kaspersky

# Kaspersky Security Center 14 Linux

© 2025 AO Kaspersky Lab

# 目录


Kaspersky Security Center 14 Linux 帮助
新闻
关于 Kaspersky Security Center Linux
- 硬件和软件要求
- 关于 Kaspersky Security Center 14 Web Console
- 兼容的卡巴斯基应用程序和解决方案
- Kaspersky Security Center 的比较：基于 Windows 与基于 Linux

基本概念
- 管理服务器
- 管理服务器层级
- 虚拟管理服务器
- Web 服务器
- 网络代理
- 管理组
- 受管理设备
- 未分配的设备
- 管理员工作站
- 管理 Web 插件
- 策略
- 策略配置文件
- 任务
- 任务范围
- 本地应用程序设置与策略的关系
- 分发点
- 连接网关

授权许可
- 关于最终用户授权许可协议
- 关于授权许可
- 关于授权许可证书
- 关于授权许可密钥
- 查看隐私策略
- Kaspersky Security Center 授权许可选项
- 关于密钥文件
- 关于数据提供
- 关于订阅
- 超出了授权许可限制事件

架构
Kaspersky Security Center 管理服务器部署图表和 Kaspersky Security Center 14 Web Console
Kaspersky Security Center Linux 使用的端口
Kaspersky Security Center 14 Web Console 使用的端口
安装
- 主要安装方案
- 配置与 Kaspersky Security Center 14 Linux 配合使用的 MariaDB x64 服务器
- 配置与 Kaspersky Security Center 14 Linux 配合使用的 MySQL x64 服务器
- Kaspersky Security Center 的安装
- 以静默模式安装 Kaspersky Security Center

- 在封闭软件环境模式下在 Astra Linux 上安装Kaspersky Security Center
- 安装 Kaspersky Security Center 14 Web Console
- Kaspersky Security Center 14 Web Console 安装参数
- 安装 Kaspersky Security Center 14 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
- 以静默模式安装 Linux 网络代理（使用应答文件）
- 在封闭软件环境模式下在 Astra Linux 上安装网络代理
- 使用 DBMS 的账户
  - 配置使用 MySQL 和 MariaDB 的 DBMS 账户
- Kaspersky Security Center Linux 故障转移集群部署
  - 方案：部署 Kaspersky Security Center Linux 故障转移集群
  - 关于 Kaspersky Security Center Linux 故障转移集群
  - 为 Kaspersky Security Center Linux 故障转移集群准备文件服务器
  - 为 Kaspersky Security Center Linux 故障转移集群准备节点
  - 在 Kaspersky Security Center 故障转移集群节点上安装 Kaspersky Security Center
  - 手动启动和停止集群节点
- 用于 Kaspersky Security Center 的证书
  - 关于 Kaspersky Security Center 证书
  - 对 Kaspersky Security Center 中使用的自定义证书的要求
  - 重新颁发 Kaspersky Security Center 14 Web Console 的证书
  - 替换 Kaspersky Security Center 14 Web Console 证书
  - 将 PFX 证书转换为 PEM 格式
  - 场景：指定自定义管理服务器证书
  - 使用 klsetsrvcert 实用程序替换管理服务器证书
  - 使用 klmover 实用程序将网络代理连接到管理服务器
- 定义共享文件夹

升级 Kaspersky Security Center Linux

- 使用安装文件升级 Kaspersky Security Center Linux
- 通过备份升级 Kaspersky Security Center Linux

登录到 Kaspersky Security Center 14 Web Console 并登出

快速启动向导

- 步骤 1：指定互联网连接设置
- 步骤 2：选择应用程序激活方法
- 步骤 3：创建基本的网络保护配置
- 步骤 4：配置邮件通知
- 步骤 5：关闭快速启动向导

保护部署向导

- 步骤 1：开始保护部署向导
- 步骤 2：选择安装包
- 步骤 3：选择分发密钥文件或激活码的方法
- 步骤 4：选择网络代理版本
- 步骤 5：选择设备
- 步骤 6：指定远程安装任务设置
- 步骤 7：安装前删除不兼容的应用程序
- 步骤 8：移动设备到受管理设备
- 步骤 9：选择访问设备的账户
- 步骤 10：开始安装

配置管理服务器

- 配置 Kaspersky Security Center 14 Web Console 到管理服务器的连接
- 配置用于连接到 Kaspersky Security Center 的 IP 地址允许列表
- 配置管理服务器连接事件记录
- 设置事件存储库中的最大事件数量
- 备份复制和管理服务器数据恢复
  - 创建管理服务器数据备份任务
  - 使用 klbackup 实用程序备份和恢复数据
- 将管理服务器移动至其他设备
- 创建虚拟管理服务器
- 管理服务器层级
- 创建管理服务器层级：添加从属管理服务器
- 查看从属管理服务器列表
- 启用账户保护以防止未经授权的修改
- 两步验证
  - 关于账户的两步验证
  - 方案：为所有用户配置两步验证
  - 为您自己的账户启用两步验证
  - 对所有用户启用必需的两步验证
  - 禁用用户账户的两步验证
  - 对所有用户禁用必需的两步验证
  - 从两步验证中排除账户
  - 生成新的 secret key
  - 编辑安全代码颁发者的名称
- 更改允许的密码输入尝试次数
- 更改 DBMS 凭据
- 删除管理服务器层级
- 配置界面

发现网络设备

- 情景：发现网络设备
- IP 范围轮询
- 添加和修改 IP 范围
- Zeroconf 轮询
- 设备标签
  - 关于设备标签
  - 创建设备标签
  - 重命名设备标签
  - 删除设备标签
  - 查看分配了标签的设备
  - 查看分配到设备的标签
  - 手动标记设备
  - 从设备上删除分配的标签
  - 查看自动标记设备规则
  - 编辑自动标记设备规则
  - 创建自动标记设备规则
  - 为自动标记设备运行规则
  - 删除自动标记设备规则
  - 使用 klscflag 实用程序管理设备标签
- 应用程序标签

- 应用程序标签
- 创建应用程序标签
- 重命名应用程序标签
- 分配标签到应用程序
- 从应用程序上删除分配的标签
- 删除应用程序标签

部署 Kaspersky 应用程序
- 方案：Kaspersky 应用程序部署
- 添加 Kaspersky 应用程序的管理插件
- 从文件创建安装包
- 创建独立安装包
- 查看独立安装包列表
- 准备 Linux 设备并在 Linux 设备上远程安装网络代理
- 使用远程安装任务安装应用程序
  - 在特定设备上安装应用程序
  - 在从属管理服务器上安装应用程序
- 指定 Unix 设备上的远程安装设置
- 启动和停止卡巴斯基应用程序
- 替换第三方安全应用程序
- 远程删除应用程序或软件更新
- 准备运行 SUSE Linux Enterprise Server 15 的设备以安装网络代理

Kaspersky 应用程序：授权许可和激活
- 受管理应用程序的授权许可
- 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
- 自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
- 从存储库删除授权许可密钥
- 撤销对最终用户授权许可协议的同意
- 续订 Kaspersky 应用程序授权许可
- 使用 Kaspersky Marketplace 选择 Kaspersky 商业解决方案

配置网络保护
- 方案：配置网络保护
- 关于以设备为中心和以用户为中心的安全管理方法
- 策略设置和传播：以设备为中心的方法
- 策略设置和传播：以用户为中心的方法
- Kaspersky Endpoint Security 更新组任务的手动设置
- 网络代理策略设置
- 任务
  - 关于任务
  - 关于任务范围
  - 创建任务
  - 手动启动任务
  - 查看任务列表
  - 常规任务设置
  - 启动更改任务密码向导
    - 步骤 1：指定凭证
    - 步骤 2：选择要采取的操作

步骤 3：查看结果
浏览保存在管理服务器中的任务运行结果
管理客户端设备
受管理设备设置
创建管理组
设备移动规则
创建设备移动规则
复制设备移动规则
设备移动规则的条件
手动将设备添加到管理组
手动将设备或者集群移动至管理组
更改客户端设备的管理服务器
通过连接网关将连接到管理服务器的设备移动到另一台管理服务器
当设备显示不活动时查看和配置操作
关于设备状态
配置设备状态切换
策略和策略配置文件
关于策略和策略配置文件
关于“锁定”和锁定的设置
策略继承和策略配置文件
策略层级
策略层级中的策略配置文件
如何在受管理设备上实施设置
管理策略
查看策略列表
创建策略
常规策略设置
修改策略
启用和禁用策略继承选项
复制策略
移动策略
强制同步
查看策略分发状态图
删除策略
管理策略配置文件
查看策略配置文件
更改策略配置文件优先级
创建策略配置文件
复制策略配置文件
创建策略配置文件激活规则
删除策略配置文件
用户和用户角色
关于用于角色
配置对应用程序功能的访问权限。基于角色的访问控制
应用程序功能的访问权限
预定义用户角色
添加内部用户账户
创建安全组

编辑内部用户账户
编辑安全组
添加用户账户到内部组
指派用户作为设备所有者
删除用户或安全组
创建用户角色
编辑用户角色
编辑用户角色范围
删除用户角色
关联策略配置文件到角色
传输用户角色到从属管理服务器
管理对象修订
回滚对象到先前修订
对象删除
使用 klscflag 实用程序开放端口 13291
使用 klscflag 实用程序打开 OpenAPI 端口
更新 Kaspersky 数据库和应用程序
方案：定期更新 Kaspersky 数据库和应用程序
关于更新 Kaspersky 数据库、软件模块和应用程序
创建"将更新下载至管理服务器存储库"任务
浏览已下载的更新
验证已下载的更新
分发点和连接网关的调整
关于分发点
分发点的标准配置：单一办公室
分发点的标准配置：多个小远程办公室
计算分发点的数量和配置
自动分配分发点
手动分配分发点
修改管理组的分发点列表
启用推送服务器
增加 klnagent 服务的文件描述符限制
创建"将更新下载至分发点存储库"任务
通过分发点下载更新
添加"将更新下载至管理服务器存储库"任务的更新源
关于使用 diff 文件更新 Kaspersky 数据库和软件模块
启用下载 diff 文件功能
更新离线设备上的 Kaspersky 数据库和软件模块
备份和恢复 Web 插件
管理客户端设备上的第三方应用程序和可执行文件
方案：应用程序管理
关于应用程序控制
获取并查看客户端设备上存储的可执行文件列表
创建含有手动添加内容的应用程序类别
查看应用程序类别列表
添加事件相关的可执行文件到应用程序类别
监控和报告
方案：监控和报告

关于监控和报告的类型
仪表板和小部件
使用控制板
添加小部件到控制板
从控制板隐藏小部件
移动小部件到控制板
更改小部件尺寸或样子
更改小部件设置
关于仅仪表板模式
配置仅仪表板模式
报告
使用报告
创建报告模板
查看和编辑报告模板属性
导出报告到文件
生成和浏览报告
创建报告发送任务
删除报告模板
事件和事件分类
关于 Kaspersky Security Center Linux 中的事件
Kaspersky Security Center Linux 组件事件
事件类型描述的数据结构
管理服务器事件
管理服务器严重事件
管理服务器功能失败事件
管理服务器警告事件
管理服务器信息事件
网络代理事件
网络代理警告事件
网络代理信息事件
使用事件分类
创建事件分类
编辑事件分类
查看事件分类列表
查看事件详情
导出事件到文件
从事件查看对象历史
删除事件
删除事件分类
设置事件存储期限
阻止频繁事件
关于阻止频繁事件
管理频繁事件阻止
移除对频繁事件的阻止
在管理服务器上的事件处理和存储
通知和设备状态
使用通知
查看屏幕通知

- 关于设备状态
- 配置设备状态切换
- 配置通知传送
- 测试通知
- 通过运行可执行文件显示的事件通知
- 卡巴斯基公告
  - 关于 Kaspersky 公告
  - 指定 Kaspersky 公告设置
  - 禁用 Kaspersky 公告
- 导出事件到 SIEM 系统
  - 配置导出事件到 SIEM 系统
  - 在您开始之前
  - 关于事件导出
  - 关于配置 SIEM 系统中的事件导出
  - 标记要以 Syslog 格式导出到 SIEM 系统的事件
    - 关于标记要以 Syslog 格式导出到 SIEM 系统的事件
    - 标记要以 Syslog 格式导出的 Kaspersky 应用程序事件
    - 标记要以 Syslog 格式导出的常规事件
  - 关于使用 Syslog 格式导出事件
  - 配置 Kaspersky Security Center Linux 以将事件导出到 SIEM 系统
  - 直接从数据库导出事件
    - 使用 klsql2 实用工具执行 SQL 查询
    - klsql2 实用工具中的 SQL 查询例子
    - 查看 Kaspersky Security Center Linux 数据库名称
  - 查看导出结果
- 设备分类
  - 从设备分类中查看设备列表
  - 创建设备分类
  - 配置设备分类
  - 从设备分类中导出设备列表
  - 在分类中从管理组中删除设备
- 更改 Kaspersky Security Center 14 Web Console 界面的语言
- API 参考指南
- 服务提供商最佳实践
  - 计划 Kaspersky Security Center Linux 部署
    - 提供到管理服务器的互联网访问
    - Kaspersky Security Center Linux 标准配置
    - 关于分发点
    - 管理服务器层级
    - 虚拟管理服务器
  - 部署和初始化设置
    - 管理服务器安装建议
      - 在失败转移集群上为管理服务器服务创建账户
      - 选择 DBMS
      - 指定管理服务器地址
    - 部署网络代理和安全应用程序
    - 在客户端组织网络中配置保护
      - Kaspersky Endpoint Security 策略的手动设置

在高级威胁防护区域配置策略
在关键威胁防护部分配置策略
在常规设置部分配置策略
在事件配置区域配置策略
Kaspersky Endpoint Security 更新组任务的手动设置
Kaspersky Endpoint Security 设备扫描组任务的手动设置
计划"查找漏洞和所需更新"任务
更新安装和漏洞修复组任务的手动设置
建立管理组结构和分配分发点
标准 MSP 客户端配置：单一办公室
标准 MSP 客户端配置：多个小远程办公室
策略层级，使用策略配置文件
策略层级
策略配置文件
任务
设备移动规则
软件分类
管理服务器设置的备份和恢复
管理服务器设备不可操作
管理服务器设置或数据库被损坏
关于漫游用户的连接配置文件
远程访问受管理设备
使用"不要断开与管理服务器的连接"选项提供受管理设备和管理服务器之间的持续连接
关于检查设备和管理服务器之间的连接时间
关于强制同步
Kaspersky Security Center 14 Web Console 与其他 Kaspersky 解决方案之间的集成
配置到 KATA / KEDR Web Console 的访问
联系技术支持
如果获得技术支持
通过 Kaspersky CompanyAccount 获得技术支持
获取管理服务器的转储文件
有关程序的信息源
已知问题
词汇表
HTTPS
JavaScript
Kaspersky Security Center System Health Validator (SHV)
Kaspersky Security Center Web Server
Kaspersky Security Center 操作员
Kaspersky Security Center 管理员
Kaspersky 更新服务器
Provisioning 配置文件
SSL
不兼容应用程序
事件严重级别
事件存储库
任务
任务设置

保护状态
共享证书
内部用户
分发点
卡巴斯基私有安全网络 (KPSN)
反病毒保护服务提供商
反病毒数据库
受管理设备
可用更新
备份文件夹
安装包
客户端管理员
密钥文件
广播域
应用程序商店
归属管理服务器
手动安装
授权许可期限
更新
服务提供商管理员
本地任务
本地安装
活动授权许可
特定设备的任务
直接应用程序管理
程序设置
策略
管理员工作站
管理员权限
管理控制台
管理服务器
管理服务器客户端（客户端设备）
管理服务器数据备份
管理服务器证书
管理组
组任务
网络代理
网络保护状态
网络反病毒保护
虚拟管理服务器
角色组
设备所有者
身份验证代理
还原
还原管理服务器数据
远程安装
连接网关
配置文件

配置文件
隔离区域（DMZ）
集中式应用程序管理
额外（或备用）授权许可密钥
有关第三方代码的信息
商标声明

# Kaspersky Security Center 14 Linux 帮助

| | | | |
|---|---|---|---|
| | 新闻<br>了解最新应用程序版本中的新增内容。 | | Kaspersky 应用程序。授权许可和激活<br>几步激活 Kaspersky 应用程序。 |
| | 替换第三方安全应用程序<br>学习卸载不兼容应用程序的方法。 | | 层级指南（仅限在线帮助）<br>要在不同的条件下优化性能，需要考虑网络设备数量、网络拓扑和您需要的 Kaspersky Security Center 功能集。 |
| | 硬件和软件要求<br>检查支持什么操作系统和应用程序版本。 | | 配置网络保护<br>管理组织的安全。 |
| | 安装<br>安装管理服务器和 Kaspersky Security Center 14 Web Console | | Kaspersky 应用程序。更新数据库和软件模块<br>维持保护系统的可靠性。 |
| | 发现网络设备<br>发现您组织网络中的现有设备和新设备。 | | 监控和报告<br>查看您的基础架构、保护状态和统计信息。 |
| | Kaspersky 应用程序。集中部署<br>计划资源使用、安装管理服务器、安装网络代理和安全应用程序到客户端设备。 | | 分发点和/或连接网关的调整<br>配置分发点。 |
| | 导出事件到 SIEM 系统<br>配置将事件导出到 SIEM 系统以进行分析。 | | |

# 新闻

## Kaspersky Security Center 14 Linux

Kaspersky Security Center 14 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 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 Kaspersky Industrial CyberSecurity for Linux Nodes 1.3。

# 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 Linux 设备的保护，以满足纯 Linux 环境的要求。

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，您可以使用详细的仪表板，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：

- 创建一台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。
- 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。

在美国境内，本软件中将不再提供更新功能（包括提供反病毒签名更新和代码库更新）以及 KSN 功能。

# 硬件和软件要求

## 管理服务器

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：存储管理服务器数据的文件夹 (/var/opt/kaspersky/klnagent_srv) 需要 10 GB。

支持以下操作系统：

- Debian GNU/Linux 11.x (Bullseye) 64 位
- Debian GNU/Linux 10.x (Buster) 64 位
- Debian GNU/Linux 9.x (Stretch) 64 位
- Ubuntu Server 20.04 LTS (Focal Fossa) 64 位
- Ubuntu Server 18.04 LTS (Bionic Beaver) 64 位
- CentOS 7.x 64 位
- Red Hat Enterprise Linux Server 8.x 64 位
- Red Hat Enterprise Linux Server 7.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 1.7）64 位
- Astra Linux 特别版 RUSB.10015-01（操作更新 1.6）64 位
- Astra Linux Common Edition（操作更新 2.12）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
- RED OS 7.3 Server 64 位
- RED OS 7.3 Certified Edition 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 Workstation 16 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
- 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 10.5（内部版本 10.5.27 及更高版本）32 位/64 位
- MariaDB 10.4.x 32 位/64 位
- MariaDB 10.3（内部版本 10.3.22 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
- MariaDB 10.1（内部版本 10.1.30 及更高版本）32 位/64 位

## Kaspersky Security Center 14 Web Console

## Kaspersky Security Center 14 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 11.x (Bullseye)
- Debian GNU/Linux 10.x (Buster)
- Debian GNU/Linux 9.x (Stretch)
- Ubuntu Server 20.04 LTS (Focal Fossa)
- Ubuntu Server 18.04 LTS (Bionic Beaver)
- CentOS 7.x
- Red Hat Enterprise Linux Server 8.x
- Red Hat Enterprise Linux Server 7.x
- SUSE Linux Enterprise Server 12 (所有服务包)
- SUSE Linux Enterprise Server 15 (所有服务包)
- SUSE Linux Enterprise Desktop 15 (Service Pack 3) ARM 64 位
- EulerOS 2.0 SP8 ARM
- Astra Linux 特别版 RUSB.10015-01（操作更新 1.7）
- Astra Linux 特别版 RUSB.10015-01（操作更新 1.6）
- Astra Linux Common Edition（操作更新 2.12）
- ALT Server 10
- ALT Server 9.2
- ALT 8 SP Server (LKNV.11100-01)
- ALT 8 SP Server (LKNV.11100-02)
- ALT 8 SP Server (LKNV.11100-03)
- Oracle Linux 8
- Oracle Linux 7
- RED OS 7.3 Server
- RED OS 7.3 Certified Edition
- 基于内核的虚拟机（Kaspersky Security Center 14 Web Console 服务器支持的所有 Linux 操作系统）

## 客户端设备

对于客户端设备，Kaspersky Security Center 14 Web Console 的使用仅需要一个浏览器。

最小屏幕分辨率为 1366x768 像素。

设备的硬件和软件需求和 Kaspersky Security Center 14 Web Console 所使用的浏览器的需求是相同的。

浏览器：

- Mozilla Firefox 扩展支持版本 91.8.0 或更高版本（91.8.0 于 2022 年 4 月 5 日发布）
- Mozilla Firefox 99.0 或更高版本（99.0 于 2022 年 4 月 5 日发布）
- 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

## 网络代理

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：

- Debian GNU/Linux 11.x (Bullseye) 32 位/64 位
- Debian GNU/Linux 10.x (Buster) 32 位/64 位
- Debian GNU/Linux 9.x (Stretch) 32 位/64 位
- Ubuntu Server 20.04 LTS (Focal Fossa) 32 位/64 位
- Ubuntu Server 20.04.04 LTS (Focal Fossa) ARM 64 位
- Ubuntu Server 18.04 LTS (Bionic Beaver) 32 位/64 位
- Ubuntu Desktop 20.04 LTS (Focal Fossa) 32 位/64 位
- Ubuntu Desktop 18.04 LTS (Bionic Beaver) 32 位/64 位
- CentOS 8.x 64 位
- CentOS 7.x 64 位

- CentOS 7.x ARM 64 位
- Red Hat Enterprise Linux Server 8.x 64 位
- Red Hat Enterprise Linux Server 7.x 64 位
- Red Hat Enterprise Linux Server 6.x 32 位/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 (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 特别版 RUSB.10015-01（操作更新 1.7）64 位
- Astra Linux 特别版 RUSB.10015-01（操作更新 1.6）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 Server 10 64 位
- ALT Server 9.2 64 位
- ALT Workstation 10 32 位/64 位
- ALT Workstation 9.2 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

- Linux Mint 19.x 32 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 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
- Lotos (Linux 核心版本 4.19.50, DE: MATE) 64 位

支持以下虚拟平台：

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware Workstation 16 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
- 基于内核的虚拟机（网络代理支持的所有 Linux 操作系统）

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

# 关于 Kaspersky Security Center 14 Web Console

Kaspersky Security Center 14 Web Console 是一个 Web 应用程序，设计用于管理由 Kaspersky 应用程序保护的网络的安全系统状态。

使用该应用程序，您可以执行以下操作：

- 管理组织的安全系统状态。
- 将 Kaspersky 应用程序安装到您网络上的设备并管理已安装的应用程序。
- 管理为您网络中的设备所创建的策略。
- 管理用户账户。
- 管理安装在您的网络设备上的应用程序任务。
- 查看有关安全系统状态的报告。
- 管理向系统管理员和其他 IT 专家传送报告的行为。

Kaspersky Security Center 14 Web Console 是一个网络接口，可确保您的设备和管理服务器能够通过浏览器进行通信。管理服务器是一个旨在对您网络中的设备上安装的 Kaspersky 应用程序进行管理的应用程序。管理服务器通过受安全套接字层 （SSL） 保护的通道连接到您的网络的设备。当您使用您的浏览器连接至 Kaspersky Security Center 14 Web Console 时，浏览器将与 Kaspersky Security Center 14 Web Console 服务器建立连接。

您按以下方式操作 Kaspersky Security Center 14 Web Console：

1. 使用浏览器连接至 Kaspersky Security Center 14 Web Console，其中显示了 Web 门户的界面。
2. 使用网页门户控件选择您想要运行的命令。Kaspersky Security Center 14 Web Console执行以下操作：
   - 如果您已选择用于接收信息的命令（例如，查看设备列表），Kaspersky Security Center 14 Web Console 会向管理服务器发送一个信息请求，接收必要数据，然后将其以适合查看的格式发送到浏览器。
   - 如果您已选择用于管理的命令（例如，远程安装应用程序），Kaspersky Security Center 14 Web Console 会从浏览器接收该命令并将其发送到管理服务器。然后，应用程序从管理服务器接收结果并以易于查看的格式将其发送到浏览器。

Kaspersky Security Center 14 Web Console 是一个多语言的应用程序。您可以在任意时刻更改界面语言，而不重新打开应用程序。当您将 Kaspersky Security Center 14 Web Console 与 Kaspersky Security Center 一起安装时，Kaspersky Security Center 14 Web Console 具有和安装文件一样的界面语言。当您仅安装 Kaspersky Security Center 14 Web Console 时，应用程序具有和您的操作系统一样的界面语言。如果 Kaspersky Security Center 14 Web Console 不支持安装文件或操作系统的语言，将默认设置英语。

## 兼容的卡巴斯基应用程序和解决方案

Kaspersky Security Center Linux 支持以下 Kaspersky 应用程序的集中部署和管理：

- Kaspersky Endpoint Security for Linux
- Kaspersky Industrial CyberSecurity for Linux Nodes

此应用程序可保护工作站和文件服务器。有关应用程序的版本，请参阅应用程序支持生命周期网页。

## Kaspersky Security Center 的比较：基于 Windows 与基于 Linux

Kaspersky 提供 Kaspersky Security Center 作为 Windows 和 Linux 这两个平台的本地解决方案。在基于 Windows 的解决方案中，在 Windows 设备上安装管理服务器，而基于 Linux 的解决方案具有设计为安装在 Linux 设备上的管理服务器版本。此在线帮助包含有关 Kaspersky Security Center Linux 的信息。有关基于 Windows 的解决方案的详细信息，请参阅 Kaspersky Security Center Windows 在线帮助。

通过下表可以比较 Kaspersky Security Center 作为基于 Windows 的解决方案和基于 Linux 的解决方案的主要功能。

Kaspersky Security Center 作为基于 Windows 的解决方案和基于 Linux 的解决方案的功能比较

| 功能或属性 | Kaspersky Security Center 14 | |
|---|---|---|
| | 基于 Windows 的解决方案 | 基于 Linux 的解决方案 |
| 管理服务器位置 | 本地 | 本地 |
| 数据库管理系统 (DBMS) 位置 | 本地 | 本地 |
| 在其中安装管理服务器的操作系统 | Windows | Linux |
| 管理控制台类型 | 本地和基于 Web | 基于 Web |
| 在其中安装基于 Web 的管理控制台的操作系统 | Windows 或 Linux | Windows 或 Linux |
| 管理服务器层级 | ✓ | ✓ |
| 管理组层级 | ✓ | ✓ |
| 网络轮询 | ✓ | ✓<br>（仅按 IP 范围） |
| 受管理设备最大数量 | 100,000 | 20,000 |
| 保护 Windows、macOS 和 Linux 管理的设备 | ✓ | —<br>（仅保护 Linux 设备） |
| 保护移动设备 | ✓ | — |
| 保护虚拟机 | ✓ | — |
| 保护公有云基础架构 | ✓ | — |
| 以设备为中心的安全管理 | ✓ | ✓ |
| 以用户为中心的安全管理 | ✓ | ✓ |
| 应用程序策略 | ✓ | ✓ |
| Kaspersky 应用程序的任务 | ✓ | ✓ |
| 卡巴斯基安全网络 | ✓ | — |
| KSN Proxy | ✓ | — |
| 卡巴斯基私有安全网络 | ✓ | — |
| 集中部署 Kaspersky 应用程序的授权许可密钥 | ✓ | ✓ |
| 支持虚拟管理服务器 | ✓ | ✓ |
| 安装第三方软件更新并修复第三方软件漏洞 | ✓ | —<br>（仅使用远程安装任务） |
| 有关受管理设备上发生的事件的通知 | ✓ | ✓ |
| 创建和管理用户账户 | ✓ | ✓ |
| 监控策略和任务状态 | ✓ | ✓ |
| 部署 Kaspersky Security Center 故障转移集群 | ✓ | ✓ |

# 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“`kladminserver_srv`”
- 设置为在操作系统启动时自动启动
- 具有“`ksc`”账户或在安装管理服务器过程中选择的用户账户

有关安装设置的完整列表，请参阅以下主题：安装 Kaspersky Security Center。

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 14 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 14 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 14 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。

*虚拟管理服务器*是从属管理服务器的一个特例。

在层次结构中，Kaspersky Security Center Linux 管理服务器只能用作辅助服务器，由基于 Windows 的 Kaspersky Security Center 或 Kaspersky Security Center Cloud Console 的主管理服务器管理。

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。

- 服务提供商如何使用 Kaspersky Security Center。服务提供商只需安装 Kaspersky Security Center 和 Kaspersky Security Center 14 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虚拟管理服务器。

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 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 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 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，您可以将该员工的设备从会计管理组移动到开发者管理组。然后，该设备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 14 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 14 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 14 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 14 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：

| 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 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 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

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 14 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 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。

> 安装在作为分发点的设备上的网络代理的功能和用例因操作系统而异。

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。

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*”的事件。事件将被发布在设备属性中，在**事故**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。

# 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。

一个连接网关最多可以接收 10,000 台设备的连接。

使用连接网关有两种选择：

- 我们建议您在隔离区域 (DMZ) 中安装连接网关。对于漫游设备上安装的其他网络代理，您需要专门配置通过连接网关与管理服务器进行的连接。

  连接网关不以任何方式修改或处理从网络代理传输到管理服务器的数据。此外，它不会将此数据写入任何缓冲区，因此不能接受来自网络代理的数据并随后将其转发到管理服务器。如果网络代理尝试通过连接网关连接到管理服务器，但是连接网关无法连接到管理服务器，则网络代理会认为管理服务器无法访问。所有数据保留在网络代理上（不在连接网关上）。

  一个连接网关无法通过另一个连接网关连接到管理服务器。这意味着网络代理不能在作为连接网关的同时，使用另一个连接网关连接到管理服务器。

  所有连接网关都包含在管理服务器属性的分发点列表中。

- 您还可以在网络内使用连接网关。例如，自动分配的分发点也将成为各自范围内的连接网关。但是，在内部网络中，连接网关的效益不高。它们会减少管理服务器收到的网络连接数量，但不会减少传入数据量。即使没有连接网关，所有设备仍可以连接到管理服务器。

# 授权许可

本节介绍与 Kaspersky Security Center 14 Linux 授权许可有关的常规概念。

## 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 Linux 网络代理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。

  请注意，在安装 Linux 网络代理时，网络代理的最终用户授权许可协议以英语显示。在安装过程中接受最终用户授权许可协议的条款之前，您可以在 /opt/kaspersky/klnagent64/share/license 文件夹中查看其他语言的网络代理最终用户授权许可协议。

- 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。

## 查看隐私策略。

在线查看隐私策略的网址为 https://www.kaspersky.com/products-and-services-privacy-policy。

隐私政策也可以离线查看：

- 您可以在安装 Kaspersky Security Center 前阅读隐私策略。
- 隐私策略文本包含在 Kaspersky Security Center 安装文件夹内的 license.txt 文件中。
- 受管理设备的网络代理安装文件夹中提供了 privacy_policy.txt 文件。
- 您可以从网络代理分发包中解压 privacy_policy.txt 文件。

## 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。

下列功能可用：

- 创建用于管理远程办公室网络或客户端组织网络的虚拟管理服务器。
- 创建一个管理组层级结构，作为一个单一实体管理特定设备。
- 控制组织的反病毒安全状态。
- 远程安装应用程序。
- 查看可用于远程安装的操作系统镜像的列表。
- 对安装在客户端设备上的应用程序的集中配置。
- 应用程序操作中的统计数据和报告，以及关于严重事件的通知。
- 查看和手动编辑网络轮询期间发现的硬件组件列表。
- 集中化操作被移至隔离区和备份区的文件以及被推迟进程的文件。
- 管理用户角色。

## 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

## 传输到权利持有人的数据

Kaspersky Security Center 14 Linux 最终用户授权许可协议中提供。

## 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：

- 作为在网络中通过扫描 IP 区间进行设备发现的结果，收到的有关组织网络中的设备的信息。管理服务器独立获取数据或从网络代理接收数据。
- 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 14 Web Console 界面中输入设备的显示名称和说明：

- 设备识别所需的受管理设备及其组件的技术说明：设备显示名称和描述、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）。

- 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。

- 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 14 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、活动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 14 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 14 Web Console 界面中输入数据。

- 漏洞和补丁管理功能处理的数据。网络代理将有关在受管理设备上检测到的硬件的信息（硬件注册表）从设备传输到管理服务器。

- 应用程序的用户类别。用户在 Kaspersky Security Center 14 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。

- 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。

- 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。

- 输入的激活码的详细信息。用户在管理控制台或 Kaspersky Security Center 14 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 14 Web Console 界面中输入数据。

- 管理对象的修订历史。用户在 Kaspersky Security Center 14 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 14 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 14 Web Console 界面中输入数据。

- 在 Kaspersky Security Center 14 Web Console 中显示 Kaspersky 公告所需的数据。用户在 Kaspersky Security Center 14 Web Console 界面中输入数据。

- Kaspersky Security Center 14 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 14 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 14 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 14 Web Console 界面中输入数据。

- 用户在 Kaspersky Security Center 14 Web Console 中输入的管理服务器数据。

- 用户在 Kaspersky Security Center 14 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 14 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。

- 管理服务器可独立获取有关联网设备的信息或从充当分发点的网络代理接收信息。

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 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 14 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。

# 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。

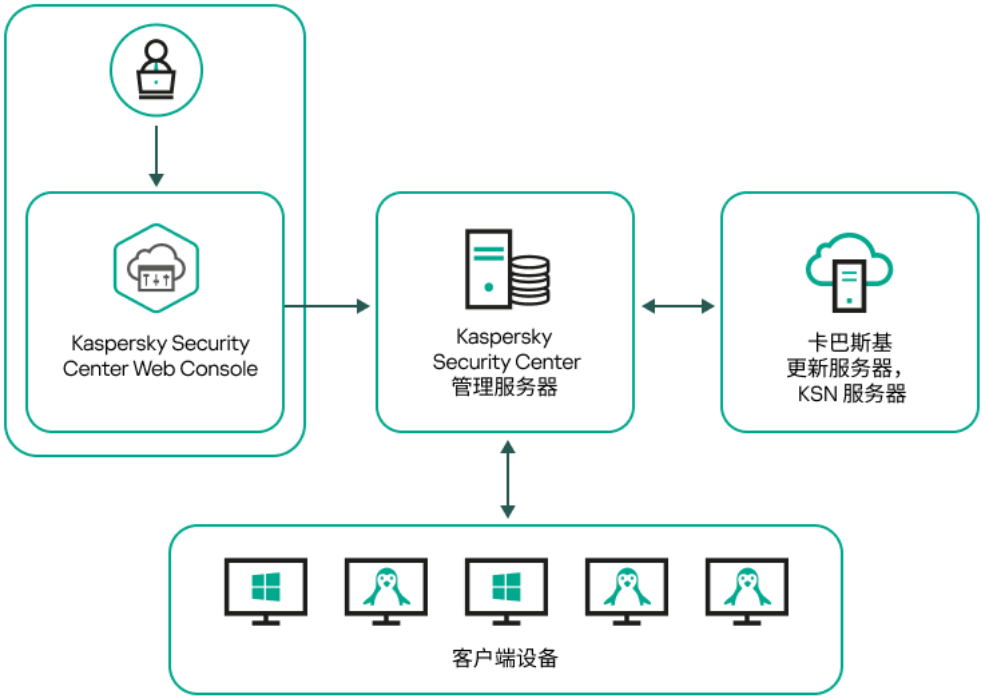
授权许可达到限制的此类事件的重要级别根据以下规则定义：

- 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。

# 架构

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



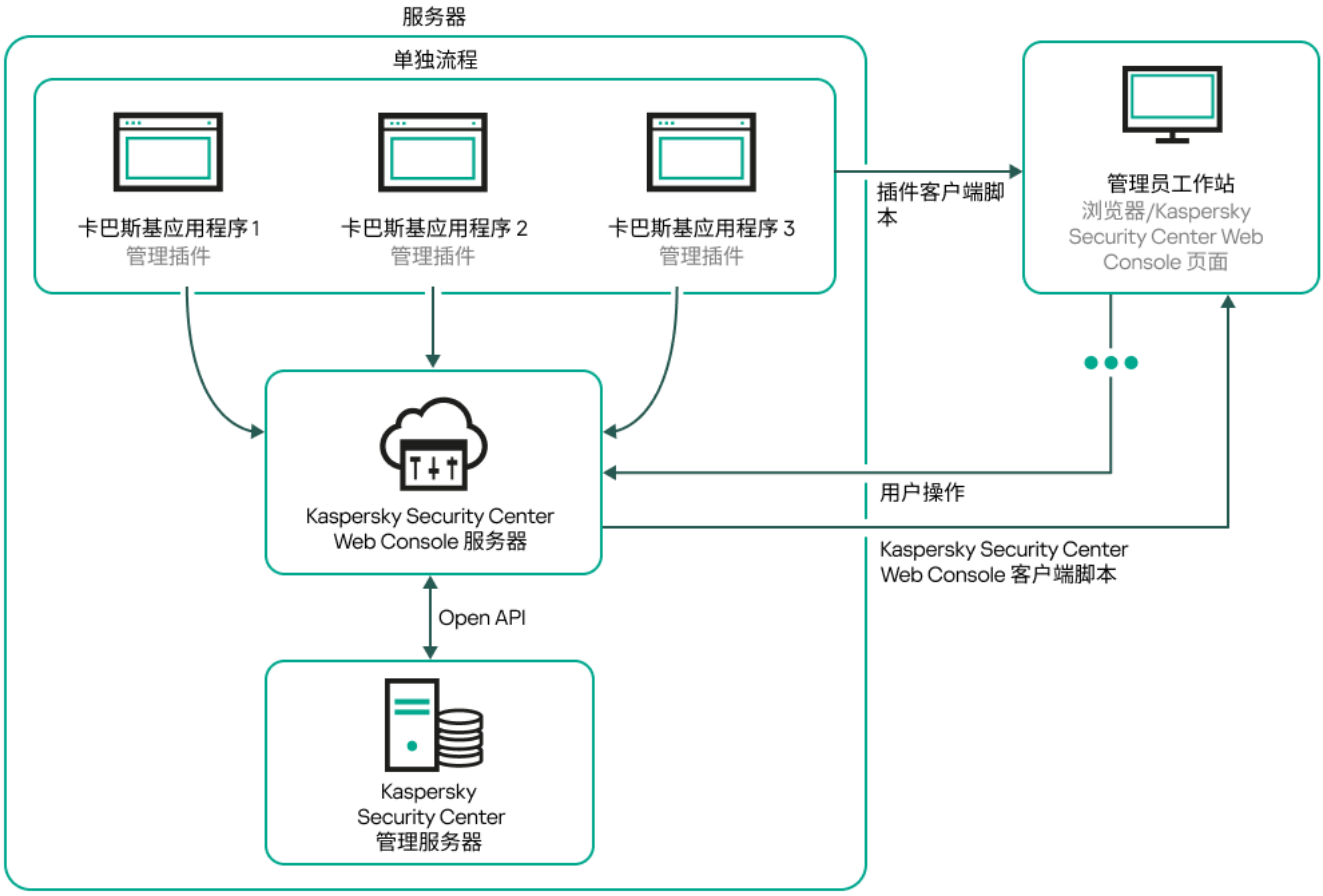

Kaspersky Security Center 14 Linux 架构

Kaspersky Security Center 14 Linux 包括以下主要组件：

- **Kaspersky Security Center 14 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。
- **客户端设备**。受 Kaspersky Security Center 14 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 管理服务器部署图表和 Kaspersky Security Center 14 Web Console

下图显示 Kaspersky Security Center 管理服务器部署图表和 Kaspersky Security Center 14 Web Console




Kaspersky Security Center 管理服务器部署图表和 Kaspersky Security Center 14 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 14 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 14 Web Console。

当您在 Kaspersky Security Center 14 Web Console 执行特定操作时，Kaspersky Security Center 14 Web Console 服务器通过 OpenAPI 与 Kaspersky Security Center 管理服务器交互。Kaspersky Security Center 14 Web Console 服务器从 Kaspersky Security Center 管理服务器请求所需信息并在 Kaspersky Security Center 14 Web Console 显示您的操作结果。

