kaspersky

# Kaspersky Security Center 16.3 Linux

© 2026 AO Kaspersky Lab

# 目录


Kaspersky Security Center Linux 帮助
新增功能
已修复问题
关于 Kaspersky Security Center Linux
- 分发包
- 硬件和软件要求
  - 管理服务器要求
  - Web Console 要求
  - 网络代理要求
- 兼容的卡巴斯基应用程序和解决方案
- 关于 Kaspersky Security Center Linux 组件的兼容性
- Kaspersky Security Center 的比较：基于 Windows 与基于 Linux
- 关于 Kaspersky Security Center 云控制台

架构和基本概念
- 架构
- Kaspersky Security Center Linux 管理服务器部署图表和 Kaspersky Security Center Web Console
- Kaspersky Security Center Linux 使用的端口
- Kaspersky Security Center Web Console 使用的端口
- 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
  - Kaspersky Security Center Linux 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政策的关系
  - 分发点
  - 连接网关
  - 虚拟管理服务器

数据流量和端口使用的 schema
- LAN 中的管理服务器和受管理设备
- 局域网中的主管理服务器和两个从属管理服务器
- 管理服务器位于 LAN、受管理设备位于互联网、反向代理使用中
- 管理服务器位于 LAN、受管理设备位于互联网、连接网关使用中

管理服务器位于 DMZ、受管理设备位于互联网
Kaspersky Security Center Linux 组件和安全应用程序的交互：更多信息
交互模式中的惯例
管理服务器和 DBMS
管理服务器和客户端设备：管理安全应用程序
通过分发点在客户端设备上升级软件
管理服务器层级：主管理服务器和从属管理服务器
DMZ 中带有从属管理服务器的管理服务器层级
管理服务器、网段连接网关和客户端设备
管理服务器和 DMZ 中的两台设备：连接网关和客户端设备
管理服务器和 Kaspersky Security Center Web Console
启动
强化指南
加固检查清单
管理服务器部署
连接安全
账户和身份验证
管理服务器保护的管理
管理客户端设备保护
配置受管理应用程序的保护
管理服务器维护
事件传输到第三方系统
第三方信息系统安全建议
有关使用卡巴斯基安全应用程序的建议
场景：验证 MySQL 服务器
场景：验证 PostgreSQL 服务器
部署准备
选择 Kaspersky Security Center Linux 的配置
标准配置：单一办公室
标准配置：由自己管理员运行的几个大规模办公室
标准配置：多个小远程办公室
选择企业保护结构
部署保护系统的常规方案
选择 DBMS
提供到管理服务器的互联网访问
互联网访问：本地网络上的管理服务器
互联网访问：DMZ 中的管理服务器
安装
配置与 Kaspersky Security Center Linux 配合使用的 MariaDB x64 服务器
配置与 Kaspersky Security Center Linux 配合使用的 PostgreSQL 或 Postgres Pro 服务器
配置与 Kaspersky Security Center Linux 配合使用的 MySQL x64 服务器
准备高可用性 DBMS 集群以与 Kaspersky Security Center Linux 配合使用
安装 Kaspersky Security Center Linux
以静默模式安装 Kaspersky Security Center Linux
在封闭软件环境模式下在 Astra Linux 上安装 Kaspersky Security Center Linux

安装 Kaspersky Security Center Web Console
Kaspersky Security Center Web Console 安装参数
在封闭软件环境模式下在 Astra Linux 上安装 Kaspersky Security Center Web Console
使用脚本安装Kaspersky Security Center for Linux
Kaspersky Security Center Linux 故障转移集群部署
Kaspersky Security Center Linux 故障转移集群。部署方案
Kaspersky Security Center Linux 故障转移集群。
方案：部署 Kaspersky Security Center Linux 故障转移集群
Kaspersky Security Center Linux 故障转移集群。硬件和软件要求
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 Linux 障转移集群节点上安装 Kaspersky Security Center Linux
手动启动和停止集群节点
重新安装故障转移集群节点
安装 Kaspersky Security Center Web Console，其已连接到安装在 Kaspersky Security Center Linux 故障转移集群节点上的管理服务器
地理分布式 Kaspersky Security Center Linux 故障转移集群
运行安装有 PostgreSQL数据库管理系统的 Ubuntu 的地理分布式集群
准备集群节点的文件系统
配置复制集群文件系统
在集群节点上安装和配置 Corosync 和 Pacemaker
安装和配置 PostgreSQL DBMS
在地理分布式故障转移集群节点上安装 Kaspersky Security Center Linux
运行安装有 Platform V Pangolin 数据库管理系统的 SberLinux 的地理分布式集群
准备集群节点的文件系统
配置复制集群文件系统
在集群节点上安装和配置 Corosync 和 Pacemaker
安装和配置 Platform V Pangolin 数据库管理系统
在地理分布式故障转移集群节点上安装 Kaspersky Security Center Linux
在地理分布式故障转移集群节点上安装 Kaspersky Security Center Web Console
使用 DBMS 的账户
配置使用 MySQL 和 MariaDB 的 DBMS 账户
配置使用 PostgreSQL 和 Postgres Pro 的 DBMS 账户
在 MySQL 或 MariaDB DBMS 中将数据从共享表空间移动到每个表一个文件的表空间
用于 Kaspersky Security Center Linux 的证书
关于 Kaspersky Security Center 证书
对 Kaspersky Security Center Linux 中使用的自定义证书的要求
重新颁发 Kaspersky Security Center Web Console 的证书
替换 Kaspersky Security Center 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
重新颁发 Web 服务器证书
将默认 IAM 证书更改为自定义证书
将管理服务器地址添加到 IAM 服务器配置中
定义共享文件夹

登录到 Kaspersky Security Center Web Console 并登出
Kaspersky Security Center Web Console 界面
更改 Kaspersky Security Center Web Console 界面的语言
更改 Kaspersky Security Center Web Console 主页
添加和移除书签
移除 Kaspersky Security Center Web Console
快速启动向导
步骤 1：指定互联网连接设置
步骤 2：下载所需更新
步骤 3：选择要保护的资产
步骤 4：选择解决方案中的加密
步骤 5：配置受管理应用程序的插件安装
步骤 6：下载分发包并创建安装包
步骤 7：配置卡巴斯基安全网络
步骤 8：选择应用程序激活方法
步骤 9：指定第三方更新管理设置
步骤 10：创建基本的网络保护配置
步骤 11：配置邮件通知
步骤 12：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：重启管理
步骤 8：安装前删除不兼容的应用程序
步骤 9：移动设备到受管理设备
步骤 10：选择访问设备的账户
步骤 11：开始安装
升级 Kaspersky Security Center Linux
将 Kaspersky Security Center Linux 从 16 版本或更高版本进行升级
使用安装文件将 Kaspersky Security Center Linux 从 16 或更高版本进行升级
通过备份将 Kaspersky Security Center Linux 从 16 版本或更高版本进行升级。
在 Kaspersky Security Center Linux 故障转移集群节点上将 Kaspersky Security Center Linux 从版本 16 或者更高版本进行升级
将 Kaspersky Security Center Linux 从 15.4 版本或更早版本进行升级
使用安装文件将 Kaspersky Security Center Linux 从 15.4 或更早版本进行升级
通过备份将 Kaspersky Security Center Linux 从 15.4 或更早版本进行升级。
在 Kaspersky Security Center Linux 故障转移集群节点上将 Kaspersky Security Center Linux 从版本 15.4 或者更早版本进行升级
升级 Kaspersky Security Center Web Console
在封闭软件环境模式下在 Astra Linux 上安装 Kaspersky Security Center Web Console
迁移到 Kaspersky Security Center Linux
使用管理服务器数据备份迁移到 Kaspersky Security Center Linux
教程视频：使用管理服务器数据备份迁移到 Kaspersky Security Center Linux

通过迁移向导迁移到 Kaspersky Security Center Linux
从 Kaspersky Security Center Windows 导出组对象
将导出文件导入到 Kaspersky Security Center Linux
将受管理设备切换为受 Kaspersky Security Center Linux 管理
配置管理服务器
配置管理服务器连接地址
配置 Kaspersky Security Center Web Console 到管理服务器的连接
配置用于连接到 Kaspersky Security Center Linux 的 IP 地址允许列表
指定管理服务器的互联网连接设置
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
管理虚拟管理服务器
创建虚拟管理服务器
启用或禁用虚拟管理服务器
为虚拟管理服务器分配管理员
更改客户端设备的管理服务器
删除虚拟管理服务器
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
将管理服务器移动至其他设备
更改管理服务器名称
通过添加新的 DNS 记录来保持连接
通过切换到基于 IP 地址的连接来保持连接
更改服务器名称后恢复中断的连接
更改 DBMS 凭据
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
使用 klbackup 实用程序切换受管理设备至另一台管理服务器的管理下
使用 MySQL 或 MariaDB 时备份和恢复管理服务器数据
管理服务器维护
删除管理服务器层级
访问公共 DNS 服务器
配置界面
到管理服务器的加密连接
使用 TLS 的加密通信
用于与外部服务交互的网络设置
子网全局列表
使用 klscmodchk 和 integrity_checker 实用程序检查模块的完整性
发现网络设备
情景：发现网络设备
Windows 网络轮询
IP 范围轮询
添加和修改 IP 范围
Zeroconf 轮询
域控制器轮询

身份验证和连接到域控制器
配置 Samba 域控制器
设备清单
添加有关新设备的信息
配置用于定义企业设备的标准
在客户端设备上使用 VDI 动态模式
在网络代理安装包属性中启用 VDI 动态模式
将组成 VDI 的设备移至管理组
管理客户端设备
受管理设备设置
手动检查客户端设备与管理服务器之间的连接。Klnagchk 工具
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
关于集群和服务器阵列
集群或服务器阵列的属性
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
在 DMZ 中添加连接网关作为分发点
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
关于设备状态
配置设备状态切换
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
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
数据加密和保护
查看加密驱动器列表
查看加密事件列表
创建和查看加密报告
授予对处于离线模式的加密驱动器的访问权限
在管理服务器之间传输加密密钥
更改客户端设备的管理服务器
避免多个管理服务器之间的冲突
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
发送消息到设备用户
远程开启、关闭和重启客户端设备
远程访问受管理设备
使用 Kaspersky Security Center Web Console从基于 Linux 的设备远程访问基于 Linux 的受管理设备
使用 Kaspersky Security Center Web Console从基于 Linux 的设备远程访问基于 Windows 的受管理设备
使用 Kaspersky Security Center Web Console从基于 Windows 的设备远程访问基于 Linux 的受管理设备
使用 Kaspersky Security Center Web Console从基于 Windows 的设备远程访问基于 Windows 的受管理设备
管理移动设备
使用 Firebase Cloud Messaging
与公共密钥基础架构整合
对管理组进行管理
创建管理组
将应用程序自动安装到管理组中的设备
移动管理组
删除管理组
部署 Kaspersky 应用程序
方案：Kaspersky 应用程序部署
添加卡巴斯基应用程序的管理插件
安装包
下载和创建卡巴斯基应用程序的安装包
从文件创建安装包
创建独立安装包
网络代理安装包设置
运行 Kaspersky Security Center Linux 创建的独立包
使用独立包安装应用程序
安全应用程序安装包上的数据库更新
更改自定义安装包数据大小的限制
将安装包分发至从属管理服务器
查看独立安装包列表
安装 Network Agent for Linux
准备 Linux 设备以安装网络代理
准备运行 SUSE Linux Enterprise Server 15 的设备以安装网络代理

准备在封闭软件环境模式下运行 Astra Linux 的设备以安装网络代理
准备在安装了 glibc 2.5（旧版操作系统）的 Linux 操作系统上安装网络代理。
准备在安装了 OpenSSH 6.4（旧版操作系统）的 Linux 操作系统上安装网络代理。
在 Linux 设备上远程安装网络代理
以静默模式安装 Linux 网络代理（使用应答文件）
以交互模式安装 Linux 网络代理
对网络代理设备文件系统回滚的支持
安装 Network Agent for Windows
以交互模式安装 Windows 网络代理
以静默模式安装 Windows 网络代理
通过捕获和复制设备镜像来部署
网络代理磁盘克隆模式
网络代理安装参数
使用远程安装任务安装应用程序
关于 Kaspersky Security Center Linux 中的远程安装任务
远程安装应用程序
在 macOS 设备上远程安装应用程序
在从属管理服务器上安装应用程序
在安装有网络代理的设备上远程安装应用程序
在远程安装任务中管理设备重启
通过 Kaspersky Security Center Linux 远程安装任务的强制部署
以静默模式安装应用程序
准备 macOS 设备以远程安装网络代理
虚拟基础架构
降低虚拟机负载的窍门
对动态虚拟机的支持
对虚拟机复制的支持
指定 Unix 设备上的远程安装设置
监控部署
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
为远程安装准备 Windows 设备
创建“远程执行脚本”任务
根据清单文件创建安装包
为“远程执行脚本”任务准备压缩文件
使用“远程执行脚本”任务在设备上远程安装应用程序
配置“远程执行脚本”任务的通知和监控
授权许可
Kaspersky Security Center 授权
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
激活 Kaspersky Security Center Linux
受管理卡巴斯基应用程序的授权许可
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
超出了授权许可限制事件
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
续订卡巴斯基应用程序授权许可
使用 Kaspersky Marketplace 选择 Kaspersky 商业解决方案
配置卡巴斯基应用程序
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
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
导出策略
导入策略
强制同步
查看策略分发状态图
在出现病毒爆发事件时自动激活策略
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
导出和导入政策配置文件
网络代理程序政策设置
Windows、Linux 和 macOS 网络代理的使用：比较
按操作系统比较网络代理设置
启用和禁用网络代理的低资源消耗模式
配置受管理应用程序的保护
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
卡巴斯基安全网络 (KSN)
关于 KSN
设置对 KSN 的访问
启用和禁用 KSN 的使用
查看已接受的 KSN 声明
接受更新的 KSN 声明
检查分发点是否充当 KSN 代理服务器
查看 KSN 代理服务器的统计信息
管理任务
关于任务
关于任务范围
创建任务
手动启动任务
为选择的设备执行任务
查看任务列表
常规任务设置
导出任务
导入任务
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
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
使用 klscflag 实用程序开放端口 13291
在 Kaspersky Security Center Web Console 中注册 Kaspersky Industrial CyberSecurity for Networks 应用程序
管理用户和用户角色
关于用户账户
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

