数据库之后初始同步	20 KB	157 KB
与管理服务器的同步（根据计划）	18 KB	23 KB
当组策略中单个设备被更改时同步（设置更改时立即）	19 KB	20 KB
当组任务中单个设备被更改时同步（设置更改时立即）	14 KB	11 KB
强制同步	110 KB	109 KB
检测到的病毒事件（1 个病毒）	44 KB	50 KB
检测到病毒事件（10 个病毒）	58 KB	77 KB
启用应用程序注册表列表后的一次性流量	最多 10 KB	最多 12 KB
启用应用程序注册表列表后的每日流量	最多 840 KB	最多 1 MB

24 小时平均流量使用

管理服务器和受管理设备之间的 24 小时平均流量使用情况如下所示：

- 从管理服务器到受管理设备的流量为 840 KB。
- 从受管理设备到管理服务器的流量为 1 MB。

流量测量在以下条件下进行：

- 受管理设备已安装网络代理和 Kaspersky Endpoint Security for Linux。
- 设备未被分配为分发点。
- 漏洞和补丁管理未启用。
- 与管理服务器的同步频率是 15 分钟。

联系技术支持

该部分描述如何获取技术支持和其可用条款。

如果获得技术支持

如果您在 Kaspersky Security Center Linux 文档或任何 Kaspersky Security Center Linux 信息源中都找不到问题的解决方案，请联系卡巴斯基技术支持。技术支持专家将回答关于安装和使用 Kaspersky Security Center Linux 的所有问题。

Kaspersky 在 Kaspersky Security Center Linux 的生命周期内提供支持（请参见产品支持生命周期页面）。与技术支持部门联系之前，请阅读支持规则。

您可以使用下列方式之一与技术支持联系：

- 通过访问技术支持网站
- 通过使用 Kaspersky CompanyAccount 门户发送请求到技术支持

通过 Kaspersky CompanyAccount 获得技术支持

Kaspersky CompanyAccount 是一个针对使用 卡巴斯基应用程序的公司的门户。Kaspersky CompanyAccount 门户设计用于方便用户与 Kaspersky 专家之间通过在线请求进行交互。您可以使用 Kaspersky CompanyAccount 跟踪您的在线请求状态并存储它们的历史。

您可在 Kaspersky CompanyAccount 上通过单个账户注册贵组织的所有员工。单个账户允许集中管理已注册员工向 Kaspersky 发送的电子请求，还允许通过 Kaspersky CompanyAccount 管理这些员工的权限。

Kaspersky CompanyAccount 门户采用以下语言提供：

- 英语
- 西班牙语
- 意大利语
- 德语
- 波兰语
- 葡萄牙语
- 俄语
- 法语
- 日语

要了解有关 Kaspersky CompanyAccount 的更多信息，请访问技术支持网站。

有关程序的信息源

Kaspersky 网站上的 Kaspersky Security Center Linux 页面

在 Kaspersky 网站的 Kaspersky Security Center Linux 页面上，您可以查看有关程序、程序功能和特性的一般信息。

知识库中的 Kaspersky Security Center Linux 页

*知识库*是 Kaspersky 技术支持网站的一部分。

在 知识库的 Kaspersky Security Center Linux 页面上，您可以阅读文章，这些文章提供了有用的信息、建议以及有关如何购买、安装和使用程序的常见问题解答。

知识库中的文章可能提供关于 Kaspersky Security Center Linux 和 Kaspersky 应用程序的问题的答案。知识库中的文章也可能包含技术支持新闻。

在社区讨论 Kaspersky 应用程序

如果您的问题不需要立即回答，您可以在我们的论坛中与卡巴斯基专家和其他用户一起进行讨论。

在该论坛上，您可以查看讨论主题，发表您的评论，创建新讨论主题。

> 需要互联网连接以访问网站资源。

如果您无法找到问题的解决方案，请联系技术支持。

Known issues

Kaspersky Security Center Linux has a number of limitations that are not critical to operation of the application:

- When you import the *Download updates to the repositories of distribution points* or *Update verification* task the **Select devices to which the task will be assigned** option is enabled. These tasks cannot be assigned to a device selection or specific devices. If you assign the *Download updates to the repositories of distribution points* or *Update verification* task to specific devices, the task will be imported incorrectly.