# Kaspersky Security Center Linux 使用的端口

下表显示管理服务器和客户端设备使用的默认端口。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。<br>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。<br>该参数可选。出于安全原因，我们建议使用 8061 TCP 端口。 |
| 8061 | klcsweb | TCP (TLS) | 传输发布的安装包到客户端设备 | 发布安装包。<br>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。<br>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。<br>您可以在网络代理策略设置中更改默认端口号。 |
| 13291 | klserver | TCP (TLS) | 接收从管理控制台到管理服务器的连接 | 管理管理服务器。<br>此端口默认关闭。如果您想使用 klakaut 实用程序来实现 Kaspersky Security Center Linux 的自动化运行，请使用 klscflag 实用程序打开 13291 端口。 |
| 13299 | klserver | TCP (TLS) | 接收从 Kaspersky Security Center 14 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 14 Web Console，OpenAPI。<br>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。<br>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。<br>该参数可选。出于安全原因，我们建议使用 1300 TCP 端口。 |
| 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。<br>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。<br>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。<br>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。 |

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 Kaspersky Security Center Web 14 Console 服务器使用的端口。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 14 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 14 Web Console 的连接 | Kaspersky Security Center 14 Web Console。<br>您可以在安装 Kaspersky Security Center 14 Web Console 时更改默认端口号。在 Linux ALT 操作系统上安装 Kaspersky Security Center 14 Web Console 时，您必须指定除 8080 以外的端口号，因为端口 8080 被操作系统使用。 |

下表显示安装网络代理的受管理设备使用的端口。

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。<br>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。<br>您可以在分发点属性窗口中更改默认端口号。 |
| 30522,<br>30523（本地主机接口上的端口） | klnagent | TCP | 使用 FileTransferBridge 组件从管理服务器接收卡巴斯基应用程序更新 | 从被指定为数据库更新源的管理服务器接收卡巴斯基应用程序更新的受管理设备。 |

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。

下表显示安装了网络代理用作分发点的受管理设备使用的端口。除了网络代理使用的端口，分发点设备也使用列出的端口（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。<br>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。<br>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。<br>您可以在分发点属性中更改默认端口号。 |

# Kaspersky Security Center 14 Web Console 使用的端口

下表列出了安装 Kaspersky Security Center 14 Web Console 服务器（也称为 Kaspersky Security Center 14 Web Console）的设备上必须开放的端口。

Kaspersky Security Center 14 Web Console 使用的端口

| 端口号 | 服务名称 | 协议 | 端口目的 | 范围 |
| --- | --- | --- | --- | --- |
| 2001 | Kaspersky Security Center 产品插件服务器 | HTTPS | 管理插件进程用于接收来自“Kaspersky Security Center Web Console 管理服务”的请求的 API 端口 | 运行管理插件的节点进程 |
| 1329, 2003 | Kaspersky Security Center Web Console 管理服务 | HTTPS | 用于从同一设备上运行的“Kaspersky Security Center Web Console 管理服务”接收请求的 API 端口 | 更新 Kaspersky Security Center 14 Web Console 组件 |
| 2005 | Kaspersky Security Center Web Console | HTTPS | 用于从同一设备上运行的“Kaspersky Security Center Web Console 管理服务”接收请求的 API 端口 | 运行 Kaspersky Security Center 14 Web Console 的节点进程 |
| 8200 | — | HTTP | 用于通过 HashiCorp Vault 生成证书的 API 端口（有关更多详细信息，请参见 HashiCorp Vault 网站 ） | 安装 Kaspersky Security Center 14 Web Console 并更新 Kaspersky Security Center 14 Web Console 组件 |
| 4150, 4151, 4152 | Kaspersky Security Center Web Console 消息队列 | HTTPS | 消息代理的 API 端口，用于 Kaspersky Security Center 14 Web Console 与管理插件的进程间通信 | Kaspersky Security Center 14 Web Console 与管理插件之间的交互 |

# 安装

该部分描述了 Kaspersky Security Center 和 Kaspersky Security Center 14 Web Console 的安装。

# 主要安装方案

按照此方案，您可以安装 Kaspersky Security Center 14 Linux 管理服务器和 Kaspersky Security Center 14 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 14 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 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。

   如果使用 MariaDB，您需要配置推荐的设置，以使 DBMS 与 Kaspersky Security Center 达到最佳工作状态。

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. **Kaspersky Security Center 的安装**

   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。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 14 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 14 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 14 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 14 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

您可以使用仪表板的小部件来监控您的网络，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。

# 配置与 Kaspersky Security Center 14 Linux 配合使用的 MariaDB x64 服务器

## my.cnf 文件的推荐设置

有关 DBMS 配置的更多详细信息，另请参阅账户配置过程。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. 将以下行输入 my.cnf 文件的 [mysqld] 部分中：

```
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=<值>
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
```

`innodb_buffer_pool_size` 的值不能小于预期 KAV 数据库大小的 80%。请注意，指定的内存是在服务器启动时分配的。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。如果您使用 MariaDB 10.4.3 或更早版本，所分配内存的实际大小大约比指定的缓冲区大小大 10%。

建议使用参数值 `innodb_flush_log_at_trx_commit=0`，因为值“1”或“2”会对 MariaDB 的运行速度产生负面影响。确保`innodb_file_per_table`参数设置为`1`。

对于 MariaDB 10.6，另外在 [mysqld] 部分输入以下行：

```
optimizer_prune_level=0
optimizer_search_depth=8
```

默认情况下，优化器加载项 `join_cache_incremental`、`join_cache_hashed`、`join_cache_bka` 已启用。如果这些加载项未启用，必须启用它们。

*要检查是否启用了优化器加载项：*

1. 在 MariaDB 客户端控制台中，执行以下命令：

```
SELECT @@optimizer_switch;
```

2. 确保其输出包含以下行：

```
join_cache_incremental=on
join_cache_hashed=on
join_cache_bka=on
```

如果这些行存在并且值为 `on`，则优化器加载项已启用。

如果缺少这些行或值为 `off`，则需要执行以下操作：

a. 在文本编辑器中打开 my.cnf 文件。

b. 在 my.cnf 文件中添加以下行：

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

加载项 `join_cache_incremental`、`join_cache_hash` 和 `join_cache_bka` 已启用。

# 配置与 Kaspersky Security Center 14 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，另请参阅账户配置过程。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.cnf 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。确保`innodb_file_per_table`参数设置为`1`。

# Kaspersky Security Center 的安装

该过程描述了如何安装 Kaspersky Security Center。

安装前：

- 安装 DBMS。
- 确保您要安装 Kaspersky Security Center 的设备运行支持的 Linux 分类。
- 确保 DNS 服务器在网络上可用。

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，请在拥有 root 权限的账户下运行以下说明中提供的命令。

*要 Kaspersky Security Center：*

1. 如果您的设备运行的是 Astra Linux 1.8 或更高版本，请执行此步骤中描述的操作。如果您的设备运行的是不同的操作系统，请转到下一步。

   a. 创建 /etc/systemd/system/kladminserver_srv.service.d 目录，并创建一个名为 override.conf 的文件，内容如下：

   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ExecStart=
   ExecStart=/opt/kaspersky/ksc64/sbin/klserver -d from_wd
   ```

   b. 创建 /etc/systemd/system/klwebsrv_srv.service.d 目录，并创建一个名为 override.conf 的文件，内容如下：

   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ExecStart=
   ExecStart=/opt/kaspersky/ksc64/sbin/klcsweb -d from_wd
   ```

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 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 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，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，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 DNS 名称或 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 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

您可以在 Linux 设备上安装 Kaspersky Security Center，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 的设备运行支持的 Linux 分类。

要以静默模式安装 Kaspersky Security Center：

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. 如果您的设备运行的是 Astra Linux 1.8 或更高版本，请执行此步骤中描述的操作。如果您的设备运行的是不同的操作系统，请转到下一步。

   a. 创建 /etc/systemd/system/kladminserver_srv.service.d 目录，并创建一个名为 override.conf 的文件，内容如下：

   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ExecStart=
   ExecStart=/opt/kaspersky/ksc64/sbin/klserver -d from_wd
   ```

   b. 创建 /etc/systemd/system/klwebsrv_srv.service.d 目录，并创建一个名为 override.conf 的文件，内容如下：

   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ```

```
ExecStart=
ExecStart=/opt/kaspersky/ksc64/sbin/klcsweb -d from_wd
```

3. 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
```

4. 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。

5. 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
```

6. 以静默模式运行 Kaspersky Security Center 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`

7. 创建一个使用 Kaspersky Security Center 14 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 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 个联网设备。<br>2 适用于 101 到 1,000 个联网设备。<br>3 适用于超过 1,000 个联网设备。 |
| 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。 | 3306 |
| 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 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<br>or<br>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<br>或<br>ExternalLoadBalancer |
| 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 | 是 | 虚拟网络适配器名称。 | |
| KLFOC_UNATT_CONN_MODE_VA_IPV4 | 这些变量之一是必需项 | 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 |

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

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

安装前：

- 安装数据库管理系统。
- 确保您要安装 Kaspersky Security Center 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。

*若要在 Astra Linux 特别版（操作更新 1.7）和 Astra Linux 特别版（操作更新 1.6）操作系统上安装Kaspersky Security Center：*

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. 如果您的设备运行的是 Astra Linux 1.8 或更高版本，请执行此步骤中描述的操作。如果您的设备运行的是不同的操作系统，请转到下一步。

   a. 创建 /etc/systemd/system/kladminserver_srv.service.d 目录，并创建一个名为 override.conf 的文件，内容如下：

   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ExecStart=
   ExecStart=/opt/kaspersky/ksc64/sbin/klserver -d from_wd
   ```

   b. 创建 /etc/systemd/system/klwebsrv_srv.service.d 目录，并创建一个名为 override.conf 的文件，内容如下：

   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ExecStart=
   ExecStart=/opt/kaspersky/ksc64/sbin/klcsweb -d from_wd
   ```

7. 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
   ```

8. 运行 Kaspersky Security Center 安装：

   ```
   # apt install /<path>/ksc64_[ 版本号 ]_amd64.deb
   ```

9. 运行 Kaspersky Security Center 配置：

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

10. 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，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，您必须接受隐私策略的条款。

11. 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 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 14 Web Console

该部分描述了如何单独安装 Kaspersky Security Center 14 Web Console 服务器 (也叫 Kaspersky Security Center 14 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 管理服务器。

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 14 Web Console：*

1. 确保您要安装 Kaspersky Security Center 14 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 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 14 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
   }
   ```

   我们建议您指定 1024 以上的端口号。如果您希望 Kaspersky Security Center 14 Web Console 在 1024 以下的端口上工作，则安装后您必须运行以下命令：

   ```
   sudo setcap 'cap_net_bind_service=+ep' /var/opt/kaspersky/ksc-web-console/node
   ```

   在 Linux ALT 操作系统上安装 Kaspersky Security Center 14 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 14 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 14 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 14 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 14 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 14 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 14 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 14 Web Console。

## Kaspersky Security Center 14 Web Console 安装参数

为了在运行 Linux 的设备上安装 Kaspersky Security Center 14 Web Console 服务器，您必须创建响应文件 —— 一个包含连接 Kaspersky Security Center 14 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": "组 1:用户 1",
  "managementServiceAccount": "组 1:用户 2",
  "serviceWebConsoleAccount": "组 1:用户 3",
  "pluginAccount": "组 1:用户 4",
  "messageQueueAccount": "组 1:用户 5"
}
```

我们建议您指定 1024 以上的端口号。如果您希望 Kaspersky Security Center 14 Web Console 在 1024 以下的端口上工作，则安装后您必须运行以下命令：

```
sudo setcap 'cap_net_bind_service=+ep' /var/opt/kaspersky/ksc-web-console/node
```

在 Linux ALT 操作系统上安装 Kaspersky Security Center 14 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 14 Web Console 到运行 Linux 的设备的参数

| 参数 | 描述 | 可用值 |
| --- | --- | --- |
| `address` | Kaspersky Security Center 14 Web Console 服务器（必需）。 | 字符串值。 |
| `port` | Kaspersky Security Center 14 Web Console 将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：<br>• 德语：`1031`<br>• 英语：`1033`<br>• 西班牙语：`3082`<br>• 西班牙语（墨西哥）：`2058`<br>• 法语：`1036`<br>• 日语：`1041`<br>• 哈萨克语：`1087`<br>• 波兰语：`1045`<br>• 葡萄牙语（巴西）：`1046`<br>• 俄语：`1049`<br>• 土耳其语：`1055`<br>• 简体中文：`4`<br>• 繁体中文：`31748`<br>如果没有指定值，则使用 English (en-US) 语言。 |
| `enableLog` | 是否要启用 Kaspersky Security Center 14 Web Console 活动日志。 | 布尔值：<br>• `true`—启用日志（默认选中）。<br>• `false`—禁用日志。 |
| `trusted` | 允许连接到 Kaspersky Security Center 14 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：<br>• 管理服务器地址<br>• Kaspersky Security Center 14 Web Console 用以连接到管理服务器的 OpenAPI 端口（默认是 13299） | 以下格式的字符串值：<br>`" server address \| port \| certificate path \| server name "`.<br>例如：<br>`"X.X.X.X\|13299\|/cert/server-1.cer\| Server 1 \|\|Y.Y.Y.Y\|13299\|/cert/server-2.cer\| Server 2 "`. |

| | | |
|---|---|---|
| | • 管理服务器证书路径<br>• 将显示在登录窗口的管理服务器名称<br><br>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。 | |
| 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：<br>• true – 本人确认已完全阅读、理解并接受本《最终用户授权许可协议》的条款和条件。<br>• false – 我不接受授权许可协议的条款（默认选择此选项）。<br><br>如果未指定任何值，Kaspersky Security Center 14 Web Console 安装程序会向您显示 EULA 并询问您是否同意接受 EULA 的条款。 |
| 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。<br>指定路径"/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"以使用现有证书。对于自定义证书，请指定此自定义证书的存储路径。 |
| 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 Kaspersky Security Center Web Console 服务的账户名称。 | 以下格式的字符串值："group name:user name".<br>例如："Group1:User1".<br>如果未指定任何值，Kaspersky Security Center 14 Web Console 安装程序会使用默认名称 user_management_%uid% 创建一个新账户。 |
| managementServiceAccount | 运行 Kaspersky Security Center Web Console 管理服务的特权账户名称。 | 以下格式的字符串值："group name:user name".<br>例如："Group1:User1".<br>如果未指定任何值，Kaspersky Security Center 14 Web Console 安装程序会使用默认名称 user_nodejs_%uid% 创建一个新账户。 |
| serviceWebConsoleAccount | 运行 Kaspersky Security Center Web Console 服务的账户名称。 | 以下格式的字符串值："group name:user name".<br>例如："Group1:User1".<br>如果未指定任何值，Kaspersky Security Center 14 Web Console 安装程序会使用默认名称 user_svc_nodejs_%uid% 创建一个新账户。 |
| pluginAccount | 运行 Kaspersky Security Center 产品插件服务的账户名称。 | 以下格式的字符串值："group name:user name".<br>例如："Group1:User1".<br>如果未指定任何值，Kaspersky Security Center 14 Web Console 安装程序会使用默认名称 user_web_plugin_%uid% 创建一个新账户。 |
| messageQueueAccount | 运行 Kaspersky Security Center Web Console 消息队列服务的账户名称。 | 以下格式的字符串值："group name:user name".<br>例如："Group1:User1".<br>如果未指定任何值，Kaspersky Security Center 14 Web Console 安装程序会使用默认名称 user_message_queue_%uid% 创建一个新账户。 |

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 14 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。

# 安装 Kaspersky Security Center 14 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 14 Web Console Server（以下也称为 Kaspersky Security Center 14 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 14 Web Console 之前，在Kaspersky Security Center 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 14 Web Console：*

1. 执行 Kaspersky Security Center 14 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 14 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 14 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 14 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 14 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 14 Web Console 的标准安装。

在安装完成后，桌面上将出现一个快捷方式，您可以登录到 Kaspersky Security Center 14 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。

# 以静默模式安装 Linux 网络代理（使用应答文件）

您可以使用应答文件（一个文本文件，其中包含一组自定义的安装参数：变量以及各自的值）安装 Linux 网络代理。使用此应答文件可以静默模式运行安装程序，即无需用户参与。

*要以静默模式安装 Linux 网络代理：*

1. 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。
2. 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。
3. 通过输入应答文件的全名（包括路径）来设置 KLAUTOANSWERS 环境变量的值，例如，如下所示：

   ```
   export KLAUTOANSWERS=/tmp/nagent_install/answers.txt
   ```
4. 在环境变量指定的目录中创建应答文件（TXT 格式）。将变量列表以 VARIABLE_NAME=variable_value 的格式添加到应答文件，每个变量一行。

   为了正确使用应答文件，必须在其中包含至少三个必需变量：

- KLNAGENT_SERVER
- KLNAGENT_AUTOINSTALL
- EULA_ACCEPTED

您还可以添加任意可选变量以使用更具体的远程安装参数。下表列出了可以包含在应答文件中的所有变量：
用作以静默模式安装 Linux 网络代理的参数的应答文件变量

用作以静默模式安装 Linux 网络代理的参数的应答文件变量

| 变量名称 | 是否必需 | 描述 | 可能值 |
|---|---|---|---|
| KLNAGENT_SERVER | 是 | 包含显示为完全限定域名 (FQDN) 或 IP 地址的管理服务器名称。 | DNS 名称或 IP 地址。 |
| KLNAGENT_AUTOINSTALL | 是 | 定义是否启用静默安装模式。 | 1—启用静默模式；安装过程中不提示用户进行任何操作。<br><br>其他—禁用静默模式；安装过程中可能提示用户进行操作。 |
| EULA_ACCEPTED | 是 | 定义用户是否接受网络代理的最终用户授权许可协议 (EULA)；如果缺失，则可以解释为不接受 EULA。 | 1 – 本人确认已完全阅读、理解并接受本《最终用户授权许可协议》的条款和条件。<br><br>其它值或未指定 – 我不接受授权许可协议的条款（将不会执行安装） |
| KLNAGENT_PROXY_USE | 否 | 定义与管理服务器的连接是否将使用代理设置。默认值是 0。 | 1—使用代理设置。<br><br>其他—不使用代理设置。 |
| KLNAGENT_PROXY_ADDR | 否 | 定义用于与管理服务器连接的代理服务器的地址。 | DNS 名称或 IP 地址。 |
| KLNAGENT_PROXY_LOGIN | 否 | 定义用于登录代理服务器的用户名。 | 任何现有用户名。 |
| KLNAGENT_PROXY_PASSWORD | 否 | 定义用于登录代理服务器的用户密码。 | 操作系统中的密码格式允许的任何字母数字字符集。 |
| KLNAGENT_VM_VDI | 否 | 定义是否在用于创建动态虚拟机的映像上安装网络代理。 | 1—在以后用于创建动态虚拟机的映像上安装网络代理。<br><br>其他—安装期间不使用任何映像。 |
| KLNAGENT_VM_OPTIMIZE | 否 | 定义网络代理设置是否对虚拟机监控程序优化。 | 1—修改网络代理的默认本地设置，以便优化在虚拟机监控程序上的使用。 |
| KLNAGENT_TAGS | 否 | 列出分配给网络代理实例的标签。 | 一个或多个标签名称，以分号分隔。 |
| KLNAGENT_UDP_PORT | 否 | 定义网络代理使用的 UDP 端口。默认值是 15000。 | 任意现有端口号。 |
| KLNAGENT_PORT | 否 | 定义网络代理使用的非 TLS 端口。默认值是 14000。 | 任意现有端口号。 |
| KLNAGENT_SSLPORT | 否 | 定义网络代理使用的非 TLS 端口。默认值是 13000。 | 任意现有端口号。 |
| KLNAGENT_USESSL | 否 | 定义是否使用传输层安全性 (TLS) 进行连接。 | 1（默认）—使用 TLS。<br><br>其他—不使用 TLS。 |
| KLNAGENT_GW_MODE | 否 | 定义是否使用连接网关。 | 1（默认）—不修改当前设置（第一次呼叫时，不指定任何连接网关）。<br><br>2—不使用连接网关。<br><br>3—使用连接网关。<br><br>4—网络代理实例用作非管制区域 (DMZ) 中的连接网关。 |
| KLNAGENT_GW_ADDRESS | 否 | 定义连接网关的地址。仅当 KLNAGENT_GW_MODE=3 时，该值才适用。 | DNS 名称或 IP 地址。 |

5. 安装网络代理：

- 要将网络代理从 RPM 包安装到 32 位操作系统，请执行以下命令：
  `# rpm -i klnagent-<内部版本号>.i386.rpm`
- 要将网络代理从 RPM 包安装到 64 位操作系统，请执行以下命令：
  `# rpm -i klnagent64-<内部版本号>.x86_64.rpm`
- 要在 Arm 架构的 64 位操作系统上从 RPM 包安装网络代理，请执行以下命令：
  `# rpm -i klnagent64-<内部版本号>.aarch64.rpm`
- 要将网络代理从 DEB 包安装到 32 位操作系统，请执行以下命令：
  `# apt-get install ./klnagent_<内部版本号>_i386.deb`
- 要将网络代理从 DEB 包安装到 64 位操作系统，请执行以下命令：
  `# apt-get install ./klnagent64_<内部版本号>_amd64.deb`
- 要在 ARM 架构的 64 位操作系统上从 DEB 包安装网络代理，请执行以下命令：
  `# apt-get install ./klnagent64_<内部版本号>_arm64.deb`

Linux 网络代理的安装以静默模式开始；在此过程中不会提示用户进行任何操作。

## 在封闭软件环境模式下在 Astra Linux 上安装网络代理

本节介绍如何在 Astra Linux 特别版操作系统上安装 Network Agent for Linux。

安装前：

- 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。
- 下载kaspersky_astra_pub_key.gpg 应用程序密钥。
- 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。

*要在 Astra Linux 特别版（操作更新 1.7）和 Astra Linux 特别版（操作更新 1.6）操作系统上安装 Network Agent for 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. 安装网络代理：

   - 要将网络代理从 DEB 包安装到 32 位操作系统，请执行以下命令：
     `# apt-get install ./klnagent_<内部版本号>_i386.deb`
   - 要将网络代理从 DEB 包安装到 64 位操作系统，请执行以下命令：
     `# apt-get install ./klnagent64_<内部版本号>_amd64.deb`
   - 要将网络代理从 DEB 包安装到 Arm 架构的 64 位操作系统，请执行以下命令：
     `# apt-get install ./klnagent64_<build number>_arm64.deb`

Network Agent for Linux 已安装。

# 使用 DBMS 的账户

要安装管理服务器并使用它，您需要创建一个内部 DBMS 账户。此账户允许您访问 DBMS 但需要特定权限。当您向 DBMS 账户授予权利和权限时，请遵循最小权限原则。这意味着授予的权限应以足以执行所需操作为限。请注意，您应该在安装和启动管理服务器之前向 DBMS 账户授予权限。

Kaspersky Security Center 14 Linux 支持 MySQL 和 MariaDB DBMS。为这些 DBMS 之一创建内部账户后，授予此账户所需的权限。请注意，内部 MySQL 账户和内部 MariaDB 账户的权限集是相同的。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）。
  - 系统方案（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）。
- 所有方案的全局权限：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。

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。

# 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 ascii
   DEFAULT COLLATE ascii_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。

# 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 故障转移集群提供 Kaspersky Security Center 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 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 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 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 安装**

   在两个节点上均以故障转移集群模式安装 Kaspersky Security Center。必须先在主动节点上安装 Kaspersky Security Center，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 14 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 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 故障转移集群提供 Kaspersky Security Center 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 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 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设备。这两台设备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设备来用作文件服务器。

  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。

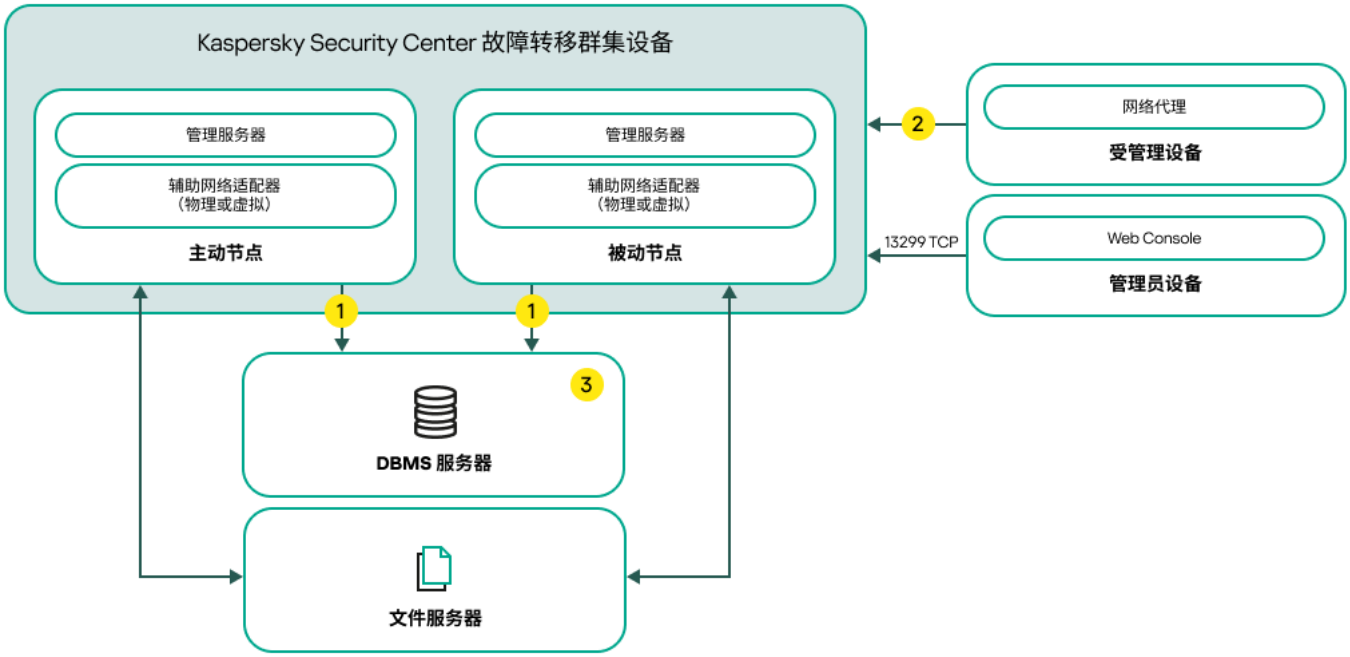
- 一台具有受支持的数据库管理系统 (DBMS) 的设备。如果使用 MariaDB Galera Cluster 作为 DBMS，则不需要专用设备。

当您同时安装 arping 和 iputils-arping 安装包或仅安装 arping 安装包时，故障转移集群部署会失败。在部署故障转移集群之前，请确保在两个节点上都安装了 iputils-arping 安装包。

## 部署方案

您可以选择以下方案之一来部署 Kaspersky Security Center 故障转移集群：

- 使用从属网络适配器的方案。
- 使用第三方负载均衡器的方案。



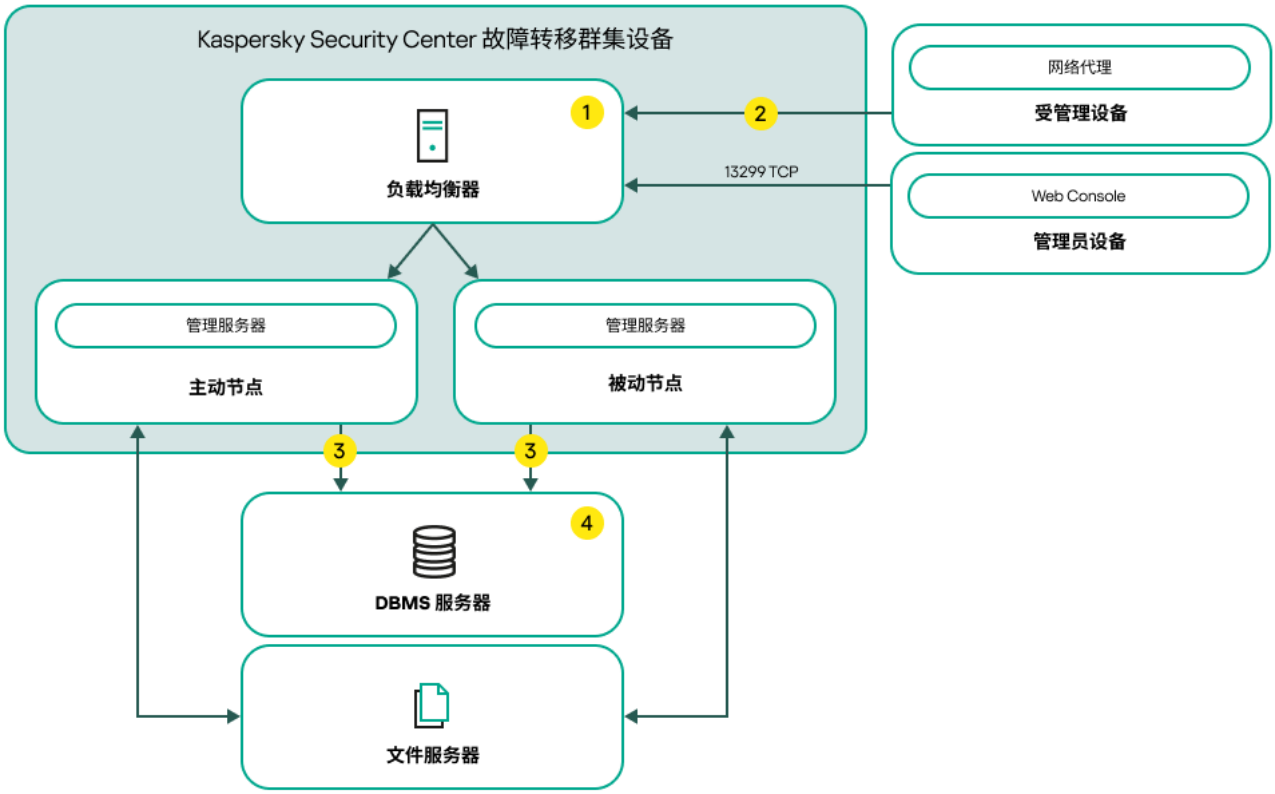

使用从属网络适配器的方案

方案图例：

1 管理服务器发送数据到数据库。在数据库所在的设备上开放必要的端口，例如，MySQL Server 的端口 3306，或 PostgreSQL 或 Postgres Pro 的端口 5432。请参阅 DBMS 文档以获取相关信息。

2 在受管理设备上，打开以下端口：TCP 13000、UDP 13000 和 TCP 17000。

3 一台具有数据库管理系统 (DBMS) 的设备。如果使用 MariaDB Galera Cluster 作为 DBMS，则不需要专用设备。在每个节点上安装 MariaDB Galera Cluster。




使用第三方负载均衡器的方案

方案图例：

1 在负载均衡器设备上，打开所有管理服务器端口：TCP 13000、UDP 13000、TCP 13299 和 TCP 17000。

> 如果您想使用 klakaut 实用程序进行自动化，您还必须打开 TCP 13291 端口。

2 在受管理设备上，打开以下端口：TCP 13000、UDP 13000 和 TCP 17000。

3 管理服务器发送数据到数据库。在数据库所在的设备上开放必要的端口，例如，MySQL Server 的端口 3306，或 PostgreSQL 或 Postgres Pro 的端口 5432。请参阅 DBMS 文档以获取相关信息。

4 一台具有数据库管理系统 (DBMS) 的设备。如果使用 MariaDB Galera Cluster 作为 DBMS，则不需要专用设备。在每个节点上安装 MariaDB Galera Cluster。

## 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 服务（或进程）故障或被用户故意终止。Kaspersky Security Center 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 的数据和设置。您在配置 Kaspersky Security Center 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,soft,auto,user,rw {server}:{KlFocStateShare 文件夹的路径}
   /mnt/KlFocStateShare
   sudo mount -t nfs -o vers=4,noauto,user,rw {server}:{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
   {server}:{KlFocStateShare 文件夹路径} /mnt/KlFocStateShare nfs
   vers=4,soft,timeo=50,retrans=2,auto,user,rw 0 0
   {server}:{KlFocDataShare_klfoc 文件夹的路径} /mnt/KlFocDataShare_klfoc nfs
   vers=4,noauto,user,rw,exec 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 <连接名称>
```

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:<接口名称>
```

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，打开所有管理服务器端口：TCP 13000、UDP 13000、TCP 13299 和 TCP 17000。

> 如果您想使用 klakaut 实用程序进行自动化，您还必须打开 TCP 13291 端口。

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

此过程描述了如何在 Kaspersky Security Center 故障转移集群的节点上安装 Kaspersky Security Center。Kaspersky Security Center 分别安装在 Kaspersky Security Center 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。

## 在主（活动）节点上安装

*在主节点上安装 Kaspersky Security Center：*

1. 确保您要安装 Kaspersky Security Center 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 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 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，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，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. 输入管理服务器端口号。默认情况下使用端口 14000。
   g. 输入管理服务器 SSL 端口号。默认情况下使用端口 13000。
   h. 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”。

i. 输入服务的安全组名称。默认情况下，使用 kladmins 组。

j. 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。

k. 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。

l. 输入安装了数据库的设备的 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。默认情况下使用端口 3306。

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：

- klfocsvc_klfoc
- kladminserver_klfoc
- klwebsrv_klfoc
- klactprx_klfoc
- klnagent_klfoc

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 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：*

1. 确保您要安装 Kaspersky Security Center 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 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 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，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，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 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 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。

# 用于 Kaspersky Security Center 的证书

本节包含有关 Kaspersky Security Center 证书的信息，并介绍如何为 Kaspersky Security Center 14 Web Console 颁发和更换证书，以及如何在管理服务器与 Kaspersky Security Center 14 Web Console 交互时为管理服务器续订证书。

# 关于 Kaspersky Security Center 证书

Kaspersky Security Center 使用以下类型的证书来启用应用程序组件之间的安全交互：

- 管理服务器证书
- 移动证书
- Web 服务器证书
- Kaspersky Security Center 14 Web Console 证书

默认情况下，Kaspersky Security Center 使用自签名证书（即，由 Kaspersky Security Center 自身颁发），但是您可以将其替换为自定义证书，以更好地满足组织网络的要求并符合安全标准。在管理服务器验证自定义证书是否满足所有适用要求之后，该证书将承担与自签名证书相同的功能范围。唯一的区别是自定义证书不会在到期后自动重新颁发。您可以通过 klsetsrvcert 实用程序或通过 Kaspersky Security Center 14 Web Console 中的管理服务器属性区域将证书替换为自定义证书，具体取决于证书类型。使用 klsetsrvcert 实用程序时，需要使用以下值之一指定证书类型：

- C—端口 13000 和 13291 的通用证书。
- CR—端口 13000 和 13291 的通用备用证书。
- M—端口 13292 的移动证书。

- MR—端口 13292 的移动备用证书。
- MCA—自动生成的用户证书的移动证书颁发机构。

管理服务器证书的最长有效期不得超过 397 天。

## 管理服务器证书

出于以下目的需要管理服务器证书：

- 连接到 Kaspersky Security Center 14 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
- 主管理服务器连接到从属管理服务器时的身份验证

管理服务器证书是在安装管理服务器组件时自动生成的，并保存在 /var/opt/kaspersky/klnagent_srv/1093/cert/ 文件夹下。在创建响应文件以安装 Kaspersky Security Center 14 Web Console 时，指定管理服务器证书。此证书称为通用（“C”）证书。

管理服务器证书的有效期为 397 天。Kaspersky Security Center 会在通用证书到期前 90 天自动生成通用备用 ("CR") 证书。通用备用证书随后用于无缝替换管理服务器证书。当通用证书即将到期时，通用备用证书用于保持与受管理设备上安装的网络代理实例的连接。为此，通用备用证书会在旧的通用证书到期前 24 小时自动成为新的通用证书。

> 管理服务器证书的最长有效期不得超过 397 天。

如果必要，您可以为管理服务器分配自定义证书。例如，为了更好的整合您企业的现有 PKI 或为了证书字段的自定义配置，这可能是必要的。当替换证书时，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，并将返回“管理服务器身份验证错误“。要消除该错误，您将必须在证书替换后恢复连接。

如果丢失了管理服务器证书，要想恢复该证书，必须重新安装管理服务器组件，然后还原数据。

您还可以将管理服务器证书与其他管理服务器设置分开备份，以将管理服务器从一台设备移动到另一台设备而不丢失数据。

> 如果您在不同的浏览器中打开 Kaspersky Security Center 14 Web Console，并在管理服务器属性窗口中下载管理服务器证书文件，则下载的文件具有不同的名称。

## 移动证书

在移动设备上对管理服务器进行身份验证需要移动证书（“M”）。您可以在管理服务器属性中指定移动证书。

此外，还存在移动备用（“MR”）证书：它用于无缝替换移动证书。Kaspersky Security Center 会在通用证书到期前 60 天自动生成此证书。当移动证书即将到期时，移动备用证书用于保持与受管理移动设备上安装的网络代理实例的连接。为此，移动备用证书会在旧的移动证书到期前 24 小时自动成为新的移动证书。

如果连接方案要求在移动设备上使用客户端证书（涉及双向 SSL 身份验证的连接），您可以通过自动生成的用户证书（“MCA”）的证书颁发机构来生成那些证书。此外，您可以在管理服务器属性中指定由其他证书颁发机构颁发的自定义客户端证书，而与组织的域公钥基础结构 (PKI) 的集成允许您通过域证书颁发机构颁发客户端证书。

此外，为了在运行 iOS 操作系统的移动设备上对管理服务器进行身份验证，需要 iOS MDM 服务器证书。有关更多信息，请参阅配置 iOS MDM 服务器证书。

### Web 服务器证书

Web 服务器是 Kaspersky Security Center 管理服务器的一个组件，使用一种特殊类型的证书。发布后续下载到受管理设备的网络代理安装包以及发布 Kaspersky Security for Mobile 安装包都需要此证书。为此，Web 服务器可以使用各种证书。

如果禁用了移动设备支持，Web 服务器将按优先级顺序使用以下证书之一：

1. 通过管理控制台手动指定的自定义 Web 服务器证书
2. 通用管理服务器证书（“C”）

如果启用了移动设备支持，Web 服务器将按优先级顺序使用以下证书之一：

1. 通过管理控制台手动指定的自定义 Web 服务器证书
2. 自定义移动证书
3. 自签名移动证书（“M”）
4. 通用管理服务器证书（“C”）

### Kaspersky Security Center 14 Web Console 证书

Kaspersky Security Center 14 Web Console（以下简称 Web Console）的服务器有自己的证书。当您打开网站时，浏览器会验证您的连接是否可信。Web Console 证书允许您对 Web Console 进行身份验证，并用于加密浏览器和 Web Console 之间的流量。

当您打开 Web Console 时，浏览器可能会通知您与 Web Console 的连接不是私有连接，并且 Web Console 证书无效。出现此警告是因为 Web Console 证书是自签名的，并且由 Kaspersky Security Center 自动生成。要移除此警告，可以执行以下操作之一：

- 将 Web Console 证书替换为自定义证书（推荐选项）。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 Web Console 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。

## 对 Kaspersky Security Center 中使用的自定义证书的要求

下表显示了为不同的 Kaspersky Security Center 组件指定的自定义证书的要求。

Kaspersky Security Center 证书的要求

| 证书类别 | 要求 | 注释 |
| --- | --- | --- |
| 通用证书，通用备用证书（“C”，“CR”） | 最小密钥长度：2048<br>基本限制：<br>• 路径长度限制：无 | 扩展密钥用法参数是可选的。<br>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：<br>• 数字签名<br>• 证书签名<br>• 密钥加密<br>• CRL 签名<br>扩展密钥用法（可选）：服务器身份验证，客户端身份验证。 | |
| Web 服务器证书 | 扩展密钥用法：服务器身份验证。<br>从中指定证书的 PKCS #12/PEM 容器包括整个公钥链。<br>证书的使用者可选名称 (SAN) 存在；即，`subjectAltName` 字段的值有效。<br>证书符合 Web 浏览器对服务器证书施加的有效要求，以及 CA/浏览器论坛的当前基线要求。 | — |
| Kaspersky Security Center 14 Web Console 证书 | 从中指定证书的 PEM 容器包括整个公钥链。<br>证书的使用者可选名称 (SAN) 存在；即，`subjectAltName` 字段的值有效。<br>证书符合 Web 浏览器对服务器证书的有效要求，以及 CA/浏览器论坛的当前基线要求。 | Kaspersky Security Center 14 Web Console 不支持加密证书。 |

# 重新颁发 Kaspersky Security Center 14 Web Console 的证书

大多数浏览器对证书有效期施加了限制。为了不超过此限制，Kaspersky Security Center 14 Web Console 证书的有效期限制为 397 天。您可以通过手动颁发新的自签名证书来替换从证书颁发机构 (CA) 收到的现有证书。或者，您可以重新颁发过期的 Kaspersky Security Center 14 Web Console 证书。