分配对特定对象的访问权限
向用户和安全组分配访问权限
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
为用户或安全组分配角色
添加用户账户到内部安全组
指派用户作为设备所有者
安装网络代理期间将用户指定为设备所有者
安装网络代理后将用户指定为 Linux 设备所有者
删除用户的设备所有者角色
启用账户保护以防止未经授权的修改
配置双重身份验证
关于账户的双重身份验证
在Kaspersky Security Center云控制台登录时配置双重身份验证密钥
允许用户配置双重身份验证
重置和删除双重身份验证密钥
从双重身份验证中排除账户
编辑安全码签发者的名称
更改允许的密码输入尝试次数
删除用户或安全组
更改用户账户的密码
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
修改账户密码
撤销本地管理员权限
配置 Kerberos 域身份验证
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
验证已下载的更新
创建"将更新下载至分发点存储库"任务
添加"将更新下载至管理服务器存储库"任务的更新源
批准和拒绝软件更新
自动安装 Kaspersky Endpoint Security for Windows 的更新
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
通过分发点下载更新
更新离线设备上的 Kaspersky 数据库和软件模块

- 监控、报告和审计
  - 方案：监控和报告
  - 关于监控和报告的类型
  - 智能培训模式中的规则触发
    - 查看并确认使用自适应异常控制规则执行的检测
    - 从自适应异常控制规则添加排除
  - 仪表板和小部件
    - 使用仪表板
    - 添加小部件到仪表板
    - 从仪表板隐藏小部件
    - 移动小部件到仪表板
    - 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
  - 管理和防护报告
    - 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
  - 防护等级指示器
    - 安全应用程序已安装
    - 政策已应用
    - 病毒数据库更新已配置
    - 备份已配置
    - 管理服务器维护已配置
    - TLS加密已启用
  - 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
        - 网络代理功能失败事件
        - 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

- 导出事件分类
- 导入事件分类
- 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

查看有关威胁检测的信息

用于响应警报的集成
- 配置与 Active Directory 的集成以执行响应操作
- 配置与 Kaspersky Automated Security Awareness Platform 的集成
- 配置与 Kaspersky Threat Intelligence Portal Sandbox 的集成

按属性分组警报

Cloud Discovery
- 使用小部件启用 Cloud Discovery
- 将 Cloud Discovery 小部件添加到仪表板
- 查看有关云服务使用的信息
- 云服务的风险级别
- 阻止对不需要的云服务进行的访问

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
- 关于使用 CEF 和 LEEF 格式导出事件
- 将事件转换为 CEF 或 LEEF 格式
- 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
监控策略和策略配置文件的更改
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
管理对象修订
查看并保存策略修订
比较策略修订
回滚对象到先前修订
活动威胁
清除未处理文件
下载未处理文件
从"活动威胁"部分中删除文件
对象删除
从隔离区和文件备份下载和删除文件
从隔离区和文件备份区下载文件
关于从隔离区、文件备份区或活动威胁存储库中删除对象
通过 SNMP 管理应用程序
在操作系统中配置 snmpd 服务
启用和禁用 SNMP 通知
在 Kaspersky Security Center Linux 中启用和禁用 SNMP
SNMP 的对象标识符的值
在 Kaspersky Next XDR Optimum 授权许可下使用 Kaspersky Security Center Linux
用于响应警报的集成
配置与 Active Directory 的集成以执行响应操作
配置与 Kaspersky Automated Security Awareness Platform 的集成
配置与 Kaspersky Threat Intelligence Portal Sandbox 的集成
按属性分组警报
Kaspersky Security Center Web Console 与其他 Kaspersky 解决方案之间的集成
建立后台连接
配置代理服务器连接
客户端设备的远程诊断
打开远程诊断窗口
启用和禁用应用程序跟踪
下载应用程序的跟踪文件
删除跟踪文件
下载应用程序设置
从客户端设备下载系统信息
下载事件日志
启动、停止和重新启动应用程序
运行 Kaspersky Security Center Linux 网络代理的远程诊断并下载结果
在客户端设备上运行应用程序
在基于 Linux 的客户端设备上运行远程诊断

管理客户端设备上的第三方应用程序和可执行文件
使用应用程序控制来管理可执行文件
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
创建包括选定设备中的可执行文件的应用程序类别
创建包括选定文件夹中的可执行文件的应用程序类别
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
在 Kaspersky Endpoint Security for Windows 策略中配置“应用程序控制”
获取并查看客户端设备上安装的应用程序列表
关于第三方应用程序
安装第三方软件更新
方案：更新第三方软件
第三方软件更新安装选项
“查找漏洞和所需更新”任务设置
创建“查找漏洞和所需更新”任务
查看有关可用的第三方软件更新的信息
将可用软件更新列表导出到文件
批准和拒绝第三方软件更新
创建“安装所需更新并修复漏洞”任务
添加更新安装规则
任务创建后指定的安装所需更新并修复漏洞任务的设置
自动更新第三方应用程序
修复第三方软件漏洞
关于查找和修复软件漏洞
方案：查找和修复第三方软件中的漏洞
修复第三方软件漏洞
创建“修复漏洞”任务
为第三方软件中的漏洞选择用户修补程序
查看有关在所有受管理设备上检测到的软件漏洞的信息
查看有关在选定受管理设备上检测到的软件漏洞的信息
查看受管理设备上的漏洞统计信息
将软件漏洞列表导出到文件
忽略软件漏洞
从 Kaspersky 数据库创建第三方应用程序的安装包
从 Kaspersky 数据库查看和修改第三方应用程序安装包的设置
从 Kaspersky 数据库设置第三方应用程序的安装包
修复隔离网络中的漏洞
方案：修复隔离网络中的第三方软件漏洞
关于修复隔离网络中的第三方软件漏洞
配置具有互联网访问权限的管理服务器以修复隔离网络中的漏洞
配置隔离的管理服务器以修复隔离网络中的漏洞
在隔离网络中传输补丁和安装更新
禁用在隔离网络中传输补丁和安装更新
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
保持空闲连接
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
关于将网络代理切换到其他管理服务器
为漫游用户创建连接配置文件
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

层级指南
关于本指南
管理服务器计算
管理服务器的硬件资源计算
DBMS 和管理服务器的硬件需求
数据库空间计算
磁盘空间计算
计算管理服务器的数量和配置
有关将动态虚拟机连接到 Kaspersky Security Center 的建议
分发点和连接网关的计算
分发点需求
计算分发点的数量和配置
连接网关数量计算
任务和策略事件信息的记录
管理大量设备的管理服务器的最佳实践
特别考虑和特定任务的优化设置
设备发现频率
管理服务器数据备份任务和数据库维护任务
更新 Kaspersky Endpoint Security 的组任务
清查任务
管理服务器和受保护设备间的网络负载详情
不同方案下的流量消耗
24 小时平均流量使用
已知问题
联系技术支持
如何获取技术支持
通过 Kaspersky CompanyAccount 获得技术支持
获取管理服务器的转储文件
有关应用程序的信息来源
词汇表
Cloud Discovery
HTTPS
Identity and Access Manager (IAM)
iOS MDM 服务器
iOS MDM 设备
JavaScript
Kaspersky Security Center Linux Web 服务器
Kaspersky Security Center Linux 管理员
Kaspersky Security Center System Health Validator (SHV)
Kaspersky Security Center 操作员
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
漏洞
特定设备的任务
病毒爆发
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
网络位置识别 (NLA)
网络保护状态
网络反病毒保护
虚拟管理服务器
补丁重要级别
角色组
设备所有者

身份验证代理
轻量级 Nagent（LWNGT）
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 Linux 帮助

## 新功能

- 新闻

## 硬件和软件要求

- 管理服务器要求
- Web Console 要求
- 网络代理要求

## 启动

- 安装
- 快速启动向导
- 保护部署向导

## 授权许可和激活

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

## 部署和配置

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

- 配置网络保护
- Kaspersky 应用程序。更新数据库和软件模块
- 配置管理服务器连接地址
- 迁移到 Kaspersky Security Center Linux
- 关于升级 Kaspersky Security Center Linux

## 监控

- 监控和报告
- Cloud Discovery

## 管理客户端设备

- 远程访问受管理设备

## 漏洞和补丁管理

- 查找和修复第三方软件中的漏洞

## 附加功能

- 导出事件到 SIEM 系统
- 查看 KSN 代理服务器的统计信息
- 层级指南（仅限在线帮助）

# 新闻

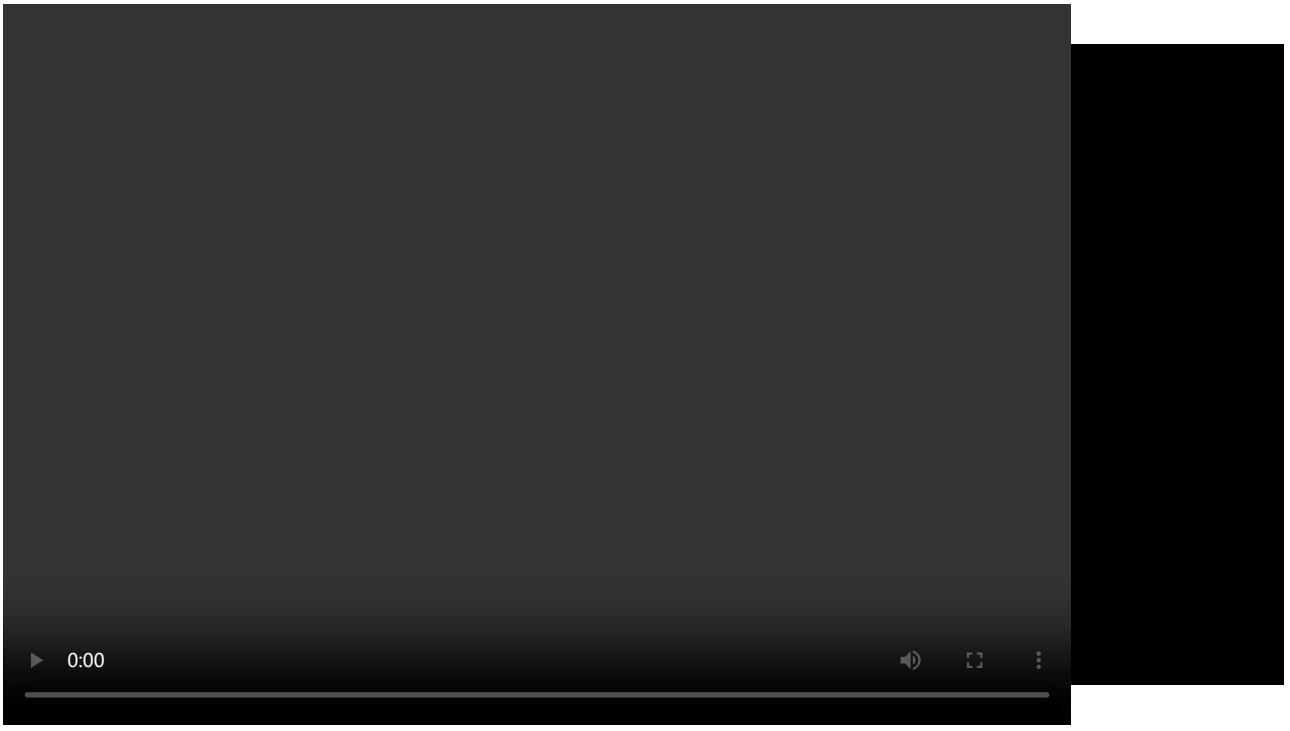
## Kaspersky Security Center 16.3 Linux

Kaspersky Security Center 16.3 Linux 具有多个新功能和改进。

- 如果修改策略，则会为每个已更改的参数创建一个单独的审计事件。事件将导出到 SIEM。
- 现在，将事件导出到 SIEM 系统功能已支持 **Kaspersky SIEM** (KUMA)。
- Kaspersky Security Center for Linux现在支持与Kaspersky Vulnerability Management解决方案配合使用。
- 为遵循强化指南，我们制定了优化的Kaspersky Endpoint Security for Linux 配置，用于安装在搭载管理服务器、Web Console 和 数据库管理系统 的设备上，以及用于部署 Kaspersky Security Center Linux 故障转移集群。
- 现在，您可以在安装Kaspersky Security Center for Linux时指定自定义数据库架构。
- 在**监控→控制板**中，防护等级指示器可帮助您评估管理服务器和分发点的安全性。如果该指示器为黄色或红色，您必须执行操作来解决问题，并将指示器状态更改为绿色。
- Kaspersky Security Center Linux 部署的简化方法现已可用：您现在可以使用安装脚本。
- 为了支持以下过时的操作系统，现已提供适用于 Kaspersky Network Agent for Linux Legacy 且带有 glibc 版本 2.5 的专用分发包：
  - CentOS 5.2
  - CentOS 5.4
  - CentOS 6.4
  - CentOS 6.6
  - Astra Linux 特别版 RUSB.10015-01（操作更新 1.4）64 位
- 网络代理现在支持与以下新操作系统版本配合使用：
  - Microsoft Windows 11 IoT Enterprise 版本25H2 64位
  - SberOS 3.6.1
  - Ubuntu Server 26.04 LTS
- 以下数据库管理系统已不再受支持：
  - Aurora MySQL 5.7
  - MariaDB 10.1.30