- If your network includes a Microsoft Active Directory domain that contains several tens of thousands of objects (managed devices, security groups, and user accounts) and the response page size (the `MaxPageSize` parameter) is less than 5,000, the domain controller polling is not available and information about domain objects is not received. When you try to poll the domain controller, the *Size limit exceeded* error occurs. Increasing the response page size may help to fix the error. You can use the Ntdsutil.exe utility to increase the `MaxPageSize` parameter value to `5000` or to `10000`, if necessary.

- When you enable KPSN in the Administration Server properties and use HTTPS port 17111, the connection with ds.kaspersky.com is not interrupted.

- Kaspersky Endpoint Security for Windows does not support the KSN Proxy service if the 使用 **HTTPS** option is enabled in the KSN Proxy settings of the Administration Server properties, and the Administration Server address contains non-Latin characters.

- When you switch to a secondary Server from the interface of a primary Kaspersky Security Center Linux Administration Server, the 无缝更新 section of the main menu cannot be opened.

- When you create the *Add key* task for Kaspersky Endpoint Security 11.3 for Mac, the wizard displays a license key table that may contain empty lines.

- The protection level displayed in the Kaspersky Endpoint Security for Windows policy does not correspond to the protection level in the interface of Kaspersky Endpoint Security for Windows.

- When you run the *远程卸载应用程序* task to remove a Kaspersky application from a managed device, the task completes successfully, but the application is not removed. This issue is valid for Kaspersky Endpoint Security for Linux, Kaspersky Embedded Systems Security for Linux, and Kaspersky Industrial CyberSecurity for Linux Nodes.

- The Administration Server properties window contains settings for mobile devices, though Kaspersky Security Center Linux does not support management of mobile devices.

- If an application from the 应用程序注册表 section was detected on a Linux device, the application properties do not contain information about related executable files.

- If you install Network Agent on a device running the ALT Linux operating system through a remote installation task and you run this task under an account with non-root privileges, the task fails. Run the remote installation task under the root account, or create and use a stand-alone installation package of Network Agent to install the application locally.

- In reports with a letter format, a page break may cut a text line horizontally.

- In the 添加从属管理服务器 wizard, if you specify an account with enabled two-step verification for authentication on the future secondary Server, the wizard finishes with an error. To resolve this issue, specify an account for which two-step verification is disabled or create the hierarchy from the future secondary Server.

- If you open Kaspersky Security Center Web Console in different browsers and download the Administration Server certificate file in the Administration Server properties window, the downloaded files have different names.

- A managed device that has more than one network adapter sends Administration Server information about the MAC address of the network adapter that is not the one that is used to connect to Administration Server.

- In Astra Linux 64-bit edition, the klnagent-astra package cannot be upgraded with klnagent64_14 package: the old package klnagent64-astra will be removed, and the new package klnagent64 will be installed instead of upgrade, so the new icon for device with klnagent64_14 package will be added. You can remove the old icon for this device.

词汇表

HTTPS

在浏览器和 Web 服务器之间使用加密传送数据的安全协议。HTTPS 用于访问受限制的信息，如企业或财务数据。

JavaScript

一种对网页性能进行扩展的编程语言。使用 JavaScript 创建的网页无需使用来自网络服务器的新数据刷新网页即可执行功能（例如，更改界面元素的视图或打开附加窗口）。要查看使用 JavaScript 创建的页面，请在您的浏览器的配置中启用 JavaScript 支持。

Kaspersky Security Center Linux Web 服务器

Kaspersky Security Center Linux 组件，与管理服务器一同安装。Web 服务器用于通过网络传输独立安装包、iOS MDM 配置文件、以及共享文件夹的文件。

Kaspersky Security Center Linux 管理员

通过 Kaspersky Security Center Linux 远程集中管理系统来管理应用程序操作的人。

Kaspersky Security Center System Health Validator (SHV)