不支持自动重新颁发 Kaspersky Security Center 14 Web Console 证书。您必须手动重新颁发过期的证书。

打开 Kaspersky Security Center 14 Web Console 时，浏览器会通知您与 Kaspersky Security Center 14 Web Console 连接不是私有，并且 Kaspersky Security Center 14 Web Console 证书无效。出现此警告是因为 Web Console 证书是自签名的，并且由 Kaspersky Security Center 自动生成。要移除或防止此警告，可以执行以下操作之一：

- 重新颁发证书时指定自定义证书（推荐选项）。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。
- 重新颁发证书后，将 Kaspersky Security Center 14 Web Console 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。

*要重新颁发过期的 Kaspersky Security Center 14 Web Console 证书：*

执行以下操作之一，重新安装 Kaspersky Security Center 14 Web Console：

- 如果要使用相同的 Kaspersky Security Center 14 Web Console 安装文件，请删除 Kaspersky Security Center 14 Web Console，然后安装相同的 Kaspersky Security Center 14 Web Console 版本。
- 如果要使用升级版本的安装文件，请运行升级命令。

重新颁发的 Kaspersky Security Center 14 Web Console 证书的有效期将增加 397 天。

# 替换 Kaspersky Security Center 14 Web Console 证书

默认下，当您安装 Kaspersky Security Center 14 Web Console Server（也叫 Kaspersky Security Center 14 Web Console）时，应用程序的浏览器证书被自动生成。您可以使用自定义证书替换自动生成的证书。

*要用自定义证书替换 Kaspersky Security Center 14 Web Console 的证书：*

1. 创建安装 Kaspersky Security Center 14 Web Console 所需的新响应文件。
2. 在此文件中，使用 `certPath` 参数和 `keyPath` 参数指定自定义证书文件和密钥文件的路径。
3. 通过指定新响应文件来重新安装 Kaspersky Security Center 14 Web Console。执行以下操作之一：
   - 如果要使用相同的 Kaspersky Security Center 14 Web Console 安装文件，请删除 Kaspersky Security Center 14 Web Console，然后安装相同的 Kaspersky Security Center 14 Web Console 版本。
   - 如果要使用升级版本的安装文件，请运行升级命令。

Kaspersky Security Center 14 Web Console 使用指定的证书工作。

# 将 PFX 证书转换为 PEM 格式

要在 Kaspersky Security Center 14 Web Console 中使用 PFX 证书，必须首先使用任何方便的基于 OpenSSL 的跨平台实用程序将该证书转换为 PEM 格式。

*要在 Linux 操作系统中将 PFX 证书转换为 PEM 格式：*

1. 在基于 OpenSSL 的跨平台实用程序中，执行以下命令：

   ```
   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. 确保证书文件和私钥生成到存储 .pfx 文件的同一目录中。
3. Kaspersky Security Center 14 Web Console 不支持受密码保护的证书。因此，在基于 OpenSSL 的跨平台实用程序中运行以下命令，从 .pem 文件中删除密码：

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

   > 输入和输出 .pem 文件不要使用相同名称。

   结果，新的 .pem 文件未加密。无需输入密码即可使用。

.crt 和 .pem 文件已可以使用，因此您可以在 Kaspersky Security Center 14 Web Console 安装程序中指定它们。

# 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：通用证书，通用备用证书（“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 分发包中。它与以前的 Kaspersky Security Center 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：<br>• `C` – 为端口 13000 和 13291 替换通用证书。<br>• `CR` – 为端口 13000 和 13291 替换通用备用证书。 |
| `-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)。<br>如果要在通用证书到期前用通用备用证书更换通用证书，请使用此参数。<br>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。<br>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）。<br>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。<br>要更改证书类型 C 或 CR 的加密密钥长度，请在 klsetsrvcert 实用程序中指定 `-o RsaKeyLen:<` 密钥长度 `>`，其中 < 密钥长度 > 参数是所需的密钥长度值。否则，使用当前证书密钥长度。 |
| `-g <DNS 名称>` | 新证书将为指定 DNS 名称创建。 |
| `-r <证书颁发机构列表文件>` | 受信任的根证书颁发机构列表，格式 PEM。 |
| `-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。

> 对于通过连接网关连接到管理服务器的客户端设备，您不能使用 klmover 实用程序。对于这样的设备，您必须重新配置网络代理或重新安装网络代理并指定连接网关。

klmover 实用程序参数的描述如下表所示。

Klmover 实用程序参数值

| 参数 | 参数值 |
| --- | --- |
| -address <服务器地址> | 用于连接的管理服务器的地址。<br>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。<br>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。<br>默认端口号是 13000。 |
| -nossl | 使用非加密连接管理服务器。<br>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。

# 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 14。当升级至版本 14 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 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 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 14 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 14，您可以使用 Kaspersky Security Center 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 14：*

1. 从卡巴斯基网站下载包含版本 14 的完整软件包的 Kaspersky Security Center 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：

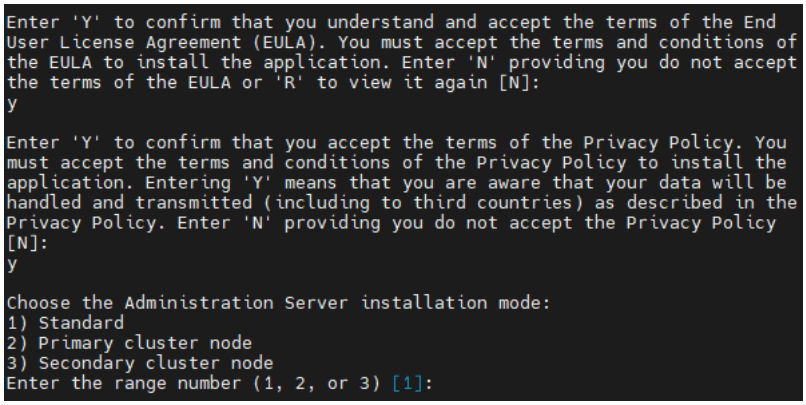
   a. 输入“Y”以确认您已完全阅读、理解并接受 EULA 的条款和条件。

   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 14，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 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 14：*

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。
3. 在以前的管理服务器上安装 Kaspersky Security Center 版本 14。
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。

# 登录到 Kaspersky Security Center 14 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 14 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 14 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。
   如果您仅添加了一个管理服务器，仅**用户名**和**密码**字段被显示。
3. 执行以下操作之一：
   - 要登录到物理管理服务器，请输入本地管理员的用户名和密码。
   - 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**高级设置**。
     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。

登录后，仪表板使用您最后使用的语言和主题显示。您可以通过 Kaspersky Security Center 14 Web Console 导航并使用其操作 Kaspersky Security Center Linux。

*要注销 Kaspersky Security Center 14 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 14 Web Console 被关闭，且登录页面被显示。

# 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病毒扫描任务、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。使用**"下一步"**按钮继续向导。

# 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。

您可以稍后独立于快速启动向导配置互联网访问。

## 步骤 2：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 3：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 4：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 5：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安全程序或网络代理。

# 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。

## 步骤 1：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，单击 **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**”按钮继续向导。

## 步骤 2：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 3：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 4：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 5：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 6：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。

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 7：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 8：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 9：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或 SSH 证书来安装应用程序。

  - **本地账户**。如果该选项被选中，请指定将运行应用程序安装程序的用户账户。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。

  - **SSH 证书**。如果要在基于 Linux 的客户端设备上安装应用程序，您可以指定 SSH 证书而不是用户账户。单击**添加**按钮，选择**SSH 证书**，然后指定证书的私钥和公钥。

    要生成私钥，您可以使用 ssh-keygen 实用程序。请注意，Kaspersky Security Center 支持 PEM 格式的私钥，但 ssh-keygen 实用程序默认生成 OPENSSH 格式的 SSH 密钥。Kaspersky Security Center 不支持 OPENSSH 格式。要以支持的 PEM 格式创建私钥，请在 ssh-keygen 命令中添加“-m PEM”选项。例如：

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "<user email>"
    ```

## 步骤 10：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。

# 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 14 Web Console 到管理服务器的连接

*要设置管理服务器连接端口：*

1. 在屏幕上方，点击所需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。

# 配置用于连接到 Kaspersky Security Center 的 IP 地址允许列表

默认情况下，允许从任何设备连接到 Kaspersky Security Center。例如，您可以在任何满足要求的设备上安装 Kaspersky Security Center 14 Web Console 服务器，Kaspersky Security Center 14 Web Console 服务器将与 Kaspersky Security Center 进行通信。不过，您可以配置管理服务器，以便只允许从具有您指定的 IP 地址的设备进行连接。在这种情况下，如果入侵者尝试通过安装在未包含在允许列表中的设备上的 Kaspersky Security Center 14 Web Console 服务器连接到 Kaspersky Security Center，他或她将无法登录Kaspersky Security Center。

当用户登录 Kaspersky Security Center 或运行通过 Kaspersky Security Center OpenAPI 与管理服务器交互的应用程序时，将验证 IP 地址。此时，设备上的应用程序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 14 Web Console 服务器
  如果您通过 Kaspersky Security Center 14 Web Console 登录 Kaspersky Security Center，您可以使用操作系统的标准方式在安装了 Kaspersky Security Center 14 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 并且 Kaspersky Security Center 14 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 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 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。

# 配置管理服务器连接事件记录

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。默认情况下，事件队列限制为 20,000 个事件。您可以通过编辑 KLEVP_MAX_POSTPONED_CNT 标记值来自定义队列限制。*

*要限制存储在管理服务器事件存储库中的事件的数量：*

1. 在屏幕上方，点击所需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。

# 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 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 14 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。

# 创建管理服务器数据备份任务

备份任务是管理服务器任务，通过快速启动向导进行创建。如果由快速启动向导创建的备份任务被删除，您可以手动创建备份任务。

“*备份管理服务器数据*”任务只能创建单份副本。如果已经为管理服务器创建了管理服务器数据备份任务，它不会显示在任务类型选择窗口中。

*若要创建管理服务器数据备份任务，请执行以下操作：*

1. 转到"**设备**" → "**任务**"。
2. 单击**添加**。

   “添加任务向导”启动。使用**下一步**按钮进行向导。
3. 在“**应用程序**”列表中，选择“**Kaspersky Security Center 14**”，然后在“**任务类型**”列表中选择“**备份管理服务器数据**”。
4. 在相应步骤中，指定以下信息：

- 用于存储备份副本的文件夹
- 备份密码（可选）
- 要保存的最大备份副本数

5. 如果在“**完成任务创建**”步骤中启用“**创建完成时打开任务详情**”选项，则可以修改默认任务设置。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。
6. 单击“**完成**”按钮。

任务被创建并显示在任务列表。

# 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。

如果您在使用早期版本的 MariaDB DBMS 时备份了 Kaspersky Security Center 15 或更早版本中包含的管理服务器的数据，然后在具有更高版本的 MariaDB 的设备上恢复数据，则可能会出现错误。有关更多信息，请参阅如何从早期 DBMS 版本创建的备份中恢复管理服务器数据。

使用 klbackup 实用程序时，网络代理标志不会被恢复。您需要手动配置网络代理标志。

*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 [-linux_path LINUX_PATH][-node_cert CERT_PATH] [-logfile
LOGFILE] [-use_ts]|[-restore] [-password PASSWORD]
```

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）。
- `-linux_path LINUX_PATH` — 包含 DBMS 备份数据的文件夹的本地路径。

  数据库服务器账户和 klbackup 实用程序需要获得更改 LINUX_PATH 文件夹中数据的权限。
- `-node_cert CERT_PATH` — 用于在恢复后配置非活动故障转移群集节点的服务器证书文件。如果未设置，它将被自动从服务器检索。
- `-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，将信息复制到 BACKUP_PATH 文件夹，复制到以`klbackup YYYY-MM-DD # HH-MM-SS`格式命名的子文件夹，其中包括 UTC 当前日期和运行时间。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 `/tmp/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` — 用于保护敏感数据的密码。

  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。要从备份中恢复管理服务器数据，我们建议您在新安装的管理服务器上运行该实用程序。

# 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动到新设备（数据库服务器可以与管理服务器一起安装在新设备上，也可以安装在另一台设备上）。

- 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 14 Web Console 运行数据备份任务或运行 klbackup 实用程序。

2. 在之前的设备上，断开管理服务器与网络的连接。

3. 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 14 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。

4. 为新设备分配相同地址。

   可以为新的管理服务器分配 NetBIOS 名称、FQDN 和静态 IP 地址。这取决于部署网络代理时在网络代理安装包中设置了哪个管理服务器地址。或者，您可以使用确定网络代理连接到的管理服务器的连接地址（您可以使用 klnagchk 实用程序在受管理设备上获取此地址）。

5. 如有需要，在另一台设备上，安装管理服务器将使用的数据库管理系统 (DBMS)。

   数据库可以与管理服务器一起安装在新设备上，也可以安装在另一台设备上。确保该设备满足硬件和软件要求。选择 DBMS 时，请考虑管理服务器覆盖的设备数量。

6. 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另一部设备，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 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 指令的“h”项中输入以前的设备的 IP 地址。

7. 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。

8. 打开 Kaspersky Security Center 14 Web Console 并连接到管理服务器。

9. 验证是否所有受管理设备都连接到了管理服务器。

10. 从以前的设备中卸载管理服务器和数据库服务器。

## 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。

   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。

6. 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 14 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 14 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 14 Web Console 中连接到该虚拟管理服务器。

1. 在安装了 Kaspersky Security Center 14 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 Web Console 安装文件。

   安装向导将启动。使用**下一步**按钮继续向导操作。

2. 选择**升级**选项。

3. 在“**修改类型**”步骤中，选择“**编辑连接设置**”选项。

4. 在“**受信任的管理服务器**”步骤中，添加所需的从属管理服务器。

5. 在最后一步中，单击**修改**以应用新设置。

6. 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 14 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 14 Web Console 中切换到该虚拟管理服务器。

# 管理服务器层级

一个 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，Kaspersky Security Center Linux 管理服务器只能用作辅助服务器，由基于 Windows 的 Kaspersky Security Center 或 Kaspersky Security Center 云控制台的主管理服务器管理。

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和任务，这防止了重复设置。
- 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，Kaspersky Security Center Linux 管理服务器只能用作辅助服务器，由基于 Windows 的 Kaspersky Security Center 或 Kaspersky Security Center 云控制台 的主管理服务器管理。

## 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 14 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**”。
“连接从属管理服务器”向导启动。使用“**下一步**”按钮继续向导操作。

6. 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. 遵照向导的进一步说明。

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），您仍可以添加从属管理服务器。

*要添加不可以通过 Kaspersky Security Center 14 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从属管理服务器，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 14 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 14 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 14 Web Console 中连接到该虚拟管理服务器。

  1. 在安装了 Kaspersky Security Center 14 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 Web Console 安装文件。

     安装向导将启动。使用**下一步**按钮继续向导操作。

  2. 选择**升级**选项。

  3. 在“**修改类型**”步骤中，选择“**编辑连接设置**”选项。

  4. 在“**受信任的管理服务器**”步骤中，添加所需的从属管理服务器。

  5. 在最后一步中，单击**修改**以应用新设置。

  6. 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 14 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 14 Web Console 中切换到该虚拟管理服务器。

# 启用账户保护以防止未经授权的修改

您可以启用一个附加选项以保护用户账户免遭未经授权的修改。如果启用此选项，修改用户账户设置需要具有修改权限的用户的授权。

*要启用或禁用账户保护以防止未经授权的修改：*

1. 在主菜单中，转到“**用户和角色**” → “**用户**”。
2. 单击要为其指定账户保护以防止未经授权的修改的内部用户账户的名称。
3. 在打开的用户设置窗口中，选择“**身份验证安全**”选项卡。
4. 在“**身份验证安全**”选项卡上，如果您希望在每次更改或修改账户设置时都请求凭据，则选择“**请求身份验证以检查修改用户账户的权限**”选项。否则，请选择“**无需其他身份验证即允许用户修改此账户**”选项。
5. 单击“**保存**”按钮。

# 两步验证

本节介绍如何使用两步验证来降低 Kaspersky Security Center 14 Web Console 被未经授权访问的风险。

# 关于账户的两步验证

Kaspersky Security Center Linux 为 Kaspersky Security Center 14 Web Console 用户提供两步验证。为您自己的账户启用两步验证后，每次登录 Kaspersky Security Center 14 Web Console 时，都需要输入用户名、密码和附加的一次性安全代码。要接收一次性安全码，计算机或移动设备上必须安装了认证应用。

安全代码具有一个称为*颁发者名称*的标识符。安全代码颁发者名称用作管理服务器在认证应用中的标识符。您可以更改安全代码颁发者的名称。安全代码颁发者名称的默认值与管理服务器的名称相同。颁发者名称用作管理服务器在认证应用中的标识符。如果更改安全代码颁发者名称，则必须颁发新的 secret key 并将其传递给认证应用。安全码为一次性，有效期最长为 90 秒（具体时间可能会有所不同）。

任何已启用两步验证的用户都可以重新颁发自己的 secret key。当用户使用重新颁发的 secret key 进行身份验证并将其用于登录时，管理服务器将保存该用户账户的新 secret key。如果用户输入的新 secret key 不正确，则管理服务器不会保存新 secret key，并使当前的 secret key 对进一步的验证有效。

任何支持基于时间的一次性密码算法 (TOTP) 的认证软件都可以用作认证应用，例如 Google Authenticator。要生成安全代码，您必须将认证应用中设置的时间与管理服务器中设置的时间同步。

要检查 Kaspersky Security Center 是否支持您要使用的身份验证器应用，请为所有用户或特定用户启用两步验证。

其中一个步骤会建议您指定由身份验证器应用生成的安全代码。如果成功，则 Kaspersky Security Center 支持所选的身份验证器。

认证应用会生成安全代码，如下所示：

1. 管理服务器生成一个特殊的 secret key 和 QR 码。
2. 您将生成的 secret key 或 QR 码传递给认证应用。
3. 认证应用生成一次性安全代码，您将其传递到管理服务器的身份验证窗口。

我们强烈建议您保存 secret key 或二维码，并将其保管在安全的地方。万一您失去对移动设备的访问权限，这将帮助您恢复对 Kaspersky Security Center 14 Web Console 的访问权限。

为了保护 Kaspersky Security Center 的使用，您可以为您自己的账户启用两步验证，并为所有用户启用两步验证。

您可以从两步验证中排除账户。对于无法接收安全代码进行身份验证的服务账户，这可能是必需的。

两步验证按照以下规则工作：

- 只有在“**常规功能：用户权限**”功能区域中拥有“修改对象 ACL”权限的用户账户才能为所有用户启用两步验证。
- 只有为自己的账户启用了两步验证的用户才能为所有用户启用两步验证选项。
- 只有为自己的账户启用了两步验证的用户才能从为所有用户启用的两步验证列表中排除其他用户账户。
- 用户只能为自己的账户启用两步验证。
- 在“**常规功能：用户权限**”功能区域中拥有“修改对象 ACL”权限，并且使用两步验证登录到 Kaspersky Security Center 14 Web Console 的用户账户可以禁用两步验证：针对任何其他用户（仅当禁用了所有用户的两步验证时），针对从为所有用户启用的两步验证列表中排除的用户。

- 使用两步验证登录到 Kaspersky Security Center 14 Web Console 的任何用户都可以重新颁发自己的 secret key。
- 您可以为当前使用的管理服务器启用所有用户的两步验证选项。如果在管理服务器上启用此选项，则也为其虚拟管理服务器的用户账户启用此选项，但不为从属管理服务器的用户账户启用两步验证。

# 方案：为所有用户配置两步验证

此方案描述如何为所有用户启用两步验证，以及如何从两步验证中排除用户账户。如果您在为其他用户启用两步验证之前没有为您的账户启用两步验证，则应用程序会先打开用于为您的账户启用两步验证的窗口。此方案还描述了如何为您自己的账户启用两步验证。

如果您为账户启用了两步验证，则可以进入为所有用户启用两步验证的阶段。

## 先决条件

在开始之前：

- 确保您的用户账户在“**常规功能：用户权限**”功能区域中拥有“修改对象 ACL”权限，以修改其他用户账户的安全设置。
- 确保管理服务器的其他用户在其设备上安装了认证应用。

## 阶段

为所有用户启用两步验证分阶段进行：

1. **在设备上安装认证应用**

   您可以安装任何支持基于时间的一次性密码算法 (TOTP) 的应用程序，例如：

   - Google Authenticator
   - Microsoft Authenticator
   - Bitrix24 OTP
   - Yandex Key
   - Avanpost 验证器
   - Aladdin 2FA

   要检查 Kaspersky Security Center 是否支持您要使用的身份验证器应用，请为所有用户或特定用户启用两步验证。

   其中一个步骤会建议您指定由身份验证器应用生成的安全代码。如果成功，则 Kaspersky Security Center 支持所选的身份验证器。

   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认证应用。

2. **将认证应用时间与安装了管理服务器的设备的时间同步**

   通过使用外部时间源，确保具有身份验证器应用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。否则，两步验证的认证和激活过程中可能会出现失败。

3. **为您的账户启用两步验证，并接收您的账户的 secret key**

   在您为您的账户启用两步验证后，可以为所有用户启用两步验证。

4. **为所有用户启用两步验证**

   启用了两步验证的用户必须使用它才能登录到管理服务器。

5. **编辑安全代码颁发者的名称**

   如果您有多个具有相似名称的管理服务器，则可能需要更改安全代码颁发者名称，以便更好地识别不同的管理服务器。

6. **排除不需要启用两步验证的用户账户**

   如果需要，您可以从两步验证中排除用户。具有已排除的账户的用户不必使用两步验证即可登录到管理服务器。

7. **为您自己的账户配置两步验证**

   如果用户未被排除在两步验证之外，并且尚未为其账户配置两步验证，则他们需要在登录 Kaspersky Security Center 14 Web Console 时打开的窗口中进行配置。否则，他们将无法按照其权限访问管理服务器。

### 结果

完成此方案后：

- 您的账户已启用两步验证。

管理服务器的所有用户账户均已启用两步验证，但已排除的用户账户除外。

## 为您自己的账户启用两步验证

您只能为您自己的账户启用两步验证。

> 在启用账户的两步验证之前，请确保移动设备上安装了认证应用。确保认证应用中设置的时间与安装了管理服务器的设备的时间设置同步。

*要为用户账户启用两步验证：*

1. 在主菜单中，转到“**用户和角色**” → “**用户**”。
2. 单击您的账户的名称。
3. 在打开的用户设置窗口中，选择“**账户保护**”选项卡。
4. 在**身份验证安全**选项卡上：
   a. 选择**请求用户名、密码和安全码(两步验证)**选项。单击“**保存**”按钮。

b. 在打开的两步验证窗口中，点击**查看如何建立两步验证**。

在认证应用中输入 secret key 或单击“**查看二维码**”并通过移动设备上的认证应用来扫描二维码以接收一次性安全码。

c. 在两步验证窗口中，指定由认证应用生成的安全代码，然后单击“**检查和应用**”按钮。

5. 单击“**保存**”按钮。

您的账户已启用两步验证。

## 对所有用户启用必需的两步验证

如果您的账户在“**常规功能：用户权限**”功能区域中拥有“修改对象 ACL”权限，并且您已通过两步验证进行了身份验证，则可以为管理服务器的所有用户启用两步验证。

*要为所有用户启用两步验证：*

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“**所有用户的两步验证**”选项的切换按钮切换到启用位置。

3. 如果您没有为您的账户启用两步验证，则应用程序会打开为您自己的账户启用两步验证的窗口。

a. 在两步验证窗口中，单击**查看如何建立两步验证**。

b. 单击“**查看二维码**”。

c. 通过移动设备上的认证应用来扫描二维码以接收一次性安全码。

或者，在认证应用中手动输入 secret key。

d. 在两步验证窗口中，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。

所有用户均已启用两步验证。从现在开始，除了从两步验证中排除的用户，管理服务器的用户（包括为所有用户启用两步验证之后添加的用户）必须为他们的账户配置两步验证。

## 禁用用户账户的两步验证

您可以禁用您自己的账户以及任何其他用户账户的两步验证。

如果您的账户在“**常规功能：用户权限**”功能区域中拥有“修改对象 ACL”权限，并且您已通过两步验证进行了身份验证，则可以对其他用户的账户禁用两步验证。

*要禁用用户账户的两步验证：*

1. 在主菜单中，转到“**用户和角色**” → “**用户**”。

2. 单击要为其禁用两步验证的内部用户账户的名称。这可能是您自己的账户或任何其他用户的账户。

3. 在打开的用户设置窗口中，选择“**账户保护**”选项卡。

4. 如果要禁用用户账户的两步验证，请在“**账户保护**”选项卡上选择“**仅请求用户名和密码**”选项。

5. 单击“**保存**”按钮。

该用户账户已禁用两步验证。

如果您想要为无法使用两步验证登录 Kaspersky Security Center 14 Web Console 的用户恢复访问权限，请禁用此用户账户的两步验证，然后按上述说明选择“**仅请求用户名和密码**”选项。之后，使用您禁用两步验证的用户账户登录 Kaspersky Security Center 14 Web Console，然后再次启用验证。

## 对所有用户禁用必需的两步验证

如果您的账户已启用两步验证，并且在“**常规功能：用户权限**”功能区域中拥有“修改对象 ACL”权限，则可以对所有用户禁用必需的两步验证。如果您的账户未启用两步验证，则必须先为您的账户启用两步验证，然后才能禁用所有用户的两步验证。

*要禁用所有用户的两步验证：*

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“**所有用户的两步验证**”选项的切换按钮切换到禁用位置。

3. 在身份验证窗口中输入您的账户的凭据。

所有用户均已禁用两步验证。对所有用户禁用两步验证并不适用于之前单独启用两步验证的特定账户。

## 从两步验证中排除账户

如果您在“**常规功能：用户权限**”功能区域中拥有“修改对象 ACL”权限，则可以从两步验证中排除用户账户。

如果某个用户账户从所有用户的两步验证列表中排除，则该用户不必使用两步验证。

对于在身份验证期间无法传递安全代码的服务账户，从两步验证中排除这些账户可能是有必要的。

*如果要从两步验证中排除某些用户账户：*

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**”选项卡上的两步验证排除表中，单击“**添加**”按钮。

3. 在打开的窗口中：

a. 选择要排除的用户账户。

b. 单击“**确定**”按钮。

所选用户账户即从两步验证中排除。

## 生成新的 secret key

仅当您通过两步验证获得授权后，才能为您的账户的两步验证生成新的 secret key。

*要为用户账户生成新的 secret key：*

1. 在主菜单中，转到“**用户和角色**” → “**用户**”。
2. 单击要为其两步验证生成新 secret key 的用户账户的名称。
3. 在打开的用户设置窗口中，选择“**身份验证安全**”选项卡。
4. 在“**身份验证安全**”选项卡中，单击“**生成新的 secret key**”链接。
5. 在打开的两步验证窗口中，指定由认证应用生成的新安全密钥。
6. 单击**检查和应用**按钮。

将为用户生成一个新的 secret key。

如果移动设备丢失，您可以在另一台移动设备上安装认证应用并生成新的 secret key 以恢复对 Kaspersky Security Center 14 Web Console 的访问权限。

## 编辑安全代码颁发者的名称

您可以有多个不同标识符（称为颁发者）来对应不同的管理服务器。您可以更改安全代码颁发者的名称，例如，当管理服务器使用的安全代码颁发者名称与其他管理服务器相似时。默认情况下，安全代码颁发者的名称与管理服务器的名称相同。

更改安全代码颁发者名称后，必须重新颁发新的 secret key 并将其传递给认证应用。

*要指定安全代码颁发者的新名称：*

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. 在打开的用户设置窗口中，选择“**账户保护**”选项卡。
3. 在“**账户保护**”选项卡上，单击“**编辑**”链接。
   将打开“**编辑安全代码颁发者**”区域。
4. 指定新的安全代码颁发者名称。
5. 单击“**确定**”按钮。

已为管理服务器指定了新的安全代码颁发者名称。

## 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。

## 更改 DBMS 凭据

有时，您可能需要更改 DBMS 凭据，例如，出于安全目的执行凭据循环。

*要在 Linux 环境下使用 klsrvconfig 实用程序更改 DBMS 凭据：*

1. 启动 Linux 命令行。
2. 在打开的命令行窗口中指定 klsrvconfig 实用程序：

   ```
   sudo /opt/kaspersky/ksc64/sbin/klsrvconfig -set_dbms_cred
   ```
3. 指定一个新的账户名。您应该指定 DBMS 中存在的账户的凭据。
4. 输入新密码。
5. 指定新密码以确认。

DBMS 凭据已更改。

## 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. 在屏幕上方，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。

# 配置界面

您可以将 Kaspersky Security Center 14 Web Console 界面配置为显示和隐藏各区域和界面元素，具体取决于所使用的功能。

*要根据当前使用的功能集配置 Kaspersky Security Center 14 Web Console 界面：*

1. 在主菜单中，单击账户菜单。

2. 在下拉列表中，选择“**界面选项**”。

3. 在打开的“**界面选项**”窗口中，启用或禁用所需选项。

4. 点击**保存**。

之后，控制台会根据启用的选项在主菜单中显示相应区域。例如，如果您启用**显示 EDR 警告**，则**监控和报告 → 警报**区域会出现在主菜单中。

# 发现网络设备

该部分描述网络设备的搜索和发现。

Kaspersky Security Center 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。

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 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 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 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 自动包含网络 192.168.0.0/24 到轮询地址。Kaspersky Security Center 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 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. 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 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 自动包含网络 192.168.0.0/24 到轮询地址。Kaspersky Security Center 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 将轮询整个网络。

*要添加新 IP 范围：*

1. 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。轮询完成后，可以使用“**设备**”按钮查看发现的设备列表。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. 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 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 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. 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 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。

## 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 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 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“**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“**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“**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“**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 “**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。在“**分配的标签**”列中，您可以看到标签是如何分配的。

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。

您还可以使用 klscflag 实用程序在命令行中查看分配给设备的标签。

*要在命令行中查看分配给设备的标签，请运行以下命令：*

```
/opt/kaspersky/klnagent64/sbin/klscflag -ssvget -pv 1103/1.0.0.0 -s
KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -svt ARRAY_T -ss "|ss_type =
\"SS_PRODINFO\";"
```

## 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 “**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“**设备 → 标签 → 自动标记规则**”。
- 在主菜单中，转到“**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 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。

## 使用 klscflag 实用程序管理设备标签

要为设备分配一组标签，您需要在要分配标签的客户端设备上运行 klscflag 实用程序。

klscflag 实用程序会覆盖分配给设备的现有标签。这意味着，您可以通过在命令中指定所需的标签集来添加或删除标签。该实用程序没有用于添加或删除单个标签的单独命令。相反，您会修改整个标签集。

在 klscflag 等命令中指定标签名称时，推荐使用一致的大小写方法，例如全部大写。使用全部大写可以帮助避免仅大小写不同的标签的潜在问题，具体取决于 DBMS 配置。

*要使用 klscflag 实用程序为您的设备分配一个或者多个标签：*

1. 在具有根特权的账户下运行命令提示符，然后将当前目录更改为包含 klscflag 实用程序的目录。klscflag 实用程序位于安装网络代理的目录中。默认安装目录为 /opt/kaspersky/klnagent64/sbin/。
2. 输入以下命令之一：

   - 要分配一组标签：

     ```
     /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"TAG NAME 1\",\"TAG NAME 2\",\"TAG NAME 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

     其中 [\"TAG NAME 1\",\"TAG NAME 2\",\"TAG NAME 3\"] 是您要分配给设备的标签列表。

     如果将方括号留空，这将从设备中删除所有标签：

     ```
     /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

   - 要将新标签分配给现有标签集：

     ```
     /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"NEW TAG NAME\",\"TAG NAME 1\",\"TAG NAME 2\",\"TAG NAME 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

     其中NEW TAG NAME是您想要分配给设备的标签的名称，而TAG NAME 1、TAG NAME 2、TAG NAME 3是已分配给设备的标签的名称。

   - 要删除特定标签而不删除已分配给设备的其他标签，请使用更新的标签集运行该命令。

     例如，如果您当前的标签是TAG NAME 1、TAG NAME 2、TAG NAME 3，而您想要删除TAG NAME 2，请运行以下命令：

     ```
     /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"TAG NAME 1\",\"TAG NAME 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

3. 重启网络代理服务。

klscflag 实用程序会将指定标签分配给您的设备。为了确保 klscflag 实用程序已成功分配指定标签，请查看分配给设备的标签。

或者，您可以手动分配设备标签。

# 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。

# 应用程序标签

通过 Kaspersky Security Center Linux，您能够从应用程序注册表中标记应用程序。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。

# 部署 Kaspersky 应用程序

本节介绍通过 Kaspersky Security Center 14 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 14 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。

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**

   从 Kaspersky 网站下载 Kaspersky Endpoint Security for Linux 的管理 Web 插件，然后将该插件添加到 Kaspersky Security Center 14 Web Console 中。

2. **下载和创建网络代理安装包**

   从 Kaspersky 网站下载网络代理分发软件包，然后创建网络代理安装软件包。

   您可以使用下载的分发包在本地安装网络代理。为此，请按照 Kaspersky Endpoint Security for Linux 文档中提供的说明操作。

3. **下载和创建 Kaspersky Endpoint Security for Linux 安装包**

   从 Kaspersky 网站下载 Kaspersky Endpoint Security for Linux 分发包，然后创建 Kaspersky Endpoint Security for Linux 安装包。

4. **创建独立安装包（可选）**

   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。如果使用独立包安装 Kaspersky 应用程序，则可以忽略下面的阶段 5 和阶段 6。

5. **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。

6. **创建和配置任务**

   必须配置 Kaspersky Endpoint Security for Linux 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，请确保任务计划符合您的要求。（默认情况下，任务的预定开始被设置为**手动**，但您可能希望选择其他选项。）

7. **创建策略**

   手动或通过快速启动向导为 Kaspersky Endpoint Security for Linux 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。

8. 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），您必须添加并安装该应用程序的管理 Web 插件。

*要添加并安装 Kaspersky 应用程序的管理 Web 插件：*

1. 从 Kaspersky 网站下载 Kaspersky Endpoint Security for Linux 的管理 Web 插件。
2. 打开 Kaspersky Security Center 14 Web Console。
3. 在“**控制台设置**”下拉列表中，选择“**Web 插件**”。
   可用管理插件列表被显示。
4. 单击**从文件添加**按钮。
   将显示“**从文件添加**”窗口。
5. 单击**上传 Zip 文件**按钮。
6. 指定下载的 Web 插件 ZIP 文件。
7. 单击**上传签名**按钮。
8. 指定下载的 Web 插件签名 TXT 文件。
9. 单击“**添加**”按钮。
   Kaspersky Security Center 会验证上传的文件，然后添加并安装 Web 插件。
10. 当安装完成时，点击“**确定**”。

管理 Web 插件使用默认配置进行安装并显示在管理 Web 插件列表中。

## 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。
- 要创建独立安装包。

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：
   - 转到**发现和部署→部署和分配→安装包**。
   - 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**。
   此时会启动新安装包向导。使用**"下一步"**按钮继续向导。
3. 选择**"从文件创建安装包"**
4. 指定包名称并单击**"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. 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，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：
   - 转到**发现和部署 → 部署和分配 → 安装包**。
   - 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. 如果随着所选的应用程序安装网络代理，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“**移动到受管理设备列表**”步骤中，默认已选择“**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. 独立安装包创建过程完成后，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。

## 查看独立安装包列表

您可以查看独立安装包列表以及每个独立安装包的属性。

*要查看所有安装包中独立安装包的列表：*

在列表上方，单击“**查看独立包列表**”按钮。

在独立安装包列表中，其属性显示如下：

- **包名称**。根据安装包中包含的应用程序名称和应用程序版本自动形成的独立安装包名称。
- **应用程序名称**。独立安装包中包含的应用程序名称。
- **应用程序版本**。
- **网络代理安装包名称**。仅当独立安装包中包含网络代理时，才显示该属性。
- **网络代理版本**。仅当独立安装包中包含网络代理时，才显示该属性。
- **大小**。文件大小（MB）。
- **组**。安装网络代理后，客户端设备将移动到的组的名称。
- **创建日期**。独立安装包的创建日期和时间。
- **修改日期**。独立安装包的修改日期和时间。
- **路径**。独立安装包所在文件夹的完整路径。

- **网址**。独立安装包位置的网址。
- **文件哈希**。该属性用于证明独立安装包没有被第三方更改，并且用户拥有的文件与您创建并传输给用户的文件相同。

*要查看特定安装包的独立安装包列表：*

在列表中选择安装包，然后在列表上方单击"**查看独立包列表**"按钮。

在独立安装包列表中，您可以执行以下操作：

- 通过单击"**发布**"按钮在 Web 服务器上发布独立安装包。您将独立安装包链接发送给的用户可以下载已发布的独立安装包。
- 通过单击"**取消发布**"按钮取消在 Web 服务器上发布独立安装包。未发布的独立安装包只能被您和其他管理员下载。
- 通过单击"**下载**"按钮将独立安装包下载到设备上。
- 通过单击"**通过电子邮件发送**"按钮发送带有独立安装包链接的电子邮件。
- 通过单击"**删除**"按钮删除独立安装包。

# 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

如果要在使用操作系统 RED OS 7.3.4 或更高版本或 MSVSPHERE 9.2 或更高版本的设备上安装网络代理，请安装 libxcrypt-compat 包以确保网络代理正确运行。

## 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（对于 Ubuntu 10.04，Sudo 版本为 1.7.2p1 或更高）
   - 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。

在打开的文件中，添加以下行到文件末尾：`<username> 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`。

## 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：

- **选择管理服务器检测到的网络设备**。此种情况下，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。
- **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。
- **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。

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。

## 在特定设备上安装应用程序

本节包含有关如何在管理组、具有特定 IP 地址的设备或选择的受管理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“**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。

如果任务已分配给管理组，任务属性窗口中将不显示“**安全**”选项卡，因为组任务受其适用的组安全设置限制。

- 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。

5. 遵照向导的说明操作。

   “添加任务向导”将创建一个任务，用于在指定设备上远程安装向导中选择的应用程序。如果您选择了“**分配任务到管理组**”选项，则任务是组任务。

6. 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。

   “添加任务向导”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。

## 指定 Unix 设备上的远程安装设置

使用远程安装任务在 Unix 设备上安装应用程序时，可以为该任务指定 Unix 特定的设置。创建任务后，这些设置在任务属性中可用。

*要为远程安装任务指定 Unix 特定的设置：*

1. 在主菜单中，转到“**设备**” → “**任务**”。
2. 单击要为其指定 Unix 特定设置的远程安装任务的名称。
   任务属性窗口打开。
3. 转到“**应用程序设置**”→“**Unix 特定的设置**”。
4. 指定下列设置：
   - 为根账户设置密码(仅对通过 SSH 的部署)

     如果在目标设备上不指定密码就无法使用 sudo 命令，则选择此选项，然后指定 root 账户的密码。Kaspersky Security Center 14 Linux 会将密码以加密形式传输到目标设备，解密密码，然后以具有指定密码的 root 账户的身份启动安装过程。

     Kaspersky Security Center 14 Linux 不会使用该账户或指定的密码创建 SSH 连接。
   - 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)

     如果目标设备上的 /tmp 目录没有执行权限，则选择此选项，然后指定具有执行权限的目录路径。Kaspersky Security Center 14 Linux 使用指定的目录作为通过 SSH 进行访问的临时目录。应用程序会将安装包放在该目录中并运行安装过程。
5. 单击“**保存**”按钮。

指定的任务设置即被保存。

## 启动和停止卡巴斯基应用程序

您可以使用*启动或停止应用程序*任务在受管设备上启动和停止卡巴斯基应用程序。

*要创建启动或停止应用程序任务：*

1. 在主菜单中，转到“**设备**” →“**任务**”。
2. 单击**添加**。
   “新任务向导”启动。使用“**下一步**”按钮继续向导操作。
3. 在**应用程序**下拉列表中，选择要为其建立任务的应用程序。
   如果您之前已为这些应用程序添加了管理 Web 插件，则卡巴斯基应用程序将显示在列表中。
4. 在**任务类型**列表中选择**应用程序激活**任务。
5. 在**任务名称**字段中，指定新任务的名称。
   任务名称不能超过 100 个字符并且不能包括任何特殊字符 ("*<>?\:|)。
6. 选择要将任务分配到的设备。