- 用户体验改进：
  - 增强了**任务**和**策略**表的筛选功能。现在，您可以使用OR逻辑添加多个条件，还可以使用新的运算符，为单个属性选择多个值，并显示至少匹配一个指定条件的记录。
  - 在主菜单中：
    - 新增了**软件管理**部分。以下部分现在已移至 **软件管理**：**安装包**、**卡巴斯基应用程序**、**第三方应用程序**、**当前应用程序版本**和**补丁管理**。
    - **未分配的设备**和**硬件**部分现已移至**资产管理**。
    - **任务**和**存储库**部分已移至菜单第一级。
    - **Web 插件备份**部分已不再使用，并已从 Web Console 中移除。

## Kaspersky Security Center 16.2 Linux




16.2 版本新增功能概述。视频

Kaspersky Security Center 16.2 Linux 具有多个新功能和改进。

- 在 Kaspersky Security Center Web Console中，您现在可以在隔离区 (DMZ) 中配置连接网关。

  使用**按地址使用 DMZ 连接网关**选项配置连接网关。
- 改进了 Linux设备上用于保留网络代理设备标识符的算法（`Device ID` 参数）。如果设备的 BIOS 序列号、主板序列号、存储磁盘标识符或 MAC 地址与之前已知的值匹配，则在操作系统更新或 MAC 地址更改后，管理服务器能够正确识别该设备，将其视为之前已发现的设备。
- 新增了对地理分布式 Kaspersky Security Center Linux 故障转移集群的支持，该集群的集群节点分布在不同数据中心。在地理分布式集群配置中，所有组件均可进行故障转移。

- 您现在可以将事件以 CEF 或 LEEF 格式导出到 SIEM 系统。
- 新增了对高可用性 PostgreSQL 集群的支持，该集群使用 Patroni 实现自动故障转移，并使用 HAProxy 实现负载均衡。
- 您可以比较政策修订版本。此选项适用于管理服务器、网络代理、 Kaspersky Endpoint Security for Windows（从 14.0 Web 插件版本开始）以及 Kaspersky Endpoint Security for Mac（从 12.2.1 Patch A Web 插件版本开始）的策略。未来版本将扩展支持此功能的卡巴斯基应用程序列表。
- SNMP现在受支持。您可以使用 SNMP 向第三方客户端应用程序提供管理服务器信息、统计信息和事件。
- 现在支持对基于 Windows 的分发点进行 Windows 网络轮询。
- 现在提供适用于 Linux 的网络代理的单一安装包。此安装包包含适用于不同软件包管理器和 CPU 架构的版本。安装过程中，系统会自动检测环境并安装相应的网络代理软件包。
- 事件现在包含有关移动设备上执行的命令发起者的信息。
- NSQ 组件被从 Kaspersky Security Center Web Console 分发包中移除。KSCWebConsoleMessageQueue.service 服务不再使用，将在 Kaspersky Security Center Web Console 更新后被移除。
- 在隔离网络中，为 Windows 设备创建安装包现在需要从卡巴斯基网站下载额外模块（ri_utils_win32.zip 和 ri_utils_arm64.zip 压缩文件）。
- 网络代理现支持 Windows ARM 64 位架构。与受管理应用程序的兼容性可以在相应的帮助文档中进行验证。
- Kaspersky Security Center Linux 支持与 Kaspersky Sandbox 配合使用。
- 用户体验改进：
  - 您现在可以一次性删除事件分类和设备事件列表中的所有事件。
    事件分类选择和设备事件列表中均提供**全部选择**和**在当前页面上全选**。
  - 您现在可以手动指定移动规则的优先级。
    选择移动规则后， **更改优先级**按钮将变为可用状态，允许您指定新的优先级。
- Kaspersky Security Center Linux 支持与 Platform V SberLinux OS Server (SLO) 9.6 配合使用。
- Kaspersky Security Center Linux 现在支持使用以下 DBMS：
  - MySQL Standard Edition 8.4
  - MySQL Enterprise Edition 8.4
  - PostgreSQL 18
  - Postgres Pro 18（所有版本）
  - Postgres Pro 18 Enterprise（集群内置高可用性）

- 网络代理现在支持与以下新操作系统版本配合使用：
  - Microsoft Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education ARM
  - Platform V SberLinux OS Server (SLO) 9.6

## Kaspersky Security Center 16.1 Linux

Kaspersky Security Center 16.1 Linux 具有多个新功能和改进。

- 双重身份验证现已默认启用。禁用双重身份验证的全局选项已不再可用。为确保用户能够登录Kaspersky Security Center云控制台并继续使用OpenAPI自动化脚本，请在升级前为所有用户启用双重身份验证。
- 您现在可以在不导出策略的情况下将策略配置文件保存为KLPROF文件，然后使用此KLPROF文件将已保存的配置文件导入策略。
- 网络代理程序现在可在运行ALT操作系统的设备上以封闭软件环境模式运行。
- 新增了对基于Kerberos的域身份验证的支持，该身份验证使用SCRIL协议，为无密码域用户提供基于证书的单点登录（SSO）。
- 用户体验改进：
  - 按操作系统版本和软件包管理器筛选客户端设备的功能现在包含Linux操作系统版本。
  - 改进了Kaspersky Security Center云控制台中表格的分页机制：默认显示的项目数已增加到50，并且自定义的显示项目数现在会在会话之间保留。
  - 应用程序类别的注释功能允许您添加包含和排除类别中应用程序的规则描述。
  - 默认情况下，可用安装包列表现在仅以Kaspersky Security Center云控制台界面语言和英语显示卡巴斯基应用程序安装包。
- Kaspersky Security Center Linux支持与Kaspersky Endpoint Security for Linux 12.4配合使用。
- Kaspersky Security Center Linux支持与以下新操作系统版本配合使用：
  - Debian GNU/Linux 13 (Trixie)
  - CentOS Stream 10
  - Red Hat Enterprise Linux Server 10.x
- 网络代理现在支持与以下新操作系统版本配合使用：
  - ALT Workstation 11
  - ALT Server 11
  - ALT Education 11
  - AlterOS 2025

- SberOS 3.4.0
- SberOS 3.5.0
- OSnova 3.*

## Kaspersky Security Center 16 Linux

Kaspersky Security Center 16 Linux 具有多个新功能和改进。

- 支持 FreeIPA 和 ALD Pro 域控制器。
- 已实现域身份验证（单点登录）。单点登录功能允许您在 Kaspersky Security Center 16 Web Console 中启用安全身份验证，而无需在公司网络上重新输入密码。要使用域身份验证，您必须在 Kaspersky Security Center Web Console 安装期间在响应文件中指定附加参数。
- Kaspersky Security Center 16 Linux 管理服务器仅与 Kaspersky Security Center 16 Web Console 兼容。无法使用早期版本的 Kaspersky Security Center Web Console。
- 现在，您可以在试用授权许可下使用 Kaspersky Next XDR Optimum 的功能，前提是您添加了从属管理服务器，在试用授权许可下激活了此服务器，并且将授权许可密钥部署到了受到从属管理服务器管理的设备。
- 用户体验改进：
  - 管理组和管理服务器的导航功能已更新：您可以从单个导航窗格轻松地在组和服务器之间切换。
  - 您的配置文件设置已移至上方窗格。
  - 主菜单的以下区域已重命名：
    - “**资产（设备）**”区域现在称为“**资产管理**”。
    - “**受管理设备**”被称为“**资产(设备)**”。
    - “**快速链接**”已重命名为“**控制台导航**”。
  - 如有必要，您可以将主菜单最小化为图标。
  - “**卡巴斯基新闻**”区域已从“**监控** ” → “**通知**”中删除。
- 您应用于“**操作**” → “**补丁管理**” → “**软件漏洞**”和“**操作**” → “**补丁管理**” → “**软件更新**”区域中表格的过滤器现已成功保存，且不会重置。
- Kaspersky Security Center Linux 兼容：
  - Kaspersky NGFW。
  - 以下操作系统版本（针对受管理设备）：
    - MosOS 15.5 Arbat
    - Microsoft Windows 11 25H2

- CentOS 6.4
- CentOS 6.6

## Kaspersky Next XDR Optimum 授权许可下的 Kaspersky Security Center 15.4 Linux

如果您在Kaspersky Next XDR Optimum 授权许可下激活了管理服务器，并将 Kaspersky Next XDR Optimum 授权许可密钥部署到了您的受管理应用程序，则可以执行以下操作：

- 按属性对警报进行分组。
- 配置响应威胁的集成。

## Kaspersky Security Center 15.4 Linux

Kaspersky Security Center 15.4 Linux 具有多个新功能和改进。

- 现在可以使用 Linux 设备漫游用户的连接配置文件。使用连接配置文件，您可以为 Linux 设备上的网络代理配置规则，以连接到相同或不同的管理服务器，具体取决于设备位置。
- 现在可以在管理服务器之间传输加密密钥。
- Kaspersky Thin Client 现在受支持。
- Platform V Pangolin 内置高可用性集群现在受支持。
- Postgres Pro 内置高可用性集群现在受支持。安装 Kaspersky Security Center Linux时，此 DBMS 集群的节点在连接字符串中指定。
- Kaspersky Security Center Linux 现在支持使用以下 DBMS：
  - Platform V Pangolin 6.5.1
  - Tantor SE 1C for Astra Linux 特别版 RUSB.10015-01（操作更新 1.8）
  - Jatoba 5
- 支持Platform V SberLinux OS Server (SLO) 版本 8.10.1、9.0.1、9.5.1。
- KlAkOAPI.tar.gz 存档被从帮助中删除。KlAkOAPI.tar.gz 存档位于 Kaspersky Security Center Linux 安装文件夹中。
- **扫描**按钮被从**隔离**部分删除。
- 网络代理独立包或在虚拟管理服务器上创建的任何包的安装包列表中不再有关于大小、文件哈希和路径的信息，因为这些独立包在下载时生成。

## Kaspersky Security Center 15.3 Linux

Kaspersky Security Center 15.3 Linux 具有多个新功能和改进。

- klcsngtgui 实用程序已被从 Kaspersky Security Center Linux 发行包中删除。我们建议使用 klnagchk 实用程序而不是 klcsngtgui 实用程序。
- 网络代理现在支持与以下新操作系统版本配合使用：
  - Windows Server 2025
  - Fedora Linux 服务器 41
  - Fedora Linux 工作站 41
- Kaspersky Security Center Linux 现在支持使用以下 DBMS：
  - PostgreSQL 17
  - Postgres Pro 17
- 现在，您可以使用卡巴斯基更新实用程序仅下载卡巴斯基安全应用程序所需的数据库和软件模块更新。在**将更新下载至管理服务器存储库**管理服务器任务属性窗口中，启用**自动下载更新请求文件**选项，然后指定 Kaspersky Security Center Linux 将创建更新请求文件以及要下载的更新相关信息的路径。
- 现在可以查看KSN 代理服务器的使用情况统计数据。
- 使用 klbackup 实用程序将 Kaspersky Security Center Windows 管理服务器数据迁移到 Kaspersky Security Center Linux 的功能已更新。现在，您可以将存储在 Microsoft SQL Server 数据库中的管理服务器数据迁移到 PostgreSQL 或Postgres Pro。
- 现在可以配置管理服务器连接地址。管理服务器连接地址在创建网络代理安装包时用作默认地址，并在将受管理设备连接到 KSN 时用作 KSN 代理服务器地址。
- 您现在可以集中重启受管理设备。
- 有关当前登录到 Linux 受管理设备的用户的信息现在显示在设备属性窗口的**常规→会话**部分。
- 您现在可以通过安装在这些设备上的网络代理远程访问 Linux 和 Windows 受管理设备。连接使用 RDP、VNC 或 WDS 建立。在与设备建立连接后，管理员会获取对此设备上存储的信息的完全访问权限，以便他或她可以管理其上安装的应用程序。
- 上传并运行应用程序（或脚本）用于在受管理设备上进行诊断。您现在可以上传包含可执行文件的目录或存档，或者可执行文件本身。应用程序成功执行后，您可以下载执行结果。
- 用户体验改进，包括新增“**快速链接**”区域。此部分显示主菜单图并为您提供对 Kaspersky Security Center Web Console 所有部分的快速访问。默认情况下，“**快速链接**”被设为主页。