在 Kaspersky Security Center Linux 和 Microsoft NAP 并行运行时，用于检查操作系统运行能力的 Kaspersky Security Center Linux 的一个组件。

Kaspersky Security Center 操作员

对通过 Kaspersky Security Center 管理的保护系统的状态和操作进行监视的用户。

Kaspersky 更新服务器

Kaspersky 程序可以从 Kaspersky 的 HTTP(S) 服务器下载数据库和应用程序模块更新。

Provisioning 配置文件

应用程序在 iOS 移动设备上运行的设置的集合。Provisioning 配置文件包含有关授权许可的信息，它连接至特定的应用程序。

SSL

互联网和本地网上的使用的数据加密协议。Secure Sockets Layer（SSL）协议用在网络应用程序中，以便在客户端和服务器之间创建安全的连接。

不兼容应用程序

第三方开发的反病毒应用程序，或不支持通过 Kaspersky Security Center Linux 管理的 Kaspersky 应用程序。

事件严重级别

在 Kaspersky 程序操作过程中遇到的事件的属性。存在以下严重级别：

- 严重事件
- 功能失败
- 警告
- 信息

根据事件发生时的情况，相同类型的事件可能具有不同的严重级别。

事件存储库

管理服务器数据库的一部分，用于存储发生在 Kaspersky Security Center Linux 中的事件信息。

任务

由 Kaspersky 应用程序执行的功能作为任务来实施，例如：实时文件保护、计算机全盘扫描、数据库更新。

任务设置

对于每个任务类型的特别应用程序设置。

保护状态

当前保护状态，反映了计算机安全级别。

共享证书

证书用于识别用户的移动设备。

内部用户

内部用户的账户可用于操作虚拟管理服务器。Kaspersky Security Center Linux 授权应用程序的内部用户拥有真实用户的所有权限。

只能在 Kaspersky Security Center Linux 内创建和使用内部用户账户。系统不会将内部用户的任何数据传送到操作系统。Kaspersky Security Center Linux 将验证内部用户。

分发点

安装了网络代理并用于更新发布、远程安装应用程序、获取管理组（广播域）中计算机信息的计算机。分发点用来降低发布更新时管理服务器的负载并优化网络流量。分发点可以被自动指定、被管理服务器指定或被管理员手动指定。分发点先前叫做更新代理。

卡巴斯基私有安全网络 (KPSN)

“卡巴斯基私有安全网络”允许安装了 Kaspersky 应用程序的设备的用户访问“卡巴斯基安全网络”信誉数据库和其他统计数据，而不从他们的设备发送数据到“卡巴斯基安全网络”。卡巴斯基私有安全网络用于由于以下原因无法参与卡巴斯基安全网络的企业客户：

- 设备未连接到互联网。
- 传输任何数据到国家以外或企业局域网以外被法律或企业安全策略禁止。

反病毒保护服务提供商

提供给客户端组织基于 Kaspersky 解决方案的反病毒保护服务的组织。

反病毒数据库

包含截至反病毒数据库发布时 Kaspersky 已知的计算机安全威胁信息。反病毒数据库中的条目使得恶意代码在被扫描对象中被检测。反病毒数据库由 Kaspersky 专家创建，每小时更新一次。

受管理设备

包括在管理组中的企业网络设备。

可用更新

Kaspersky 应用程序模块的更新集，包含特定时间段积累的关键更新和应用程序架构更改。

备份文件夹

用于存储使用备份实用工具创建的管理服务器数据副本的专用文件夹。

安装包

使用 Kaspersky Security Center 远程管理系统创建的一组用于远程安装 Kaspersky 程序的文件。安装包包含安装应用程序所需的一系列设置，这些设置在安装后立即运行。应用程序默认设置。使用包含在应用程序分发工具中的扩展名为 .kpd 和 .kud 的文件创建安装包。

客户端管理员

客户组织中负责监控反病毒保护状态的员工。

密钥文件

带有.key扩展名的文件，可以用来以试用或商用授权许可使用 Kaspersky 应用程序。

广播域

网络的一个逻辑区域，在这里所有节点可以使用广播通道在 OSI 层（Open Systems Interconnection Basic Reference Model）交换数据。