7. 在“应用程序”窗口中，执行以下操作：

   - 选中要为其创建任务的应用程序名称旁边的复选框。
   - 选择启动应用程序或停止应用程序选项。

8. 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”步骤的“完成任务创建”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。

9. 单击“完成”按钮。

   任务被创建并显示在任务列表。

10. 点击创建的任务的名称以打开任务属性窗口。

11. 在任务属性窗口中，根据需要指定常规任务设置，然后保存设置。

任务被创建和配置。

要运行任务，请在任务列表中选择它，然后单击“开始”按钮。

# 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 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 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。

使用说明：安装前删除不兼容的应用程序

## 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，您可以选择计划类型“在完成其他任务时”，这里，其他任务就是“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。

使用说明：创建任务

# 远程删除应用程序或软件更新

您只能使用网络代理删除远程运行 Linux 的受管理设备上的应用程序或软件更新。

*要从选定设备中远程删除应用程序或软件更新：*

1. 在主菜单中，转到“设备” → “任务”。

2. 单击**添加**。

   “添加任务向导”启动。使用**下一步**按钮进行向导。

3. 对于 Kaspersky Security Center 应用程序，选择“**远程卸载应用程序**”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. 选择要将任务分配到的设备。

6. 选择要删除的软件种类，然后选择要删除的特定应用程序、更新或补丁：

   - 卸载受管理应用程序

     显示 Kaspersky 应用程序列表。选择要删除的应用程序。

   - 卸载不兼容的应用程序

     显示与 Kaspersky 安全应用程序或 Kaspersky Security Center 不兼容的应用程序列表。选中要删除的应用程序旁边的复选框。

   - 从应用程序注册表中卸载应用程序

默认情况下，网络代理会向管理服务器发送有关受管理设备上安装的应用程序的信息。已安装应用程序的列表存储在应用程序注册表中。

*要从应用程序注册表中选择应用程序：*

a. 单击“**要卸载的应用程序**”字段，然后选择要删除的应用程序。

如果您选择 Kaspersky Security Center 网络代理，则运行任务时，状态“*已成功完成*”将显示删除进程已开始。如果删除 Kaspersky Security Center 网络代理，状态不会改变。如果任务失败，状态更改为“*失败*”。

b. 指定卸载选项：

- 卸载模式

选择要如何删除应用程序：

- **自动定义卸载命令**

  如果应用程序具有应用程序供应商定义的卸载命令，则 Kaspersky Security Center 将使用此命令。我们建议您选择此选项。

- **指定卸载命令**

  如果要指定您自己的应用程序卸载命令，请选择此选项。

  我们建议您先尝试使用“**自动定义卸载命令**”选项来卸载应用程序。如果通过自动定义的命令卸载失败，则使用您自己的命令。

  在该字段中键入卸载命令，然后指定以下选项：

  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 会检查所选应用程序是否具有应用程序供应商定义的卸载命令。如果找到，Kaspersky Security Center 将使用该命令，而不使用在“**应用程序卸载命令**”字段中指定的命令。

  我们建议您启用此选项。

- 应用程序成功卸载后执行重启

如果应用程序要求在成功卸载后重新启动受管理设备上的操作系统，操作系统将自动重新启动。

7. 指定客户端设备将如何下载卸载实用程序：

- 使用网络代理

通过这些客户端设备上安装的网络代理将文件传送到客户端设备。

如果禁用此选项，则使用 Linux 操作系统工具传送文件。

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。

- 通过管理服务器使用操作系统资源

  该选项已过时。请改用**使用网络代理**或**通过分发点使用操作系统资源**选项。

  使用管理服务器操作系统工具将文件传输到客户端设备。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。

- 通过分发点使用操作系统资源

  使用操作系统工具通过分发点将文件传输到客户端设备。如果网络中存在不止一个分发点，则可以启用此选项。

  如果启用"**使用网络代理**"选项，仅当网络代理工具不可用时才通过操作系统工具传送文件。

- 同时下载的最大数量

  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。该数字越大，应用程序的卸载速度越快，但管理服务器上的负载也越高。

- 尝试卸载的最大次数

  如果在运行"*远程卸载应用程序*"任务时，Kaspersky Security Center 未能在由参数指定的安装程序运行次数内卸载受管理设备上的应用程序，Kaspersky Security Center 将停止向该受管理设备传送卸载实用程序，并且不再在该设备上启动安装程序。

  "**尝试卸载的最大次数**"参数允许您节省受管理设备资源，以及减少流量（卸载、MSI 文件运行和错误消息）。

  重复的任务启动尝试可能表示设备上存在妨碍卸载的问题。管理员应在指定的卸载尝试次数内解决问题，然后重新启动该任务（手动或按计划）。

  如果卸载始终未完成，问题被视为无法解决且后续任务启动被认为是不必要的资源和流量浪费。

  创建任务时，尝试计数器设置为 `0`。返回错误的安装程序的每次运行都增加计数。

  如果已超过参数中指定的尝试次数，且设备已准备好应用程序卸载，您可以增加"**尝试卸载的最大次数**"参数的值并启动任务以卸载应用程序。或者，您可以创建新的"*远程卸载应用程序*"任务。

- 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 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 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。

8. 指定操作系统重新启动设置：

- 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。

9. 如果必要，添加要用于启动远程卸载任务的账户：

   - 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*远程卸载应用程序*任务的设备上未安装网络代理，请选择此项。在这种情况下，您可以指定用户账户或 SSH 证书来卸载应用程序。

     - **本地账户**。如果该选项被选中，请指定将运行应用程序安装程序的用户账户。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。

     - **SSH 证书**。如果要从基于 Linux 的客户端设备上卸载应用程序，您可以指定 SSH 证书而不是用户账户。单击**添加**按钮，选择**SSH 证书**，然后指定证书的私钥和公钥。

       要生成私钥，您可以使用 ssh-keygen 实用程序。请注意，Kaspersky Security Center 支持 PEM 格式的私钥，但 ssh-keygen 实用程序默认生成 OPENSSH 格式的 SSH 密钥。Kaspersky Security Center 不支持 OPENSSH 格式。要以支持的 PEM 格式创建私钥，请在 ssh-keygen 命令中添加"-m PEM"选项。

       例如：

       ```
       ssh-keygen -m PEM -t rsa -b 4096 -C "<user email>"
       ```

10. 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。

11. 单击"**完成**"按钮。

    任务被创建并显示在任务列表。

12. 点击创建的任务的名称以打开任务属性窗口。

13. 在任务属性窗口中，指定常规任务设置。

14. 单击“保存”按钮。

15. 手动运行任务，或者按照任务设置中指定的计划等待任务启动。

远程卸载任务完成后，所选应用程序从选定设备中删除。

### 远程卸载问题

有时远程卸载第三方应用程序可能会在结束时出现以下警告：“远程卸载已在该设备上结束，但是有警告：要移除的应用程序未安装。”当要卸载的应用程序已经被卸载或者仅为单个用户安装时，会发生该问题。如果用户未登录，则为单个用户安装的应用程序（也称为按用户发放的应用程序）不可见且无法进行远程卸载。

该行为与供多个用户在同一台设备上使用的应用程序（也称为按设备发放的应用程序）不同。按设备发放的应用程序可供设备上的所有用户看见和访问。

因此，按用户发放的应用程序必须在用户登录时才能卸载。

### 有关安装的应用程序的信息源

网络代理可从以下注册表键值提取有关 Windows 设备上安装的软件的信息：

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall
  包含有关为所有用户安装的应用程序的信息。
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall
  包含有关为所有用户安装的应用程序的信息。
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall
  包含有关为当前用户安装的应用程序的信息。
- HKEY_USER<...>\Software\Microsoft\Windows\CurrentVersion\Uninstall
  包含有关为特定用户安装的应用程序的信息。

## 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。

# Kaspersky 应用程序：授权许可和激活

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**”→“**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 14 Web Console 可让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“**设备**” → “**任务**”。
2. 单击**添加**。
   “**添加任务向导**”启动。使用“**下一步**”按钮继续向导操作。
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“**关闭**”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密钥添加窗格中。

c. 单击“**关闭**”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. 在向导的**授权许可信息**步骤中，如果要替换当前的活动授权许可密钥，请清除默认的**用作备用密钥**复选框。

例如，当组织发生变化时，设备上需要另一个组织的密钥时，或者重新颁发了密钥，新授权许可比当前授权许可更早到期，等等，需要这样做。为了避免错误，您必须清除**用作备用密钥**复选框。

如果您想了解有关向 Kaspersky Security Center 添加授权许可密钥时可能出现的问题及其解决方法的更多信息，请参阅Kaspersky Security Center 知识库。

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。

虚拟管理服务器自动从其存储库和管理服务器的存储库中分发授权许可密钥。我们建议您：

- 使用“*添加授权许可密钥*”任务来选择必须部署到设备的授权许可密钥。
- 避免在虚拟管理服务器设置中禁用“**允许从该虚拟管理服务器自动部署授权许可密钥到它的设备**”选项。否则，虚拟管理服务器将不会向设备分发授权许可密钥，包括来自管理服务器存储库的授权许可密钥。

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，您可以稍后使用任务分发授权许可密钥。

自动分发在主管理服务器上配置的授权许可密钥不会扩展到由非虚拟从属管理服务器管理的设备。

# 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“**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。

## 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. 转到“**操作**”→“**授权许可**”→“**卡巴斯基授权许可**”。
2. 选择要从存储库中删除的密钥文件或激活码。
3. 单击“**删除**”按钮。
4. 单击“**确定**”按钮确认操作。

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。

## 撤销对最终用户授权许可协议的同意

如果您决定停止保护某些客户端设备，可以撤销任何受管理 Kaspersky 应用程序的最终用户授权许可协议 (EULA)。您必须先卸载所选应用程序，再撤销其 EULA。

*要撤销受管理 Kaspersky 应用程序的 EULA：*

1. 在管理服务器属性窗口中的“**常规**”选项卡上，选择“**最终用户授权许可协议**”区域。
   将显示在创建安装包时、无缝安装更新时或部署 Kaspersky Security for Mobile 时接受的 EULA 列表。
2. 在该列表中，选择要撤销的 EULA。
   您可以查看 EULA 的以下属性：
   - EULA 的接受日期
   - 接受 EULA 的用户名

3. 单击任意 EULA 的接受日期以打开其属性窗口，其中显示以下数据：

   - 接受 EULA 的用户名
   - EULA 的接受日期
   - EULA 的唯一标识符 (UID)
   - EULA 的全文
   - 链接到 EULA 的对象（安装包、无缝更新、移动应用程序）列表以及各自的名称和类型

4. 在 EULA 属性窗口的下部，单击“**撤回授权许可协议**”按钮。

   如果存在任何对象（安装包以及各自的任务）阻止撤销 EULA，则会显示相应通知。在删除这些对象之前，无法继续撤销。

   在打开的窗口中，系统提示您必须先卸载与 EULA 对应的 Kaspersky 应用程序。

5. 单击按钮以确认撤销。

EULA 即被撤销。它不再显示在“**最终用户授权许可协议**”区域的授权许可协议列表中。EULA 属性窗口关闭；不再安装应用程序。

## 续订 Kaspersky 应用程序授权许可

您可以续订已到期或即将到期（少于 30 天内）的 Kaspersky 应用程序授权许可。

*要续订到期的授权许可或即将到期的授权许可：*

1. 做以下之一：

   - 在主菜单中，转到“**操作**”→“**授权许可**”→“**卡巴斯基授权许可**”。
   - 在主菜单中，转到“**监控和报告**”→“**控制板**”，然后单击通知旁边的“**查看即将到期的授权许可**”链接。

   “**卡巴斯基授权许可**”窗口打开，您可以在其中查看和续订授权许可。

2. 单击所需授权许可旁边的“**续费授权许可**”链接。

   单击授权许可续订链接，即表示您同意向 Kaspersky 传输以下有关 Kaspersky Security Center 的信息：版本、您使用的本地化、软件授权许可 ID（即您要续订的授权许可 ID）以及您是否通过合作伙伴公司购买了授权许可。

3. 在打开的授权许可续订服务窗口中，按照说明续订授权许可。

   授权许可即被续订。

在 Kaspersky Security Center 14 Web Console 中，当授权许可即将到期时，会按照以下计划显示通知：

- 到期前 30 天

- 到期前 7 天
- 到期前 3 天
- 到期前 24 小时
- 授权许可到期后

## 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。选择某个解决方案后，Kaspersky Security Center 14 Linux 会将您重定向到 Kaspersky 网站上的相关网页，以了解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。

# 配置网络保护

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创建其他策略和任务（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 管理服务器
- 安装了 Kaspersky Security Center 14 Web Console
- 完成了 Kaspersky Security Center 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

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。这两种方法也可以被合并。

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：设置更新 Kaspersky Endpoint Security 的组任务。

   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。

   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事故时。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 管理服务器和 Kaspersky Security Center 14 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配置您网络的保护时，Kaspersky Security Center 为 Kaspersky Endpoint Security for Linux 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. **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 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 管理服务器和 Kaspersky Security Center 14 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 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 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 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。

## 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）。

## 网络代理策略设置

*若配置网络代理策略：*

1. 在主菜单中，转到“**设备**”→“**策略和配置文件**“。
2. 单击网络代理策略的名称。

网络代理策略的属性窗口打开。

### 常规

在该选项卡上，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：
  - 活动策略

    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。
  - 非活动策略

    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

在该选项卡上，您可以配置事件记录和事件通知。事件按照“**事件配置**”选项卡上以下区域中的重要级别进行分布：

- **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）。单击事件类型后，您可以指定有关列表中选择的事件的事件记录和通知的设置。默认下，为整个管理服务器指定的通用通知设置被用于所有事件类型。然后，您可以更改所需事件类型的特别设置。

例如，在“**警告**”区域中，您可以配置 **发生了事故** 事件类型。此类事件可能会发生，例如，当 分发点的可用磁盘空间 小于 2 GB（至少需要 4 GB 才能远程安装应用程序和下载更新）。若要配置“**发生了事故**”事件，单击它并指定存储发生的事件的位置以及如何通知它们。

如果网络代理检测到事件，您可以使用受管理设备的设置管理此事件。

## 应用程序设置

### 设置

在**设置**区域，您可以配置网络代理策略：

- 事件队列的最大大小(MB)

  在该字段中，您可以指定事件队列可在驱动器上占据的最大空间。
  默认值为 2 MB。

- 应用程序被允许在设备上检索策略扩展数据

安装在受管理设备上的网络代理会将有关已应用的安全应用程序策略的信息传输到安全应用程序（例如，Kaspersky Endpoint Security for Linux）。您可以在安全应用程序界面查看传输的信息。

网络代理传输以下信息：

- 策略传输至受管理设备的时间
- 策略传输至受管理设备时的活动策略或漫游策略的名称
- 策略传输至受管理设备时包含受管理设备的管理组的名称和完整路径
- 活动策略配置文件列表

  您可以使用该信息来确保将正确的策略应用于设备并用于故障排除。默认情况下已禁用该选项。

## 存储库

在“**存储库**”区域，您可以选择将其信息从网络代理发送到管理服务器的对象类型。如果本区域中的某些设置被网络代理策略禁止，则您无法修改它们。

- 已安装应用程序详情

  如果启用此选项，则有关客户端设备上安装的应用程序的信息将发送至管理服务器。

  默认情况下已启用该选项。

- 硬件注册表的详细信息

  安装在设备上的网络代理会将设备硬件的相关信息发送到管理服务器。您可以在设备属性中查看硬件详细信息。

  确保在要从中获取硬件详细信息的 Linux 设备上安装了 lshw 实用程序。根据所使用的 hypervisor，从虚拟机获取的硬件详细信息可能不完整。

## 网络

“**网络**”区域包含三个子区域：

- **连接**
- **连接配置文件**
- **连接计划**

在“**连接**”子区域中，可以配置与管理服务器的连接，启用 UDP 端口和指定 UDP 端口号。

- 在“**连接到管理服务器**”设置组，您可以配置到管理服务器的连接并指定同步客户端设备和管理服务器的时间间隔：
  - 同步间隔(分钟)

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。

如果同步间隔设置为少于 15 分钟，则每 15 分钟执行一次同步。如果同步间隔设置为 15 分钟或更长时间，则以指定的同步间隔执行同步。

- 压缩网络流量

  如果启用此选项，则通过减少所传输的流量进而减少管理服务器的负载来提高网络代理的数据传输速度。

  客户端设备上的 CPU 负载可能会增加。

  默认情况下启用该复选框。

- 使用 SSL 连接

  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。

  默认情况下已启用该选项。

- 以默认连接设置在分发点(如果可用)上使用连接网关

  如果启用此选项，分发点上的连接网关在管理组属性指定的设置下使用。

  默认情况下已启用该选项。

- 使用 UDP 端口

  如果需要网络代理通过 UDP 端口连接到管理服务器，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。连接到管理服务器的默认 UDP 端口是 15000。

- UDP 端口号

  在该字段中，您可以输入 UDP 端口号。默认端口号是 15000。

  使用十进制系统记录。

在“**网络**”区域的“**连接配置文件**”子区域中，可以指定网络位置设置并在管理服务器不可用时启用漫游模式。

- 网络位置设置

  网络位置设置用于定义客户端设备所连接的网络属性，并指定当网络特性改变时，网络代理从一个管理服务器连接配置文件切换到另一个配置文件的规则。

- 管理服务器连接配置文件

连接配置文件仅支持运行 Windows 的设备。我们不建议使用此选项。

您可以查看和向管理服务器添加网络代理连接配置文件。在该区域，您也可以创建当以下事件发生时，切换网络代理到不同管理服务器的规则：

- 当客户端设备连接到另一个本地网络时
- 当设备与组织的本地网络丢失连接时
- 当连接网关的地址更改或 DNS 服务器地址修改时

在“**连接配置文件**”设置组中，无法向“**管理服务器连接配置文件**”列表添加任何新项目，因此“**添加**”按钮处于不活动状态。预设的连接配置文件也不能修改。

- 当管理服务器不可用时启用漫游模式

  如果启用此选项，则在通过该配置文件连接的情况下，客户端设备上安装的应用程序将使用漫游模式设备的策略配置文件，以及漫游策略。如果没有为应用程序定义漫游策略，则使用激活策略。

  如果禁用此选项，则应用程序将使用已激活的策略。

  默认情况下已禁用该选项。

在“**连接计划**”子区域中，您可以指定网络代理发送数据到管理服务器的时间间隔：

- 必要时连接

  如果选中此选项，当网络代理需要发送数据到管理服务器时连接才被建立。

  默认情况下已选定该选项。

- 在指定时间间隔连接

  如果选中此选项，网络代理在指定时间连接到管理服务器。您可以添加若干个连接时间段。

## 通过分发点的网络轮询

在“**通过分发点的网络轮询**”区域中，可以配置网络自动轮询。您可以使用以下选项启用轮询并设置其频率：

- Zeroconf

如果启用此选项，分发点将使用零配置网络（也称为 *Zeroconf*）轮询带有 IPv6 设备的网络。在这种情况下，已启用的 IP 范围轮询将被忽略，因为分发点将轮询整个网络。

要开始使用 Zeroconf，必须满足以下条件：

- 分发点必须运行 Linux。
- 您必须在分发点上安装 avahi-browse 实用程序。

如果禁用此选项，分发点不会轮询带有 IPv6 设备的网络。

默认情况下已禁用该选项。

- **IP 范围**

  如果启用此选项，则分发点将按照所配置的计划自动轮询 IP 范围，单击“**设置轮询计划**”按钮可配置轮询计划。

  如果禁用此选项，则分发点将不轮询 IP 范围。

  对于 10.2 版之前的网络代理，可在“**轮询间隔(分钟)**”字段中配置 IP 范围的轮询频率。如果启用此选项，则该字段可用。

  默认情况下已禁用该选项。

## 分发点网络设置

在“**分发点网络设置**”区域中，可以指定互联网连接设置：

- 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**

  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
- 密码

## 更新(分发点)

在**更新(分发点)**区域，您可以启用下载差异文件功能，以便分发点以差异文件的形式从卡巴斯基更新服务器获取更新。

### 修订历史

在此选项卡上，您可以查看策略修订列表和回滚策略更改（如有必要）。

# 任务

该部分描述了 Kaspersky Security Center 使用的任务。

# 关于任务

Kaspersky Security Center 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 14 Web Console 创建，仅在该应用程序的管理插件安装在 Kaspersky Security Center 14 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 14 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“**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“**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。

# 手动启动任务

应用程序根据每个任务的属性中指定的计划设置来启动任务。您可以随时从任务列表中手动启动任务。或者，您也可以在“**受管理设备**”列表中选择设备，然后对这些设备启动现有任务。

*要手动启动任务：*

1. 在主菜单中，转到“**设备**” → “**任务**”。

2. 在任务列表中，选中要启动的任务旁边的复选框。

3. 单击“**开始**”按钮。

任务启动。您可以在“**状态**”列中或单击“**结果**按钮”来检查任务状态。

# 查看任务列表

您可以查看在 Kaspersky Security Center Linux 中创建的任务列表。

*要查看任务列表，*

转到"**设备**" →" **任务**"。

将显示任务列表。这些任务按与它们相关的应用程序的名称分组。例如，“*远程安装应用程序*”任务与管理服务器相关，“*更新*”任务涉及 Kaspersky Endpoint Security for Linux。

*要查看任务的属性，*

单击任务的名称。

将显示任务属性窗口，其中包含几个已命名的选项卡。例如，“**任务类型**”显示在“**常规**”选项卡上，任务计划显示在“**计划**”选项卡上。

# 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 6 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，任务每星期五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

  任务在每周指定日期的指定时间定期运行。

  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。

  默认情况下已选定该选项。

- 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，不选择任何月份中的日期。默认开始时间为 18:00。

- 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。

  如果禁用此选项，则只有计划任务会在客户端设备上运行。对于“手动”、“一次”和“立即”计划，仅在网络上可见的客户端设备上运行任务。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。

  默认情况下已禁用该选项。

- 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。

  如果任务已分配给管理组，任务属性窗口中将不显示“**安全**”选项卡，因为组任务受其适用的组安全设置限制。

- 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：
  - 通过 Wake-On-LAN 在任务启动之前激活设备(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。

  - 如果任务运行长于此时间则停止任务(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。

## 启动更改任务密码向导

对于非本地任务，可以指定必须在其下运行任务的账户。您可以在任务创建过程中或在现有任务的属性中指定账户。如果根据组织的安全性说明使用了指定的账户，则这些说明可能需要不时更改账户密码。账户密码过期且您设置了新密码后，任务将无法启动，直到您在任务属性中指定了新的有效密码。

更改任务密码向导使您可以在指定账户的所有任务中自动将旧密码替换为新密码。或者，您可以在每个任务的属性中手动更改此密码。

*要启动更改任务密码向导：*

1. 在“**设备**”选项卡上，选择“**任务**”。
2. 单击**管理启动任务的账户凭证**。

遵照向导的说明。

## 步骤 1：指定凭证

指定当前在系统中有效的新凭据。当您切换到向导的下一步时，Kaspersky Security Center 将检查指定的账户名是否与每个非本地任务的属性中的账户名匹配。如果账户名匹配，则任务属性中的密码将自动替换为新的密码。

要指定新账户，请选择一个选项：

- 使用当前账户

  该向导使用您当前登录 Kaspersky Security Center 14 Web Console 所使用的账户名。然后手动在“**在任务中使用的当前密码**”字段中指定账户密码。

- 指定不同账户

指定必须启动任务的账户名。然后在“**在任务中使用的当前密码**”字段中指定账户密码。

如果您填写“**先前密码(可选，如果您要使用当前密码替换它)**”字段，Kaspersky Security Center 仅为找到账户名和旧密码的任务替换密码。替换将自动执行。在所有其他情况下，您必须选择要在向导的下一步执行的操作。

## 步骤 2：选择要采取的操作

如果未在向导的第一步中指定先前密码，或者指定的旧密码与任务属性中的密码不匹配，则必须选择要对找到的任务执行的操作。

*要选择对任务的操作：*

1. 选中要对其选择操作的任务旁边的复选框。
2. 执行以下操作之一：
   - 要删除任务属性中的密码，请单击“**删除凭证**”。
     任务将切换为在默认账户下运行。
   - 要将密码替换为新密码，请单击“**即便旧密码错误或未指定也强制密码更改**”。
   - 要取消密码更改，请单击“**未选择操作**”。

移至向导的下一步后，将应用所选操作。

## 步骤 3：查看结果

在向导的最后一步，查看每个找到的任务的结果。要完成向导，请单击“**完成**”按钮。

# 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. 单击“**结果**”链接打开“**任务结果**”窗口。

# 管理客户端设备

Kaspersky Security Center Linux 可让您管理客户端设备：

- 查看受管理设备的设置和状态，包括群集和服务器阵列。
- 配置分发点。
- 管理任务。

您可以使用管理组将客户端设备合并成一组，并作为一个单元进行管理。一个客户端设备只能包含在一个管理组中。设备可根据 规则条件 自动分配到组中：

- 创建设备移动规则。
- 复制设备移动规则。
- 设备移动规则的条件。

您可以使用设备分类来根据条件筛选设备。您还可以标记设备以创建分类、查找设备以及将设备分配到各管理组中。

# 受管理设备设置

*要查看受管理设备设置：*

1. 选择**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，单击带有所需设备名称的链接。

   将显示所选设备的属性窗口。

以下选项卡显示在代表主要设置组的属性窗口的上部：

- 常规

此选项卡包括以下区域：

- “常规”区域显示有关客户端设备的常规信息。信息基于上一次客户端设备与管理服务器之间的同步接收的数据来提供：
  - 名称

    在该字段中，您可以查看和修改管理组中的客户端设备名称。
  - 描述

    在该字段中，您可以输入客户端设备的附加描述。
  - 完整组名称

    包括了客户端设备的管理组。
  - 保护上次更新

    设备上病毒数据库或应用程序最后更新日期。
  - 上一次可见

    设备在网络中最后可见的日期和时间。
  - 连接到管理服务器

    客户端设备上安装的网络代理上一次连接到管理服务器的日期和时间。
  - 不断开与管理服务器的连接

    如果启用此选项，将保持受管理设备和管理服务器之间的持续连接。如果正在使用的不是提供此类连接的推送服务器，您可能希望使用此选项。

    如果禁用此选项且推送服务器不在使用中，受管理设备将仅在同步数据或传输信息时连接至管理服务器。

    选中“不断开与管理服务器的连接”选项时的最大设备总数为 300。

    默认情况下已在受管理设备上禁用该选项。此选项在安装了管理服务器的设备上默认启用，即使您尝试禁用它也保持启用状态。
- “网络”部分显示有关客户端设备的网络属性的以下信息：
  - IP 地址

    设备 IP 地址。
  - Windows 域

包含设备的工作组。

- DNS 名称

  客户端设备的 DNS 域名称。

- NetBIOS 名称

  客户端设备名称。

- “**系统**”区域提供有关安装在客户端设备上的操作系统的信息。
- “**保护**”区域提供有关客户端设备上反病毒保护当前状态的以下信息：
  - 设备状态

    基于管理员定义的标准分配的关于设备上反病毒保护和网络中设备活动的客户端设备的状态。

  - 所有问题

    该表格包含了客户端设备上安装的受管理应用程序检测到的问题的完整列表。每个问题都伴有一个状态，应用程序建议您分配该状态到该问题的设备。

  - 实时保护

    该字段显示当前的客户端设备实时保护状态。

    当设备状态更改时，新状态仅在客户端设备与管理服务器同步之后显示在设备属性窗口。

  - 上一次按需扫描时间

    客户端设备上次执行恶意软件扫描的日期和时间。

  - 检测到的威胁总数

    自安装安全应用程序（第一次扫描）或自上次重置威胁计数器以来，在客户端设备上检测到的威胁总数。

  - 活动威胁

    客户端设备上的未处理文件数量。

    该字段移动设备上的未处理文件数量。

- “**应用程序定义的设备状态**”区域提供有关由安装在设备上的受管理应用程序定义的设备状态的信息。该设备状态可能与 Kaspersky Security Center Linux 定义的状态不同。

- 应用程序

该选项卡列出了客户端设备上安装的所有卡巴斯基应用程序。该选项卡包含**开始**和**停止**按钮，可让您启动和停止所选的卡巴斯基应用程序（不包括网络代理）。如果受管理设备上的15000 UDP 端口可用，则可以使用这些按钮来接收来自管理服务器的推送通知。如果受管理设备无法接收推送通知，但启用了与管理服务器的持续连接模式（启用了**不断开与管理服务器的连接**部分中的**常规**选项），则**开始**和**停止**按钮也可用。否则，当您尝试启动或停止应用程序时，将显示一条错误消息。您也可以单击应用程序名称以查看有关该应用程序的常规信息、发生在设备上的事件的列表以及应用程序设置。

- 活动策略和策略配置文件

  此选项卡列出了当前分配给受管理设备上的策略和策略配置文件。

- 任务

  在“**任务**”选项卡上，您可以管理客户端设备任务：查看现有任务列表、创建新任务、删除、启动和停止任务、修改任务设置以及查看执行结果。该任务列表由客户端最近一次与管理服务器进行同步的会话期间收到的数据提供。管理服务器请求客户端设备的任务状态详情。如果受管理设备上的15000 UDP 端口可用于接收来自管理服务器的推送通知，则会显示任务状态并启用用于管理任务的按钮。如果受管理设备无法接收推送通知，但启用了与管理服务器的持续连接模式（启用了**不断开与管理服务器的连接**部分中的**常规**选项），则也可以使用对任务的操作。

  如果未建立连接，则不显示状态，按钮被禁用。

- 事件

  “**事件**”选项卡将显示选定客户端设备在管理服务器上所记录的事件。

- 标签

  在“**标签**”区域，您可以管理用于查找客户端设备的关键字列表：查看现有标签列表、从列表中分配标签、配置自动标记规则、添加新标签和重命名旧标签以及删除标签。

- 高级

此选项卡包括以下区域：

- **应用程序注册表**。在此区域，您可以查看客户端设备上安装的应用程序及其更新的注册表，您还可以设置应用程序注册表的显示。

  如果客户端设备上安装的网络代理将所需信息发送到管理服务器，则将提供有关已安装应用程序的信息。您可以在网络代理或其策略的属性窗口中的“**存储库**”区域中配置将信息发送到管理服务器。

  单击应用程序名称将打开一个窗口，其中包含应用程序详细信息以及为该应用程序安装的更新安装包的列表。

- **可执行文件**。此区域显示在客户端设备上发现的可执行文件。

- **分发点**。该区域提供设备与之交互的分发点列表。

  - 导出到文件

    点击**导出到文件**按钮保存设备与之交互的分发点列表文件。默认下，程序导出设备列表到 CSV 文件。

  - 属性

    点击**属性**按钮查看和配置设备与之交互的分发点。

- **硬件注册表**。在此区域，您可以查看客户端设备上安装的硬件的信息。

# 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. 转到“**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. 转到“**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“**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、根据标准方案分配网络代理。

# 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“**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。

- 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）。

- 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。

- 启用规则

  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。

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。

如果选择了“**持续应用规则**”选项，则移动规则的应用与优先级设置无关。这些规则会根据管理服务器自动设置的时间表来应用。

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“**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。
   - 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）。

- 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。

- 启用规则

  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。

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 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 14 网络代理** 或 **Kaspersky Security Center 14 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**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。

## 手动将设备添加到管理组

您可以通过创建设备移动规则来自动将设备移动到管理组，或通过将设备从一个管理组移动到另一管理组或将设备添加到选定的管理组来手动移动设备。本节介绍如何手动将设备添加到管理组。

*要手动将一台或多台设备添加到选定的管理组：*

1. 转到“**设备**”→“**受管理设备**”。
2. 单击列表上方的“**当前路径：** <当前路径>”链接。
3. 在打开的窗口中，选择您要添加到设备的管理组。
4. 单击“**添加设备**”按钮。
   移动设备向导启动。
5. 生成要添加到管理组的设备列表。

   您只能添加在连接设备时或设备发现后其信息已经添加至管理服务器数据库的设备。

   选择要将设备添加到列表的方式：

   - 单击“**添加设备**”按钮，然后通过以下方式之一指定设备：

- 从管理服务器检测到的设备列表中选择设备。
- 指定设备 IP 地址或 IP 范围。
- 指定设备 DNS 名称。

> 设备名称字段不得包含空格、退格或以下禁止的字符：, \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %

- 单击"**从文件导入设备**"按钮以从 .txt 文件导入设备列表。每个设备地址或名称都必须在单独一行中指定。

> 该文件不得包含空格、退格或以下禁止的字符：, \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %

6. 查看要添加到管理组的设备列表。您可以通过添加或删除设备来编辑列表。
7. 确保列表正确后，单击"**下一步**"按钮。

向导将处理设备列表并显示结果。处理成功的设备将添加到管理组并以管理服务器生成的名称显示在设备列表中。

# 手动将设备或者集群移动至管理组

您可以将设备从一个管理组移动到另一个管理组，或从未分配的设备组移动到管理组。

您还可以将集群或服务器阵列从一个管理组移动到另一个管理组。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。当您在**设备**选项卡上选择单个集群节点时， **移动到组**按钮将变得不可用。

*要将一台或多台设备或者集群移动到选定的管理组：*

1. 打开要从中移动设备的管理组。为此，请执行以下操作之一：
   - 要打开管理组，请在主菜单中转到"**设备**"→"**受管理设备**"，单击"**当前路径**"字段中的路径链接，然后在打开的左侧窗格中选择一个管理组。
   - 要打开"**未分配的设备**"组，请转到"**发现和部署**"→"**未分配的设备**"。
2. 如果管理组包含集群或服务器阵列，则**受管理设备**区域将被分为两个选项卡：**设备**选项卡和**集群和服务器阵列**选项卡。打开要移动的对象的选项卡。
3. 选中要移动到其他组的设备或者集群旁边的复选框。
4. 单击**移动到组**按钮。
5. 在管理组的层级中，选中要将选定设备或者集群移动到的管理组旁边的复选框。
6. 单击"**移动**"按钮。

选定设备或者集群将被移动到选定管理组。

# 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。

   “添加任务向导”启动。遵照向导的说明。在“添加任务向导”的“**新任务**”窗口中，选择“**Kaspersky Security Center 14**”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。

     如果任务已分配给管理组，任务属性窗口中将不显示“**安全**”选项卡，因为组任务受其适用的组安全设置限制。

   - 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。

在任务执行完毕后，为其创建任务的客户端设备将由任务设置中指定的管理服务器进行管理。

# 通过连接网关将连接到管理服务器的设备移动到另一台管理服务器

您可以将通过连接网关连接到管理服务器的设备移动到另一台管理服务器。例如，如果您安装了另一个版本的管理服务器并且不想在设备上重新安装网络代理（因为这可能很耗时），则可能需要这样做。

说明中描述的命令必须在具有管理员权限的账户下在客户端设备上运行。

*要将通过连接网关连接的设备移动到另一台管理服务器：*

1. 使用 `-address <服务器地址>` 参数运行klmover 实用程序，切换到新的管理服务器。
2. 运行 `klnagchk -nagwait -tl 4` 命令。

3. 运行以下命令设置新的连接网关：

   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_mode -sv false -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"`
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_loc -sv "gateway_ip_or_name" -svt STRING_T -ss "|ss_type = \"SS_SETTINGS\";"`

     在此，`gateway_ip_or_name`是可从互联网访问的连接网关的地址。
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_ssl_port -sv 13000 -svt INT_T -ss "|ss_type = \"SS_SETTINGS\";"`

     `13000`是连接网关正在监听的 TCP 端口号。

4. 运行`klnagchk -restart -tl 4`命令，启动网络代理服务。

该设备将被移动到新的管理服务器并通过新的连接网关进行连接。

## 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“**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。

# 关于设备状态

Kaspersky Security Center Linux 为每个受管理设备都分配一个状态。具体状态取决于是否满足用户定义的条件。在某些情况下，为设备分配状态时，Kaspersky Security Center Linux 会考虑设备在网络中的可见性标志（请参见下表）。如果 Kaspersky Security Center Linux 在两小时内未在网络中找到设备，则该设备的可见性标志将设置为“*不可见*”。

状态如下：

- “*严重*”或“*严重/可见*”
- “*警告*”或“*警告/可见*”
- “*正常*”或“*正常/可见*”

下表列出了为设备分配“*严重*”或“*警告*”状态所必须满足的默认条件，以及所有可能值。

分配状态到设备的条件

| 条件 | 条件描述 | 可用值 |
| --- | --- | --- |
| 安全应用程序未安装 | 网络代理已安装到设备，但是安全应用程序未安装。 | • 开关按钮被开启。<br>• 开关按钮被关闭。 |
| 检测到太多病毒 | 一些病毒被病毒检测任务在设备上发现，例如，病毒扫描任务，且发现的病毒数量超过指定值。 | 超过 0。 |
| 实时保护级别与管理员设置的级别不同 | 设备在网络中可见，但实时保护级别与管理员在设备状态条件中设置的级别不同。 | • 已停止。<br>• 已暂停。<br>• 正在运行。 |
| 病毒扫描已长时间 | 设备在网络中可见且安全应用程序已安装到设备，但不论*恶意软件扫描*任务还是本地扫描任务都没有在指 | 超过 1 |

| | | |
|---|---|---|
| 未执行 | 定时间内未运行。条件仅应用到于 7 天之前或更早添加到管理服务器数据库的设备。 | 天。 |
| 数据库已过期 | 设备在网络中可见且安全应用程序已安装到设备，但反病毒数据库在指定时间内未在该设备上更新。条件仅应用到于 1 天之前或更早添加到管理服务器数据库的设备。 | 超过 1 天。 |
| 长时间没有连接 | 网络代理已安装到设备，但由于设备关闭，设备在指定时间段内未连接到管理服务器。 | 超过 1 天。 |
| 检测到活动威胁 | "**活动威胁**"文件夹中的未处理的对象的数量超过指定的值。 | 超过 0 项。 |
| 需要重新启动 | 设备在网络中可见，但应用程序基于所选原因之一在指定时间之前请求设备重启。 | 超过 0 分钟。 |
| 安装了不兼容的应用程序 | 设备在网络中可见，但通过网络代理执行的软件清查在设备上检测到了不兼容的应用程序。 | • 开关按钮被关闭。<br>• 开关按钮被开启。 |
| 授权许可已过期 | 设备在网络中可见，但授权许可已过期。 | • 开关按钮被关闭。<br>• 开关按钮被开启。 |
| 授权许可即将过期 | 设备在网络中可见，但设备上的授权许可即将在指定天数内过期。 | 超过 0 天。 |
| 检测到未处理的事故 | 设备上发现了一些未处理的事故。事件可以通过安装在客户端设备上的受管 Kaspersky 应用程序自动创建，也可以由管理员手动创建。 | • 开关按钮被关闭。<br>• 开关按钮被开启。 |
| 应用程序定义的设备状态 | 设备状态由受管理应用程序定义。 | • 开关按钮被关闭。<br>• 开关按钮被开启。 |
| 设备磁盘空间不足 | 设备剩余磁盘空间少于指定值或设备无法与管理服务器同步。当设备已与管理服务器成功同步且设备上的剩余空间大于或等于指定值时，*严重*或*警告*状态被更改为*正常*状态。 | 大于 0 MB |
| 设备已失去管理 | 在设备发现过程中，设备在网络中可见，但是超过三次尝试与管理服务器同步都失败了。 | • 开关按钮被关闭。<br>• 开关按钮被开启。 |
| 保护已禁用 | 设备在网络中可见，但设备上的安全应用程序已被禁用长于指定的时间段。 | 超过 0 分钟。 |

| | | |
|---|---|---|
| | 在这种情况下，安全应用程序的状态为*stopped*或*failure*，不同于以下状态：*starting*、*running*或*suspended*。 | |
| 安全应用程序没有运行 | 设备在网络中可见且安全应用程序已安装到设备，但其未在运行。 | • 开关按钮被关闭。<br>• 开关按钮被开启。 |

Kaspersky Security Center Linux 允许您设置管理组中设备状态在指定条件满足时的自动切换。当指定条件满足时，客户端设备被分配以下状态之一：*严重*或*警告*。未满足指定条件时，客户端设备被分配“*正常*”状态。

一个条件的不同值可对应于不同的状态。例如，默认情况下，如果“**数据库已过期**”条件的值为“**超过 3 天**”，将为客户端设备分配“*警告*”状态；如果值为“**超过 7 天**”，则将分配“*严重*”状态。

如果从以前的版本升级 Kaspersky Security Center Linux，则分配状态到“*严重*”或“*警告*”的“**数据库已过期**”条件的值不变。