## Kaspersky Security Center 15.2 Linux

Kaspersky Security Center 15.2 Linux 具有多个新功能和改进。

- 用于管理内部用户账户密码的新功能：
  - 您现在可以强制内部用户在首次（或下次）尝试登录 Kaspersky Security Center Web Console 时更改密码。
  - 配置内部用户账户密码有效期的新选项。
- 您现在可以通过使用 klbackup 实用程序备份 Kaspersky Security Center Windows 管理服务器数据并在 Kaspersky Security Center Linux 中恢复它。可以在同类型的 DBMS 之间或 Microsoft SQL Server → MySQL 或 MariaDB 之间进行迁移，且不会丢失数据。
- Kaspersky Security Center Linux 现在支持使用以下 DBMS：
  - PostgreSQL 16.x
  - Postgres Pro 16.x
- Kaspersky Security Center Linux 现在支持某些类型的 PostgreSQL 和 Postgres Pro 集群。
- 支持新的操作系统和新的操作系统版本，包括新版本的 OS MES (Moscow Electronic School)、MosTech 和 MosTech Server。
- 用户体验改进包括：
  - 策略设置窗口中的新**保存**按钮。如果您想保存更改而不关闭策略设置窗口，请使用此按钮。
- 您现在可以在卡巴斯基移动设备保护和管理插件的新"应用和文件"部分中管理向 Android 设备发送文件、删除以前发送的文件以及配置其设置。
- 您现在可以将应用安装包和设备管理配置文件传输到移动设备，而无需使用连接网关上的新 Web 服务器服务将它们直接连接到管理服务器。

## Kaspersky Security Center 15.1 Linux

Kaspersky Security Center 15.1 Linux 具有多个新功能和改进。

- Kaspersky Security Center Web Console 现在支持通过卡巴斯基移动设备保护和管理插件进行移动设备管理。
- 您现在可以通过 iOS MDM 服务器设置插件安装和配置 iOS MDM 服务器来管理 iOS MDM 设备。
- 您现在可以管理移动设备的证书。
- Kaspersky Endpoint Security for Android 现在受支持。
- Kaspersky Security for iOS 现在受支持。

- Kaspersky Endpoint Security for Aurora 现在受支持。
- Windows 受管理设备的漏洞和补丁管理。您可以管理安装在 Windows 受管理设备上的第三方软件的更新，并通过安装所需的更新来修复此类软件中的漏洞。
- Kaspersky Security Center Linux 现在逐页轮询域控制器，而不是一次性轮询整个域控制器。因而，您可以轮询包含大量条目的域控制器。
- 自适应异常控制。这是 Kaspersky Endpoint Security for Windows 的一项功能，该功能使用一组规则来跟踪客户端设备上的非典型行为，并且允许您阻止异常操作。
- 对安装在 Windows 设备和 Linux 网络代理上的卡巴斯基应用程序进行无缝更新。通过批准必须安装的更新和拒绝不得安装的更新，可以管理更新安装过程。
- 扩展的策略审计。现在可以查看策略修订的内容以及保存策略修订到文件。目前，这些功能仅适用于管理服务器策略和网络代理策略。
- Cloud Discovery。这项新功能可让您监控运行 Windows 的受管理设备上云服务的使用情况，并阻止对您认为不需要的云服务进行的访问。
- 主菜单的“**监控**”区域中的新“**警报**”子区域。在“**警报**”子区域中，可以查看有关端点设备上检测到的威胁的信息。这些威胁由卡巴斯基安全应用程序检测到。
- Kaspersky Security Center Linux 现在可以作为 Kaspersky Managed Detection and Response 解决方案的组成部分。
- 支持 Kaspersky Security for Virtualization Light Agent。
- 扩展的 macOS 设备硬件清单。macOS 设备上的网络代理会将 MAC 地址和设备序列号发送到管理服务器。
- 现在，当您通过自定义脚本在受管理设备上安装软件时，可以收到有关远程安装的报告。
- 当您在受管理设备上执行多个自定义脚本时，可以为每个脚本设置优先级来定义执行顺序。这些脚本将按照优先级从高到低的顺序执行。
- 为了减少 Kaspersky Endpoint Security for Linux 和 Linux 网络代理消耗的 RAM 量，您可以为 Linux 网络代理启用特殊工作模式。在这种模式下，Linux 网络代理需要的 RAM 较少，但其功能也会受限。
- 您可以通过“*远程卸载应用程序*”任务从受管理设备卸载不兼容的软件。
- 网络攻击报告现在包括实施攻击的设备的 MAC 地址和端口。
- 内部用户的最长密码长度增加到 256 个字符。
- 用户体验改进包括：
  - 通过添加 Kaspersky Security Center Web Console 的部分到书签来实现主菜单个性化，以便从“**书签**”部分快速访问。
  - 优化表格工作。现在，每个表格的默认视图会包含最常用的列。此外，您现在可以选择当前页面或整个表格中的所有项目，并对整个表格中的项目进行排序。
  - 改进的报告传送配置。您现在可以指定最多 20 个电子邮件地址用于接收报告，还可以指定报告传送时间表。
- 支持多种操作系统和新操作系统版本。

- 已开发新的筛分向导并将其发布到在线帮助中。
- 经过用户界面审查，已解决导致管理服务器属性窗口中出现"**远程诊断**"部分的问题。
- 您可以创建"*远程执行脚本*"任务来在客户端设备上执行安装包并远程安装应用程序。
- 在 Linux 客户端设备上安装网络代理期间或之后，可将用户指定为设备所有者。
- 您可以根据设备所有者、设备所有者在安全组中的成员资格以及设备所有者的角色来配置设备分类或创建设备移动规则。
- 您可以从账户中撤销本地管理员权限。这为您提供了对用户账户的额外控制。例如，您可以在一次性分配完成后撤销本地管理员权限。
- 您可以更改本地账户密码，例如当用户忘记本地账户密码或要执行计划的密码更改时。
- 在"**用户证书管理**"子部分中，您可以指定要安装的根证书。例如，这些证书可用于验证网站或网络服务器的真实性。

## Kaspersky Security Center 15 Linux

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

- 域控制器轮询允许您轮询 Microsoft Active Directory 域控制器和 Samba 域控制器。您可以使用管理服务器或分发点来轮询 Microsoft Active Directory。您只能通过基于 Linux 的分发点轮询 Samba 域控制器。当您轮询域控制器时，管理服务器或分发点会检索有关域中包含的设备的域结构、用户账户、安全组和 DNS 名称的信息。
- Kaspersky Security Center Linux 现在支持使用以下 DBMS：
  - PostgreSQL 15.x
  - Postgres Pro 15.x
- 如果您使用 PostgreSQL 或 Postgres Pro 作为 DBMS，则 Kaspersky Security Center Linux 可支持多达 50,000 个受管理设备。
- 从 Kaspersky Security Center Windows 迁移到 Kaspersky Security Center Linux。您可以运行向导来迁移 Kaspersky Security Center对象，包括任务、策略和管理组结构。之后，您可以将导入的受管理设备移至 Kaspersky Security Center Linux 的管理之下。
- Kaspersky Security Center Linux 现在支持使用以下卡巴斯基应用程序：
  - Kaspersky Security for Virtualization Light Agent
  - Kaspersky Embedded Systems Security for Windows
  - Kaspersky Embedded Systems Security for Linux
  - Kaspersky Industrial CyberSecurity for Nodes
  - Kaspersky Industrial CyberSecurity for Networks

  - Kaspersky Endpoint Security for Mac
  - Kaspersky Endpoint Agent
  - Kaspersky Security for Virtualization Light Agent
- 远程诊断基于 Windows 和 Linux 的受管理设备。
- 改进的应用程序控制组件。您现在可以根据选定文件夹中的可执行文件列表或卡巴斯基应用程序类别创建应用程序类别。然后，您可以指定在组织中允许还是阻止创建的类别中的应用程序。
- 导出和导入事件分类。您可以将用户定义的事件分类及其设置导出到 KLO 文件，然后将保存的事件分类导入到 Kaspersky Security Center Windows 或 Kaspersky Security Center Linux。
- 在威胁报告中，您现在可以通过单击**查看警报**链接来打开威胁发展链。
- Kaspersky Security Center Linux 现在支持集群技术。如果管理组包含集群或服务器阵列，则"**资产(设备)**"页面将显示两个选项卡：一个用于单个设备，另一个用于集群和服务器阵列。受管理设备被检测为集群节点后，集群将被作为单独对象添加到**集群和服务器阵列**选项卡。集群节点与其他受管理设备一起列在**设备**选项卡上。
- Kaspersky Security Center Linux 对某些平台的支持已终止，因为这些平台不再受到其供应商的支持。

## Kaspersky Security Center 14.2 Linux

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

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

  只有通过基于 Windows 的分发点使用操作系统工具，才能在客户端设备上远程安装 Windows 网络代理。
- 基于 Windows 的受管理设备上的数据现在可以加密以降低笔记本电脑或硬盘被盗或丢失时敏感数据和公司数据意外泄露的风险。此功能可通过 Kaspersky Endpoint Security for Windows 实现。
- Kaspersky Security Center Linux 允许您直接在 Kaspersky Security Center Linux 的用户界面中下载和更新卡巴斯基应用程序的分发包和管理 Web 插件。
- 默认情况下，有关安装在基于 Linux 和基于 Windows 的受管理设备上的应用程序的信息会被发送到管理服务器。
- 现在自动验证对卡巴斯基服务器的访问。如果无法使用系统 DNS 访问服务器，应用程序将使用公共 DNS。
- 在主管理服务器、从属管理服务器和网络代理之间传输的敏感数据现在受到 AES 加密算法的保护。
- 虚拟管理服务器上的用户权限可随时独立于主管理服务器进行配置。此外，您可以为主服务器用户分配管理虚拟服务器的权限。

- Kaspersky Security Center Linux 现在支持使用以下 DBMS：
  - PostgreSQL 13.x
  - PostgreSQL 14.x
  - Postgres Pro 13.x（所有版本）
  - Postgres Pro 14.x（所有版本）
- 您可以使用 Kaspersky Security Center Web Console 将策略和任务导出到一个文件，然后将策略和任务导入到 Kaspersky Security Center Windows 或 Kaspersky Security Center Linux。
- "**不使用代理服务器**"选项已从以下任务中删除：
  - *将更新下载至管理服务器存储库*
  - *将更新下载至分发点存储库*

## Kaspersky Security Center 14 Linux

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

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

# 已修复问题

下表列出了 Kaspersky Security Center Linux 先前版本中发现的所有问题，这些问题已在当前版本中修复。

## Kaspersky Security Center Linux 16.3 中已修复的问题列表

| Kaspersky Security Center Linux 版本中首次出现此问题 | 问题 ID | 问题描述 |
|---|---|---|
| 16.2 | 9959974 | 修复了以下问题：设备属性窗口的 **事件**选项卡包含 **全部选择**选项，该选项可能会从管理服务器数据库中删除所有事件。 |
| 16.2 | 9392997 | 修复了以下问题：成功轮询 ALD Pro 或 FreeIPA 域控制器后，事件日志中添加了错误消息。 |
| 16.2 | 9504495 | 修复了以下问题：通过网络代理安装包参数分配设备所有者时，可能导致用户分配不正确。 |
| 16.1 | 9316206 | 修复了以下问题：打开 **双重身份验证**选项卡后刷新浏览器时，该选项卡中的控制按钮可能会消失。 |
| 16.1 | 7555541 | 修复了以下问题：创建 *更改帐户密码（仅限 Linux）*任务时，如果启用 **设置为一次性密码(用户必须在首次登录后更改密码)**选项，则可能导致无法登录 Web Console。 |
| 15.4 | 7555788 | 修复了以下问题：如果用户设备上启用了 SELinux，*更改帐户密码*任务可能无法正常工作。 |
| 16.2 | 9603496 | 修复了以下问题：必须在管理服务器设备上安装网络代理，才能获取有关该设备的诊断信息。 |
| 16.2 | 9704308 | 修复了以下问题：在管理组数量较多的环境中，如果在页面加载期间打开**组层级**部分，可能会导致出现 `429 Too Many Requests` 错误、中断与管理服务器的连接，并将用户重定向到登录页面。 |
| 16.2 | 9989231 | 修复了以下问题：按连接 IP 地址筛选设备可能会返回不正确的结果。 |
| 16.2 | 9990025 | 修复了以下问题：在页面之间导航时，**策略**和**任务**部分中的表格视图设置未保留。 |
| 15.3 | 9632613 | 修复了以下问题：当 LDAP 域控制器不可用或不包含该用户账户时，域用户登录 Web Console 可能会显著延迟。 |
| 15.1 | 9829027 | 修复了以下问题：在**反病毒数据库使用报告**中配置**更新状态**筛选器时，可能会导致错误。 |
| 15.1 | 9844707 | 即使配置了代理服务器，Kaspersky Security Center 和 FCM (Firebase Cloud Messaging) 也会直接交互。 |

## Kaspersky Security Center Linux 16.2 中已修复的问题列表

| Kaspersky Security Center Linux 版本中首次出现此问题 | 问题 ID | 问题描述 |
|---|---|---|
| 15.1 | 10071566 | 修复了如果计划使用了"按星期几"设置则对任务计划所做的更改不会传播到受管理设备的问题。 |
| 15.4 | 9067754 | 修复了更新 Kaspersky Mobile Devices Protection and Management 插件后，新事件在先前创建的策略中显示不正确的问题。 |
| 16 | 9329729 | 修复了将 Kaspersky Security Center Linux 从版本 16 升级到版本 16.1 后，如果为某些用户在升级前已配置双重身份验证，卡巴斯基事件日志中出现错误的问题。 |
| 16.1 | 9256000 | 修复了如果在 Microsoft Windows XP 上安装了网络代理则无法获取有关受管理应用程序组件的信息的问题。 |
| 16.1 | 9251629 | 修复了登录 Kaspersky Security Center Web Console 时某些必需的 HTTP 响应标头未添加的问题。 |