应用程序商店

Kaspersky Security Center Linux 组件。应用程序商店用于安装应用程序到用户 Android 设备。应用程序商店允许您发布应用程序 APK 文件和链接到 Google Play。

归属管理服务器

归属管理服务器是网络代理安装过程中指定的管理服务器。归属管理服务器可在网络代理连接配置文件中被使用。

手动安装

从分发包安装安全应用程序到企业网络中的设备。手动安装需要管理员或其他 IT 专家的参与。通常情况下，如果远程安装发生错误，则执行手动安装。

授权的应用程序组

由管理员根据标准设置（例如，根据供应商）创建的应用程序组，系统将维护已安装至客户端设备的应用程序的统计信息。

授权许可期限

可以访问程序功能并且有权使用附加服务的时间段。您可以使用的服务取决于授权许可的类型。

更新

替换或者添加从 Kaspersky 更新服务器接收到的新文件（数据库或应用程序模块）的过程。

服务提供商管理员

反病毒保护服务提供商的员工。该管理员为基于 Kaspersky 反病毒产品的反病毒保护系统执行安装和维护工作，并且向客户提供技术支持。

本地任务

在单台客户端计算机上定义和运行的任务。

本地安装

将安全应用程序安装在企业网络的设备上，手动安装始于安全应用程序分发包或者预先下载到设备的已发布安装包。

活动授权许可

应用程序当前使用的密钥。

特定设备的任务

从任意管理组分配给一组客户端设备并且在那些设备上执行的任务。

直接应用程序管理

通过本地界面进行的应用程序管理。

程序设置

对所有任务类型通用并且掌管应用程序总体操作的应用程序设置，例如：应用程序性能设置、报告设置和备份设置。

策略

策略决定应用程序设置并管理应用程序在管理组中计算机上的配置。必须为每个应用程序都创建单独的策略。您可以为安装在每个管理组中计算机上的应用程序创建多个策略，但是对于管理组中的每个应用程序，一次只能应用一个策略。

管理员工作站

在其上打开 Kaspersky Security Center Web Console 的设备。该组件提供了 Kaspersky Security Center Linux 管理界面。

管理员工作站用于配置和管理 Kaspersky Security Center Linux 的服务器部分。使用管理员工作站，管理员基于 Kaspersky 应用程序为企业局域网创建和管理一个集中的反病毒保护系统。

管理员权限

在 Exchange 组织内管理 Exchange 对象所需的用户权限。

管理控制台

基于 Windows 的 Kaspersky Security Center 的组件（也称为基于 MMC 的管理控制台）。此组件提供管理服务器和网络代理的管理服务用户界面。管理控制台类似于 Kaspersky Security Center Web Console。

管理服务器

Kaspersky Security Center Linux 的一个组件，可集中存储企业网络内安装的所有 Kaspersky 应用程序的信息。它也可用于管理这些应用程序。

管理服务器客户端（客户端设备）

安装网络代理和运行受管理的 Kaspersky 程序的设备、服务器或工作站。

管理服务器数据备份

使用备份实用工具复制管理服务器数据，以便进行备份和后续的恢复。该实用工具可以保存：

- 管理服务器数据库（策略、任务、应用程序设置、管理服务器上保存的事件）
- 有关管理组和客户端设备的结构的配置详情
- 用于远程安装应用程序的安装文件存储库（文件夹内容：软件包、卸载更新）
- 管理服务器证书

管理服务器证书

管理服务器用于以下目的的证书：

- 连接到 Kaspersky Security Center Web Console 时的管理服务器身份验证
- 受管理设备上管理服务器和网络代理之间的安全交互
- 将主管理服务器连接到从属管理服务器时的管理服务器身份验证