当 Kaspersky Security Center Linux 为设备分配状态时，对于某些条件（请参见“条件描述”列），将考虑可见性标志。例如，如果某个受管理设备由于满足“数据库已过期”条件而被分配“*严重*”状态，稍后为设备设置了可见性标志，则该设备被分配“*正常*”状态。

# 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“**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“**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。

# 策略和策略配置文件

在 Kaspersky Security Center 14 Web Console，您可以为 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：

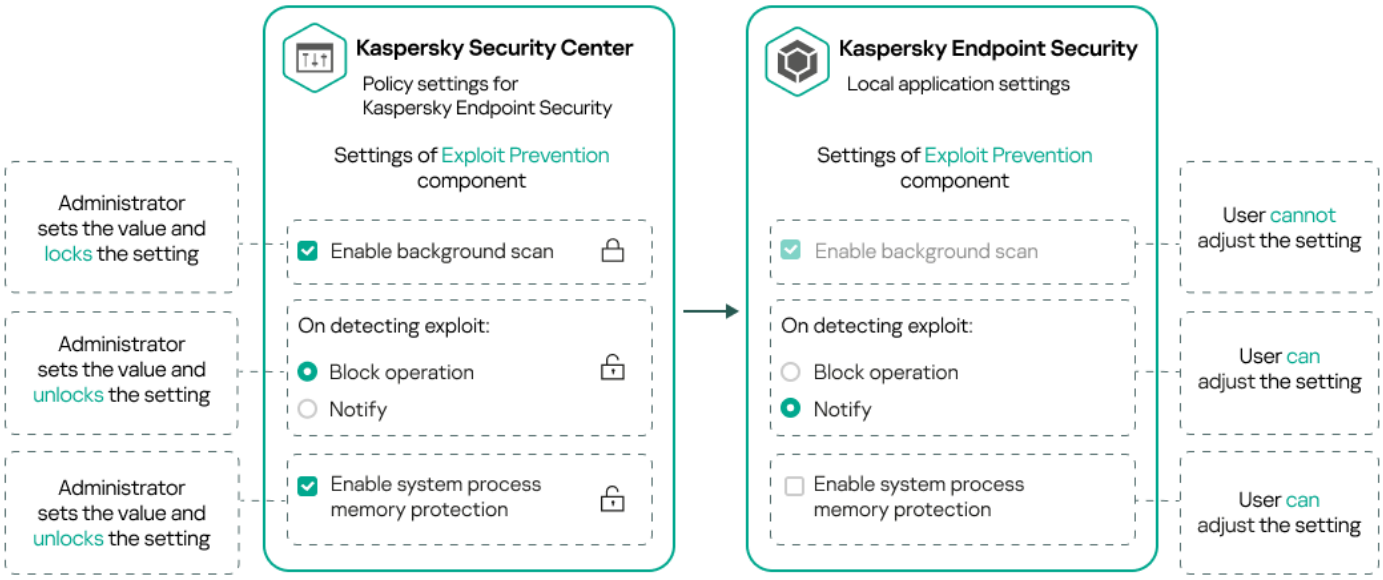
- 锁定管理子组策略的设置
- 在受管理设备上锁定本地 Kaspersky 应用程序的设置

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

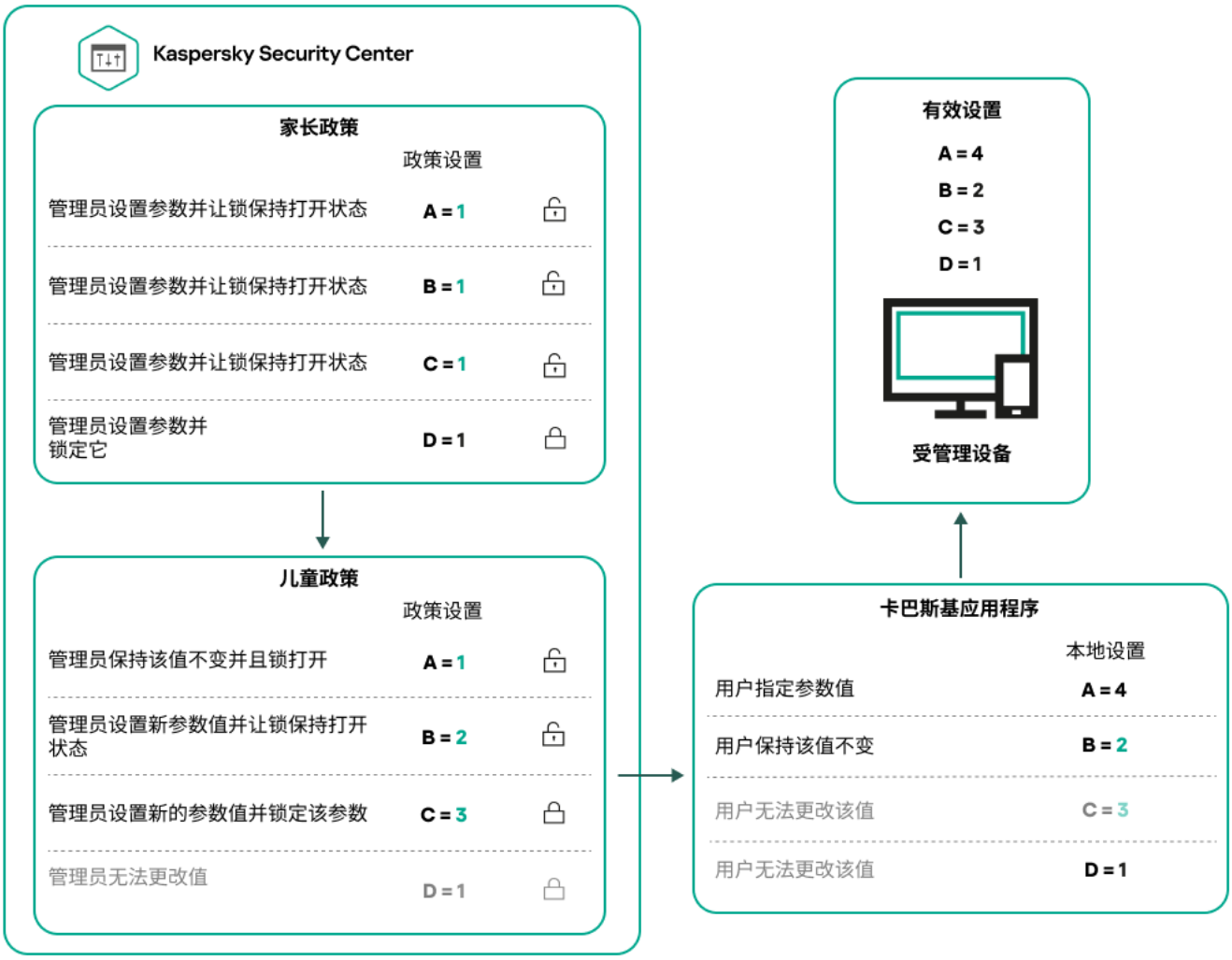
如果不同的设备需要不同的设置，则可以将设备组织到管理组中。

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）。

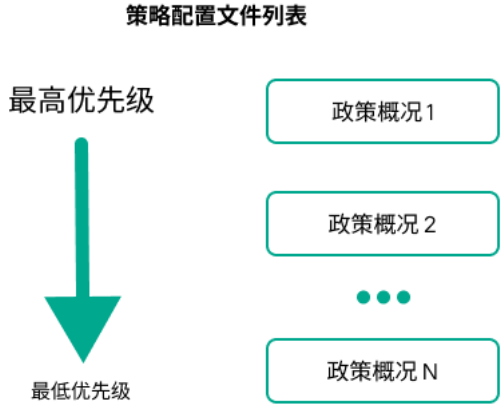



策略层级

# 策略层级中的策略配置文件

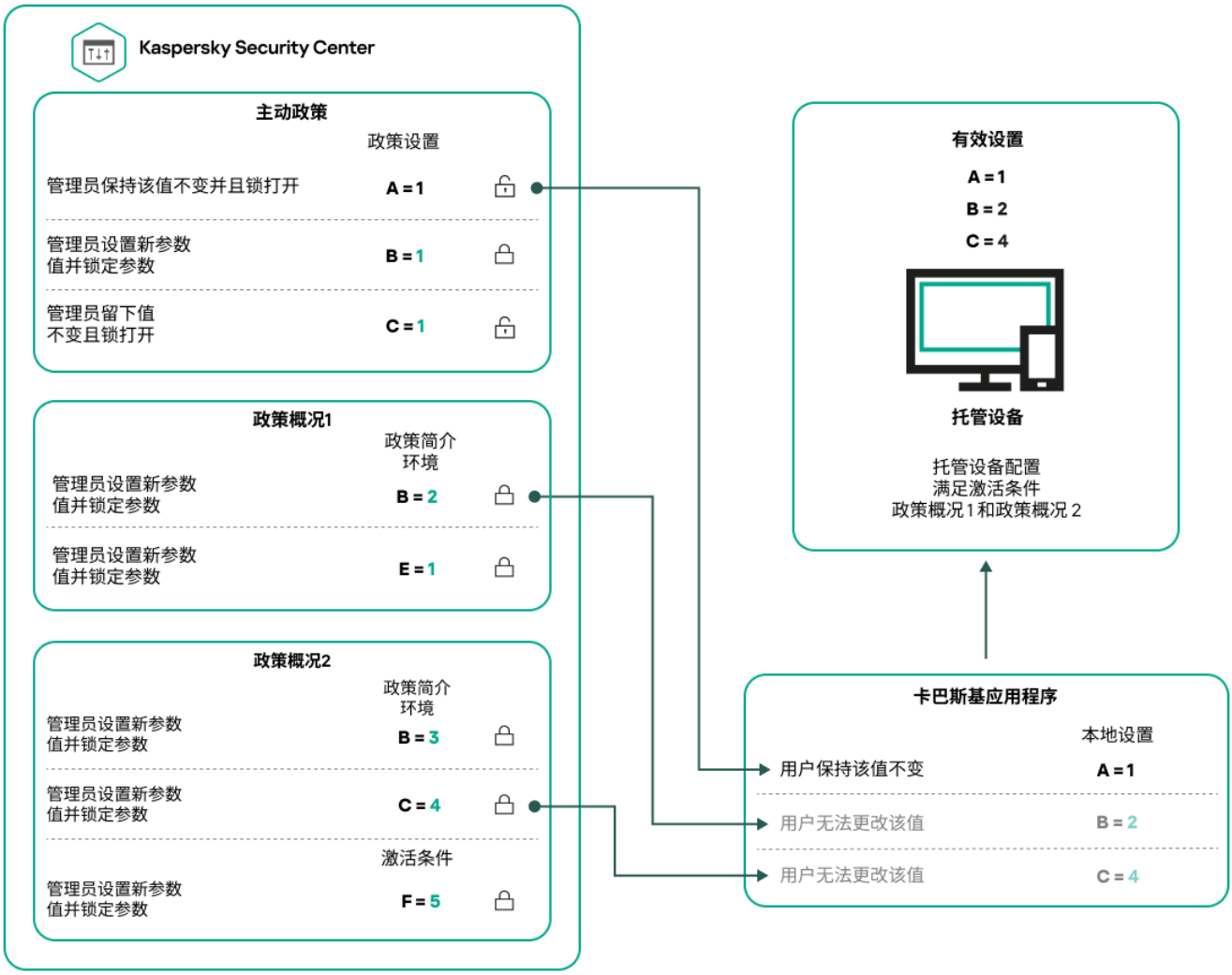
策略配置文件具有以下优先级分配条件：

- 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）。

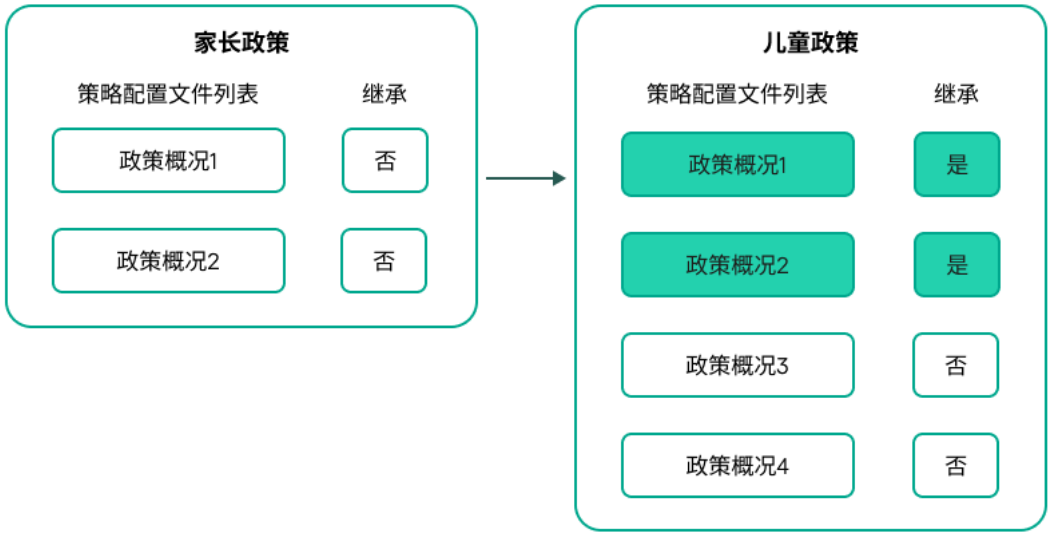



受管理设备配置满足多个策略配置文件的激活条件

## 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）。

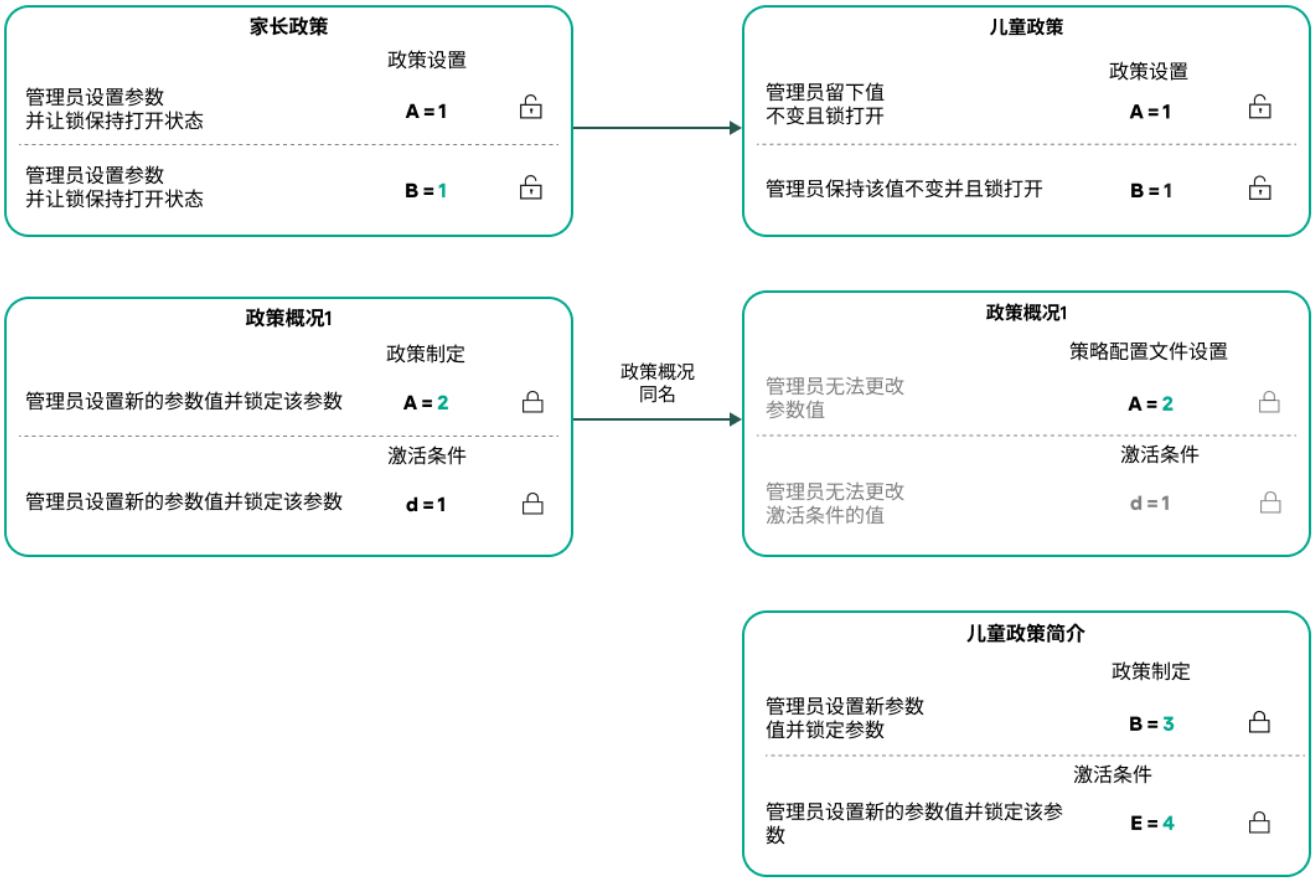



继承策略配置文件

## 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。

# 如何在受管理设备上实施设置

在受管理设备上有效设置的实现可以描述如下：

- 所有未锁定的设置的值均取自策略。
- 然后，它们将被受管理应用程序设置的值覆盖。
- 然后，将应用有效策略中的锁定设置值。锁定的设置值会更改解锁的有效设置的值。

# 管理策略

本节介绍管理策略并提供有关查看策略列表、创建策略、修改策略、复制策略、移动策略、强制同步、查看策略分发状态图以及删除策略的信息。

# 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“**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. 转到“**设备**”→“**策略和配置文件**”。
2. 选择要为其创建策略的管理组：
   - 对于根组。
     在这种情况下，您可以继续下一步。
   - 对于子组：
     a. 单击窗口顶部的当前路径链接。

b. 在打开的面板中，单击带有所需子组名称的链接。

当前路径会发生变化以反映所选的子组。

3. 单击**添加**。

“**选择应用程序**”窗口将打开。

4. 选择您要为其创建策略的应用程序。

5. 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。

6. 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。

7. 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。

8. 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

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。

9. 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. 转到**"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

   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。

## 启用和禁用策略继承选项

*要在策略中启用或禁用继承选项：*

1. 打开所需策略。
2. 打开**"常规"**选项卡。
3. 启用或禁用策略继承：

- 如果您在子策略中启用“从父策略继承设置”，并且管理员在父策略中锁定了一些设置，那么您无法在子组策略中更改这些设置。
- 如果您在子策略中禁用“从父策略继承设置”，那么您可以在子策略中更改所有设置，即便一些设置在父策略中是锁定的。
- 如果在父组中启用“在子策略中强制继承设置”，这将为每个子策略启用“从父策略继承设置”选项。此种情况下，您无法为任何子策略禁用该选项。所有在父策略中被锁定的设置被强制继承到子组，且您无法在子组中更改这些设置。

4. 单击“保存”按钮保存更改，或单击“取消”按钮拒绝更改。

默认情况下，为新策略启用“从父策略继承设置”选项。

如果一个策略具有配置文件，所有子策略都继承这些配置文件。

## 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“ 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“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）。

# 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. 转到“**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**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. 转到**"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。

## 查看策略分发状态图

在 Kaspersky Security Center 中，您可以在策略分发状态图中查看每个设备上的策略应用程序状态。

*要查看每个设备上的策略分发状态：*

1. 转到**"设备"→"策略和配置文件"**。
2. 选中要针对其查看设备上的分发状态的策略名称旁边的复选框。
3. 在出现的菜单中，选择**"分发"**链接。
   将打开**"<策略名称> 分发结果"**窗口。
4. 在打开的**"<策略名称> 分发结果"**窗口中，将显示策略的**状态描述**。

您可以更改列表中显示的策略分发结果数量。最大设备数量为 100,000。

*要更改带有策略分发结果的列表中显示的设备数量：*

1. 转到工具栏中的**"界面选项"**区域。
2. 在**策略分发结果中显示的设备数量限制**中，输入设备数量（最多 100,000）。
   默认情况下，该数字为 5000。
3. 点击**"保存"**。

设置已保存并应用。

## 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“**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。

## 管理策略配置文件

本节介绍管理策略配置文件并提供有关查看策略配置文件、更改策略配置文件优先级、创建策略配置文件、复制策略配置文件、创建策略配置文件激活规则以及删除策略配置文件的信息。

## 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“**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。

# 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的安全组集。

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。

# 配置对应用程序功能的访问权限。基于角色的访问控制

Kaspersky Security Center Linux 针对 Kaspersky Security Center Linux 和受管理 Kaspersky 应用程序的功能提供了基于角色的访问手段。

您可以通过以下方式之一为 Kaspersky Security Center Linux 用户配置对应用程序功能的访问权限：

- 通过为每个用户或用户组单独配置权限。
- 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。

应用用户角色旨在简化和缩短配置用户对应用程序功能的访问权限的常规程序。角色内的访问权限根据标准任务和用户的职责范围进行配置。

可为用户角色分配与其各自的目的对应的名称。您可在程序中创建无限数量的角色。

您可以将预定义的用户角色与已经配置的权限集一起使用，或者创建新角色并自行配置所需的权限。

## 应用程序功能的访问权限

下表显示了 Kaspersky Security Center Linux 的功能，以及用于管理关联任务、报告、设置和执行关联用户操作的访问权限。

要执行表中列出的用户操作，用户必须拥有该操作旁边指定的权限。

**读取**、**修改**和**执行**权限适用于任何任务、报告或设置。除这些权限外，要针对设备分类管理任务、报告或设置，用户还需要拥有“**对设备分类执行操作**”权限。

表中缺少的所有任务、报告、设置和安装包均属于“**常规功能：基本功能**”功能区域。

应用程序功能的访问权限

| 功能区域 | 权限 | 用户操作：执行操作所需的权限 | 任务 | 报告 | 其他 |
| --- | --- | --- | --- | --- | --- |
| 常规功能：管理组的管理 | 修改 | • 将设备添加到管理组：**修改**<br>• 从管理组中删除设备：**修改**<br>• 将管理组添加到另一个管理组：**修改**<br>• 将管理组从另一个管理组中删除：**修改** | 无 | 无 | 无 |
| 常规功能：访问对象而不考虑它们的 ACL | 读取 | 获取对所有对象的读取权限：**读取** | 无 | 无 | 无 |
| 常规功能：基本功能 | • 读取<br>• 修改<br>• 执行<br>• 对设备分类执行操作 | • 虚拟服务器的设备移动规则（创建、修改或删除）：**修改**、**对设备分类执行操作**<br>• 获取移动 (LWNGT) 协议自定义证书：**读取**<br>• 设置移动 (LWNGT) 协议自定义证书：**写入**<br>• 获取 NLA 定义的网络列表：**读取**<br>• 添加、修改或删除 NLA 定义的网络列表：**修改**<br>• 查看组的访问控制列表：**读取**<br>• 查看操作系统日志：**读取** | • “将更新下载至管理服务器存储库”<br>• “提交报告”<br>• “分发安装包”<br>• “在从属管理服务器上远程安装应用程序” | • “保护状态报告”<br>• “威胁报告”<br>• “感染最严重的设备报告”<br>• “反病毒数据库状态报告”<br>• “错误报告”<br>• “网络攻击报告”<br>• “已安装的周边防护应用程序汇总报告”<br>• “已安装的应用程序类型汇总 | 无 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | 报告”<br>• “受感染的设备用户报告”<br>• “事故报告”<br>• “事件报告”<br>• “分发点活动报告”<br>• “从属管理服务器报告”<br>• “设备控制事件报告”<br>• “禁止的应用程序报告”<br>• “Web 控制报告”<br>• “有效用户权限报告”<br>• “权限报告” | |
| 常规功能：已删除对象 | • 读取<br>• 修改 | • 查看回收站中的已删除对象：**读取**<br>• 删除回收站中的对象：**修改** | 无 | 无 | 无 |
| 常规功能：事件处理 | • **删除事件**<br>• **编辑事件通知设置**<br>• **编辑事件记录设置**<br>• 修改 | • 更改事件注册设置：**编辑事件记录设置**<br>• 更改事件通知设置：**编辑事件通知设置**<br>• 删除事件：**删除事件** | 无 | 无 | 设置：<br>• 数据库中存储的最大事件数量<br>• 已删除设备中事件的存储时间段 |
| 常规功能：对管理服务器的操作 | • 读取<br>• 修改<br>• **执行**<br>• **修改对象 ACL**<br>• **对设备分类执行操作** | • 指定用于连接网络代理的管理服务器端口：**修改**<br>• 指定在管理服务器上启动的激活代理端口：**修改**<br>• 指定在管理服务器上启动的移动激活代理端口：**修改**<br>• 指定用于分发独立安装包的 Web 服务器端口：**修改**<br>• 指定用于分发 MDM 配置文件的 Web 服务器端口：**修改**<br>• 指定用于通过 Web 控制台连接的管理服务器 SSL 端口：**修改**<br>• 指定用于移动连接的管理服务器端口：**修改**<br>• 指定管理服务器数据库中存储的最大事件数量：**修改**<br>• 指定管理服务器可以发送的最大事件数量：**修改** | • “备份管理服务器数据”<br>• “数据库维护” | 无 | 无 |

| | | | | | |
|---|---|---|---|---|---|
| | | • 指定管理服务器可以发送事件的时间段：**修改** | | | |
| 常规功能：**Kaspersky** 软件部署 | • 管理 **Kaspersky** 补丁<br>• 读取<br>• 修改<br>• 执行<br>• 对设备分类执行操作 | 批准或拒绝安装补丁：**管理 Kaspersky 补丁** | 无 | • “虚拟管理服务器授权许可密钥使用报告”<br>• “Kaspersky 软件版本报告”<br>• “不兼容的应用程序报告”<br>• “Kaspersky 软件模块更新版本报告”<br>• “保护部署报告” | 安装包：“Kaspersky” |
| 常规功能：密钥管理 | • 导出密钥文件<br>• 修改 | • 导出密钥文件：**导出密钥文件**<br>• 修改管理服务器授权许可密钥设置：**修改** | 无 | 无 | 无 |
| 常规功能：强制报告管理 | • 读取<br>• 修改 | • 创建报告而不考虑它们的 ACL：**写入**<br>• 执行报告而不考虑它们的 ACL：**读取** | 无 | 无 | 无 |
| 常规功能：管理服务器层级 | 配置管理服务器的层级 | • 注册、更新或删除从属管理服务器：**配置管理服务器层级** | 无 | 无 | 无 |
| 常规功能：用户权限 | 修改对象 **ACL** | • 更改任何对象的“安全”属性：**修改对象 ACL**<br>• 管理用户角色：**修改对象 ACL**<br>• 管理内部用户：**修改对象 ACL**<br>• 管理安全组：**修改对象 ACL**<br>• 管理别名：**修改对象 ACL** | 无 | 无 | 无 |
| 常规功能：虚拟管理服务器 | • 管理虚拟管理服务器<br>• 读取<br>• 修改<br>• 执行<br>• 对设备分类执行操作 | • 获取虚拟管理服务器列表：**读取**<br>• 获取关于虚拟管理服务器的信息：**读取**<br>• 创建、更新或删除虚拟管理服务器：**管理虚拟管理服务器**<br>• 将虚拟管理服务器移动到另一个组：**管理虚拟管理服务器**<br>• 设置管理虚拟服务器权限：**管理虚拟管理服务器** | 无 | 无 | 无 |

# 预定义用户角色

分配给 Kaspersky Security Center Linux 用户的用户角色为他们提供了对应用程序功能的访问权限集。

您可以将预定义的用户角色与已经配置的权限集一起使用，或者创建新角色并自行配置所需的权限。Kaspersky Security Center Linux 中可用的一些预定义用户角色可以与特定职位相关联，例如**审计员**、**安全官**、**主管**。这些角色的访问权限是根据标准任务和相关职位的职责范围预先配置的。下表显示了角色如何与特定职位相关联。

特定职位角色示例

| 角色 | 注释 |
| --- | --- |
| 审计员 | 允许所有报告类型操作、所有查看操作，包括查看已删除对象（授予在**"已删除对象"**区域的**读取**和**写入**权限）。不允许其他操作。您可以分配该角色到执行您组织的审计的人。 |
| 管理者 | 允许所有查看操作；不允许其他操作。您可以分配该角色到负责您组织的 IT 安全的安全官和其他管理员。 |
| 安全官 | 允许所有查看操作，允许报告管理；在**系统管理：连接**区域授予有限的权限。您可以分配该角色到负责您组织的 IT 安全的安全官。 |

下表显示了分配给每个预定义用户角色的访问权限。

功能区域**"移动设备管理：常规"**和**"系统管理"**的功能在 Kaspersky Security Center Linux 中不可用。具有**"'漏洞和补丁管理'管理员/操作员"**以及**"'移动设备管理'管理员/操作员"**角色的用户只拥有**"常规功能：基本"**功能区域中的权限。

预定义用户角色的访问权限

| 角色 | 描述 |
| --- | --- |
| 管理服务器管理员 | 在**"常规功能"**中，允许以下功能区域中的所有操作：<br>• 基本功能<br>• 事件处理<br>• 管理服务器层级<br>• 虚拟管理服务器 |
| 管理服务器操作员 | 在**"常规功能"**中授予以下所有功能区域的**读取**和**执行**权限：<br>• 基本功能<br>• 虚拟管理服务器 |
| 审计员 | 在**"常规功能"**中，允许以下功能区域中的所有操作：<br>• 访问对象而不考虑它们的 ACL<br>• 删除对象<br>• 强制报告管理<br>您可以分配该角色到执行您组织的审计的人。 |
| 安装管理员 | 在**"常规功能"**中，允许以下功能区域中的所有操作：<br>• 基本功能<br>• Kaspersky 软件部署<br>• 授权许可密钥管理<br>授予在**"常规功能：虚拟管理服务器"**功能区域的**读取**和**执行**权限。 |
| 安装操作员 | 在**"常规功能"**中授予以下所有功能区域的**读取**和**执行**权限：<br>• 基本功能<br>• Kaspersky 软件部署（也授予在该区域的**管理 Kaspersky Lab 补丁**权限）<br>• 虚拟管理服务器 |
| Kaspersky Endpoint Security 管理员 | 允许在以下功能区域的所有操作：<br>• 常规功能：基本功能 |

| | |
|---|---|
| | • Kaspersky Endpoint Security 区域，包括所有功能 |
| Kaspersky Endpoint Security 操作员 | 授予在以下所有功能区域的**读取**和**执行**权限：<br>• **常规功能：基本功能**<br>• Kaspersky Endpoint Security 区域，包括所有功能 |
| 主管理员 | 在“**常规功能**”中，*除*以下区域外，允许功能区域内的所有操作：<br>• **访问对象而不考虑它们的 ACL**<br>• **强制报告管理** |
| 主要操作员 | 授予在以下所有功能区域的**读取**和**执行**（如果适用）权限：<br>• **常规功能：**<br>• **基本功能**<br>• **删除对象**<br>• **管理服务器上的操作**<br>• **Kaspersky Lab 软件部署**<br>• **虚拟管理服务器**<br>• Kaspersky Endpoint Security 区域，包括所有功能 |
| “移动设备管理”管理员 | 允许“**常规功能：基本功能**”功能区域中的所有操作。 |
| 安全官 | 在“**常规功能**”中，允许以下功能区域中的所有操作：<br>• **访问对象而不考虑它们的 ACL**<br>• **强制报告管理**<br>授予在“**系统管理：连接**”功能区域的“**读取**”、“**修改**”、“**执行**”、“**将设备中的文件保存到管理员工作站**”和“**对设备分类执行操作**”权限。<br>您可以分配该角色到负责您组织的 IT 安全的安全官。 |
| Self Service Portal 用户 | 允许在“**移动设备管理：Self Service Portal**”功能区域的所有操作。Kaspersky Security Center 11 和更高版本不支持此功能。 |
| 管理者 | 授予在“**常规功能：访问对象而不考虑它们的 ACL**”和“**常规功能：强制报表管理**”功能区域的**读取**权限。<br>您可以分配该角色到负责您组织的 IT 安全的安全官和其他管理员。 |

# 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**，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，转到“**用户和角色**” → “**用户**”。
2. 单击**添加**。
3. 在打开的“**新实体**”窗口中，选择“**组**”。
4. 为新安全组指定以下设置：
   - **组名称**
   - **描述**
5. 单击“**正常**”保存更改。

新安全组出现在用户和安全组列表。

# 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**，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

您仅可以编辑内部组。

*要编辑安全组：*

1. 在主菜单中，转到“**用户和角色**” → “**用户**”。
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：
   - **名称**
   - **描述**
4. 单击“**保存**”保存设置。

更新的安全组出现在用户和安全组列表。

## 添加用户账户到内部组

您仅可以添加内部用户账户到内部组。

*要添加用户账户到内部组：*

1. 在主菜单中，转到“**用户和角色**” → “**用户**”。
2. 选择您要添加到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组。
5. 单击“**分配**”按钮。

用户账户被添加到组。

## 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. 在主菜单中，转到“**用户和角色**” → “**用户**”。
2. 点击您要分配为设备所有者的用户账户名称。
3. 在打开的用户设置窗口中，选择“**设备**”选项卡。
4. 单击**添加**。
5. 从设备列表中，选择您要分配给用户的设备。
6. 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“**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。

## 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，转到“**用户和角色**” → “**用户**”。
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，转到“**用户和角色**” → “**用户**”。
2. 选择您要添加到用户角色范围的用户和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**”按钮继续向导。
4. 在“**选择角色**”步骤中，选择要分配的用户角色。

5. 在“**定义范围**”步骤中，选择要添加到用户角色范围的管理组。

6. 单击“**分配角色**”按钮关闭向导。

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**”按钮继续向导。

5. 在“**定义范围**”步骤中，选择要添加到用户角色范围的管理组。

6. 在“**选择用户**”步骤中，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**”按钮关闭向导。

8. 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。

*方法 3：*

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，选中要添加到用户角色范围的用户或安全组名称旁边的复选框，然后单击“**角色**”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，“**角色**”按钮将被禁用。

3. 在“**角色**”窗口中，选择要分配的用户角色，然后单击“**确定**”并保存更改。
所选用户或安全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对配置文件设置进行配置。
     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。

## 传输用户角色到从属管理服务器

默认情况下，主管理服务器和从属管理服务器的用户角色列表是独立的。您可以配置应用程序自动传输在主管理服务器上创建的用户角色到所有从属管理服务器。用户角色也可以从从属管理服务器传输到其自己的从属管理服务器。

*要从主管理服务器传输用户角色到从属管理服务器：*

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ()。

   管理服务器属性窗口打开，**常规**选项卡被选中。

2. 转到“**管理服务器层级**”区域。

3. 启用**转发角色列表到从属管理服务器**选项，然后单击**保存** 按钮。

   应用程序将主管理服务器的用户角色复制到从属管理服务器。

启用**转发角色列表到从属管理服务器**选项并传播用户角色后，不能在从属管理服务器上编辑或删除这些用户角色。当您创建新角色或在主管理服务器上编辑现有角色时，更改被自动复制到从属管理服务器。当您在主管理服务器上删除用户角色时，该角色在从属管理服务器上被保留，但无法被编辑或删除。

从主管理服务器传播到从属管理服务器的角色显示为绿色复选标记 ()。您无法在从属管理服务器上编辑这些角色。

如果您在主管理服务器上创建角色，且在从属管理服务器上有相同名称的角色，新角色被复制到从属管理服务器，其名称后被添加索引，例如，~~1、~~2（索引可以随机）。

如果禁用“**转发角色列表到从属管理服务器**”选项，所有用户角色在从属管理服务器上被保留，但是独立于主管理服务器上的角色。独立后，从属管理服务器上的用户角色可以被编辑或删除。

# 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：

- 管理服务器属性
- 策略
- 任务
- 管理组
- 用户账户
- 安装包

您可以查看修订列表并将对对象所做的更改回滚至选定的修订。

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：

- **修订** — 对象修订版本号。
- **时间** — 对象修改的日期和时间。
- **用户** — 修改对象的用户的名称。
- **操作** — 运行在对象上的操作。

- **描述** – 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“**编辑描述**”按钮。在打开的窗口中，输入一些修订描述的文本。

## 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 14 Linux 会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。

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 14 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。

# 使用 klscflag 实用程序开放端口 13291

您可以使用 klbackup 自动化 Kaspersky Security Center 的操作。klakaut 实用程序及其帮助系统位于 Kaspersky Security Center 的安装文件夹中。如果要使用 klakaut 实用程序，请使用 klscflag 实用程序打开 13291 端口。

klscflag 实用程序会更改 KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN 参数的值。

*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。

# 使用 klscflag 实用程序打开 OpenAPI 端口

OpenAPI 端口被 Kaspersky Security Center 14 Web Console 用以连接到管理服务器。OpenAPI 端口的默认值为 13299。

*要打开 OpenAPI 端口：*

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_OPEN_OAPI_PORT -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
```

OpenAPI 端口已打开。

*要检查 OpenAPI 端口是否开启成功，请在命令行中执行如下命令：*

```
$ /opt/kaspersky/ksc64/sbin/klscflag -ssvget -pv klserver -s 87 -n
KLSRV_SP_OPEN_OAPI_PORT -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
```

此命令会返回以下结果：