# 关于 Kaspersky Security Center Linux

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

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

Kaspersky Security Center Linux 允许您在公司网络中的设备上安装 Kaspersky 安全应用程序，远程运行扫描和更新任务，以及管理受管理应用程序的安全策略。作为管理员，您可以使用详细的仪表板，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。
- 管理存储在 Windows 设备的硬盘驱动器和可移动驱动器上的信息的加密。
- 管理用户对 Windows 设备上的加密数据的访问。
- 创建已连接至组织网络的硬件清查列表。
- 集中管理被安全应用程序移动到隔离区或备份区中的文件，以及安全应用程序已经推迟处理的文件。

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

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

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。

# 分发包

在卡巴斯基网站。您可以下载该应用程序的所有必要分发包。
Kaspersky Security Center Linux 分发包包含以下文件：

**Kaspersky Security Center Linux 管理服务器：**

- 要安装在运行 Debian 操作系统的设备上的管理服务器：
  ksc64_16.2.0-<build>_amd64.deb
- 要安装在运行 Red Hat Enterprise Linux 操作系统的设备上的管理服务器：
  ksc64_16.2.0-<build>.x86_64.rpm

**Kaspersky Security Center Web Console：**

- 要安装在运行 Debian 操作系统的设备上的 Web Console：
  ksc-web-console-16.2.<build>.x86_64.deb
- 要安装在运行 Red Hat Enterprise Linux 操作系统的设备上的 Web Console：
  ksc-web-console-16.2.<build>.x86_64.rpm

**Network Agent for Windows**：

- 要安装在 x86-32 或 x64 架构设备上的网络代理：
  ksc_16_16.2.0.<build>_NetAgent_<localization>.zip
- 要安装在 Arm 架构设备上的网络代理：
  klnagent_winarm64-16.2.0.<build>-win_<localization>.zip
- 用于在运行 Arm 64 位操作系统的设备上远程安装网络代理的实用程序：
  ri_utils_arm64.zip
- 用于在运行 32 位或 64 位操作系统的设备上进行远程安装网络代理的实用程序：
  ri_utils_win32.zip

**Network Agent for Linux：**

- 要安装在运行 Debian 操作系统的设备上的网络代理：
  klnagent64_16.2.0-<build>_<architecture>.deb
- 要安装在运行 Red Hat Enterprise Linux 操作系统的设备上的网络代理：
  klnagent64-16.2.0-<build>_<architecture>.rpm
- 用于在运行 Debian 操作系统的设备上远程安装网络代理的文件：
  klnagent-<architecture>-16.2.0.<build>-deb_<localization>.tar.gz
- 用于在运行 Red Hat Enterprise Linux 操作系统的设备上远程安装网络代理的文件：
  klnagent-<architecture>-16.2.0.<build>-rpm_<localization>.tar.gz

- 适用于 Linux 的网络代理的单个分发包：

  klnagent-ALL-16.2.0.<build>-ALL_<localization>.tar.gz

  如果您有许多客户端设备，它们的 CPU 架构和 Linux 操作系统各不相同，则此单个分发包可能会有用。系统会自动选择所需版本的网络代理，以便后续在设备上进行安装。

**Kaspersky Endpoint Detection and Response Optimum Web 插件：**

- signed_irp.zip

  > 您只能从远程安装应用程序分发包存储库下载此 Web 插件。

如果您在选择 Linux 网络代理的安装包时遇到困难，请参阅文章：如何选择适用于 Linux 网络代理的安装包。

# 硬件和软件要求

- 管理服务器要求
- Web Console 要求
- 网络代理要求

若要理解部署保护和管理移动设备的 Android 和 iOS 版本要求，请参阅Kaspersky Security for Mobile 帮助和Kaspersky Secure Mobility Management 帮助。

## 管理服务器要求

最小硬件条件：

- 运行频率为 2.5 GHz 或更高、2 核的 CPU。
- RAM：6 GB。

  您必须在安装了管理服务器的设备上启用交换文件。交换文件的最小大小必须是 RAM 容量的 1.5 倍。
- 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。

> 我们建议在设备上安装管理服务器后，在该设备上安装 Kaspersky Endpoint Security for Linux。
> 对于同时安装，最低必须具备 300 IOPS，并且在管理服务器要求的基础上还需要增加 1.5 GB RAM 和 15% 的 CPU 资源。
> 有关 Kaspersky Endpoint Security 的硬件要求，请参阅Kaspersky Endpoint Security for Linux 帮助。

支持以下操作系统：

> 对于操作系统中的进程间通讯，必须提供环回接口。

- Debian GNU/Linux 12 (Bookworm) 64 位
- Debian GNU/Linux 13 (Trixie) 64 位
- Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64 位
- Ubuntu Server 24.04 LTS (Noble Numbat) 64 位
- Ubuntu Server 26.04 LTS (Resolute Raccoon) 64位
- CentOS Stream 9 64 位
- CentOS Stream 10 64 位
- Red Hat Enterprise Linux Server 7.x 64 位
- Red Hat Enterprise Linux Server 8.x 64 位
- Red Hat Enterprise Linux Server 9.x 64 位
- Red Hat Enterprise Linux Server 10.x 64 位
- SUSE Linux Enterprise Server 12 (所有服务包) 64 位
- SUSE Linux Enterprise Server 15 (所有服务包) 64 位
- Astra Linux 特别版 RUSB.10015-01（操作更新 1.6）64 位
- Astra Linux 特别版 RUSB.10015-01（操作更新 1.7）64 位
- Astra Linux 特别版 RUSB.10015-01（操作更新 1.8）64 位
- Astra Linux 特别版 RUSB.10015-16（发布版 1）（操作更新 1.6）64 位
- Astra Linux 特别版 RUSB.10015-17（操作更新 1.7.3）64 位
- Astra Linux 特别版 RUSB.10015-03（操作更新 7.6）64 位
- Astra Linux 特别版 RUSB.10015-37 （操作更新 7.7）64 位
- Astra Linux Common Edition（操作更新 2.12）64 位
- ALT SP Server 10 64 位
- ALT SP Workstation 10 64 位
- Oracle Linux 7 64 位
- Oracle Linux 8 64 位

- Oracle Linux 9 64 位
- Platform V SberLinux OS Server (SLO) 8.10.1 64 位
- Platform V SberLinux OS Server (SLO) 9.5.1 64 位
- Platform V SberLinux OS Server (SLO) 9.6 64 位
- Platform V SberLinux OS Server (SLO) 9.7 64 位
- RED OS 7.3 Server 64 位
- RED OS 7.3 Certified Edition 64 位
- RED OS 8 64 位
- ROSA COBALT 7.9 64 位
- M OS (Moscow Electronic School) 12 Server 64 位
- Mostech Server 64 位
- MosOS 15.5 Arbat 64 位

> 我们建议您使用 EXT4 文件系统及其默认设置。

支持以下数据库服务器（可以安装在其他设备上）：

- MySQL Standard Edition 8.0（版本 8.0.20 及更高版本）32 位/64 位
- MySQL Enterprise Edition 8.0（版本 8.0.20 及更高版本）32 位/64 位
- MySQL Standard Edition 8.4 32 位/64 位
- MySQL Enterprise Edition 8.4 32 位/64 位
- MariaDB 10.3（内部版本 10.3.22 及更高版本）32 位/64 位
- MariaDB 10.4（内部版本 10.4.20 及更高版本）32 位/64 位
- MariaDB 10.5（内部版本 10.5.27 及更高版本）32 位/64 位
- MariaDB 10.6（内部版本 10.6.20 及更高版本）32 位/64 位
- MariaDB 10.11（内部版本 10.11.10 及更高版本）32 位/64 位
- 搭载 InnoDB 存储引擎的 MariaDB Galera Cluster 10.3 32 位/64 位
- PostgreSQL 13.x 64 位
- PostgreSQL 14.x 64 位
- PostgreSQL 15.x 64 位

- PostgreSQL 15.x 64 位（集群Corosync/Pacemaker）
- PostgreSQL 16.x 64 位
- PostgreSQL 17 64 位
- PostgreSQL 18 64 位
- Postgres Pro 13.x 64 位（所有版本）
- Postgres Pro 14.x 64 位（所有版本）
- Postgres Pro 15.x 64 位（所有版本）
- Postgres Pro 15.x 64 位（集群Corosync/Pacemaker）
- Postgres Pro 16.x 64 位（所有版本）
- Postgres Pro 16.x Enterprise 64 位（集群内置高可用性）
- Postgres Pro 17.x 64 位（所有版本）
- Postgres Pro 17.x Enterprise 64 位（集群内置高可用性）
- Postgres Pro 18 64 位（所有版本）
- Postgres Pro 18 Enterprise 64 位（集群内置高可用性）
- Platform V Pangolin 6.5.1 64 位
- Platform V Pangolin 6.5.1 64 位（集群内置高可用性）
- Jatoba 4 64 位
- Jatoba 5 64 位
- Tantor SE 1C 64-bit

支持高可用性 PostgreSQL 集群。详情请参阅以下文章：为使用 Kaspersky Security Center Linux 准备高可用性 DBMS集群。

有关受支持的虚拟化平台的信息，请参阅Kaspersky Security for Virtualization Light Agent在线帮助。

# Web Console 要求

Kaspersky Security Center Web Console 服务器

最小硬件条件：

- CPU：2 核，工作频率 2.5 GHz。
- RAM：4 GB。
- 可用磁盘空间：存储 Web Console 数据的文件夹 (/var/opt/kaspersky) 需要 40 GB。

我们建议在设备上安装 Kaspersky Security Center Web Console 后，在该设备上安装 Kaspersky Endpoint Security for Linux。有关Kaspersky Endpoint Security的硬件要求，请参阅Kaspersky Endpoint Security for Linux 帮助。

以下操作系统之一（**仅限 64 位版本**）：

> 对于操作系统中的进程间通讯，必须提供环回接口。

- Debian GNU/Linux 12 (Bookworm)
- Debian GNU/Linux 13 (Trixie)
- Ubuntu Server 22.04 LTS (Jammy Jellyfish)
- Ubuntu Server 24.04 LTS (Noble Numbat)
- Ubuntu Server 26.04 LTS (Resolute Raccoon) 64位
- CentOS Stream 9
- CentOS Stream 10
- Red Hat Enterprise Linux Server 7.x
- Red Hat Enterprise Linux Server 8.x
- Red Hat Enterprise Linux Server 9.x
- Red Hat Enterprise Linux Server 10.x
- SUSE Linux Enterprise Server 12 (所有服务包)
- SUSE Linux Enterprise Server 15 (所有服务包)
- Astra Linux 特别版 RUSB.10015-01（操作更新 1.6）

- Astra Linux 特别版 RUSB.10015-16（发布版 1）（操作更新 1.6）
- Astra Linux 特别版 RUSB.10015-01（操作更新 1.7）
- Astra Linux 特别版 RUSB.10015-17（操作更新 1.7.3）
- Astra Linux 特别版 RUSB.10015-01（操作更新 1.8）
- Astra Linux Special Edition RUSB.10015-03 （操作更新 7.6）
- Astra Linux 特别版 RUSB.10015-37 （操作更新 7.7）
- Astra Linux Common Edition（操作更新 2.12）
- ALT SP Server 10
- ALT SP Workstation 10
- Oracle Linux 7
- Oracle Linux 8
- Oracle Linux 9
- Platform V SberLinux OS Server (SLO) 8.10.1
- Platform V SberLinux OS Server (SLO) 9.5.1
- Platform V SberLinux OS Server (SLO) 9.6 64 位
- Platform V SberLinux OS Server (SLO) 9.7 64 位
- RED OS 7.3 Server
- RED OS 7.3 Certified Edition
- RED OS 8
- ROSA COBALT 7.9
- M OS (Moscow Electronic School) 12 Server
- Mostech Server
- MosOS 15.5 Arbat

有关受支持的虚拟化平台的信息，请参阅Kaspersky Security for Virtualization Light Agent在线帮助。

客户端设备

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

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 Web Console 所使用的浏览器的需求是相同的。

浏览器：

- Google Chrome 149.0.7827.115 或更高版本
- Microsoft Edge 149.0.4022.62 或更高版本
- macOS 上的 Safari 18.6 (20621.3.11.11.3)
- Yandex Browser 26.4.4.799 或更高版本
- Mozilla Firefox 扩展支持版本 140.11.0 或更高版本