安装管理服务器时会自动创建证书，然后存储在管理服务器上。

管理组

以功能和安装的 Kaspersky 应用程序分组的设备集。设备被分组成一个单一实体以便管理。组可以包含其他组。组策略和组任务可以为组中每个安装的应用程序创建。

组任务

为某个管理组定义并在该管理组中所有客户端设备上执行的任务。

网络代理

Kaspersky Security Center Linux 的一个组件，它实现了管理服务器和特定网络节点（工作站或服务器）上安装的 Kaspersky 应用程序之间的交互。该组件是公司内所有 Microsoft® Windows® 应用程序的通用组件。对于为 Unix 和 MacOS 之类的平台开发的 Kaspersky 产品，分别有不同版本的网络代理。

网络保护状态

当前保护状态，它定义了企业网络设备的安全。网络保护状态包括已安装的安全应用程序、授权许可密钥的使用状态及检测到的威胁的数量和类型等因素。

网络反病毒保护

一组能够降低病毒和垃圾邮件感染组织网络的可能性并防止网络攻击、钓鱼和其他威胁的技术和组织措施。当您使用安全应用程序和服务和应用企业数据安全策略时，网络安全被增加。

虚拟管理服务器

Kaspersky Security Center Linux 组件，用于管理客户端式组织的网络的保护系统。

虚拟管理服务器是从属管理服务器的特例，与物理管理服务器相比，具有以下限制：

- 只能在主管理服务器上创建虚拟管理服务器。
- 虚拟管理服务器在其操作中使用主管理服务器数据库。虚拟管理服务器不支持数据备份和还原任务以及更新扫描和下载任务。
- 虚拟服务器不支持从属管理服务器（包括虚拟服务器）的创建。

角色组

授予相同的管理员权限的 Exchange ActiveSync 移动设备的一组用户。

设备所有者

设备所有者就是管理员需要在设备上运行操作时可以联系的用户。

身份验证代理

允许您完成访问已加密硬盘驱动器的身份验证和在可启动磁盘驱动器加密后加载操作系统的界面。

还原

将对象从隔离区或备份区恢复至其在隔离、清除或删除前所在的原始位置或移动至用户定义的文件夹。

还原管理服务器数据

使用备份实用程序从备份区中保存的信息还原管理服务器数据。该实用程序可以还原：

- 管理服务器数据库（策略、任务、应用程序设置、管理服务器上保存的事件）

- 有关管理组和客户端计算机的结构的配置详情
- 用于远程安装应用程序的安装文件存储库（文件夹内容：软件包、卸载更新）
- 管理服务器证书

远程安装

使用 Kaspersky Security Center Linux 提供的服务安装卡巴斯基实验室程序。

连接网关

*连接网关*是以特殊模式运行的网络代理。连接网关接受来自其他网络代理的连接，并通过其自身与服务器的连接将它们与管理服务器建立隧道连接。与普通的网络代理不同，连接网关等待来自管理服务器的连接，而不是建立与管理服务器的连接。

配置文件

Exchange 移动设备的设置集合，定义了移动设备连接至 Microsoft Exchange Server 后的行为。

配置文件

包含设置集合和 iOS MDM 移动设备限制的策略。

附加订阅密钥

证明程序的使用权限、但是目前尚未使用的密钥。

隔离区域（DMZ）

隔离区是一段本地网络，其包含响应来自全局网络的请求的服务器。为确保组织的本地网络的安全性，对隔离区中的 LAN 的访问受防火墙的保护。

集中式应用程序管理

使用 Kaspersky Security Center 中提供的管理服务进行远程应用程序管理。

有关第三方代码的信息

有关第三方代码的信息包含在应用程序安装目录内的 legal_notices.txt 文件中。

商标声明

注册商标和服务标志均为其各自拥有者的财产。

Adobe、Acrobat、Flash、Shockwave 和 PostScript 是 Adobe 在美国和/或其他国家/地区的商标或注册商标。

AMD 和 AMD64 是 Advanced Micro Devices, Inc. 的商标或注册商标。

Amazon、Amazon Web Services、AWS、Amazon EC2、AWS Marketplace 是 Amazon.com, Inc. 或其附属公司的商标。