```
+--- (PARAMS_T)
+---KLSRV_SP_OPEN_OAPI_PORT = (BOOL_T)true
```

`true` 值表示端口已开放。否则，将显示 `false` 值。

# 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 组件和安全应用程序

在美国境内，本软件中将不再提供更新功能（包括提供反病毒签名更新和代码库更新）以及 KSN 功能。

# 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 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 14 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**

   您可以使用若干个 scheme 以安装更新到 Kaspersky Security Center 组件和安全应用程序。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 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 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 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。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 组件和安全应用程序

  Kaspersky Security Center 无法自动更新 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：

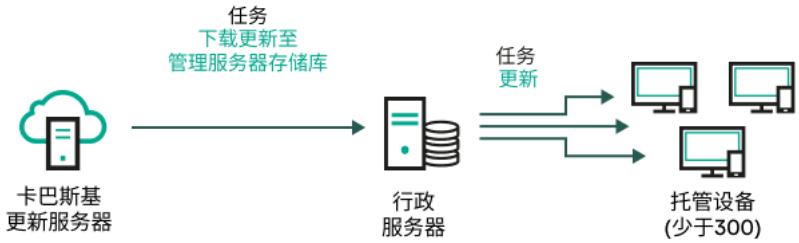
  - Kaspersky Security Center 管理服务器，Kaspersky Security Center 14 Web Console
  - 网络代理、Kaspersky Endpoint Security for Linux、管理 Web 插件

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 Kaspersky 更新服务器到受管理设备上的 Kaspersky Endpoint Security for Linux
- 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 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）。



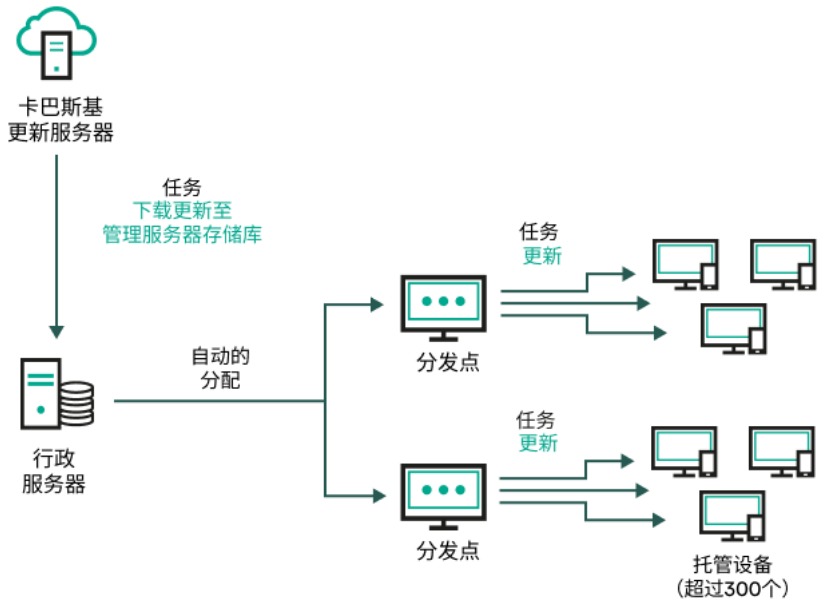

通过使用"将更新下载至管理服务器存储库"任务更新，而不使用分发点

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 for Linux 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 for Linux 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。

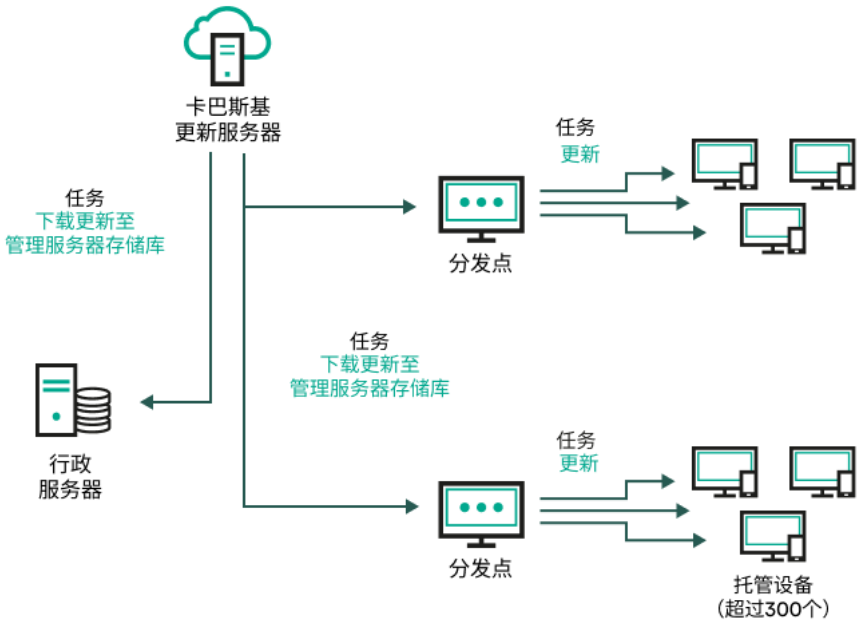
每个 Kaspersky 应用程序都从管理服务器请求所需更新。管理服务器集合这些更新并仅下载应用程序请求的更新。这确保了相同更新不被下载多次，且不必要更新不被下载。当运行"*将更新下载至管理服务器存储库*"任务时，管理服务器自动发送以下信息到 Kaspersky 更新服务器以便确保相关版本的 Kaspersky 数据库和软件模块的下载：

- 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

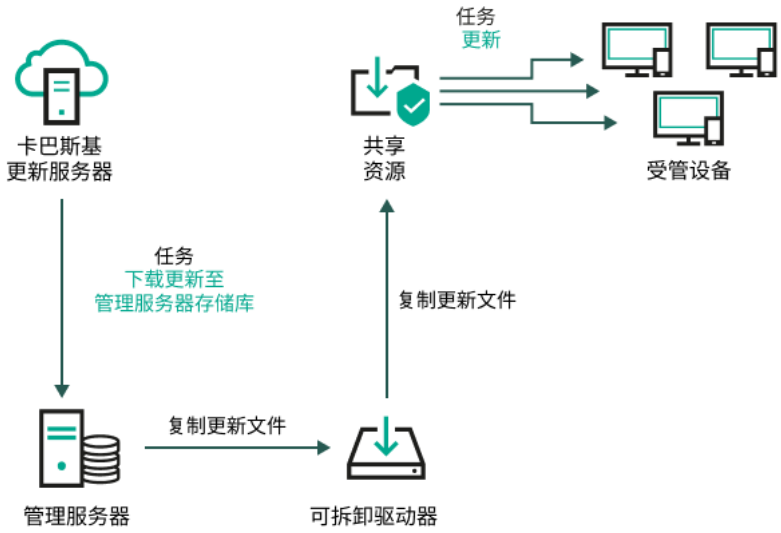
默认下，管理服务器和分发点与 Kaspersky 更新服务器通信并使用 HTTPS 协议下载更新。您可以配置管理服务器和/或分发点使用 HTTP 协议，而不是 HTTPS。

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 软件模块。

## 通过本地文件夹、共享文件夹或 FTP 服务器手动

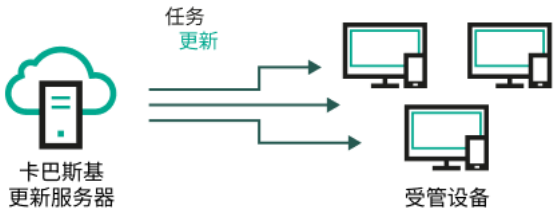
如果客户端设备未连接到管理服务器，您可以使用本地文件夹或共享资源作为 Kaspersky 数据库、软件模块和应用程序的更新源。在此方案中，您需要从管理服务器存储库复制所需更新到可移动驱动器，然后复制更新到 Kaspersky Endpoint Security for Linux 设置中指定的本地文件夹或共享文件夹（参见下图）。




通过本地文件夹、共享文件夹或 FTP 服务器更新

## 直接从 Kaspersky 更新服务器到受管理设备上的 Kaspersky Endpoint Security for Linux

在受管理设备上，您可以配置 Kaspersky Endpoint Security for Linux 直接从 Kaspersky 更新服务器接收更新（参加下图）。




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 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。对于这些设置的完整描述，请参考 Kaspersky Endpoint Security for Linux 文档。

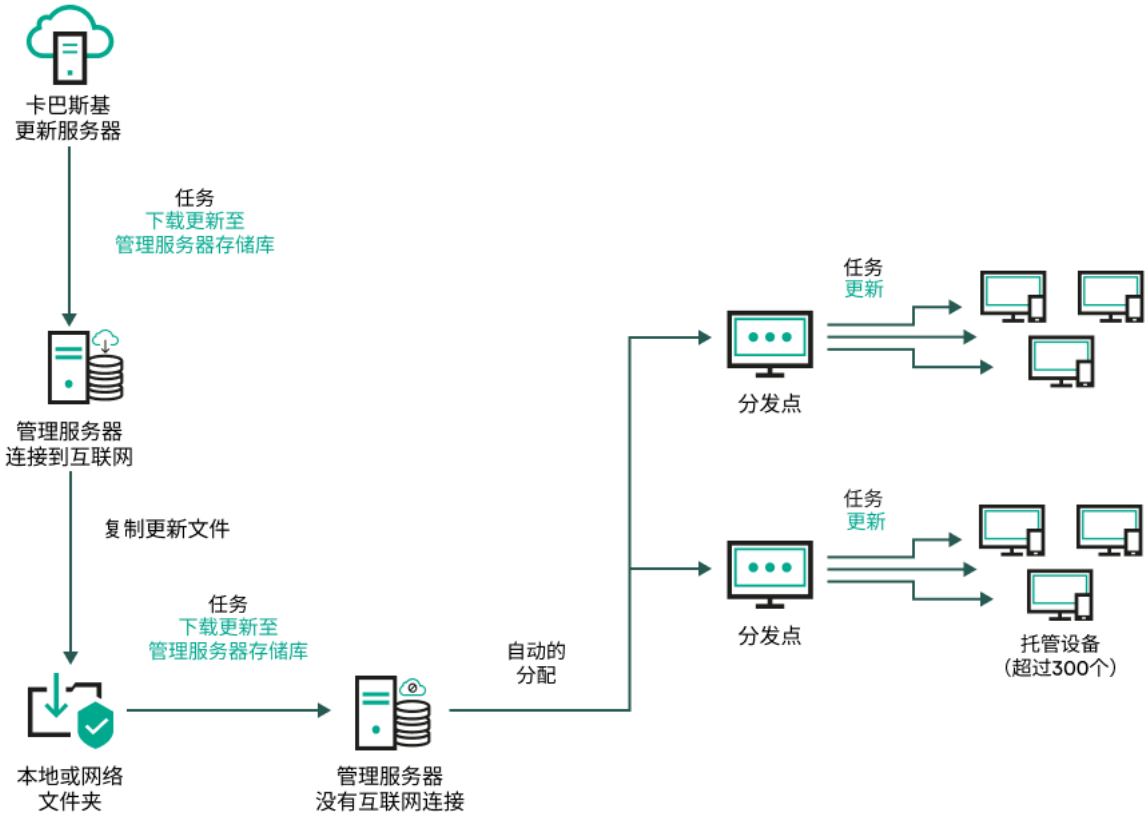
## 如果管理服务器没有互联网连接，则通过本地或网络文件夹

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. 转到"**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。

   任务被创建并显示在任务列表。

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 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。

   - 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 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：

  选择任务运行计划并配置所选计划。

  - 手动（默认选择）

    任务不自动运行。您仅可以手动启动。

    默认情况下已选定该选项。

  - 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 6 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，任务每星期五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

  任务在每周指定日期的指定时间定期运行。

  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，不选择任何月份中的日期。默认开始时间为 18:00。

- 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。

如果禁用此选项，则只有计划任务会在客户端设备上运行。对于“**手动**”、“**一次**”和“**立即**”计划，仅在网络上可见的客户端设备上运行任务。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。

默认情况下已禁用该选项。

- 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。

- 如果任务运行长于此时间则停止任务(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。

## 浏览已下载的更新

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。您可以在“**卡巴斯基数据库和软件模块更新**”区域中查看下载的更新。

*要查看已下载的更新，*

在主菜单中，转到“**操作**”→“**卡巴斯基应用程序**”→“**卡巴斯基数据库和软件模块更新**”。

可用更新列表被显示。

## 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）创建更新和病毒扫描任务。创建更新和病毒扫描任务时，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病毒扫描任务，以检查所有更新是否有效。此外，在创建“*更新验证*”任务时，您需要指定更新和病毒扫描任务。

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“**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. 如果要更改预设任务名称，则在打开的“添加任务向导”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 支持的所需应用程序的更新任务，然后选择病毒扫描任务。
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。

# 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。

## 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。

如果您使用基于 Linux 的设备作为分发点，我们强烈建议增加 klnagent 服务的文件描述符限制，因为如果分发点的范围包括许多设备，则默认的最大可打开文件数可能不够。

## 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。

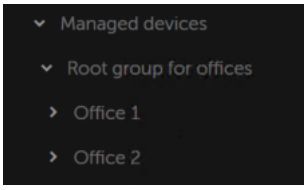
有以下构建管理组结构的方法：

- 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。

- 远程设备的网关地址

  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 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。“添加任务向导”启动。遵照向导的说明。

- 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“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 14 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。

  当通过充当连接网关的分发点将移动设备连接到管理服务器时，您可以启用以下选项：

  - 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。移动设备将检查管理服务器证书。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。移动设备将检查管理服务器证书，管理服务器也将检查移动设备证书。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。

  在这两种情况下，仅在分发点上建立 TLS 会话期间检查证书。证书不会被转发供管理服务器检查。与移动设备建立 TLS 会话后，分发点使用管理服务器证书创建移动设备和管理服务器之间的同步隧道。如果打开双向 SSL 身份认证的端口，则分发移动设备证书的唯一方式是通过安装包。

- 按分发点配置 IP 范围轮询。
  - IP 范围

    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 Zerocong 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 “**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“**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。

# 启用推送服务器

在 Kaspersky Security Center 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。

您可能希望将分发点用作推送服务器，以确保受管理设备和管理服务器之间存在持续连接。某些操作需要持续连接，例如运行和停止本地任务、接收受管理应用程序的统计信息或创建隧道。如果将分发点用作推送服务器，则不必在受管理设备上使用“不要断开与管理服务器的连接”选项或将数据包发送到网络代理的 UDP 端口。

推送服务器支持最多 50,000 个同时连接的负载。

*要在分发点上启用推送服务器：*

1. 单击所需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. 单击要在其上启用推送服务器的分发点的名称。

   分发点属性窗口将打开。

4. 在“**常规**”区域中，启用“**运行推送服务器**”选项。

5. 在“**推送服务器端口**”字段中，键入端口号。您可以指定任何未占用的端口号。

6. 在“**远程主机地址**”字段中，指定分发点设备的 IP 地址或名称。

7. 单击“**确定**”按钮。

在所选分发点上已启用推送服务器。

# 增加 klnagent 服务的文件描述符限制

如果基于 Linux 的分发点的范围包括许多设备，则可打开的文件（文件描述符）的默认限制可能不够。为了避免这种情况，您可以增加 klnagent 服务的文件描述符的限制。

*要增加 klnagent 服务的文件描述符限制：*

1. 在作为分发点的 Linux 设备上，打开 `/lib/systemd/system/klnagent64.service` 文件，然后在 `[Service]` 部分的 `LimitNOFILE` 参数中指定文件描述符的硬限制和软限制：

   `LimitNOFILE=<soft_resource_limit>:<hard_resource_limit>`

   例如， `LimitNOFILE=32768:131072`。请注意，文件描述符的软限制必须小于或等于硬限制。

2. 运行以下命令以确保参数指定正确：

   ```
   systemd-analyze verify klnagent64.service
   ```

   如果参数指定不正确，此命令可能会输出以下错误之一：

- `/lib/systemd/system/klnagent64.service:11: Failed to parse resource value, ignoring: 32768:13107`

  如果出现此错误，则`LimitNOFILE`行中的符号指定不正确。您必须检查并更正输入的行。

- `/lib/systemd/system/klnagent64.service:11: Soft resource limit chosen higher than hard limit, ignoring: 32768:13107`

  如果出现此错误，则表示您输入的文件描述符的软限制超过了硬限制。您必须检查输入的行并确保文件描述符的软限制小于或等于硬限制。

3. 运行以下命令重新加载 systemd 进程：

   ```
   systemctl daemon-reload
   ```

4. 运行以下命令重新启动网络代理服务：

   ```
   systemctl restart klnagent
   ```

5. 运行以下命令以确保正确应用指定的参数：

   ```
   less /proc/<nagent_proc_id>/limits
   ```

   其中`<nagent_proc_id>`参数是网络代理进程的标识符。您可以运行以下命令来获取标识符：

   ```
   ps -ax | grep klnagent
   ```

对于基于 Linux 的分发点，可以打开的文件的限制增加了。

# 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“**设备**”→“**任务**”。
2. 单击“**添加**”按钮。

   “添加任务向导”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。网络文件夹可以是 FTP 或 HTTP 服务器，或者 SMB 共享。如果网络文件夹需要身份验证，则仅支持 SMB 协议。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。

    更新源所使用的 FTP 或 HTTP 服务器或网络文件夹必须包含匹配 Kaspersky 更新服务器所创建的结构的文件夹结构（带有更新）。

    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 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 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

  选择任务运行计划并配置所选计划。

  - 手动（默认选择）

    任务不自动运行。您仅可以手动启动。

    默认情况下已选定该选项。

  - 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 6 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，任务每星期五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

  任务在每周指定日期的指定时间定期运行。

  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，不选择任何月份中的日期。默认开始时间为 18:00。

- 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安全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。

如果禁用此选项，则只有计划任务会在客户端设备上运行。对于“**手动**”、“**一次**”和“**立即**”计划，仅在网络上可见的客户端设备上运行任务。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。

默认情况下已禁用该选项。

- 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。

# 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. 在主应用程序窗口，点击所需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。“添加任务向导”启动。遵照向导的说明。

- 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。

## 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 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。

*要添加更新源：*

1. 转到"**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。

# 启用下载 diff 文件功能

## 阶段

1. **在管理服务器上启用该功能**

在*"将更新下载至管理服务器存储库"任务的设置*中启用该功能。

2. **为分发点启用该功能**

   对通过"*将更新下载至分发点存储库*"任务接收更新的分发点启用该功能。

   然后在网络代理策略设置中对从管理服务器接收更新的分发点启用该功能。

   然后对从管理服务器接收更新的分发点启用该功能。

   在"网络代理策略设置"中启用了此功能，并且在管理服务器属性的"分发点"区域中也已启用（如果手动分配了分发点，并且您想覆盖策略设置）。

要检查下载 diff 文件功能是否被成功启用，您可以在执行方案之前和之后分别测试内部流量。

# 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 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 for Linux 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。

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，开始 Kaspersky Endpoint Security for Linux 的更新任务。

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 14 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。

# 管理客户端设备上的第三方应用程序和可执行文件

本节介绍与管理客户端设备上运行的第三方应用程序和可执行文件有关的 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。

应用程序控制组件适用于 Kaspersky Endpoint Security 11.2 for Linux 及更高版本。

### 先决条件

- Kaspersky Security Center Linux已部署在您的组织中。
- Kaspersky Endpoint Security for Linux 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

2. **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可执行文件列表。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。

   使用说明：创建含有手动添加内容的应用程序类别

3. **在 Kaspersky Endpoint Security for Linux 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。

4. **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”。

### 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。

## 关于应用程序控制

"应用程序控制"组件监控用户启动应用程序的尝试，并使用应用程序控制规则来管理应用程序启动。

应用程序控制组件适用于 Kaspersky Endpoint Security 11.2 for Linux 及更高版本。

其设置与任何应用程序控制规则都不匹配的应用程序的启动由该组件的选定操作模式管理：

- *拒绝列表*。如果要允许启动除了阻止规则中指定的应用程序外的所有应用程序，则使用该模式。默认情况下选择此模式。
- *允许列表*。如果要阻止启动除了允许规则中指定的应用程序外的所有应用程序，则使用该模式。

应用程序控制规则通过应用程序类别实现。您创建定义特定条件的应用程序类别。在 Kaspersky Security Center Linux 中，只能创建含有手动添加内容的类别。您定义将可执行文件包括在类别中的条件，例如元数据、文件哈希码、文件证书、KL 类别、文件路径。

有关应用程序控制的详细信息，请参阅 Kaspersky Endpoint Security for Linux 帮助。

## 获取并查看客户端设备上存储的可执行文件列表

您可以获取受管理设备上存储的可执行文件列表。要清查可执行文件，必须创建清查任务。

清查可执行文件的功能适用于 Kaspersky Endpoint Security 11.2 for Linux 及更高版本。

*要在客户端设备上为可执行文件创建清查任务：*

1. 转到"**设备**" → "**任务**"。
   将显示任务列表。
2. 单击"**添加**"按钮。
   新任务向导启动。遵照向导的说明。
3. 在"**新任务**"页面上的"**应用程序**"下拉列表中，选择 Kaspersky Endpoint Security for Linux。
4. 在"**任务类型**"下拉列表中，选择"**清单**"。
5. 在**完成任务创建**页面上，单击**完成**按钮。

   新任务向导完成后，将创建并配置"**清单**"任务。如果需要，可以更改已创建任务的设置。新创建的任务显示在任务列表中。

有关清查任务的详细说明，请参阅 Kaspersky Endpoint Security for Linux 在线帮助。

执行“清单”任务后，将形成受管理设备上存储的可执行文件列表，您可以查看该列表。

清查过程中，将检测以下格式的可执行文件：MZ、COM、PE、NE、SYS、CMD、BAT、PS1、JS、VBS、REG、MSI、CPL、DLL、JAR 和 HTML。

*要查看客户端设备上存储的可执行文件列表：*

在“操作” → “第三方应用程序”下拉列表中，选择“可执行文件”。

该页面显示客户端设备上存储的可执行文件列表。

# 创建含有手动添加内容的应用程序类别

您可以指定一组条件作为要在组织中允许或阻止启动的可执行文件的模板。在对应于条件的可执行文件的基础上，您可以创建一个应用程序类别，并在“应用程序控制”组件配置中使用该应用程序类别。

*要创建含有手动添加内容的应用程序类别：*

1. 在“操作”→“第三方应用程序”下拉列表中，选择“应用程序类别”。
   将显示含有应用程序类别列表的页面。
2. 单击“添加”按钮。
   新类别向导启动。使用“下一步”按钮继续向导操作。
3. 在“选择策略创建方法”步骤，选择“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”选项。
4. 在“条件”步骤中，单击“添加”按钮以添加在所创建类别中包含文件的条件标准。
5. 在“条件标准”步骤中，从列表中选择创建类别时所遵循的规则类型：

   - 从存储库选择证书

     如果选中此选项，则可以指定来自存储空间的证书。已按照指定的证书签名的可执行文件将被添加到用户类别。

   - 指定应用程序路径 (支持掩码)

     如果选中此选项，您可以指定包含了要添加到用户应用程序类别的可执行文件的客户端设备上的文件夹。

   - 可移动驱动器

     如果选中此选项，您可以指定应用程序在其上运行的媒体类型（任意设备或可移动驱动器）。在所选驱动类型上运行的应用程序被添加到用户应用程序类别。

   - 哈希、元数据或证书：

- 从可执行文件列表选择

  如果选中此选项，可以使用客户端设备上的可执行文件列表来选择可执行文件并将应用程序添加到类别。

- 从应用程序注册表选择

  如果选择此选项，将显示应用程序注册表。您可以从注册表中选择应用程序，然后指定以下文件元数据：

  - 文件名。
  - 文件版本。您可以指定版本的精确值或描述一个条件，例如“高于 5.0”。
  - 应用程序名称。
  - 应用程序版本。您可以指定版本的精确值或描述一个条件，例如“高于 5.0”。
  - 供应商。

- 手动指定

  如果选择此选项，您必须指定文件哈希、元数据或证书作为将应用程序添加到用户类别的条件。

  文件哈希

  您应该根据网络中设备上安装的安全应用程序版本，为此类别中的文件选择 Kaspersky Security Center Linux 的哈希值计算算法。计算的哈希值信息存储在管理服务器数据库。哈希值的存储不显著增加数据库尺寸。

  未在 SHA256 算法中找到漏洞，它被视为现今最可靠的加密功能。Kaspersky Endpoint Security for Linux 支持 SHA256 计算。

  为该类别中的文件选择任意 Kaspersky Security Center Linux 使用的哈希值算法选项：

  - 如果网络上安装的所有安全应用程序实例都是 Kaspersky Endpoint Security for Linux，请选中“**SHA-256**”复选框。
  - 仅当使用 Kaspersky Endpoint Security for Windows 时，才选择 **MD5 哈希**复选框。Kaspersky Endpoint Security for Linux 不支持 MD5 哈希函数。

  元数据

  如果选择此选项，则可以指定文件名、文件版本、供应商形式的文件元数据。元数据将发送到管理服务器。包含相同元数据的可执行文件将添加到该应用程序类别。

  证书

  如果选中此选项，则可以指定来自存储空间的证书。已按照指定的证书签名的可执行文件将被添加到用户类别。

- 从压缩文件夹

如果选择此选项，则可以指定压缩文件夹的文件，然后选择要用于将应用程序添加到用户类别的条件。压缩文件夹将解压，并且您选择的条件将应用于该文件夹中的文件。作为条件，您可以选择以下标准之一：

- 文件哈希

  选择要用于计算哈希值的哈希函数（MD5 或 SHA256）。与压缩文件夹中的文件具有相同哈希值的应用程序将添加到用户应用程序类别。

  仅当使用 Kaspersky Endpoint Security for Windows 时，才选择 MD5 哈希函数。Kaspersky Endpoint Security for Linux 不支持 MD5 哈希函数。

- 元数据

  选择要用作标准的元数据。包含相同元数据的可执行文件将被添加到用户应用程序类别。

- 证书

  选择要用作标准的证书属性（证书主题、指纹或颁发者）。已签署具有相同属性的证书的可执行文件将添加到用户类别。

所选条件将添加到条件列表中。

您可以根据需要为创建应用程序类别添加任意数量的条件。

6. 在“**排除项**”步骤中，单击“**添加**”按钮以添加从所创建类别中排除文件的排除条件标准。

7. 在“**条件标准**”步骤中，从列表中选择规则类型，方式与选择创建类别时所遵循的规则类型相同。

当向导结束时，将创建应用程序类别。它显示在应用程序规则列表中。配置“应用程序控制”时，可以使用已创建的应用程序类别。

有关应用程序控制的详细信息，请参阅 Kaspersky Endpoint Security for Linux 帮助。

## 查看应用程序类别列表

您可以查看已配置的应用程序类别列表以及每个应用程序类别的设置。

*要查看应用程序类别列表，*

在“**操作**”选项卡，在“**第三方应用程序**”下拉列表中，选择“**应用程序类别**”。

将显示含有应用程序类别列表的页面。

*要查看应用程序类别的属性，*

单击应用程序类别的名称。

将显示应用程序类别的属性窗口。这些属性被分组在几个选项卡上。

# 添加事件相关的可执行文件到应用程序类别

在 Kaspersky Endpoint Security for Linux 策略中配置“应用程序控制”后，以下事件将显示在事件列表中：

- **应用程序启动被禁止**（*严重*事件）。如果已将“应用程序控制”配置为应用规则，则显示此事件。
- **应用程序启动在测试模式中被禁止**（*信息*事件）。如果已将“应用程序控制”配置为测试规则，则显示此事件。
- **向管理员发送的有关应用程序启动禁止的消息**（*警告*事件）。如果已将“应用程序控制”配置为应用规则，并且用户请求访问在启动时被阻止的应用程序，则会显示此事件。

建议创建事件分类以查看与“应用程序控制”操作相关的事件。

您可以将与“应用程序控制”事件相关的可执行文件添加到现有应用程序类别或新的应用程序类别。您只能将可执行文件添加到含有手动添加内容的应用程序类别。

*要将与“应用程序控制”事件相关的可执行文件添加到应用程序类别：*

1. 转到**监控和报告 → 事件分类**。
   将显示事件分类列表。
2. 选择事件分类以查看与“应用程序控制”相关的事件并启动此事件分类。
   如果尚未创建与“应用程序控制”相关的事件分类，可以选择并启动预定义分类，例如“**最近的事件**”。
   将显示事件列表。
3. 选择要将其相关可执行文件添加到应用程序类别的事件，然后单击“**分配到类别**”按钮。
   新类别向导启动。使用**下一步**按钮进行向导。
4. 在向导页面上，指定相关设置：
   - 在“**对事件相关可执行文件所采取的操作**”区域中，选择以下选项之一：
     - 添加到新的应用程序类别
       如果要基于事件相关的可执行文件创建新的应用程序类别，则选择此选项。
       默认情况下已选定该选项。
       如果选择了此选项，请指定新的类别名称。
     - 添加到现有应用程序类别
       如果要将事件相关的可执行文件添加到现有应用程序类别，则选择此选项。
       默认情况下未选定该选项。
       如果选择了此选项，请选择要将可执行文件添加到的含有手动添加内容的应用程序类别。
   - 在“**规则类型**”区域中，选择以下选项之一：
     - 添加到包含的规则

- 添加到排除的规则

- 在**用作条件的参数**部分中，选择以下选项之一：

  - 证书详情(或没有证书的文件的 SHA-256 哈希)

    文件可能使用证书签署。多个文件可能使用相同的证书签署。例如，相同应用程序的不同版本可能使用相同的证书签署，或者相同供应商的多个不同应用程序可能使用相同证书签署。当您选择证书时，应用程序的多个版本或相同供应商的多个应用程序可能组成一个类别。

    每个文件都有单独的 SHA256 哈希。当您选择 SHA256 哈希时，仅一个对应的文件，例如，定义的应用程序版本，组成类别。

    如果您要将可执行文件的证书详情（或者无证书文件的 SHA256 哈希函数）添加到类别规则，则选择该选项。

    默认情况下已选定该选项。

  - 证书详情(没有证书的文件将被跳过)

    文件可能使用证书签署。多个文件可能使用相同的证书签署。例如，相同应用程序的不同版本可能使用相同的证书签署，或者相同供应商的多个不同应用程序可能使用相同证书签署。当您选择证书时，应用程序的多个版本或相同供应商的多个应用程序可能组成一个类别。

    如果您要将可执行文件的证书详情添加到类别规则，则选择该选项。如果可执行文件没有证书，该文件将被跳过。该文件的信息将不被添加到类别。

  - 仅 SHA-256 (没有哈希的文件将被跳过)

    每个文件都有单独的 SHA256 哈希。当您选择 SHA256 哈希时，仅一个对应的文件，例如，定义的应用程序版本，组成类别。

    如果您要仅添加可执行文件的 SHA256 哈希详情，则选择该选项。

  - 仅 MD5 (停产模式，仅对 Kaspersky Endpoint Security 10 Service Pack 1 版本)

    仅当使用 Kaspersky Endpoint Security for Windows 时，才选择此选项。Kaspersky Endpoint Security for Linux 不支持 MD5 哈希函数。

    每个文件都有单独的 MD5 哈希。当您选择 MD5 哈希时，仅一个对应的文件，例如，定义的应用程序版本，组成类别。

5. 单击“**确定**”。

向导完成后，与“应用程序控制”事件相关的可执行文件将添加到现有应用程序类别或新的应用程序类别。您可以查看您已修改或创建的应用程序类别的设置。

有关应用程序控制的详细信息，请参阅 Kaspersky Endpoint Security for Linux 帮助。

# 监控和报告

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运行报告。

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”小组件添加到仪表板并查看
   - 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 14 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 14 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 14 Web Console 的"**监控和报告**"区域中单击"**控制板**"可打开仪表板。

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 14 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。

当配置仪表板时，您可以添加您需要的小部件或隐藏您不需要的小部件，更改小部件的大小或外观，移动小部件以及更改它们的设置。

## 添加工具到控制板

*要添加小部件到仪表板：*

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. 在可用小部件列表，选择您要添加到仪表板的小部件。
   小部件按类别分组。要查看包含在类别中的小部件列表，点击类别名称旁边的臂章图标(>)。
4. 单击“**添加**”按钮。

所选的小部件被添加到仪表板结尾。

您现在可以编辑所添加小部件的展示和参数。

## 从控制板隐藏工具

*要从仪表板隐藏小部件：*

1. 在主菜单中，转到“**监控和报告**”→“**控制板**”。
2. 点击您要隐藏的小部件旁边的设置图标（⚙）。
3. 选择**隐藏 Web 小部件**。
4. 在打开的“**警告**”窗口中，单击“**确定**”。

所选小部件被隐藏。稍后，您可以再次添加该小部件到仪表板。

## 移动工具到控制板

*要移动小部件到仪表板：*

1. 在主菜单中，转到“**监控和报告**” → “**控制板**”。
2. 点击您要移动的小部件旁边的设置图标（⚙）。
3. 选择**移动**。
4. 点击您要移动小部件的地方。您仅可以选择其他小部件。

所选小部件的地方被清扫。

## 更改小部件的大小或外观

对于显示图表的小部件，您可以更改其展示–线条图或线形图。对于一些小部件，您可以更改其大小：最小、中度或最大。

*要更改小部件展示：*

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**

所选小部件的展示被更改。

# 更改小部件设置

*要更改小部件设置：*

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. 在打开的小部件设置窗口，更改所需的小部件设置。
5. 单击“**保存**”保存设置。

所选小部件的设置被更改。

设置集合取决于特定小部件。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 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，则要配置仅仪表板模式，请转到在“**用户和角色**”→“**用户**”区域中提供了用户账户的服务器。可以是主服务器或物理辅助服务器。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，转到“**用户和角色**” → “**用户**”。
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 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 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 14 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**”。
2. 单击**添加**。
   程序将启动“新报告模板向导”。使用“**下一步**”按钮继续向导。
3. 输入报告名称并选择报告类型。
4. 在向导的“**范围**”步骤中，选择基于该报告模板，其数据会显示在报告中的客户端设备集合（管理组、设备分类、所选设备或所有网络设备）。
5. 在向导的“**报告周期**”步骤中，指定报告期间。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。
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。

       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

您可以导出报告到 XML、HTML 或 PDF 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. 选择您要导出到文件的报告旁边的复选框。

3. 单击“**导出报告**”按钮。

4. 在打开的窗口的“**名称**”字段中更改报告文件名。默认下，文件名称与所选的报告模板名称一致。

5. 选择报告文件类型：XML、HTML 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。

6. 单击“**导出报告**”按钮。

   所选格式的报告将被下载到您的设备—到您设备的默认文件夹—或您浏览器中打开的标准**另存为**窗口将允许您保存文件到您想要的位置。

报告被保存到文件。

## 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. 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**”按钮继续向导。
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. 是否将报告保存到文件夹中，以及相应的设置。
      启用 **保存报告到文件夹**选项后，您必须指定该文件夹的 POSIX 路径。如果要将报告保存到共享文件夹，您还必须选择**指定账户以访问共享文件夹**复选框，然后指定用于访问此文件夹的用户账户和密码。

      > 如果选择将报告保存到共享文件夹，则必须确保可以从安装了管理服务器的设备访问该文件夹。确保访问的方法和使用的工具取决于您的基础设施。

      将报告保存到本地文件夹时通常不需要凭证，因为运行管理服务器的账户可以访问此文件夹。如有必要，您可以在向导的**选择账户以运行任务**步骤中指定用户凭证。
      无论选择哪个文件夹，如果您希望新的报告文件覆盖上次任务启动时保存在报告文件夹中的文件，您也可以选择**覆盖相同类型的旧报告**复选框。
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仪表板等方面。
- 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*指示在应用程序运行期间或过程执行期间发生了严重问题、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

# 管理服务器事件

该部分包含管理服务器相关事件信息。

## 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。<br>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。<br>即便当该事件发生时，客户端设备是被保护的。<br>您可以通过以下方式响应事件：<br>• 查看受管理设备列表。删除不在使用的设备。<br>• 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）。<br>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，但指定时间未连接到管理服务器，则该类型的事件发生。<br>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。<br>联系技术支持获得更多详情。 | 180 天 |
| 授权许可即将过期 | 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。<br>Kaspersky Security Center 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。<br>当商业授权许可到期后，Kaspersky Security Center Linux 仅提供基本功能。<br>您可以通过以下方式响应事件：<br>• 请确保将备用授权许可密钥添加到管理服务器中。<br>• 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。 | 180 天 |
| 证书已 | 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。 | 180 天 |

| | | | | |
|---|---|---|---|---|
| 过期 | | | 您需要更新过期的证书。 | |

## 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 Linux 管理服务器事件。

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。<br>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。<br>事件详情可以在事件描述中找到。 | 180 天 |
| 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。<br>您可以通过以下方式响应事件：<br>• 检查用于获取文件夹访问的用户账户是否具有写权限。<br>• 检查文件夹的用户名和/或密码是否被更改。<br>• 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。<br>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。<br>您可以通过以下方式响应事件：<br>• 检查管理服务器(共享文件夹所在位置)是否已开启并可用。<br>• 检查文件夹的用户名和/或密码是否被更改。<br>• 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。<br>您可以通过以下方式响应事件：<br>• 检查安装了 SQL Server 的远程服务器是否可用。<br>• 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。<br>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。<br>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：<br>• 您使用 SQL Server Express 版本 DBMS： | 180 天 |

| | | | | |
|---|---|---|---|---|
| | | | • 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。<br>• 限制存储在管理服务器数据库的事件数量。<br>• 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 for Linux 策略的设置。<br>• 您使用 DBMS 而不是 SQL Server Express Edition：<br>• 不限制存储在管理服务器数据库的事件数量。<br>• 降低存储在管理服务器数据库的事件数量。<br>在 DBMS 选项处查看信息。 | |

## 管理服务器警告事件

该表显示具有“**警告**”重要性级别的 Kaspersky Security Center Linux 管理服务器事件。

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。请参阅以下部分了解详情：阻止频繁事件。 | 90 天 |
| 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。<br>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。<br>即便当该事件发生时，客户端设备是被保护的。<br>您可以通过以下方式响应事件：<br>• 查看受管理设备列表。删除不在使用的设备。<br>• 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）。<br>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。<br>这种情况通常发生在受管理设备已解除授权时。<br>您可以通过以下方式响应事件：<br>• 要从受管理设备列表中手动删除该设备。<br>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。<br>• 指定时间间隔，在该间隔后，使用 Kaspersky Security Center 14 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。<br>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。<br>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。 | 90 天 |

| | | | | |
|---|---|---|---|---|
| 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 |
| 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。<br>以下是事件的可能原因和对事件的适当响应：<br>• 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。<br>• 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、邮件、VPN）时，会发生此类事件。<br>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。<br>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。 | 90 天 |