# 网络代理要求

最小硬件条件：

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

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

**网络代理。支持的平台**

| | |
|---|---|
| 操作系统。Microsoft Windows 工作站 | Microsoft Windows Embedded POSReady 2009 with latest Service Pack 32 位<br>Microsoft Windows Embedded 7 Standard with Service Pack 1 32 位/64 位<br>Microsoft Windows Embedded 8.1 工业专业版 32 位/64 位<br>Microsoft Windows 10 Enterprise 2015 LTSB 32 位 / 64 位<br>Microsoft Windows 10 Enterprise 2016 LTSB 32 位 / 64 位<br>Microsoft Windows 10 IoT Enterprise 2015 LTSB 32 位 / 64 位<br>Microsoft Windows 10 IoT Enterprise 2016 LTSB 32 位 / 64 位<br>Microsoft Windows 10 Enterprise 2019 LTSC 32 位/64 位<br>Microsoft Windows 10 IoT Enterprise 版本 1703、1709、1803、1809 32 位/64 位<br>Microsoft Windows 10 20H2、21H2 IoT Enterprise 32 位/64 位<br>Microsoft Windows 10 IoT Enterprise 32 位/64 位<br>Microsoft Windows 10 IoT Enterprise version 1909 32 位/64 位<br>Microsoft Windows 10 IoT Enterprise LTSC 2021 32 位/64 位<br>Microsoft Windows 10 IoT Enterprise 版本 1607 32 位/64 位<br>Microsoft Windows 10 TH1（2015 年 7 月）Home/Pro/Pro for Workstations/Enterprise/Education 32 位/64 位<br>Microsoft Windows 10 TH2（2015 年 11 月）Home/Pro/Pro for Workstations/Enterprise/Education 32 位/64 位<br>Microsoft Windows 10 RS1（2016 年 8 月）Home/Pro/Pro for Workstations/Enterprise/Education 32 位/64 位<br>Microsoft Windows 10 RS2（2017 年 4 月）Home/Pro/Pro for Workstations/Enterprise/Education 32 位/64 位<br>Microsoft Windows 10 RS3 (Fall Creators Update, v1709) Home/Pro/Pro for Workstations/Enterprise/Education 32 位/64 位<br>Microsoft Windows 10 RS4（2018 年 4 月更新，17134）Home/Pro/Pro for Workstations/Enterprise/Education 32 位/64 位<br>Microsoft Windows 10 RS5（2018 年 10 月）Home/Pro/Pro for Workstations/Enterprise/Education 32 位/64 位<br>Microsoft Windows 10 RS6（2019 年 5 月）Home/Pro/Pro for Workstations/Enterprise/Education 64 位<br>Microsoft Windows 10 19H1、19H2 Home/Pro/Pro for Workstations/Enterprise/Education 32 位/64 位<br>Microsoft Windows 10 20H1（2020 年 5 月更新）Home/Pro/Pro for Workstations/Enterprise/Education 32 位/64 位<br>Microsoft Windows 10 20H2（2020 年 10 月更新）Home/Pro/Pro for Workstations/Enterprise/Education 32 位/64 位<br>Microsoft Windows 10 21H1（2021 年 5 月更新）Home/Pro/Pro for Workstations/Enterprise/Education 32 位/64 位<br>Microsoft Windows 10 21H2（2021 年 10 月更新）Home/Pro/Pro for Workstations/Enterprise/Education 32 位/64 位<br>Microsoft Windows 10 22H2（2023 年 10 月更新）Home/Pro/Pro for Workstations/Enterprise/Education 32 位/64 位<br>Microsoft Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education ARM 64 位<br>Microsoft Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education 64 位<br>Microsoft Windows 11 IoT Enterprise version 25H2 64位<br>Microsoft Windows 11 22H2 Home/Pro/Pro for Workstations/Enterprise/Education 64 位<br>Microsoft Windows 11 23H2 Home/Pro/Pro for Workstations/Enterprise/Education 64 位<br>Microsoft Windows 11 24H2 Home/Pro/Pro for Workstations/Enterprise/Education 64 位<br>Microsoft Windows 11 25H2 Home/Pro/Pro for Workstations/Enterprise/Education 64 位<br>Microsoft Windows 8.1 Pro/Enterprise 32 位/64 位<br>Microsoft Windows 8 Pro/Enterprise 32 位/64 位<br>Microsoft Windows 7 Professional/Enterprise/Ultimate/Home Basic/Premium（Service Pack 1 及更高版本）32 位/64 位<br>Microsoft Windows XP Professional with Service Pack 2 32 位/64 位（仅受网络代理版本 10.5.1781 支持）<br>Microsoft Windows XP Professional Service Pack 3 及更高的32位版本（由网络代理程序版本14.0.0.20023支持，需要Windows XP的安全更新KB2868626）<br>适用于嵌入式系统的 Microsoft Windows XP Professional Service Pack 3 32 位（受网络代理版本 14.0.0.20023 支持） |

| | |
|---|---|
| 操作系统。Microsoft Windows 服务器 | Microsoft Windows MultiPoint Server 2011 Standard/Premium 64 位<br>Microsoft Windows Server 2003 SP1 32 位/64 位（仅受网络代理版本 10.5.1781 支持，可通过技术支持进行申请）<br>Microsoft Windows Server 2003 SP2 标准版/企业版 32 位/64 位（仅受网络代理版本 10.5.1781 支持）<br>Microsoft Windows Server 2003 R2 标准版/企业版 SP2 32 位/64 位（仅受网络代理版本 10.5.1781 支持）<br>Microsoft Windows Server 2008 Foundation with Service Pack 2 32 位/64 位<br>Microsoft Windows Server 2008 Standard/Enterprise/Datacenter（Service Pack 2）32 位/64 位<br>Microsoft Windows Server 2008 R2 Datacenter/Enterprise/Foundation/Standard（含 Service Pack 1 及更高版本）64 位<br>Microsoft Windows Server 2012 Server Core/Datacenter/Essentials/Foundation/Standard 64 位<br>Microsoft Windows Server 2012 R2 Server Core/Datacenter/Essentials/Foundation/Standard 64 位<br>Microsoft Windows Server 2016 Datacenter/Standard/Server Core (安装选项) (LTSB) 64 位<br>Microsoft Windows Server 2019 Standard/Datacenter/Core 64 位<br>Microsoft Windows Server 2019 RS5 Essentials/Standard 64 位<br>Microsoft Windows Server 2022 Standard/Datacenter/Core 64 位<br>Microsoft Windows Server 2025 Standard/Datacenter/Core 64 位<br>Microsoft Windows Server 2022 21H2 Standard/Datacenter 64 位<br>Microsoft Windows Storage Server 2019 64 位<br>Microsoft Windows Small Business Server 2011 Standard 64 位<br>Microsoft Windows Small Business Server 2011 Essentials 64 位<br>Microsoft Windows Small Business Server 2011 Premium Add-on 64 位 |

| | |
|---|---|
| 操作系统。Linux | Debian GNU/Linux 10.x (Buster) 32 位/64 位<br>Debian GNU/Linux 11.x (Bullseye) 32 位/64 位<br>Debian GNU / Linux 12 (Bookworm) 32 位/64 位<br>Debian GNU/Linux 13 (Trixie) 64 位<br>Ubuntu Server 10.04 LTS (Lucid Lynx) 32 位/64 位<br>Ubuntu Server 16.04 LTS (Xenial Xerus) 32 位/64 位<br>Ubuntu Server 18.04 LTS (Bionic Beaver) 64 位<br>Ubuntu Server 20.04 LTS (Focal Fossa) 64 位<br>Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64 位<br>Ubuntu Server 22.04 LTS ARM 64 位<br>Ubuntu Server 24.04 LTS (Noble Numbat) 64 位<br>Ubuntu Server 26.04 LTS (Resolute Raccoon) 64位<br>Ubuntu Server 26.04 LTS ARM 64 位<br>Ubuntu Desktop 10.04 LTS (Lucid Lynx) 32 位/64 位<br>Ubuntu Desktop 16.04 LTS (Xenial Xerus) 32 位/64 位<br>CentOS 5.2 32 位/64 位（仅受 Linux 旧版网络代理支持，您可以使用 Web Console 界面或从卡巴斯基网站下载该代理程序）<br>CentOS 5.4 32 位/64 位（仅受 Linux 旧版网络代理支持，您可以使用 Web Console 界面或从卡巴斯基网站下载该代理程序）<br>CentOS 6.4 32 位/64 位（仅受 Linux 旧版网络代理支持，您可以使用 Web Console 界面或从卡巴斯基网站下载该代理程序）<br>CentOS 6.6 32 位/64 位（仅受 Linux 旧版网络代理支持，您可以使用 Web Console 界面或从卡巴斯基网站下载该代理程序）<br>CentOS 7.2 及更高版本 64 位<br>CentOS Stream 8 64 位<br>CentOS Stream 9 64 位<br>CentOS Stream 9 ARM 64 位<br>CentOS Stream 10 64 位<br>Red Hat Enterprise Linux Server 6.x 32 位/64 位<br>Red Hat Enterprise Linux Server 7.2 和更高版本 64 位<br>Red Hat Enterprise Linux Server 8.x 64 位<br>Red Hat Enterprise Linux Server 9.x 64 位<br>Red Hat Enterprise Linux Server 10.x 64 位<br>SUSE Linux Enterprise Server 12.5 和更高版本 (所有服务包) 64 位<br>SUSE Linux Enterprise Server 15 (所有服务包) 64 位<br>SUSE Linux Enterprise Server 15（所有服务包）ARM 64 位<br>openSUSE Leap 15 64 位<br>EulerOS 2.0 SP10 64 位<br>EulerOS 2.0 SP10 ARM 64 位<br>Astra Linux 特别版 RUSB.10015-01（操作更新 1.4）32 位<br>Astra Linux 特别版 RUSB.10015-01（操作更新 1.4）64 位（仅受适用于 Linux Legacy 的网络代理支持，您可以通过 Web Console 界面或从卡巴斯基网站下载该网络代理）<br>Astra Linux 特别版 RUSB.10015-01（操作更新 1.5）64 位<br>Astra Linux 特别版 RUSB.10015-01（操作更新 1.6）64 位<br>Astra Linux 特别版 RUSB.10015-16（发布版 1）（操作更新 1.6）64 位<br>Astra Linux 特别版 RUSB.10015-17（操作更新 1.7.3）64 位<br>Astra Linux 特别版 RUSB.10015-01（操作更新 1.7）64 位<br>Astra Linux 特别版 RUSB.10015-01（操作更新 1.8）64 位<br>Astra Linux 特别版 RUSB.10015-03（操作更新 7.6）64 位<br>Astra Linux 特别版 RUSB.10015-37 （操作更新 7.7）64 位<br>Astra Linux 特别版 RUSB.10152-02（操作更新 4.7）ARM 64 位<br>Astra Linux Common Edition（操作更新 2.12）64 位<br>ALT Workstation 11 64 位<br>ALT Server 11 64 位<br>ALT Education 11 64 位<br>ALT Workstation 10.1 64 位<br>ALT Server 10.1 64 位 |

ALT Education 10.1 64 位
ALT SP Server 10 32 位/64 位
ALT SP Server 10 ARM 64 位
ALT SP Workstation 10 32 位/64 位
ALT SP Workstation 10 ARM 64 位
ALT 8 SP Server (LKNV.11100-01) 32 位/64 位
ALT 8 SP Server (LKNV.11100-02) 32 位/64 位
ALT 8 SP Server (LKNV.11100-03) 32 位/64 位
ALT 8 SP Workstation (LKNV.11100-01) 32 位/64 位
ALT 8 SP Workstation (LKNV.11100-02) 32 位/64 位
ALT 8 SP Workstation (LKNV.11100-03) 32 位/64 位
Oracle Linux 7 64 位
Oracle Linux 8 64 位
Oracle Linux 9 64 位
Linux Mint 21.1 及更高版本 64 位
Linux Mint 22.x 64 位
AlterOS 7.5 及更高版本 64 位
AlterOS 2025 64 位
GosLinux IC6/7.17 64 位
GosLinux IC6/7.2 64 位
SberOS 3.4.0 64 位
SberOS 3.5.0 64 位
SberOS 3.6.1 64 位
Platform V SberLinux OS Server (SLO) 8.10.1 64 位
Platform V SberLinux OS Server (SLO) 9.1 64 位
Platform V SberLinux OS Server (SLO) 9.5.1 64 位
Platform V SberLinux OS Server (SLO) 9.6 64 位
Platform V SberLinux OS Server (SLO) 9.7 64 位
RED OS 7.3 Server 64 位
RED OS 7.3 Certified Edition 64 位
RED OS 8 64 位
RED OS 8 ARM 64 位
ROSA Enterprise Linux Server 7.9 64 位
ROSA Enterprise Linux Desktop 7.9 64 位
ROSA COBALT 7.9 64 位
ROSA CHROME 12 64 位
AlmaLinux 8 及更高版本 64 位
AlmaLinux 9 及更高版本 64 位
Rocky Linux 8 及更高版本 64 位
Rocky Linux 9 及更高版本 64 位
Atlant，Alcyone 内部版本，版本 2022.02 64 位
MSVSPHERE 9.2 SERVER 64 位
MSVSPHERE 9.2 ARM 64 位
MSVSPHERE 9.4 SERVER 64 位
MSVSPHERE 9.4 ARM 64 位
SynthesisM Server 8.6 64 位
SynthesisM Client 8.6 64 位
OSnova 2.* 64 位
OSnova 3.* 64 位
Kylin 10 64 位
EMIAS 1.0 64 位
Amazon Linux 2 64 位
MosOS 15.5 Arbat 64 位
OS MES (Moscow Electronic School) 12（适用于电脑和笔记本电脑）64 位
OS MES (Moscow Electronic School) 12（适用于互动平板电脑）64 位
M OS (Moscow Electronic School) 12 Server 64 位

| | |
|---|---|
| | Mostech 64 位<br>Mostech Server 64 位<br>Fedora Linux Server 41 64 位<br>Fedora Linux Workstation 41 64 位 |
| 操作系统。macOS | 有关受支持的操作系统列表，请参阅 Kaspersky Endpoint Security for Mac 帮助。 |
| 虚拟化平台 | 有关受支持的虚拟化平台的信息，请参阅Kaspersky Security for Virtualization Light Agent在线帮助。 |