Apache 是 Apache Software Foundation 的注册商标或商标。

Apple、AirPlay、AirDrop、AirPrint、App Store、Apple Configurator、AppleScript、FaceTime、FileVault、iBook、iBooks、iCloud、iPad、iPhone、iTunes、Leopard、macOS、Mac、Mac OS、OS X、Safari、Snow Leopard、Tiger、QuickTime 和 Touch ID 是 Apple Inc. 的商标。

Arm 是 Arm Limited（或其子公司）在美国和/或其他地方的注册商标。

蓝牙词语，标志和标识都为 Bluetooth SIG, Inc. 所有。

Ubuntu、LTS 是 Canonical Ltd. 的注册商标。

Cisco、Cisco Systems、IOS 是 Cisco Systems, Inc. 和/或其附属公司在美国和其他特定国家的注册商标。

Citrix 和 XenServer 是 Citrix Systems, Inc. 和/或其附属公司在美国专利及商标局和其他国家的注册商标。

Corel 是 Corel Corporation 和/或其附属公司在美国和其他特定国家的注册商标。

Cloudflare、Cloudflare 徽标和 Cloudflare Workers 是 Cloudflare, Inc. 在美国和其他司法管辖区的商标和/或注册商标。

Dropbox 是 Dropbox, Inc. 的商标。

Firebird 是 Firebird Foundation 的注册商标。

Foxit 是 Foxit Corporation 的注册商标。

FreeBSD 是 FreeBSD foundation 的注册商标。

Google、Android、Chrome、Chromium、Dalvik、Firebase、Google Chrome、Google Earth、Google Play、Google Maps、Google Public DNS、Hangouts 和 YouTube 是 Google, LLC. 的商标。

EulerOS、FusionCompute、FusionSphere 是华为技术有限公司的商标。

Intel、Core 和 Xeon 是 Intel Corporation 在美国和其他国家/地区注册的商标。

IBM、QRadar 是 International Business Machines Corporation 在全球众多司法管辖区的注册商标。

Node.js 是 Joyent, Inc. 的商标。

Linux 是 Linus Torvalds 在美国和其他国家的注册商标。

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 和 Windows Azure 是 Microsoft 公司集团的商标。

Mozilla、Firefox、Thunderbird 是 Mozilla Foundation 在美国和其他国家/地区的商标。

Novell 是 Novell Enterprises Inc. 在美国和其他国家/地区的注册商标。

OpenSSL 是 OpenSSL 软件基金会拥有的商标。

Oracle、Java、JavaScript 和 TouchDown 是 Oracle 和/或其附属公司的注册商标。

Parallels、Parallels 徽标和 Coherence 是 Parallels International GmbH 的商标或注册商标。

Chef 是 Progress Software Corporation 和/或其子公司或附属公司之一在美国和/或其他国家/地区的商标或注册商标。

Puppet 是 Puppet, Inc. 的商标或注册商标。

Python 是 Python Software Foundation 的商标或注册商标。

Red Hat、Fedora 和 Red Hat Enterprise Linux 是 Red Hat Inc. 或其子公司在美国和其他国家/地区的商标或注册商标。

Ansible 是 Red Hat, Inc. 在美国和其他国家/地区的注册商标。

CentOS 是 Red Hat, Inc. 或其附属公司在美国和其他国家/地区的注册商标。

BlackBerry 是 Research In Motion Limited 所有的商标，在美国和/或其他国家注册。

Debian 是 Public Interest, Inc. 公司的软件的注册商标。

Splunk、SPL 是 Splunk Inc. 在美国和其他国家/地区的商标和注册商标。

SUSE 是 SUSE LLC 在美国和其他国家/地区的注册商标。

Symbian 是 Symbian Foundation Ltd. 所拥有的商标。

OpenAPI 是 The Linux Foundation 的商标。

VMware、VMware vSphere 和 VMware Workstation 是 VMware, Inc. 在美国和/或其他国家的注册商标或商标。

UNIX 是在美国和其他国家的注册商标，通过 X/Open Company Limited 授权。

Zabbix 是 Zabbix SIA 的注册商标。