| **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。<br>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。<br>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。<br>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。<br>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 FCM 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。<br>以下是事件的可能原因和对事件的适当响应：<br>• FCM 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（参见“下游消息错误响应代码”一章）。<br>• 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。 | 90 天 |
| 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。<br>读取事件描述中的详细信息，并相应做出响应。 | 90 天 |

| | | | | |
|---|---|---|---|---|
| | | | 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。 | |
| 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。<br>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。<br>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。<br>您使用 SQL Server Express 版本 DBMS：<br>• 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。<br>• 限制存储在管理服务器数据库的事件数量。<br>• 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 for Linux 策略的设置。<br>您使用 DBMS 而不是 SQL Server Express Edition：<br>• 不限制存储在管理服务器数据库的事件数量<br>• 降低存储在管理服务器数据库的事件数量<br>在 DBMS 选项处查看信息。 | 90 天 |
| 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。<br>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。<br>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。<br>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。<br>您可以通过以下方式响应事件：<br>• 更改存储在管理服务器数据库的事件最大数量<br>• 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。<br>您可以通过以下方式响应事件：<br>• 更改允许存储在管理服务器数据库的事件最大数量<br>• 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

该表显示具有“信息”重要性级别的 Kaspersky Security Center Linux 管理服务器事件。

管理服务器信息事件

| 事件类型显示名称 | 事件类型 ID | 事件类型 | 默认存储期限 | 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 | |
| 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 | 当用户使用管理控制台或 Web Console 连接到管理服务器时，会发生此类事件。这些事件包括安装基于 MMC 的管理控制台或 Web Console 服务器的设备的 IP 地址。 |
| 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：<br>• 管理组<br>• 安全组<br>• 用户<br>• 任务<br>• 任务<br>• 策略<br>• 服务器<br>• 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：<br>• 用户<br>• 授权许可<br>• 服务器<br>• 虚拟服务器 |
| 审计：用户许可已被修改 | 4153 | KLAUD_EV_OBJECTACLMODIFIED | 30 天 | |

# 网络代理事件

该部分包含管网络代理相关事件信息。

## 网络代理警告事件

下表显示具有“**警告**”严重级别的 Kaspersky Security Center Linux 网络代理事件。

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 |
|---|---|---|---|
| 发生了事故 | 549 | GNRL_EV_APP_INCIDENT_OCCURED | 30 天 |

## 网络代理信息事件

下表显示具有“**信息**”严重级别的 Kaspersky Security Center Linux 网络代理事件。

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 |

# 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 14 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 14 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。

## 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. 选择“**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，请在屏幕顶部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 Linux 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。

# 阻止频繁事件

本节提供有关管理频繁事件阻止和移除阻止频繁事件的信息。

# 关于阻止频繁事件

单个或多个受管理设备上安装的受管理应用程序（例如 Kaspersky Endpoint Security for Linux）可以将许多相同类型的事件发送到管理服务器。接收频繁事件可能会使管理服务器数据库超载并覆盖其他事件。当接收的事件总数超过指定的数据库限制时，管理服务器将开始阻止最频繁的事件。

管理服务器会自动阻止接收频繁事件。您自己不能阻止频繁事件，也不能选择要阻止的事件。

如果要了解某个事件是否被阻止，可以查看通知列表或者检查该事件是否出现在管理服务器属性的“**阻止频繁事件**”区域中。如果该事件被阻止，可以执行以下操作：

- 如果要防止覆盖数据库，可以继续阻止接收此类事件。
- 例如，如果要查找将频繁事件发送到管理服务器的原因，可以解除阻止频繁事件并继续接收此类事件。

- 如果要继续接收频繁事件直到它们被再次阻止，可以将它们从频繁事件的阻止中移除。

## 管理频繁事件阻止

管理服务器会阻止自动接收频繁事件，但是您可以解除阻止并继续接收频繁事件。您还可以阻止接收您以前解除阻止的频繁事件。

*要管理对频繁事件的阻止：*

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“**阻止频繁事件**”区域。
3. 在“**阻止频繁事件**”区域中：
   - 如果要解除阻止接收频繁事件：
     a. 选择要解除阻止的频繁事件，然后单击“**排除**”按钮。
     b. 单击“**保存**”按钮。
   - 如果要阻止接收频繁事件：
     a. 选择要阻止的频繁事件，然后单击“**阻止**”按钮。
     b. 单击“**保存**”按钮。

管理服务器将接收未阻止的频繁事件，并且不接收被阻止的频繁事件。

## 移除对频繁事件的阻止

您可以移除对频繁事件的阻止并开始接收它们，直到管理服务器再次阻止这些频繁事件。

*要移除对频繁事件的阻止：*

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“**阻止频繁事件**”区域。
3. 在“**阻止频繁事件**”区域中，选择要为其移除阻止的频繁事件类型。
4. 点击“**移除阻止**”按钮。

该频繁事件将从频繁事件列表中移除。管理服务器将接收此类事件。

## 在管理服务器上的事件处理和存储

关于应用程序和受管理设备运行过程中发生的事件的信息保存在管理服务器数据库中。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。默认情况下，事件队列限制为 20,000 个事件。您可以通过编辑 KLEVP_MAX_POSTPONED_CNT 标记值来自定义队列限制。

# 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*。您已对通知执行推荐操作或您已手动为通知分配该状态。
- *未查看*。您未对通知执行推荐操作或您未手动为通知分配该状态。

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，右侧面板会显示所有通知。
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 14 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。

# 关于设备状态

Kaspersky Security Center Linux 为每个受管理设备都分配一个状态。具体状态取决于是否满足用户定义的条件。在某些情况下，为设备分配状态时，Kaspersky Security Center Linux 会考虑设备在网络中的可见性标志（请参见下表）。如果 Kaspersky Security Center Linux 在两小时内未在网络中找到设备，则该设备的可见性标志将设置为“*不可见*”。

状态如下：

- “*严重*”或“*严重/可见*”
- “*警告*”或“*警告/可见*”
- “*正常*”或“*正常/可见*”

下表列出了为设备分配“*严重*”或“*警告*”状态所必须满足的默认条件，以及所有可能值。

分配状态到设备的条件

| 条件 | 条件描述 | 可用值 |
| --- | --- | --- |
| 安全应用程序未安装 | 网络代理已安装到设备，但是安全应用程序未安装。 | • 开关按钮被开启。<br>• 开关按钮被关闭。 |
| 检测到太多病毒 | 一些病毒被病毒检测任务在设备上发现，例如，病毒扫描任务，且发现的病毒数量超过指定值。 | 超过 0。 |
| 实时保护级别与管理员设置的级别不同 | 设备在网络中可见，但实时保护级别与管理员在设备状态条件中设置的级别不同。 | • 已停止。<br>• 已暂停。<br>• 正在运行。 |
| 病毒扫描已长时间未执行 | 设备在网络中可见且安全应用程序已安装到设备，但不论*恶意软件扫描*任务还是本地扫描任务都没有在指定时间内未运行。条件仅应用到于 7 天之前或更早添加到管理服务器数据库的设备。 | 超过 1 天。 |
| 数据库已过期 | 设备在网络中可见且安全应用程序已安装到设备，但反病毒数据库在指定时间内未在该设备上更新。条件仅应用到于 1 天之前或更早添加到管理服务器数据库的设备。 | 超过 1 天。 |
| 长时间没有连接 | 网络代理已安装到设备，但由于设备关闭，设备在指定时间段内未连接到管理服务器。 | 超过 1 天。 |

| | | |
|---|---|---|
| 检测到活动威胁 | "**活动威胁**"文件夹中的未处理的对象的数量超过指定的值。 | 超过 0 项。 |
| 需要重新启动 | 设备在网络中可见，但应用程序基于所选原因之一在指定时间之前请求设备重启。 | 超过 0 分钟。 |
| 安装了不兼容的应用程序 | 设备在网络中可见，但通过网络代理执行的软件清查在设备上检测到了不兼容的应用程序。 | • 开关按钮被关闭。<br>• 开关按钮被开启。 |
| 授权许可已过期 | 设备在网络中可见，但授权许可已过期。 | • 开关按钮被关闭。<br>• 开关按钮被开启。 |
| 授权许可即将过期 | 设备在网络中可见，但设备上的授权许可即将在指定天数内过期。 | 超过 0 天。 |
| 检测到未处理的事故 | 设备上发现了一些未处理的事故。事件可以通过安装在客户端设备上的受管 Kaspersky 应用程序自动创建，也可以由管理员手动创建。 | • 开关按钮被关闭。<br>• 开关按钮被开启。 |
| 应用程序定义的设备状态 | 设备状态由受管理应用程序定义。 | • 开关按钮被关闭。<br>• 开关按钮被开启。 |
| 设备磁盘空间不足 | 设备剩余磁盘空间少于指定值或设备无法与管理服务器同步。当设备已与管理服务器成功同步且设备上的剩余空间大于或等于指定值时，*严重*或*警告*状态被更改为*正常*状态。 | 大于 0 MB |
| 设备已失去管理 | 在设备发现过程中，设备在网络中可见，但是超过三次尝试与管理服务器同步都失败了。 | • 开关按钮被关闭。<br>• 开关按钮被开启。 |
| 保护已禁用 | 设备在网络中可见，但设备上的安全应用程序已被禁用长于指定的时间段。<br>在这种情况下，安全应用程序的状态为*stopped*或*failure*，不同于以下状态：*starting*、*running*或*suspended*。 | 超过 0 分钟。 |
| 安全应用程序没有运行 | 设备在网络中可见且安全应用程序已安装到设备，但其未在运行。 | • 开关按钮被关闭。 |

| | | |
|---|---|---|
| | | • 开关按钮被开启。 |

Kaspersky Security Center Linux 允许您设置管理组中设备状态在指定条件满足时的自动切换。当指定条件满足时，客户端设备被分配以下状态之一：*严重*或*警告*。未满足指定条件时，客户端设备被分配“*正常*”状态。

一个条件的不同值可对应于不同的状态。例如，默认情况下，如果“**数据库已过期**”条件的值为“**超过 3 天**”，将为客户端设备分配“*警告*”状态；如果值为“**超过 7 天**”，则将分配“*严重*”状态。

如果从以前的版本升级 Kaspersky Security Center Linux，则分配状态到“*严重*”或“*警告*”的“**数据库已过期**”条件的值不变。

当 Kaspersky Security Center Linux 为设备分配状态时，对于某些条件（请参见“条件描述”列），将考虑可见性标志。例如，如果某个受管理设备由于满足“数据库已过期”条件而被分配“*严重*”状态，稍后为设备设置了可见性标志，则该设备被分配“*正常*”状态。

## 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“**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“**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（请见下表）。

描述事件的占位符

| 占位符 | 占位符描述 |
| --- | --- |
| %SEVERITY% | 事件严重级别。可能值： |

| | |
|---|---|
| | • 信息<br>• 警告<br>• 错误<br>• 严重 |
| %COMPUTER% | 发生事件的设备的名称。<br>设备名称的最大长度为 256 个字符。 |
| %DOMAIN% | 发生事件的设备的域名称。 |
| %EVENT% | 事件类型的名称。<br>事件类型名称的最大长度为 50 个字符。 |
| %DESCR% | 事件描述。<br>描述的最大长度为 1000 个字符。 |
| %RISE_TIME% | 事件创建时间。 |
| %KLCSAK_EVENT_TASK_DISPLAY_NAME% | 任务名称。<br>任务名称的最大长度为 100 个字符。 |
| %KL_PRODUCT% | 产品名称。 |
| %KL_VERSION% | 产品版本号。 |
| %KLCSAK_EVENT_SEVERITY_NUM% | 事件严重编号。可能值：<br>• 1—信息<br>• 2—警告<br>• 3—Error<br>• 4—严重 |
| %HOST_IP% | 发生事件的设备的 IP 地址。 |
| %HOST_CONN_IP% | 发生事件的设备的连接 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。

# 关于 Kaspersky 公告

“Kaspersky 公告”区域（**监控和报告 → Kaspersky 公告**）提供与您的 Kaspersky Security Center 版本和受管理设备上安装的受管理应用程序相关的信息，让您了解最新动态。Kaspersky Security Center 会定期删除过时的公告并添加新信息来更新该区域中的信息。

Kaspersky Security Center 仅显示与当前连接的管理服务器和该管理服务器的受管理设备上安装的 Kaspersky 应用程序相关的 Kaspersky 公告。对于任何类型的管理服务器（主要、从属或虚拟）都单独显示公告。

管理服务器必须具有互联网连接才能接收 Kaspersky 公告。

公告包括以下类型的信息：

- 与安全相关的公告

  与安全相关的公告旨在使网络中安装的 Kaspersky 应用程序保持最新并具有完整功能。公告可能包括有关 Kaspersky 应用程序的关键更新、已发现漏洞的修复以及修复 Kaspersky 应用程序中的其他问题的方法的信息。默认情况下，安全相关的公告已启用。如果您不想接收这些公告，可以禁用此功能。

  为了显示与您的网络保护配置相对应的信息，Kaspersky Security Center 会将数据发送到 Kaspersky 云服务器，并仅接收与网络中安装的 Kaspersky 应用程序有关的公告。您安装 Kaspersky Security Center 管理服务器时接受的最终用户授权许可协议中描述了可以发送到服务器的数据集。

- 营销公告

  营销公告包括您的 Kaspersky 应用程序的特别优惠信息、广告和 Kaspersky 新闻。默认情况下禁用营销公告。仅当启用卡巴斯基安全网络 (KSN) 时，才会收到此类公告。您可以通过禁用 KSN 来禁用营销公告。

  为了仅向您显示可能对保护网络设备和日常任务有帮助的相关信息，Kaspersky Security Center 会将数据发送到 Kaspersky 云服务器并接收相应公告。KSN 声明的“处理的数据”部分中描述了可发送到服务器的数据集。

新信息根据重要性分为以下几个类别：

1. 关键信息
2. 重要新闻
3. 警告
4. 信息

当“Kaspersky 公告”区域中出现新信息时，Kaspersky Security Center 14 Web Console 将显示一个与公告重要级别相对应的通知标签。您可以单击该标签以在“Kaspersky 公告”区域中查看此公告。

您可以指定 Kaspersky 公告设置，包括您要查看的公告类别以及显示通知标签的位置。如果您不想接收公告，可以禁用此功能。

# 指定 Kaspersky 公告设置

在“Kaspersky 公告”区域中，您可以指定 Kaspersky 公告设置，包括您要查看的公告类别以及显示通知标签的位置。

*要配置 Kaspersky 公告：*

1. 在主菜单中，转到“**监控和报告**” → “**卡巴斯基通告**”。
2. 单击“**设置**”链接。

   将打开“Kaspersky 公告设置”窗口。
3. 指定下列设置：
   - 选择您要查看的公告的重要级别。其他类别的公告将不会显示。
   - 选择您希望显示通知标签的位置。标签可以显示在所有控制台区域，或“**监控和报告**”区域及其子区域。

4. 单击“**确定**”按钮。

   Kaspersky 公告设置已指定。

## 禁用 Kaspersky 公告

“Kaspersky 公告”区域（**监控和报告 → Kaspersky 公告**）提供与您的 Kaspersky Security Center 版本和受管理设备上安装的受管理应用程序相关的信息，让您了解最新动态。如果您不想接收 Kaspersky 公告，可以禁用此功能。

*要禁用 Kaspersky 公告：*

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“**Kaspersky 公告**”区域。

3. 将开关按钮切换到“**安全相关公告已禁用**”位置。

4. 单击“**保存**”按钮。

   Kaspersky 公告已禁用。

## 导出事件到 SIEM 系统

本节介绍如何配置导出事件到 SIEM 系统。

## 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

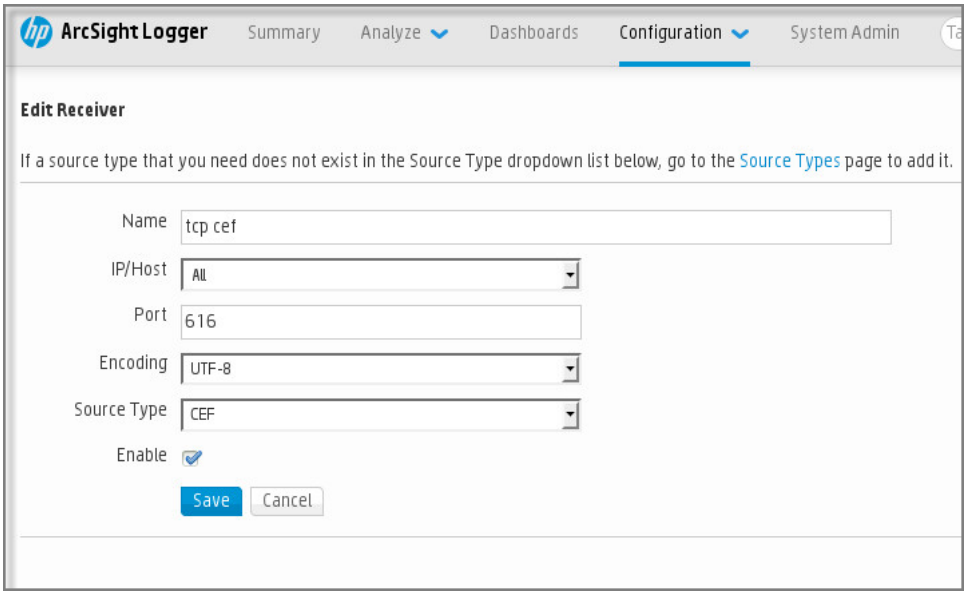
  指定用于连接到 Kaspersky Security Center Linux 的端口号。该端口必须与您在配置 SIEM 系统期间在 Kaspersky Security Center Linux 中指定的端口相同。

- 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。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。

## 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。

## 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。

## 标记要以 Syslog 格式导出的 Kaspersky 应用程序事件

如果要导出受管理设备上安装的特定受管理应用程序中发生的事件，则标记事件为在应用程序策略中导出。在这种情况下，标记的事件将从策略范围内的所有设备中导出。

*要为特定受管理应用程序标记要导出的事件：*

1. 在主菜单中，转到“**设备**”→“**策略和配置文件**”。
2. 点击您要为其标记事件的应用程序的策略。
   策略设置窗口打开。
3. 转到“**事件配置**”区域。
4. 选中要导出到 SIEM 系统的事件旁边的复选框。
5. 单击“**使用 Syslog 标记以导出到 SIEM 系统**”按钮。

   您也可以在“**事件注册**”区域中标记要导出到 SIEM 系统的事件，通过单击事件链接可打开该区域。

6. 在您标记为导出到 SIEM 系统的一个或多个事件的“**Syslog**”列中会显示一个复选标记 (✓)。
7. 单击“**保存**”按钮。

受管理应用程序中的标记事件已准备好导出到 SIEM 系统。

您可以为特定受管理设备标记要导出到 SIEM 系统的事件。如果先前导出的事件已在应用程序策略中标记，您将不能为受管理设备重新定义所标记的事件。

*要为受管理设备标记要导出的事件：*

1. 在主菜单中，转到“**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单击带有所需设备名称的链接。
   将显示所选设备的属性窗口。
3. 转到“**应用程序**”区域。
4. 在应用程序列表中单击带有所需应用程序名称的链接。
5. 转到“**事件配置**”区域。
6. 选中要导出到 SIEM 的事件旁边的复选框。
7. 单击“**使用 Syslog 标记以导出到 SIEM 系统**”按钮。

此外，还可以在“**事件注册**”区域中标记要导出到 SIEM 系统的事件，通过单击事件链接可打开该区域。

8. 在您标记为导出到 SIEM 系统的一个或多个事件的“**Syslog**”列中会显示一个复选标记 (✓)。

从现在开始，如果配置了到 SIEM 系统的导出，管理服务器会将标记的事件发送到 SIEM 系统。

## 标记要以 Syslog 格式导出的常规事件

您可以标记管理服务器将使用 Syslog 格式导出到 SIEM 系统的常规事件。

*要标记常规事件以导出到 SIEM 系统：*

1. 执行以下操作之一：
   - 单击所需管理服务器名称旁边的“设置”图标 ()。
   - 在主菜单中，转到“**设备**”→“**策略和配置文件**”，然后单击某个策略的链接。
2. 在打开的窗口中，转到“**事件配置**”选项卡。
3. 单击“**使用 Syslog 标记以导出到 SIEM 系统**”。

此外，还可以在“**事件注册**”区域中标记要导出到 SIEM 系统的事件，通过单击事件链接可打开该区域。

4. 在您标记为导出到 SIEM 系统的一个或多个事件的“**Syslog**”列中会显示一个复选标记 (✓)。

从现在开始，如果配置了到 SIEM 系统的导出，管理服务器会将标记的事件发送到 SIEM 系统。

## 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。

# 配置 Kaspersky Security Center Linux 以将事件导出到 SIEM 系统

要将事件导出到 SIEM 系统，必须在 Kaspersky Security Center Linux 中配置导出流程。

*要在 Kaspersky Security Center 14 Web Console 中配置到 SIEM 系统的导出：*

1. 在“**控制台设置**”下拉列表中，选择“**整合**”。
   “**控制台设置**”窗口将开启。
2. 选择“**整合**”选项卡。
3. 在“**整合** ”选项卡上，选择“**SIEM**”区域。
4. 单击“**设置**”链接。
   “**导出设置**”区域将打开。
5. 在“**导出设置**”区域指定设置：

   - **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**

选择该协议用于传输消息到 SIEM 系统。您可以选择 TCP、UDP 或 TLS over TCP 协议。

如果选择 TLS over TCP 协议，则指定以下 TLS 设置：

- **服务器身份验证**

  在“**服务器身份验证**”字段中，可以选择值“**受信任证书**”或“**SHA 指纹**”：

  - **受信任证书**。您可以接收来自受信任证书颁发机构 (CA) 的完整证书链（包括根证书），并将该文件上传到 Kaspersky Security Center Linux。Kaspersky Security Center Linux 会检查 SIEM 系统服务器的证书链是否也具有受信任 CA 的签名。

    要添加受信任证书，请单击“**浏览 CA 证书文件**”按钮，然后上传证书。

  - **SHA 指纹**。您可以在 Kaspersky Security Center 中指定 SIEM 系统的完整证书链（包括根证书）的 SHA1 指纹。要添加 SHA1 指纹，请在“**指纹**”字段中输入，然后单击“**添加**”按钮。

  使用“**添加客户端身份验证**”设置，可以生成证书来对 Kaspersky Security Center 进行身份验证。因此，您将使用 Kaspersky Security Center 颁发的自签名证书。在这种情况下，您可以同时使用受信任证书和 SHA 指纹来对 SIEM 系统服务器进行身份验证。

- **添加主题名称/主题备选名称**

  主题名称是接收证书的域名。如果 SIEM 系统服务器的域名与 SIEM 系统服务器证书的主题名称不匹配，Kaspersky Security Center Linux 将无法连接到 SIEM 系统服务器。但是，SIEM 系统服务器的域名在证书中发生变化，则可以更改该域名。在这种情况下，您可以在“**添加主题名称/主题备选名称**”字段中指定主题名称。如果任一指定主题名称与 SIEM 系统证书的主题名称匹配，Kaspersky Security Center Linux 将验证 SIEM 系统服务器证书。

- **添加客户端身份验证**

  对于客户端身份验证，可以插入证书或在 Kaspersky Security Center 中生成证书。

  - **插入证书**。您可以使用从任何来源（例如，从任何受信任 CA）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 PEM**。在“**证书文件**”字段中上传包含证书的文件，并在“**密钥文件**”字段中上传包含私钥的文件。这两个文件不相互依赖，文件的加载顺序也不重要。上传这两个文件后，在“**密码或证书验证**”字段中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。

    - **X.509 证书 PKCS12**。在“**证书文件**”字段中上传包含证书及其私钥的单个文件。上传该文件后，在“**密码或证书验证**”字段中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。

  - **生成密钥**。您可以在 Kaspersky Security Center 中生成自签名证书。结果，Kaspersky Security Center Linux 将存储生成的自签名证书，您可以将证书的公共部分或 SHA1 指纹传递给 SIEM 系统。

6. 如果需要，您可以从管理服务器数据库中导出压缩的事件，并设置要开始导出的压缩事件的开始日期：

   a. 单击**设置导出起始日期**链接。

   b. 在打开的区域的“**导出的起始日期**”字段中，指定开始日期。

   c. 单击“**确定**”按钮。

7. 将选项切换到“**自动导出事件至 SIEM 系统数据库已启用**”位置。

8. 单击“保存”按钮。

到 SIEM 系统的导出已配置。从现在开始，如果您在 SIEM 系统中配置了事件接收，管理服务器会将标记的事件导出到 SIEM 系统。如果设置了导出的开始日期，管理服务器还会从管理服务器数据库中导出从指定日期开始的标记事件。

# 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检索事件数据，也可以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 实用工具执行 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 实用工具执行 SQL 查询

本文描述了如何使用 klsql2 实用工具，以及如何使用该实用工具执行 SQL 查询。当您使用 klsql2 实用工具执行 SQL 查询时，您不必提供数据库名称和访问参数，因为查询直接定位 Kaspersky Security Center Linux 公共视图。

*要使用 klsql2 实用程序：*

1. 转到安装 Kaspersky Security Center Linux 管理服务器的目录。默认安装路径为/opt/kaspersky/ksc64/sbin。
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 Linux 管理服务器设备上，在命令行，输入以下命令以从 src.sql 文件执行 SQL 查询并保存结果到 result.xml 文件：
   ```
   sudo ./klsql2 -i src.sql -o result.xml
   ```
6. 打开新创建的 result.xml 文件以查看 SQL 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 SQL 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 实用工具执行。

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 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 脚本编辑器连接该数据库。

*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。

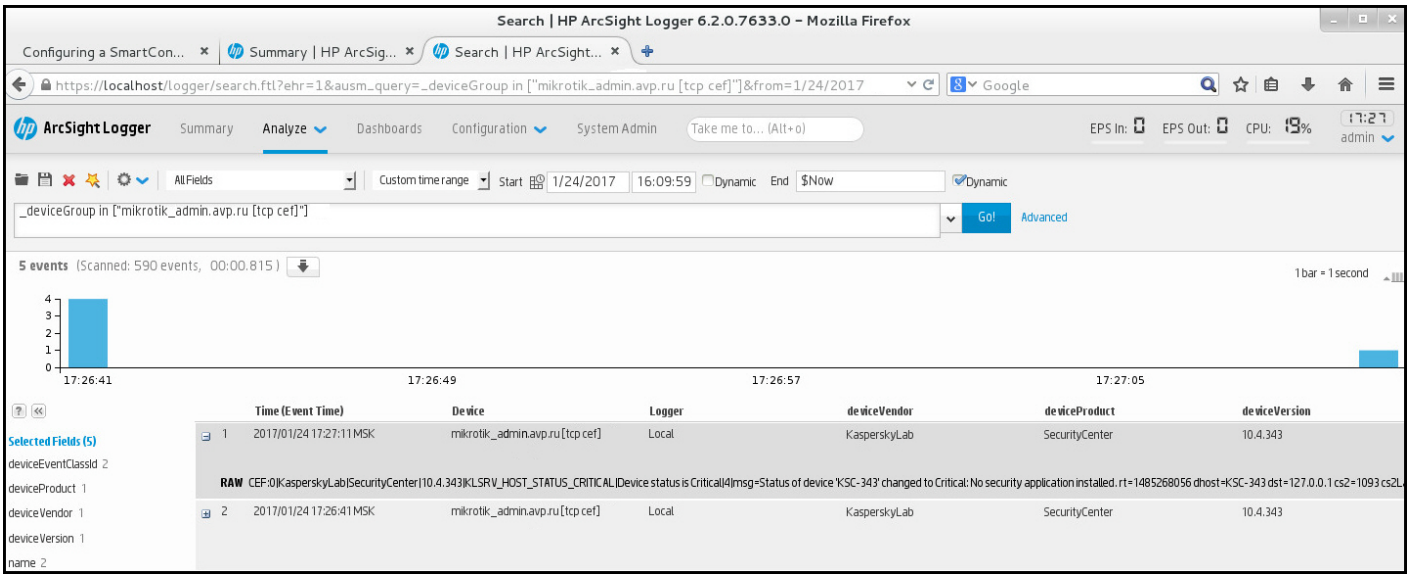
## 查看导出结果

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

# 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 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 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"**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。

## 创建设备分类

*要创建设备分类，请执行以下操作：*

1. 在主菜单中，转到**"设备"→"设备分类"**。
   将显示含有设备分类列表的页面。
2. 单击**"添加"**按钮。
   **"设备分类设置"**窗口打开。
3. 输入新分类的名称。
4. 指定包含要被包括在设备分类中的设备的组：
   - **查找任何设备**— 搜索符合选择标准并被包括在**受管理设备**或**未分配的设备**组中的设备。
   - **查找受管理设备** — 搜索符合选择标准并被包括在**受管理设备**组中的设备。
   - **查找未分配的设备**— 搜索符合选择标准并被包括在**未分配的设备**组中的设备。

   您可以启用**包含来自从属管理服务器的数据**复选框以启用搜索满足选择条件并由从属管理服务器管理的设备。
5. 单击**"添加"**按钮。
6. 在打开的窗口中，指定要将设备包括在此分类中所必须满足的条件，然后单击**"确定"**按钮。
7. 单击**"保存"**按钮。

设备分类即被创建并添加到设备分类列表中。

## 配置设备分类

*要配置设备分类：*

1. 在主菜单中，转到**"设备" → "设备分类"**。
   将显示含有设备分类列表的页面。
2. 选择相关的用户自定义设备分类，然后单击**属性**按钮。
   **"设备分类设置"**窗口打开。
3. 在**常规**选项卡上，单击**新条件**链接。
4. 指定包含设备到该分类必须满足的条件。
5. 单击**"保存"**按钮。

设备被应用并保存。

以下是分配设备到分类的条件描述。多个条件使用 OR 逻辑运算符组合在一起：选择范围将包含至少符合列出的一个条件的设备。

## 常规

在“**常规**”区域，您可以更改分类条件的名称，指定条件是否必须被倒转：

反转分类条件

> 如果启用此选项，指定的分类条件将倒转。此分类将包含所有不符合该条件的设备。
> 默认情况下已禁用该选项。

## 网络基础架构

在“**网络**”子区域，您可以指定根据网络数据包含设备到分类的标准：

- 设备名称

  > 设备的 Windows 网络名称（NetBIOS 名称）或者 IPv4 或 IPv6 地址。

- Windows 域

  > 显示指定工作组中包括的所有设备。

- 管理组

  > 显示指定的管理组中包括的设备。

- 描述

设备属性窗口中的文本：在“**描述**”区域的“**常规**”字段。
要描述“**描述**”字段中的文本，您可以使用以下字符：

- 在单词中：
  - *****。用任意数量的字符替换任何字符串。

    **例如：**
    要描述单词 **Server** 或 **Server's**，您可以输入 **Server***。
  - **?**。替换任意单个字符。

    **例如：**
    要描述 **SUSE Linux Enterprise Server 12** 或 **SUSE Linux Enterprise Server 15** 等短语，可以输入 **SUSE Linux Enterprise Server 1?**。
    星号(*)或问号(?)不能用于查询中的第一个字符。
- 要查找多个单词：
  - 空格。显示所有在其描述中包含列出的任何单词的设备。

    **例如：**
    要查找包含“**从属**”或“**虚拟**”单词的短语，可以在查询中包含“**从属 虚拟**”行。
  - **+**。当单词带有加号前缀时，所有搜索结果都将包含该单词。

    **例如：**
    要查找同时包含“**从属**”和“**虚拟**”的短语，请输入“**+从属+虚拟**”查询。
  - **-**。当单词带有减号前缀时，所有搜索结果都不包含该单词。

    **例如：**
    要查找包含“**从属**”但不包含“**虚拟**”的短语，请输入“**+从属-虚拟**”查询。
  - **“<某些文本>”**。引号中围绕的文本必须存在于文本中。

    **例如：**
    要查找包含“**从属服务器**”单词组合的短语，可以在查询中输入“**从属服务器**”。

- 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。

- 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。

在“**活动目录**”子区域，您可以配置基于活动目录数据包含设备到分类的标准：

- 设备在活动目录组织单元中

  如果启用此选项，选择范围将包括输入字段中指定的活动目录单元中的设备。
  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。

- 该设备是活动目录组成员

  如果启用此选项，选择范围将包括输入字段中指定的活动目录组中的设备。
  默认情况下已禁用该选项。

在“**网络活动**”子区域，您可以指定根据网络活动包含设备到分类的标准：

- 作为分发点

  在下拉列表中，可设置执行搜索时在分类中包含设备的标准：
  - **是**。选择范围将包括充当分发点的设备。
  - **否**。选择范围将不包括充当分发点的设备。
  - **未选择值**。将不应用标准。

- 不断开与管理服务器的连接

  在下拉列表中，可设置执行搜索时在分类中包含设备的标准：
  - **已启用**。分类将包含选中了“**不断开与管理服务器的连接**”复选框的设备。
  - **已禁用**。分类将包含清空了“**不断开与管理服务器的连接**”复选框的设备。
  - **未选择值**。将不应用标准。

- 连接配置文件已切换

在下拉列表中，可设置执行搜索时在分类中包含设备的标准：

- **是**。该分类将包含连接配置文件切换后连接到管理服务器的设备。
- **否**。该分类将不包含连接配置文件切换后连接到管理服务器的设备。
- **未选择值**。将不应用标准。

- 上一次连接到管理服务器

  您可使用此选框设置按上一次连接到管理服务器的时间搜索设备的标准。

  如果选择该选框，则在输入字段中，您可以指定在客户端设备上安装的网络代理和管理服务器之间建立上一次连接的时间间隔（日期和时间）。选择将包括位于指定间隔的设备。

  如果清除此选框，则将不会应用标准。

  默认情况下已清除该选框。

- 网络轮询时检测到新设备

  搜索最近几天通过网络轮询检测到的新设备。

  如果启用此选项，分类将只包括在“**检测周期 (天)**”字段中指定的天数内通过设备发现检测到的新设备。

  如果禁用此选项，分类将包括通过设备发现检测到的所有设备。

  默认情况下已禁用该选项。

- 设备可见

  在下拉列表中，可设置执行搜索时在分类中包含设备的标准：

  - **是**。程序在分类中包括网络中当前可见的设备。
  - **否**。应用程序在分类中包括网络中当前不可见的设备。
  - **未选择值**。将不应用标准。

## 设备状态

在“**受管理设备状态**”子区域，您可以配置基于受管理应用程序的设备状态的描述包含设备到分类的标准：

- 设备状态

  在该下拉列表中，您可以选择下列设备状态之一：“*正常*”、“*严重*”或“*警告*”。

- 实时保护状态

  您可以在该下拉列表中选择实时保护状态。具有指定实时保护状态的设备将被包括在选择范围中。

- 设备状态描述

在该字段中，您可以选中条件旁边的选框，这些条件如果被满足，程序会为设备分配下列状态之一：*正常*、*严重* 或 *警告*。

在“**受管理应用程序组件的状态**”子区域，您可以配置根据受管理应用程序组件状态包含设备到分类的标准：

- 数据泄漏防护状态

  根据数据泄漏防护状态（*设备上无数据*、*已停止*、*正在启动*、*已暂停*、*运行中*、*失败*）搜索设备。

- 协作服务器保护状态

  根据服务器协作保护状态（*设备上无数据*、*已停止*、*正在启动*、*已暂停*、*运行中*、*失败*）搜索设备。

- 邮件服务器的反病毒保护状态

  根据邮件服务器保护状态（*设备上无数据*、*已停止*、*正在启动*、*已暂停*、*运行中*、*失败*）*搜索设备*。

- 端点传感器状态

  根据端点传感器组件状态（*设备上无数据*、*已停止*、*正在启动*、*已暂停*、*运行中*、*失败*）搜索设备。

在“**影响受管理应用程序状态的问题**”子区域，您可以指定根据由受管理应用程序检测到的可能问题列表包含设备到分类的标准。如果至少一个您选择的问题存在于设备，设备将被包含到分类。当您选择几个应用程序的问题时，您可以选择在所有列表中自动选择该问题。

您可以选择受管理应用程序状态描述的复选框；接收这些状态时，设备将被包含在分类。当您选择几个应用程序的状态时，您可以选择在所有列表中自动选择该状态。

## 系统详情

在“**操作系统**”区域，您可以指定根据操作系统类型包含设备到分类的标准。

- 平台类型

  如果选中该选框，您可以从列表中选择一个操作系统。安装了指定操作系统的设备会包含在搜索结果中。

- 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。

- 操作系统 bit 大小

  在该下拉列表中，可选择操作系统的架构，这将决定将移动规则应用到设备（**未知**、**x86**、**AMD64** 或 **IA64**）的方式。默认情况下，不选择列表中的任何选项，这样就不会对操作系统的架构进行定义。

- 操作系统内部版本

该设置仅应用到 Windows 操作系统。

操作系统版本号。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。您也可以配置对所有版本号的搜索，除了指定版本号。

- 操作系统发布号

该设置仅应用到 Windows 操作系统。

操作系统发布 ID。您可以指定所选操作系统是否必须具有相等、更早或更晚的发布 ID。您也可以配置对所有版本 ID 号的搜索，除了指定的版本 ID 号。

在“**虚拟机**”区域，您可以设置基于它们是否是虚拟机或虚拟桌面基础架构 (VDI) 的一部分来包含设备到分类的标准：

- 这是一台虚拟机

在该下拉列表中，您可以选择以下选项：

- **未定义**。
- **否**。查找非虚拟机设备。
- **是**。查找虚拟机设备。

- 虚拟机类型

在该下拉列表中，您可以选择虚拟机生产商。
如果在“**这是一台虚拟机**”下拉列表中选择了“**是**”或“**不重要**”值，则该下拉列表可用。

- 虚拟桌面基础架构的一部分

在该下拉列表中，您可以选择以下选项：

- **未定义**。
- **否**。查找不属于虚拟桌面基础架构的设备。
- **是**。查找术语虚拟桌面基础架构 （VDI） 一部分的设备。

在“**硬件注册表**”子区域，您可以配置基于所安装的硬件包含设备到分类的标准：

确保在要从中获取硬件详细信息的 Linux 设备上安装了 lshw 实用程序。根据所使用的 hypervisor，从虚拟机获取的硬件详细信息可能不完整。

- 设备

在该下拉列表中，您可以选择单元类型。所有带有该单元的设备被包含在搜索结果。
该字段支持完整文本搜索。

- 供应商

  在该下拉列表中，您可以选择单元生产商的名称。所有带有该单元的设备被包含在搜索结果。
  该字段支持完整文本搜索。

- 设备名称

  具有指定名称的设备将包括在该分类中。

- 描述

  设备或硬件单元的描述。带有该字段中指定的描述的设备将包括在分类范围内。
  可在设备的属性窗口输入任何格式的设备描述。该字段支持完整文本搜索。

- 设备制造商

  设备制造商的名称。被指定生产商制造的设备将包括在分类范围内。
  您可以在设备的属性窗口中输入制造商的名称。

- 序列号

  带该字段中指定序列号的所有硬件设备将包括在该分类中。

- 清单号

  带有该字段中指定的清单编号的设备将包括在选择范围内。

- 用户

  该字段中指定用户的所有硬件设备都将包括在该分类中。

- 位置

  设备或硬件单元的位置（例如，在总部或分公司）。在该字段中指定的位置部署的计算机或其他设备将包括在该分类中。
  您可以在该设备的属性窗口中以任何格式描述设备的位置。

- CPU 时钟频率 (MHz)，从

  CPU 的最小时钟速率。CPU 与输入字段中指定的时钟速率范围（含）相匹配的设备将包含在分类中。

- CPU 时钟频率 (MHz)，到

  CPU 的最大时钟速率。CPU 与输入字段中指定的时钟速率范围（含）相匹配的设备将包含在分类中。

- 虚拟 CPU 内核数量，从

  虚拟 CPU 内核的最小数量。CPU 与输入字段中指定的虚拟核心数范围（含）匹配的设备将包含在分类中。

- 虚拟 CPU 内核数量，到

  虚拟 CPU 内核的最大数量。CPU 与输入字段中指定的虚拟核心数范围（含）匹配的设备将包含在分类中。

- 硬盘卷(GB)，从

  设备上硬盘的最小容量。硬盘与输入字段中指定的容量范围（含）匹配的设备将被包括在分类内。

- 硬盘卷(GB)，到

  设备上硬盘的最大容量。硬盘与输入字段中指定的容量范围（含）匹配的设备将被包括在分类内。

- 内存大小(MB)，从

  设备 RAM 的最小大小。RAM 与输入字段中指定的大小范围（含）匹配的设备将被包括在分类中。

- 内存大小(MB)

  设备 RAM 的最大大小。RAM 与输入字段中指定的大小范围（含）匹配的设备将被包括在分类中。

## 第三方软件详情

在“应用程序注册表”子区域，您可以设置基于已安装的应用程序搜索设备的标准：

- 应用程序名称

  在该下拉列表中，您可以选择应用程序。安装有指定应用程序的设备将包括在选择范围中。

- 应用程序版本

  在该输入字段中，您可以指定选定应用程序的版本。

- 供应商

  在该下拉列表中，您可以选择已安装应用程序的生产商。

- 应用程序状态

在该下拉列表中，您可以选择应用程序的状态（*已安装*、*未安装*）。已安装或未安装指定应用程序的设备，取决于所选状态，将被包含在分类。

- 根据更新查找

  如果启用此选项，则搜索操作将使用相关设备内应用程序更新的有关信息来执行。选中复选框后，“**应用程序名称**”、“**应用程序版本**”和“**应用程序状态**”字段将分别更改为“**更新名称**”、“**更新版本**”和“**状态**”。

  默认情况下已禁用该选项。

- 不兼容安全应用程序名称

  在该下拉列表中，您可以选择第三方安全应用程序。在搜索过程中，安装有指定程序的设备将包括在选择范围中。

- 应用程序标签

  在该下拉列表中，您可以选择应用程序标签。所有安装了描述中带有所选标签的应用程序的设备都被包含在设备分类。

- 应用到没有指定标签的设备

  如果启用此选项，分类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。

## 卡巴斯基应用程序详情

在“**卡巴斯基应用程序**”子区域，您可以配置基于所选的受管理应用程序包含设备到分类的标准：

- 应用程序名称

  在下拉列表中，可设置按 Kaspersky 应用程序名称执行搜索时在分类中包括设备的标准。

  列表仅提供管理员工作站上已安装管理插件的应用程序的名称。

  如果未选择任何应用程序，则将不会应用该标准。

- 应用程序版本

  在输入字段，可设置按 Kaspersky 应用程序版本号执行搜索时在分类中包括设备的标准。

  如果未指定版本号，则将不会应用该标准。

- 关键更新名称

  在输入字段中，可设置按应用程序名称或更新包编号执行搜索时在分类中包括设备的标准。

  如果字段留空，则将不会应用该标准。

- 应用程序状态

  在该下拉列表中，您可以选择应用程序的状态（*已安装*、*未安装*）。已安装或未安装指定应用程序的设备，取决于所选状态，将被包含在分类。

- 上一次模块更新

  您可以使用此选项来设置按这些设备上安装的程序模块上次更新的时间搜索设备的标准。

  如果选中此选框，则您可以在输入字段中指定执行这些设备上安装的程序模块的上一次更新的时间间隔（日期和时间）。

  如果清除此选框，则将不会应用标准。

  默认情况下已清除该选框。

- 设备通过 Kaspersky Security Center 14 管理

  在该下拉列表，您可以包含通过 Kaspersky Security Center Linux 管理的设备到分类：

  - **是**。应用程序包含通过 Kaspersky Security Center Linux 管理的设备。
  - **否**。应用程序在分类中包含不通过 Kaspersky Security Center Linux 管理的设备。
  - **未选择值**。将不应用标准。

- 安全应用程序已安装

  在该下拉列表，您可以包含已安装安全应用程序的设备到分类：

  - **是**。应用程序包含安装了安全应用程序的设备到分类。
  - **否**。应用程序在分类中包含未安装安全应用程序的设备。
  - **未选择值**。将不应用标准。

在“**反病毒保护**”子区域，您可以设置基于保护状态包含设备到分类的标准：

- 数据库发布日期

  如果选择此选项，您可以按反病毒数据库发布日期搜索客户端设备。在该输入字段中，您可以设置执行搜索的时间间隔。

  默认情况下已禁用该选项。

- 数据库记录数

  如果启用此选项，可以按数据库记录数量搜索客户端设备。在输入字段中，您可以设置反病毒数据库记录数的上限值和下限值。

  默认情况下已禁用该选项。

- 上一次扫描

如果启用此选项，您可以按上次病毒扫描时间来搜索客户端设备。在该输入字段中，您可以指定执行上一次病毒扫描的时段。

默认情况下已禁用该选项。

- 检测到的威胁

  如果启用此选项，您可以根据发现的病毒数量来搜索客户端设备。在输入字段中，您可以设置发现病毒总数的上限值和下限值。

  默认情况下已禁用该选项。

**应用程序组件**子区域包含在 Kaspersky Security Center 14 Web Console 中安装了相应管理插件的那些应用程序的组件列表。

在“**应用程序组件**”子区域，您可以指定根据所选应用程序组件的状态和版本号包含设备到分类的标准：

- 状态

  根据应用程序发送到管理服务器的组件状态搜索设备。您可以选择以下状态之一：*N/A*、*已停止*、*已暂停*、*正在开始*、*正在运行*、*已失败*、*未安装*、*不受授权许可支持*。如果安装在受管理设备上的应用程序的所选组件具有指定状态，设备被包含到设备分类。

  由应用程序发送的状态：

  - *已停止* - 组件被禁用且不在工作。
  - *已暂停* - 组件被暂停，例如，在用户在受管理应用程序上停止了保护后。
  - *正在启动* - 组件处于初始化进程中。