在早于Microsoft Windows Server 2008 R2（服务器版本）和Microsoft Windows 7（桌面版本）的Windows版本上，网络代理程序不支持以下功能：

- 更新重译（分发点使用）
- KSN代理（分发点使用）
- 漏洞扫描任务

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

在运行 Windows 7、Windows Server 2008、Windows Server 2008 R2 或 Windows MultiPoint Server 2011 的设备上安装网络代理之前，请确保已安装适用于操作系统 Windows 的安全更新 KB3063858（Windows 7 安全更新（KB3063858）、适用于基于 x64 系统的 Windows 7 安全更新 (KB3063858)、Windows Server 2008 安全更新 (KB3063858)、Windows Server 2008 x64 版本安全更新 (KB3063858)、Windows Server 2008 R2 x64 版本安全更新 (KB3063858)。

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

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

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

Kaspersky Security Center Linux 完全支持相同或更新版本网络代理。

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

# 兼容的卡巴斯基应用程序和解决方案

Kaspersky Security Center Linux 支持集中部署和管理当前支持的所有卡巴斯基应用程序和解决方案。要了解应用程序和解决方案的版本，请参阅应用程序支持生命周期网页。

支持的卡巴斯基应用程序：

- Kaspersky Endpoint Security for Windows（支持文件服务器）
- Kaspersky Endpoint Security for Linux（支持文件服务器）
- Kaspersky Endpoint Security for Linux Elbrus Edition
- Kaspersky Endpoint Security for Mac
- Kaspersky Endpoint Security for Android
- Kaspersky Endpoint Security for Aurora
- Kaspersky Security for iOS
- Kaspersky Industrial CyberSecurity for Linux Nodes
- Kaspersky Industrial CyberSecurity for Nodes
- Kaspersky Industrial CyberSecurity for Networks
- Kaspersky Endpoint Agent
- Kaspersky Embedded Systems Security for Windows
- Kaspersky Embedded Systems Security for Linux
- Kaspersky Security for Virtualization Light Agent
- KATA Sandbox（Kaspersky Anti Targeted Attack Platform 组件之一）
- Kaspersky Thin Client
- Kaspersky NGFW
- Kaspersky Sandbox
- Kaspersky Vulnerability Management

Kaspersky Security Center Linux 包含在以下解决方案中：

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

有关应用程序的版本，请参阅产品支持生命周期网页。

已知问题

Kaspersky Industrial CyberSecurity for Networks 不支持单点登录 (SSO)。

# 关于 Kaspersky Security Center Linux 组件的兼容性

在下表中，您可以找到有关 Kaspersky Security Center Linux 组件兼容性的信息。

Kaspersky Security Center Linux 组件的兼容性

| 组件 | 兼容 |
| --- | --- |
| Kaspersky Security Center 16.3 Linux 管理服务器 | • 以下版本的 Kaspersky Security Center Web Console：16.3、16.2、16.1<br>• 以下版本的 Kaspersky Security Center 网络代理：16.3、16.2、16.1、16、15.4、15.3、15.2、15.1、15、14*、10.5** |
| Kaspersky Security Center 16.3 Web Console | 以下版本的 Kaspersky Security Center Linux 管理服务器：16.3、16.2、16.1、16 |
| Kaspersky Security Center 16.3 Linux 主管理服务器 | 从属管理服务器：<br>• 以下版本的 Kaspersky Security Center Linux：16.3、16.2、16.1、16、15.4、15.3、15.2、15.1、15<br>• 以下版本的 Kaspersky Security Center Windows：15.1 |
| Kaspersky Security Center 16.3 Linux 从属管理服务器 | 主管理服务器：<br>• 以下版本的 Kaspersky Security Center Linux：16.3、16.2、16.1、16、15.4、15.3、15.2、15.1、15<br>• 以下版本的 Kaspersky Security Center Windows：15.1 |
| Kaspersky Security Center 16.3 网络代理 | 管理服务器：<br>• 以下版本的 Kaspersky Security Center Linux：16.3、16.2、16.1、16、15.4、15.3、15.2、15.1、15<br>• 以下版本的 Kaspersky Security Center Windows：15.1 |
| Kaspersky Security Center 管理服务器数据的备份和恢复 | 以下 Kaspersky Security Center Linux 管理服务器版本支持数据备份和恢复：<br>16.2、16.1、16、15.4、15.3、15.2、15.1、15 |

*此版本支持安装了 Service Pack 3 的 Microsoft Windows XP Professional。您可以从此页面下载此网络代理程序版本。

**此版本支持安装了 Service Pack 2 的 Microsoft Windows XP Professional。您可以通过技术支持请求此网络代理程序版本。

我们建议您使用最新版本的 Kaspersky Security Center 管理服务器和 Kaspersky Security Center Web Console。否则，Kaspersky Security Center 的功能可能会受到限制。您可以独立安装和升级 Kaspersky Security Center 管理服务器以及 Kaspersky Security Center Web Console。在这种情况下，您必须确保已安装的 Kaspersky Security Center Web Console 版本与您连接的管理服务器版本兼容。

如果您有最新版本的 Kaspersky Security Center Web Console 和先前版本的 Kaspersky Security Center，域身份验证期间会发生错误，错误文本将包含一条默认消息。

# 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 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 15.1 Windows | Kaspersky Security Center 16.3 Linux |
|---|---|---|
| **管理服务器** | | |
| 数据库管理系统 (DBMS) 位置 | 本地 | 本地<br>（不支持 Microsoft SQL） |
| 在其中安装管理服务器的操作系统 | Windows | Linux |
| 管理服务器层级 | ✓ | ✓ |
| 支持虚拟管理服务器 | ✓ | ✓ |
| 部署 Kaspersky Security Center 故障转移集群 | ✓<br>仅限单站点集群 | ✓<br>从 Kaspersky Security Center 16.2 Linux 开始，支持地理分布式故障转移集群 |
| 使用 SNMP 将管理服务器统计信息发送到第三方应用程序 | ✓ | ✓ |
| 用于发布安装包和其他文件的 Web 服务器 | ✓ | ✓ |
| **管理控制台** | | |
| 管理控制台类型 | 基于 MMC 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 | Linux |
| 使用域身份验证登录控制台 | ✓ | ✓ |
| **管理客户端设备和从属管理组** | | |
| 最大受管理设备数量（每台管理服务器） | 100,000（使用 Microsoft SQL Server） | 50,000（使用 PostgreSQL 和 Postgres Pro） |
| 网络轮询 | ✓ | ✓ |
| 保护 Windows、macOS 和 Linux 管理的设备 | ✓ | ✓ |
| 保护移动设备 | ✓<br>移动设备的基本管理 | ✓<br>MDM 和使用 Kaspersky Secure Mobility Management 功能（需获得授权许可）。 |
| 虚拟机保护管理 | ✓ | ✓ |
| 保护公有云基础架构 | ✓ | – |
| 远程连接到客户端设备桌面 | ✓ | ✓ |
| 数据加密和保护 | ✓<br>在安装了 Kaspersky Endpoint Security for Windows 或 Kaspersky Endpoint Security for Mac 的 Windows 受管理设备上 | ✓<br>在安装了 Kaspersky Endpoint Security for Windows 或 Kaspersky Endpoint Security for Mac 的 Windows 受管理设备上 |

| 功能或属性 | Kaspersky Security Center 15.1 Windows | Kaspersky Security Center 16.3 Linux |
| --- | --- | --- |
| 管理组中对集群和服务器阵列的支持 | ✓ | ✓ |
| 管理组层级 | ✓ | ✓ |
| 在 DMZ 中添加连接网关作为分发点 | ✓<br>（Web Console 不支持）。 | ✓ |
| **使用用户** | | |
| 创建和管理用户账户 | ✓ | ✓ |
| **管理卡巴斯基应用程序** | | |
| 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 | ✓ | ✓ |
| 客户端设备的远程诊断 | ✓ | ✓ |
| 自动更新卡巴斯基应用程序 | ✓ | ✓ |
| 自适应异常控制支持 | ✓ | ✓ |
| 以设备为中心的安全管理 | ✓ | ✓ |
| 以用户为中心的安全管理 | ✓ | ✓ |
| **系统管理** | | |
| 在客户端设备上部署操作系统 | ✓ | — |
| 管理第三方授权许可 | ✓ | 计划于 2026 年实现 |
| 将管理服务器用作 WSUS 服务器 | ✓ | ✓<br>（仅限 Windows Update 被动搜索模式） |
| **在客户端设备上管理第三方应用程序** | | |
| 安装第三方软件更新并修复第三方软件漏洞 | ✓ | ✓ |
| 导入和导出应用程序类别 | ✓<br>（Web Console 不支持）。 | 计划于 2026 年实现 |
| **监控、报告和审计** | | |
| 管理对象修订 | ✓ | ✓ |
| 比较策略修订 | ✓ | ✓ |
| 查看和使用 Kaspersky Endpoint Detection and Response Optimum 检测到的警报 | ✓ | ✓ |
| 有关受管理设备上发生的事件的通知 | ✓ | ✓ |
| 监控策略状态和任务状态 | ✓ | ✓ |
| **集成** | | |
| 与 Kaspersky Managed Detection and Response 整合 | ✓ | ✓ |
| 与 SIEM 系统集成 | ✓ | ✓ |
| 通过 Active Directory、KASAP 和 Kaspersky TIP Sandbox 聚合警报和执行响应操作 | — | ✓<br>您必须在 Kaspersky Next XDR Optimum 授权许可下激活管理服务器，然后将 Kaspersky Next XDR Optimum 授权许可密钥部署到您的受管理应用程序。 |

# 关于 Kaspersky Security Center 云控制台

将 Kaspersky Security Center 用作本地应用程序意味着，您在本地设备上安装 Kaspersky Security Center（包括管理服务器），并通过基于 Microsoft 管理控制台的管理控制台（仅在 Kaspersky Security Center Windows 中可用）或 Kaspersky Security Center Web Console 来管理网络安全系统。

但是，您可以将 Kaspersky Security Center 用作云服务。在这种情况下，卡巴斯基专家将在云环境中安装和维护 Kaspersky Security Center，卡巴斯基将以服务的形式为您提供对管理服务器的访问。您可以通过基于云的管理控制台（名为 Kaspersky Security Center 云控制台）管理网络安全系统。该控制台的界面类似于 Kaspersky Security Center Web Console 的界面。

Kaspersky Security Center 云控制台的界面和文档以下列语言提供：

- 英语
- 法语
- 德语
- 意大利语
- 日语
- 葡萄牙语（巴西）
- 俄语
- 简体中文
- 西班牙语
- 西班牙语（拉丁美洲）
- 繁体中文

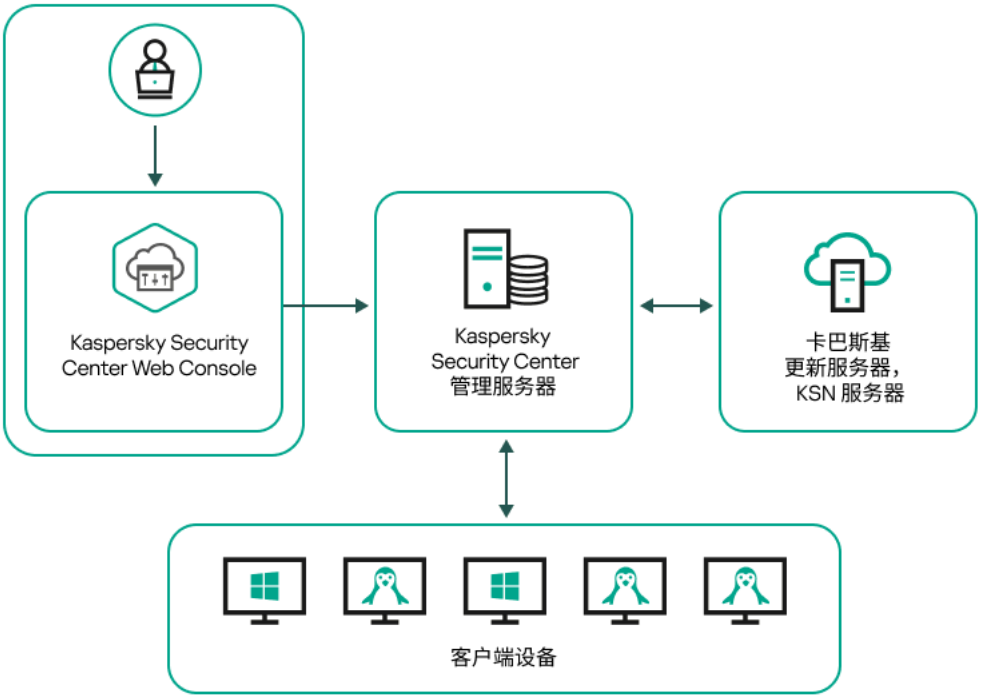
关于 Kaspersky Security Center 云控制台及其特征的更多信息请参见 Kaspersky Security Center 云控制台文档和 卡巴斯基网络安全解决方案文档。