  - *运行中* - 组件被启用且在正常工作。
  - *已失败* - 组件操作中发生错误。
  - *未安装* - 当配置应用程序自定义安装时，用户未选择该组件以安装。
  - *不受授权许可支持* — 授权许可不涵盖所选组件。

  不同于其他状态，*N/A* 状态不由应用程序发送。该选项显示应用程序没有所选组件状态的信息。例如，这可能发生在所选组件不属于任何在设备上安装的应用程序时，或设备关闭时。

- 版本

  根据您在列表中选择的版本号搜索设备。您可以输入版本号，例如 `3.4.1.0`，然后指定所选组件是否必须具有相同、更早或更新版本。您也可以配置对所有版本的搜索，除了指定的值。

## 标签

在“**标签**”区域，您可以基于先前添加到受管理设备的描述的关键字（标签）配置包含设备到分类的标准：

如果至少一个指定的标签匹配则应用

如果启用此选项，搜索结果将显示包含带有所选标签的描述的设备。

如果禁用此选项，搜索结果将仅显示包含带有所有标签的描述的设备。

默认情况下已禁用该选项。

要将标签添加到条件，请单击**添加**按钮，然后通过单击**标签**输入字段来选择标签。指定是否在设备分类中包括或排除具有所选标签的设备。

- 必须被包含

  如果选择了该选项，搜索结果将显示带有包含了所选标签的描述的设备。要查找设备，您可以使用星号，它表示任何字符长度的字符串。

  默认情况下已选定该选项。

- 必须被排除

  如果选择了该选项，搜索结果将显示不带有包含了所选标签的描述的设备。要查找设备，您可以使用星号，它表示任何字符长度的字符串。

### 用户

在“**用户**”区域，您可以设置根据登录到操作系统的用户账户包含设备到分类的标准。

- 最后一次登录系统的用户

  如果启用此选项，您可以选择用于配置标准的用户账户。搜索结果包含所选用户上一次登录系统的设备。

- 登录系统至少一次的用户

  如果启用此选项，单击“**浏览**”按钮可以指定用户账户。搜索结果包含指定用户至少登录一次的设备。

## 从设备分类中导出设备列表

Kaspersky Security Center 允许您将设备分类中的设备信息保存在 CSV 或 TXT 文件中。

*要将设备列表从设备分类导出到文件：*

1. 从设备分类中打开包含设备的表格。
2. 您可以通过以下方式之一从表中导出有关设备的信息：
   - 导出选定的设备。

     选中所需设备旁边的复选框，然后单击**将行导出到 csv 文件**或**将行导出到 txt 文件**按钮，具体取决于您喜欢的导出格式。表中包含的有关所选设备的所有信息都将被导出到 TXT 或 CSV 文件。

- 导出当前页面上显示的所有设备。

  单击“**将行导出到 csv 文件**”或“**将行导出到 txt 文件**”按钮，具体取决于您喜欢的导出格式。您不需要从表中选择设备。当前页面上显示的所有设备信息都将被导出到 TXT 文件。

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到 CSV 或 TXT 文件。

# 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“**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。

# 更改 Kaspersky Security Center 14 Web Console 界面的语言

您可以选择 Kaspersky Security Center 14 Web Console 界面的语言。

*要更改界面语言：*

1. 在主菜单中，转到您的账户设置，然后选择**语言**。
2. 选择一种受支持的本地化语言。

# API 参考指南

本 Kaspersky Security Center OpenAPI 参考指南旨在帮助完成以下任务：

- 自动化和自定义。您可以将您可能不想手动处理的任务自动化。例如，作为管理员，您可以使用 Kaspersky Security Center OpenAPI 创建和运行脚本，这些脚本将有助于开发管理组的结构并使该结构保持最新。
- 自定义开发。使用 OpenAPI 可以开发客户端应用程序。

您可以使用屏幕右侧的搜索字段在 OpenAPI 参考指南中查找所需的信息。

OPENAPI 参考指南

## 脚本示例

OpenAPI 参考指南包含下表中列出的 Python 脚本示例。这些示例展示了如何调用 OpenAPI 方法并自动完成保护网络的各种任务，例如，创建"主要/从属"层级，在 Kaspersky Security Center 中运行任务，或分配分发点。您可以按原样运行示例，也可以基于示例创建您自己的脚本。

*要调用 OpenAPI 方法并运行脚本：*

1. 下载 KlAkOAPI.tar.gz 压缩文件。此压缩文件包括 KlAkOAPI 软件包和示例（您可以从压缩文件或 OpenAPI 参考指南中复制它们）。KlAkOAPI.tar.gz 存档也位于 Kaspersky Security Center 安装文件夹中。
2. 在安装了管理服务器的设备上安装来自 KlAkOAPI.tar.gz 压缩文件的 KlAkOAPI 软件包。

   您只能在安装了管理服务器和 KlAkOAPI 软件包的设备上调用 OpenAPI 方法、运行示例和您自己的脚本。

用户方案与 Kaspersky Security Center OpenAPI 方法示例之间的匹配

| 示例 | 示例目的 | 方案 |
| --- | --- | --- |
| Log KlAkParams | 您可以使用 `KlAkParams` 数据结构提取和处理数据。该示例展示了如何使用此数据结构。<br>该示例输出可以以不同的方式呈现。您可以获取数据以发送 HTTP 方法或在您的代码中使用它。 | 监控和报告 |
| 创建和删除"主要/从属"层次结构 | 您可以添加从属管理服务器，并建立"主要/从属"层次结构。或者，您可以断开从属管理服务器与层次结构的连接。 | 创建管理服务器层次结构，添加从属管理服务器和删除管理服务器层次结构 |
| 使用基于 Active Directory 单元的结构创建组层次结构 | 您可以通过使用连接网关连接到所需设备上的网络代理，然后将包含网络列表的文件下载到您的设备。 | 分发点和连接网关的调整 |
| 使用基于缓存的 Active Directory 单元的结构创建组层次结构 | 您可以连接到主管理服务器，从中下载所需的授权许可密钥，然后将此密钥传输到层次结构中包含的所有从属管理服务器。 | 受管理应用程序的授权许可 |
| 通过连接网关下载网络列表文件到指定设备 | 您可以创建不同的报告。例如，您可以使用此示例生成有效用户权限的报告。此报告描述了用户拥有的权限，具体取决于他或她的组和角色。<br>您可以下载 HTML、PDF 或 Excel 格式的报告。 | 生成和浏览报告 |
| 将主管理服务器存储库中存储的授权许可密钥安装到从属管理服务器上 | 您可以通过使用连接网关连接到所需设备上的网络代理，然后允许必要的任务。 | 手动启动任务 |
| 创建有效用户权限报告 | 您可以将受管理设备分配为分发点（以前称为更新代理）。 | 更新 Kaspersky 数据库和应用程序 |
| 为设备启动任务 | 您可以对管理组采取不同操作。该示例显示了如何执行以下操作：<br>• 获取"受管理设备"根组的标识符<br>• 在组层次结构中移动 | 配置管理服务器 |

| | | |
|---|---|---|
| | • 检索完整的、扩展的组层次结构以及它们的名称和嵌套 | |
| 基于 Active Directory 站点和服务创建 IP 子网 | 您可以找到以下信息：<br>• 任务进度历史<br>• 当前任务状态<br>• 不同状态的任务数<br>您还可以运行任务。默认情况下，示例在输出统计信息后运行任务。 | 管理任务 |
| 为组中的设备注册分发点 | 您可以创建任务。在示例中指定以下任务参数：<br>• 类型<br>• 运行方法<br>• 名称<br>• 将使用任务的设备组<br>默认情况下，示例创建了一个"显示消息"类型的任务。您可以为管理服务器的所有受管理设备运行此任务。如有需要，您可以指定自己的任务参数。 | 创建任务 |
| 对所有组进行枚举 | 您可以获得安装在管理服务器受管理设备上的 Kaspersky 应用程序的所有活动授权许可密钥的列表。该列表包含关于每个授权许可密钥的详细数据，例如名称、类型或到期日期。 | 查看使用中授权许可密钥的相关信息 |
| 枚举任务、查询任务统计信息和运行任务 | 您可以创建一个账户以进行进一步的工作。 | 添加内部用户账户 |
| 创建并运行任务 | 您可以根据所需参数创建应用程序类别。 | 创建含有手动添加内容的应用程序类别 |
| 枚举授权许可密钥 | 您可以使用 SrvView 类向管理服务器请求详细信息。例如，您可以使用此示例获取用户列表。 | 管理用户和用户角色 |

## 通过 OpenAPI 与 Kaspersky Security Center 交互的应用程序

一些应用程序通过 OpenAPI 与 Kaspersky Security Center 交互。例如，此类应用程序包括 Kaspersky Anti Targeted Attack Platform 或 Kaspersky Security for Virtualization。这也可以是您基于 OpenAPI 开发的自定义客户端应用程序。

通过 OpenAPI 与 Kaspersky Security Center 交互的应用程序连接到管理服务器。如果您配置了可连接到管理服务器的 IP 地址允许列表，请添加安装了使用 Kaspersky Security Center OpenAPI 的应用程序的设备的 IP 地址。要了解您使用的应用程序是否通过 OpenAPI 工作，请参阅此应用程序的帮助。

# 服务提供商最佳实践

该区域提供有关如何配置和使用 Kaspersky Security Center Linux 的信息。

该区域包含如何部署、配置和使用应用程序的建议，描述了解决应用程序操作中的典型问题的方法。

# 计划 Kaspersky Security Center Linux 部署

当在组织网络中计划 Kaspersky Security Center Linux 组件的部署时，您必须考虑到项目的大小和范围，尤其是以下因素：

- 设备总数
- MSP 客户端数量

一个管理服务器可以支持最多 50,000 台设备。如果组织网络中的设备总数超过 50,000，必须在服务提供商端部署多个管理服务器，并合并到一个方便集中管理的层级。

500 台虚拟服务器可以被创建在单一管理服务器，因此每 500 台 MSP 客户端需要一个单一管理服务器。

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 终端代理检查安全套接层（SSL）流量
- 在证书字段中指定所需值
- 提供所需的证书加密长度

# 提供到管理服务器的互联网访问

要允许客户端网络设备通过互联网访问管理服务器，您必须启用以下管理服务器端口：

- 13000 TCP—管理服务器 TLS 端口，用于连接部署在客户端网络的网络代理
- 8061 TCP—HTTPS 端口，用于使用 Kaspersky Security Center 14 Web Console 工具发布独立包
- 8060 TCP—HTTPS 端口，用于使用 Kaspersky Security Center 14 Web Console 工具发布独立包
- 13292 TCP—TLS 端口，仅在有需要被管理的移动设备时需要
- 8080 TCP—HTTPS 端口，用于 Kaspersky Security Center 14 Web Console

# Kaspersky Security Center Linux 标准配置

一个或几个管理服务器被部署到 MSP 服务器。管理服务器数量可以基于可用硬件、服务的 MSP 客户端总数或受管理设备总数来选择。

一个管理服务器可以支持最多 50,000 台设备。您必须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。

500 台虚拟服务器可以被创建在单一管理服务器，因此每 500 台 MSP 客户端需要一个单一管理服务器。

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允许您避免冗余策略和任务、处理整个受管理设备，使它们看起来是被单一管理服务器管理：例如，搜索设备、创建设备分类和创建报告。

在每个对应于 MSP 客户端的虚拟服务器上，您必须分配一个或几个分发点。如果 MSP 客户端和管理服务器通过互联网连接，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 Kaspersky 服务器直接下载更新，而不是从管理服务器。

如果 MSP 客户端网络的一些设备不能直接访问互联网，您必须切换分发点到连接网关模式。此种情况下，MSP 客户端网络中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 MSP 客户端网络，最好把该功能转给分发点。

管理服务器将无法发送通知到 MSP 客户端网络 NAT 以外的受管理设备的端口 15000 UDP。要解决该问题，最好在作为分发点并运行在连接网关模式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**选项）。如果分发点总数不超过 300 则持续连接模式可用。

MSP 客户可能想要管理员工的 Android 和 iOS设备。管理服务器通过 TLS、TCP 端口 13292 管理移动设备。

# 关于分发点

网络代理设备可以用作分发点。在该模式中，网络代理可以运行以下功能：

- 传输文件到客户端设备，包括：
  - 卡巴斯基数据库和软件模块更新

    更新可以从管理服务器或者从卡巴斯基服务器提取。在后一种情况下，"*将更新下载至分发点存储库*"任务必须为作为分发点的设备创建。
  - 第三方软件更新
  - 安装包
- 安装软件（包括网络代理初始化部署）到其他设备。
- 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。

在组织网络中部署分发点可以带来以下好处：

- 如果管理服务器作为更新源，则降低其负载。
- 在这种情况下，由于 MSP 客户端网络上的每个设备都没有必要访问卡巴斯基服务器或管理服务器以进行更新，因此优化互联网流量。
- 提供管理服务器到 MSP 客户端网络 NAT 之外的访问(与管理服务器相关)，这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和其所有子组中的所有设备。然而，作为分发点的设备不必须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被通过网关，而不是直接连接到管理服务器。该模式用在不允许在网络代理和管理服务器设备之间建立直接连接的情景。

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。

## 管理服务器层级

一个 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，Kaspersky Security Center Linux 管理服务器只能用作辅助服务器，由基于 Windows 的 Kaspersky Security Center 或 Kaspersky Security Center 云控制台的主管理服务器管理。

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和任务，这防止了重复设置。
- 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。

## 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。为了最大限度地相互隔离 MSP 客户端，我们建议您选择虚拟管理服务器作为要使用的功能。而且，为每个 MSP 客户端创建虚拟管理服务器使您能够提供客户端通过 Kaspersky Security Center 14 Web Console 进行网络管理的基本选项。

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。

# 部署和初始化设置

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 14 Web Console — 设计用于基本操作的管理服务器 Web 界面。您可以安装该组件到满足硬件和软件需求的设备。
- 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。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
- Kaspersky Security Center 14 Web Console 的安装
- 网络代理和企业设备上安全应用程序的安装

# 管理服务器安装建议

该部分包含了如何安装管理服务器的建议。该部分还提供了使用管理服务器上的共享文件夹以便部署网络代理到客户端设备的方案。

# 在失败转移集群上为管理服务器服务创建账户

在故障转移集群上开始部署 Kaspersky Security Center 之前，您必须为Kaspersky Security Center 服务创建账户。

为此，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”。

# 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。

对 DBMS 的建议和限制

| 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MySQL、MariaDB、PostgreSQL 或 Postgres Pro，请使用建议的设置以确保 DBMS 正常运行。

如果您使用 PostgreSQL、MariaDB 或 MySQL DBMS，则**事件**选项卡可能会显示所选客户端设备的不完整事件列表。当 DBMS 存储大量事件时就会发生这种情况。您可以通过执行以下操作之一来增加显示的事件数量：

- 删除不必要的事件。
- 减少不必要事件的存储期限。

要查看设备管理服务器上记录的完整事件列表，请使用报告。

## 指定管理服务器地址

当安装管理服务器时，您必须指定管理服务器的 DNS 名称或者静态 IP 地址。该地址将用作创建网络代理安装包时的默认地址。此后，您将可以通过使用 Kaspersky Security Center 14 Web Console 工具更改管理服务器主机地址；地址将不会在所创建的网络代理安装包中自动更改。

## 部署网络代理和安全应用程序

为了管理组织中的设备并保护它们免受安全威胁，您必须在每个受管理设备上安装网络代理和卡巴斯基安全应用程序。

有关保护部署的信息，请参阅部署网络代理和安全应用程序部分。

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）。

## 在客户端组织网络中配置保护

管理服务器安装完成后，Kaspersky Security Center 14 Web Console 启动并提示您通过相关向导执行初始化设置。当快速启动向导运行时，以下策略和任务在根管理组中被创建：

- Kaspersky Endpoint Security 策略

- 更新 Kaspersky Endpoint Security 的组任务
- 扫描 Kaspersky Endpoint Security 设备的组任务
- 网络代理策略
- 漏洞扫描任务(网络代理任务)
- 更新安装和漏洞修复任务(网络代理任务)

策略和任务使用默认设置创建，这对组织来说可能是不佳的或不合理的。因此，您必须检查所创建对象的属性并在必要时手动修改它们。

该部分包含了手动配置策略、任务和其他管理服务器设置的信息，以及分发点、构建管理组结构和任务层级以及其他设置的信息。

# Kaspersky Endpoint Security 策略的手动设置

本节提供关于如何配置 Kaspersky Endpoint Security 策略的建议，该策略由快速启动向导创建。您可以在策略属性窗口中执行设置。

编辑设置时，请记住您可以锁定或解锁设置以禁止或允许在工作站上编辑其值。

## 在高级威胁防护区域配置策略

对于该区域设置的完整描述，请参考 Kaspersky Endpoint Security for Windows 文档。

在**高级威胁防护**区域中，您可以为 Kaspersky Endpoint Security for Windows 配置卡巴斯基安全网络的使用。您还可以配置 Kaspersky Endpoint Security for Windows 模块，例如行为检测、漏洞利用防御、主机入侵防御和修复引擎。

在**卡巴斯基安全网络**子区域，建议您启用**卡巴斯基安全网络**选项。使用此选项有助于重新分发和优化网络流量。如果“**卡巴斯基安全网络**”选项被禁用，您可以启用直接“使用 KSN 服务器”。

## 在关键威胁防护部分配置策略

对于该区域设置的完整描述，请参考 Kaspersky Endpoint Security for Windows 文档。

在策略属性窗口的**基本威胁防护**区域，建议您在**防火墙**和**文件威胁防护**子区域指定附加设置。

**防火墙**子区域包含允许您控制客户端设备上应用程序的网络活动的设置。客户端设备使用分配了“公共”、“本地”或“受信任”状态的网络。根据网络状态，Kaspersky Endpoint Security 可以选择允许或拒绝设备上的网络活动。向组织添加新网络时，您必须为其分配适当的网络状态。例如，如果客户端设备是笔记本电脑，则建议使用公共或受信任的网络，因为笔记本电脑有时连接的不是本地网络。在**防火墙**子区域，您可以检查是否为组织所用的网络分配了正确的状态。

*要查看网络列表：*

1. 在策略属性中，转到**基本威胁防护 → 防火墙**。
2. 在**可用网络**区域中，单击**设置**按钮。
3. 在打开的**防火墙**窗口中，转到**网络**选项卡以查看网络列表。

在**文件威胁防护**子区域，您可以禁用网络驱动器扫描。网络驱动器扫描可以显著提高网络驱动器负载。在文件服务器上执行间接扫描更方便。

*要禁用网络驱动器扫描：*

1. 在策略属性中，转到**基本威胁防护 → 文件威胁防护**。
2. 在**安全级别**区域中，单击**设置**按钮。
3. 在打开的**文件威胁防护**窗口中，在**常规**选项卡，清空**所有网络驱动器**复选框。

## 在常规设置部分配置策略

对于该区域设置的完整描述，请参考 Kaspersky Endpoint Security 文档。

描述了附加配置操作，我们建议您在 Kaspersky Endpoint Security 的策略属性窗口中执行，在“**常规设置**”区域。

### “常规设置”区域，“报告和存储”子区域

在“**到管理服务器的数据传输**”区域中，请注意“**关于已启动的应用程序**”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)。因此，如果**关于已启动的应用程序**复选框依然在顶级策略中被选中，它必须被清空。

### “常规设置”区域，“界面”子区域

如果组织网络中的威胁防护必须通过管理控制台集中管理，则必须禁用在工作站上显示 Kaspersky Endpoint Security 用户界面（通过清除“**与用户交互**”区域中的“**显示应用程序界面**”复选框），并启用密码保护（通过选中“**密码保护**”区域中的“密码保护”复选框）。

## 在事件配置区域配置策略

在**事件配置**区域，您应该禁用保存任何事件到管理服务器，除了以下事件：

- 在**严重**选项卡上：
  - *应用程序自动运行被禁用*
  - *访问被拒绝*
  - *已禁止应用程序启动*

- *无法清除*
- *违反了最终用户授权许可协议*
- *无法加载加密模块*
- *不能同时启动两项任务*
- *检测到活动威胁。应该启动高级清除*
- *检测到网络攻击*
- *未更新所有组件*
- *激活错误*
- *启用便携模式时出错*
- *与 Kaspersky Security Center 交互时出错*
- *禁用便携模式时出错*
- *更改应用程序组件时出错*
- *应用文件加密/解密规则时出错*
- *无法应用策略*
- *进程已终止*
- *网络活动已阻止*

- 在**功能失败**选项卡上：*任务设置无效，未应用设置*
- 在**警告**选项卡上：
  - *"自我保护"被禁用*
  - *备用密钥不正确*
  - *用户选择了退出加密策略*
- 在"**信息**"选项卡上：*禁止应用程序在测试模式下启动*

## Kaspersky Endpoint Security 更新组任务的手动设置

如果管理服务器作为更新源，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**"，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，时段性计划将是最优的并被推荐给 Kaspersky Endpoint Security 组更新任务。此种情况下，随机时段值应该被设置为 1 小时。

## 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。

## 计划“查找漏洞和所需更新”任务

快速启动向导为网络代理创建*查找漏洞和所需更新*任务。默认情况下，为任务分配**在星期二下午 7:00 运行**计划，并且取消选中**运行错过的任务**复选框。

如果组织的工作规则要在此时关闭所有设备，*查找漏洞和所需更新*任务将在设备再次开启时运行，也就是，在星期三早晨。此活动可能不是必须的，因为漏洞扫描可能增加 CPU 和磁盘子系统负载。您必须基于组织的工作规则为该任务设置最方便的计划。

## 更新安装和漏洞修复组任务的手动设置

该快速启动向导为网络代理创建更新安装和漏洞修复组任务。默认情况下，任务设置为在每天 01:00 AM 自动随机运行，并且未启用“**运行错过的任务**”选项。

如果组织工作规则整夜关闭所有设备，则更新安装将永远不会运行。您必须基于组织的工作规则为漏洞扫描任务设置最方便的计划。值得注意的是，更新的安装可能需要重启设备。

## 建立管理组结构和分配分发点

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。在这种情况下，策略的范围通过（例如）设备标签或者用户角色来设置。

- 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 MSP 客户端采用的网络拓扑，以下标准配置可以被应用到管理组结构：

- 单一办公室
- 多个独立的小型办公室

## 标准 MSP 客户端配置：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。

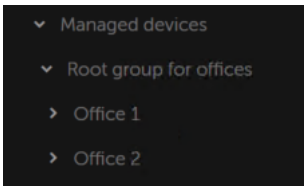
有以下构建管理组结构的方法：

- 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 实用程序或者 traceroute 实用程序进行跟踪。

## 标准 MSP 客户端配置：多个小远程办公室

该标准配置用于一定数量的小远程办公室，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。

# 策略层级，使用策略配置文件

本部分提供有关如何应用策略到管理组设备的信息。本部分还提供有关策略配置文件的信息。

## 策略层级

在 Kaspersky Security Center Linux，您使用策略来定义一个单一设置集到多个设备。例如，应用程序 P 的策略范围，为管理组 G 定义，包含安装了应用程序 P 的部署在组 G 和其子组的受管理设备， 除了在属性中清空了**从父组继承**复选框的子组。

策略通过设置旁边的锁图标（🔒）不同于本地设置。如果一个设置（或设置组）在策略属性中被锁定，您必须首先在创建有效设置时使用该设置（或设置组），其次，必须将设置或设置组写入 downstream 策略。

在设备上创建有效设置可以如此描述：所有未锁定的设置值必须来自策略，然后被本地设置覆盖，然后结果集被来自策略的锁定设置的值覆盖。

相同应用程序的策略通过管理组层级互相影响：来自 upstream 策略的锁定设置覆盖来自 downstream 策略的相同设置。

漫游用户有特殊策略。该策略在设备切换到漫游模式时在设备上生效。漫游策略不通过管理组层级影响其他策略。

## 策略配置文件

仅通过管理组层级应用策略到设备可能在许多环境下不方便。有必要创建单一策略的几个实例，这些实例对于不同的管理组在一两个设置上有所不同，可以在将来同步这些策略的内容。

为帮助您避免此类问题，Kaspersky Security Center Linux 支持*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，并在客户端设备（计算机或移动设备）上活动。激活配置文件会修改配置文件激活之前已在计算机上活动的策略设置。这些设置将使用已在配置文件中指定的值。

以下限制被施加在策略配置文件：

- 策略可以包含最多 100 个配置文件。
- 策略配置文件不能包含其他配置文件。
- 策略配置文件不能包含通知设置。

## 配置文件内容

策略配置文件包含以下组成部分：

- Name。带有相同名称的配置文件通过管理组层级互相影响。
- 策略设置子集。不同于包含所有设置的策略，配置文件仅包含实际所需的设置(锁定设置)。
- 激活条件是设备属性的逻辑表达。配置文件仅在配置文件激活条件为真是活动(补充策略)。在其他所有情况，配置文件是非激活和忽略的。以下设备属性可以被包含在逻辑表达：
  - 漫游模式状态。
  - 网络环境属性 — 网络代理连接的活动规则的名称。
  - 设备上指定标签的出现和消失。

- 设备在活动目录组织单元（OU）上的分配：明确(设备在指定 OU 中)，或不明确(设备是 OU，以嵌套级别包含在指定 OU)。
- 设备在活动目录安全组中的成员关系（明确或不明确）。
- 活动目录安全组中设备所有者的成员关系（明确或不明确）。

- 配置文件禁用复选框。被禁用的配置文件总是被忽略，并且它们的激活条件不被验证。
- 配置文件优先级。不同配置文件的激活条件是独立的，因此几个配置文件可以一起激活。如果活动配置文件包含设置的非重叠集合，将不会发生问题。然而，如果两个活动配置文件包含不同的相同设置的值，将发生歧义。该歧义可以通过策略优先级避免：歧义变量的值将来自高优先级的配置文件(在配置文件列表中评级较高)。

### 策略通过层级互相影响时的配置文件行为

带有相同名称的配置文件根据策略合并规则合并到一起。upstream 策略的配置文件比 downstream 策略的配置文件拥有更高优先级。如果编辑设置在 upstream 策略中被禁止(锁定)，downstream 策略使用 upstream 策略的配置文件激活条件。如果编辑设置在 upstream 策略中被允许，downstream 策略的配置文件激活条件被使用。

既然策略配置文件可能在激活条件中包含"**设备已离线**"属性，配置文件完全替换漫游用户策略功能，后者将不被支持。

漫游用户的策略可能包含配置文件，但是它们配置文件仅可以在设备切换到漫游模式后激活。

## 任务

Kaspersky Security Center 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

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 14 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 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。

## 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“**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、根据标准方案分配网络代理。

## 软件分类

监控应用程序运行的主要工具是 *Kaspersky 类别*(也叫 *KL 类别*)。KL 类别帮助 Kaspersky Security Center Linux 管理员简化软件分类和减少到受管理设备的流量。

用户类别必须仅对无法被分类成现有 KL 类别的应用程序创建(例如，对于自定义软件)。基于应用程序安装包(MSI)或带有安装包的文件夹创建的用户类别。

如果有未通过 KL 类别分类的大软件集可用，最好创建一个自动更新的类别。每次对包含分发包的文件夹进行修改时，可执行文件的校验和将被自动添加到该类别。

## 管理服务器设置的备份和恢复

管理服务器设置和其数据库的备份通过备份任务和 klbackup 实用工具执行。备份副本包括与管理服务器有关的所有主要设置和对象，例如证书、受管理设备上驱动器加密的主密钥、各种授权许可的密钥、管理组的结构及其所有内容、任务、策略等。使用备份副本，您可以尽快恢复管理服务器的操作，为此花费十几分钟到几个小时。

如果没有备份副本可用，失败可能导致证书和管理服务器设置的不可挽回的损失。这将导致要重新开始配置 Kaspersky Security Center Linux，并在组织网络上重新执行网络代理初始化部署。所有受管理设备驱动器加密主密钥也将丢失，导致 Kaspersky Endpoint Security 设备上不可挽回的加密数据丢失。因此，不要忽略使用标准备份任务对管理服务器进行定期备份。

快速启动向导为管理服务器设置创建备份任务，并将其设置为每天凌晨 4:00 运行。备份副本默认保存在文件夹 %ALLUSERSPROFILE%\Application Data\KasperskySC 中。

因为备份副本包含重要数据，备份任务和 klbackup 实用工具用于备份副本密码保护。默认下，备份任务使用空密码创建。您必须在备份任务属性中设置密码。忽略该需求将导致管理服务器证书所有密钥、授权许可密钥和受管理设备驱动器加密主密钥保持未加密。

除了常规备份，您必须在每个显著更改之前创建备份副本，包括管理服务器升级和补丁的安装。

从备份副本的恢复使用管理服务器实例上刚刚安装的与备份副本具有相同或更新版本的实用工具 klbackup 来执行。

对于要执行还原的管理服务器的实例，必须使用相同类型和相同版本或更新版本的 DBMS。管理服务器版本可以相同（带有相同或更新补丁）或更新。

这部分描述了恢复管理服务器设置和对象的标准方案。

## 管理服务器设备不可操作

如果管理服务器设备由于失败而不可操作，建议您执行以下操作：

- 新管理服务器必须分配相同的地址：DNS 名称或静态 IP(取决于部署网络代理时的设置)。
- 安装管理服务器，使用相同类型、相同版本（或更新）的 DBMS。您可以安装带有相同（或更新）补丁的相同（或更新）版本的服务器。安装后，不要通过向导执行初始化安装。
- 运行 klbackup 实用程序并执行恢复。

# 管理服务器设置或数据库被损坏

如果管理服务器由于设置或数据库损坏（例如断电）而不可操作，建议您使用以下恢复方案：

1. 扫描被损坏设备上的文件系统。
2. 卸载管理服务器的不可操作版本。
3. 重新安装管理服务器，使用相同类型、相同版本（或更新）的 DBMS。您可以安装带有相同（或更新）补丁的相同（或更新）版本的服务器。安装后，不要通过向导执行初始化安装。
4. 运行 klbackup 实用程序并执行恢复。

禁止用除了通过 klbackup 实用工具的其他方法恢复管理服务器。

任何试图通过第三方软件恢复管理服务器的操作都将不可避免地导致 Kaspersky Security Center Linux 分发节点上的数据的不一致和应用程序操作不正常。

# 关于漫游用户的连接配置文件

便携式电脑（也叫“设备”）的漫游用户需要更改连接到管理服务器的方法或者根据当前设备在企业网络中的位置在管理服务器之间进行切换。

连接配置文件仅支持运行 Windows 和 macOS 的设备。

## 使用单一管理服务器的不同地址

网络代理设备从组织网络或内部网可以连接到管理服务器。该情况可能需要网络代理使用不同的地址以连接到管理服务器：对于互联网连接的外部管理服务器地址和对于内部网络连接的内部管理服务器地址。

为此，您必须添加配置文件(为了从互联网连接到管理服务器)到网络代理策略。在策略属性中添加配置文件（**连接**区域，**连接配置文件**子区域）。在配置文件创建窗口，您必须禁用“**仅用来接收更新**”选项，并选择“**与此配置文件中指定的管理服务器设置同步连接设置**”选项。如果您使用连接网关访问管理服务器（例如，在“互联网访问：DMZ 中作为连接网关的网络代理”部分描述的 Kaspersky Security Center Linux 配置中），您必须在连接配置文件的对应字段指定连接网关地址。

## 根据当前网络在管理服务器之间进行切换

如果组织有带有多个管理服务器的多个办公室，并且一些网络代理设备在期间进行移动，您需要网络代理连接到设备所在的本地网络中的管理服务器。

此种情况下，您必须为每个办公室在网络代理策略属性中创建连接管理服务器的配置文件，除了原始归属管理服务器所在的主办公室。您必须在连接配置文件中指定管理服务器地址并启用或禁用“**仅用来接收更新**”选项：

- 在使用本地服务器下载更新时，如果您需要网络代理与归属管理服务器同步，则选择该选项。
- 如果网络代理必须被本地管理服务器完全管理，则禁用此选项。

此后，您必须设置切换到新创建的配置文件的条件：每个办公室至少一个条件，除了归属办公室。每个条件的目的包括办公室网络环境条目的检测。如果条件是真，对应配置文件被激活。如果没有条件是真，网络代理切换到归属管理服务器。

# 远程访问受管理设备

该部分提供了远程访问受管理设备的信息。

# 使用“不要断开与管理服务器的连接”选项提供受管理设备和管理服务器之间的持续连接

如果您不使用推送服务器，则 Kaspersky Security Center Linux 不提供受管理设备和管理服务器之间的持续连接。受管理设备上的网络代理定期建立连接并与管理服务器同步。同步会话之间的时间间隔定义在网络代理策略中。如果需要提前同步，管理服务器（或分发点，如果正在使用）会通过 IPv4 或 IPv6 网络将签名的网络数据包发送到网络代理的 UDP 端口。默认情况下，端口号指定为 15000。如果在管理服务器和受管理设备之间无法通过 UDP 建立连接，则在同步间隔内的下次网络代理和管理服务器常规连接时将运行同步。

如果没有网络代理和管理服务器之间的早期连接，某些操作将无法执行，例如运行和停止本地任务或者接收受管理应用程序的统计信息。要解决此问题，如果您不使用推送服务器，可以使用“**不断开与管理服务器的连接**”选项以确保受管理设备和管理服务器之间存在持续连接。

*要提供客户端设备与管理服务器之间的持续连接：*

1. 在主菜单中，转到“**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，单击带有所需设备名称的链接。
3. 在设备属性窗口的**常规**部分中，启用**不断开与管理服务器的连接**选项。
   持续连接在受管理设备和管理服务器之间被建立。

选中“**不断开与管理服务器的连接**”选项时的最大设备总数为 300。

# 关于检查设备和管理服务器之间的连接时间

在关闭设备时，网络代理通知管理服务器该事件。在 Kaspersky Security Center 14 Web Console中，该设备显示为已关闭。然而，网络代理无法通知管理服务器所有此类事件。因此，管理服务器会定期分析每台设备的“**连接到管理服务器**”属性（该属性的值显示在 Kaspersky Security Center 14 Web Console 的“设备”属性中的“**常规**”区域中），并将它与网络代理当前设置中的同步间隔相比较。如果一台设备在超过三次成功的同步间隔后未响应，该设备被标记为已关闭。

# 关于强制同步

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，一些情况下，管理员需要准确知道是否同步已经在指定设备上执行。

受管理设备的属性窗口包含强制同步按钮。当 Kaspersky Security Center 14 Linux 执行同步命令时，管理服务器会试图连接到设备。如果该尝试成功，强制同步将被执行。否则，同步将仅在网络代理与管理服务器的下一次计划连接后被强制。

# Kaspersky Security Center 14 Web Console 与其他 Kaspersky 解决方案之间的集成

本节介绍如何配置从 Kaspersky Security Center 14 Web Console 访问其他 Kaspersky 应用程序，例如 Kaspersky Anti Targeted Attack (KATA) 和 Kaspersky Endpoint Detection and Response (KEDR)。此部分还介绍了如何配置导出到 SIEM 系统。

## 配置到 KATA / KEDR Web Console 的访问

Kaspersky Anti Targeted Attack (KATA) 和 Kaspersky Endpoint Detection and Response (KEDR) 是 Kaspersky Anti Targeted Attack Platform 的两个功能块。您可以通过 Kaspersky Anti Targeted Attack Platform 的 Web Console (KATA / KEDR Web Console) 管理这些功能块。如果您使用 Kaspersky Security Center 14 Web Console 和 KATA/KEDR Web Console，您可以从 Kaspersky Security Center 14 Web Console 界面直接配置到 KATA/KEDR Web Console 的访问。

*要配置到 KATA / KEDR Web Console 的访问：*

1. 在应用程序主窗口中，单击屏幕上方的**"控制台设置"**。
2. 在下拉菜单中，选择**整合**。
   "控制台设置"窗口将开启。
3. 在"**整合**"选项卡上的"**KATA / KEDR Web Console 的网址**"字段中输入 KATA/KEDR Web Console 的 URL。
4. 单击"**保存**"按钮。

"**高级管理**"下拉列表即添加到主应用程序窗口中。您可以使用该菜单打开 KATA / KEDR Web Console。单击"**高级网络安全**"后，浏览器中将打开一个新选项卡，其中包含您指定的 URL。

# 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（请参见应用程序支持生命周期页面）。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。

# 获取管理服务器的转储文件

管理服务器的转储文件包含某一时间点的管理服务器进程的所有信息。管理服务器的转储文件存储在 /var/lib/systemd/coredump 目录中。只要 Kaspersky Security Center 正在使用，转储文件就会被存储，当删除时，转储文件会被永久删除。文件不会自动发送给卡巴斯基。

如果管理服务器崩溃，您可以联系卡巴斯基技术支持团队，技术支持专家可能会要求您发送管理服务器的转储文件以供卡巴斯基进一步分析。

转储文件可能包含个人数据。我们建议在将信息发送给卡巴斯基之前，保护信息免受未经授权的访问。

# 有关程序的信息源

## Kaspersky 网站上的 Kaspersky Security Center 页面

在卡巴斯基网站的 Kaspersky Security Center 页面上，您可以查看有关应用程序、程序功能和特性的一般信息。

## 知识库中的 Kaspersky Security Center 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 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。

# 已知问题

Kaspersky Security Center Linux 具有许多对于应用程序运行并不重要的限制：

- 如果列表包含 20 个以上条目（在此情况下，条目显示在多页上），您选择**全部选择**复选框，网页控制台将只选择显示在当前页面上的条目。
- 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 不会要求您输入凭据。
- 在任务计划中设置"**立即**"选项并保存更改后，"*更改管理服务器*"任务不会自动启动。
- 如果您在不同的浏览器中打开 Kaspersky Security Center 14 Web Console，并在管理服务器属性窗口中下载管理服务器证书文件，则下载的文件具有不同的名称。
- 当您尝试从"**备份**"存储库（**操作 → 存储库 → 备份**）恢复对象或将该对象发送到卡巴斯基时，会发生错误。
- Kaspersky Endpoint Security for Linux 的父策略中锁定的设置会被继承，而子策略中锁定的设置不会被继承。
- 从受管理设备发送到管理服务器的硬件信息可能不完整；某些硬件项目可能未指定。
- 可以删除您添加到 Kaspersky Endpoint Security for Linux 策略中的应用程序控制功能的应用程序类别。
- 具有多个网络适配器的受管理设备会将未用于连接到管理服务器的网络适配器的 MAC 地址信息发送到管理服务器。
- 如果在响应文件中的 webConsoleAccount 和 managementServiceAccount 参数中指定自定义用户账户来安装 Kaspersky Security Center 14 Web Console，并且这些账户属于不同的安全组，则 Kaspersky Security Center 14 Web Console 在安装后将不起作用。
- 在 Astra Linux 64 位版中，klnagent-astra 软件包不能使用 klnagent64_14 软件包升级：旧软件包 klnagent64-astra 将被删除，将安装新软件包 klnagent64 而不是升级，因此将为具有 klnagent64_14 软件包的设备添加新图标。您可以删除此设备的旧图标。

# 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 System Health Validator (SHV)

在 Kaspersky Security Center 和 Microsoft NAP 并行运行时，用于检查操作系统运行能力的 Kaspersky Security Center 的一个组件。

## Kaspersky Security Center Web Server

Kaspersky Security Center 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 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 Security Center 管理员

通过 Kaspersky Security Center 远程集中管理系统来管理应用程序操作的人。

## 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 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 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 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 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 14 Web Console 的设备。该组件提供了 Kaspersky Security Center 管理界面。

管理员工作站用于配置和管理 Kaspersky Security Center 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 14 Web Console。

## 管理服务器

Kaspersky Security Center 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 14 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 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 组件，用于管理客户组织网络的保护系统。

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

## 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。

## 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。

## 额外（或备用）授权许可密钥

证明程序的使用权限、但是目前尚未使用的密钥。

# 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 Jabber、Cisco Systems、IOS 是 Cisco Systems, Inc. 和/或其附属公司在美国和其他特定国家/地区的注册商标。

Citrix、XenServer 是 Cloud Software Group, Inc. 和/或其子公司在美国和/或其他国家/地区的注册商标或商标。

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。

Radmin 是 Famatech 的注册商标。

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、Xeon 是 Intel Corporation 或其子公司的商标。

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。

Logitech 是 Logitech 在美国和/或其他国家/地区的注册商标或商标。

Microsoft、Active Directory、ActiveSync、BitLocker、Excel、Forefront、Internet Explorer、InfoPath、Hyper-V、Microsoft Edge、MultiPoint、MS-DOS、PowerShell、PowerPoint、SharePoint、SQL Server、Office 365、OneNote、Outlook、Skype、Tahoma、Visio、Win32、Windows、Windows PowerShell、Windows Media、Windows Server、Windows Phone、Windows Vista 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。

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。