# 架构和基本概念

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

## 架构

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



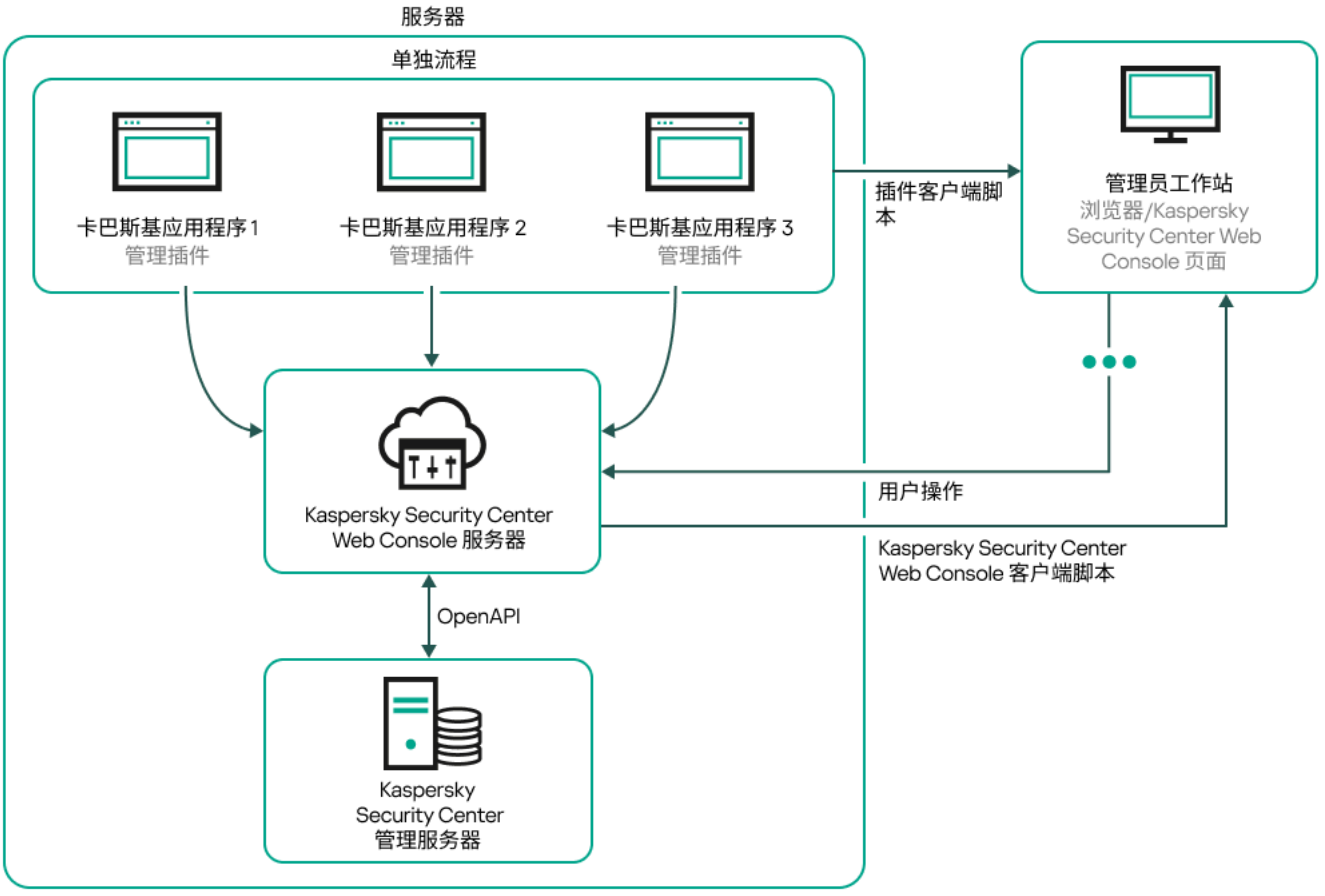

Kaspersky Security Center Linux 架构

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

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

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

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




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

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

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

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

# Kaspersky Security Center Linux 使用的端口

下表显示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。

| 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) | 使用 klakaut 实用程序自动化 Kaspersky Security Center Linux 操作 | 使用 klakaut 实用程序。klakaut 实用程序及其帮助系统位于 Kaspersky Security Center Linux 的安装文件夹中。<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 Identity and Access Manager (IAM) 到管理服务器的连接；接收通过 OpenAPI 到管理服务器的连接 | 使用 Kaspersky Security Center Web Console 对管理服务器进行管理；使用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>此端口可选，默认情况下关闭。出于安全原因，我们建议使用 13000 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。 |
| 17111（仅当设备上运行 KSN 代理服务时） | ksnproxy | HTTPS | 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。 |
| 13292（仅当管理移动设备时） | klserver | TCP (TLS) | 接收从移动设备的连接 | 移动设备管理。<br>您可以在管理控制台的管理服务器属性窗口中或在 Kaspersky Security Center Web Console 中更改默认端口号。 |
| 19170 | klserver | HTTPS (TLS) | 使用 klsctunnel 实用程序建立与受管理设备的隧道连接 | 使用 Kaspersky Security Center Web Console 远程连接到受管理设备。<br>您可以在管理服务器属性窗口（**常规→连接端口→ RDP 连接通道**）中更改默认端口号。 |

| 端口号 | 打开端口的进程名称 | 协议 | 端口目的 | 范围 |
|---|---|---|---|---|
| 4444 | kliam | HTTPS | 使用 OpenID Connect 协议进行身份验证 | 浏览器与 Identity and Access Manager (IAM) 之间的身份验证令牌交换。 |
| 9050 | kliam | HTTPS | 使用 IAM 连接到管理服务器 | 在 Kaspersky Security Center Web Console 和 IAM 之间交换身份验证令牌。 |

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 iOS™ MDM 服务器使用的端口（仅当您管理移动设备时）。

iOS MDM 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 |
|---|---|---|---|---|
| 443 | kliosmdmservicesrv | TCP (TLS) | 接收从 iOS 移动设备的连接 | 移动设备管理。<br>您可以在安装 iOS MDM 服务器时更改默认端口号。 |

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

| 端口号 | 打开端口的进程名称 | 协议 | 端口目的 | 范围 |
|---|---|---|---|---|
| 8080 | Node.js：服务器端 JavaScript | TCP (TLS) | 接收从浏览器到 Kaspersky Security Center Web Console 的连接 | Kaspersky Security Center Web Console。<br>您可以在安装 Kaspersky Security Center Web Console 时更改默认端口号。在 Linux ALT 操作系统上安装 Kaspersky Security Center Web Console 时，必须指定除 8080 以外的端口号，因为端口 8080 被操作系统使用。 |

下表显示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。 |
| 17111（仅当设备上运行 KSN 代理服务时） | ksnproxy | HTTPS | 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。 |
| 13295（仅当将分发点用作推送服务器时） | klnagent | TCP (TLS) | 从客户端设备接收连接 | 推送服务器。<br>您可以在分发点属性中更改默认端口号。 |
| 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。 |
| 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。 |

下表显示域控制器设备上使用的端口。

域控制器设备上使用的端口

| 端口号 | 协议 | 端口目的 | 范围 |
|---|---|---|---|
| 389 | TCP 或 UDP 上的 LDAP | 连接到 LDAP 服务器 | 域控制器轮询 |
| 636 | LDAP over TLS | 连接到 LDAP 服务器 | 域控制器轮询 |

下表包含未安装网络代理的客户端设备上必须开放的端口。

未分配客户端设备上使用的端口

| 端口号 | 协议 | 端口目的 | 范围 |
|---|---|---|---|
| 22 | SSH | 通过 SSH 连接到客户端设备 | 远程安装卡巴斯基应用程序。 |

# Kaspersky Security Center Web Console 使用的端口

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

Kaspersky Security Center 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 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 Web Console 的节点进程 |

| 端口号 | 服务名称 | 协议 | 端口目的 | 范围 |
| --- | --- | --- | --- | --- |
| 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 Web Console 并更新 Kaspersky Security Center Web Console 组件 |
| 4222 | Kaspersky Security Center Web Console NATS | HTTPS | 基于 NATS 的消息代理的 API 端口，用于 Kaspersky Security Center Web Console 与管理插件的进程间通信。<br>8222 端口用于监控 NATS。 | Kaspersky Security Center Web Console 与管理插件之间的交互 |
| 4444 | Identity and Access Manager (IAM) | HTTPS | OpenID Connect 身份验证协议使用的端口。 | 在 Kaspersky Security Center Web Console 与 Identity and Access Manager (IAM) 之间交换身份验证令牌 |
| 9050 | IAM | HTTPS | IAM 使用的端口。 | Kaspersky Security Center Web Console 与 IAM 之间的交互 |

# 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，请参阅以下文章：安装 Kaspersky Security Center Linux。

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
- 更新卡巴斯基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

- 生成有关卡巴斯基应用程序操作的报告
- 向客户端设备部署授权许可密钥并存储授权许可密钥信息
- 转发有关任务进度的通知（例如在客户端设备上检测到病毒）

在应用程序界面中命名管理服务器

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

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

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

# 管理服务器层级

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

在层次结构中，基于 Linux 的管理服务器既可以作为主服务器也可以作为从属服务器。基于 Linux 的主服务器可以管理基于 Linux 和基于 Windows 的从属服务器。基于 Windows 的主服务器可以管理基于 Linux 的从属服务器。

*虚拟管理服务器*是从属管理服务器的一个特例。

您可以使用管理服务器的层次结构执行以下操作：

- 降低管理服务器的负载（与整个网络中安装的单个管理服务器相比）。
- 减少 Intranet 流量并简化远程办公室的工作。您不必在主管理服务器和所有网络设备（例如，它们可能位于不同地区）之间建立连接。只需在每个网络节点中安装从属管理服务器，在从属服务器的各个管理组中分发设备，以及通过快速通信通道在从属服务器和主服务器之间建立连接。

- 在反病毒安全管理员之间分配责任。用于集中管理和监控企业网络中的反病毒安全状态的所有功能仍然可用。
- 服务提供商使用 Kaspersky Security Center。服务提供商只需安装 Kaspersky Security Center 和 Kaspersky Security Center Web Console。为了管理大量的多个组织的更多客户端设备，服务提供商可以向管理服务器层级中添加从属管理服务器（包括虚拟服务器）。

管理组层次结构中包括的每台设备都只能连接到一台管理服务器。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卡巴斯基应用程序，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 Server name>:<HTTPS port>/public/<object>
```

其中：

- `<Web Server name>`为 Kaspersky Security Center Web Server 的名称。
- `<HTTPS port>`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。
- `<object>`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。

# Kaspersky Security Center Linux Web 服务器

Kaspersky Security Center Linux Web Server（以下简称“Web 服务器”）是 Kaspersky Security Center Linux 的一个组件。Web 服务器用于发布独立安装包以及共享文件夹的文件。

所创建的安装包被自动发布在 Web 服务器并在第一次下载后被删除。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移动设备。

## Web 服务器设置

如果需要 Web 服务器的 fine-tuning，其属性允许您更改 HTTP (8060) 和 HTTPS (8061) 端口。除了更改端口，您可以为 HTTPS 替换服务器证书并为 HTTP 更改 Web 服务器的 FQDN。

## 连接网关上的 Web 服务器设置

单独的 Web 服务器服务在分发点上以连接网关模式实现，允许与连接到 Kaspersky Security Center Linux 的移动设备协同工作。该服务负责将应用安装包和设备管理配置文件传输到设备而无需将其直接连接到管理服务器。文件在服务处理连接网关上的 HTTP/HTTPS 文件请求时进行传输。

连接网关上的 Web 服务器服务与网络代理 Linux 一起安装。要使用此功能，您必须分配一个将充当连接网关模式的分发点的设备作为 Web 服务器，然后指定相应的设置。有关在连接网关上配置 Web 服务器设置的详细信息，请参阅Kaspersky Secure Mobility Management 帮助。

# 网络代理

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

安装了网络代理的设备被称为*受管理设备*或*设备*。您可以从以下来源下载网络代理的安装包：

- 管理服务器存储（您必须安装了管理服务器）
- 卡巴斯基网站

Network Agent for Linux作为服务安装在设备上，且具有以下属性集：

- 名称“卡巴斯基网络代理”
- 设置为在操作系统启动时自动启动
- 使用根账户

Network Agent for Windows作为服务安装在设备上，且具有以下属性集：

- 名称“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

macOS 网络代理作为服务安装在设备上，且具有以下属性集：

- 名称“com.kaspersky.klnagent.core”
- 设置为在操作系统启动时自动启动
- 使用根账户

服务进程的名称：

- 对于 Linux：
  - klnagent64.service（对于 64 位操作系统）
  - klnagent.service（对于 32 位操作系统）
- 对于 Windows：
  - klnagent
- 对于 macOS：
  - com.kaspersky.klnagent

默认情况下，网络代理安装程序在以下位置：

- 对于 Linux：
  - 32位系统：/opt/kaspersky/klnagent/
  - 64 位系统：/opt/kaspersky/klnagent64/
- 对于 Windows：
  - 32 位系统：C:\Program Files\Kaspersky Lab\NetworkAgent
  - 64 位系统：C:\Program Files (x86)\Kaspersky Lab\NetworkAgent
- 对于 macOS：
  - 64位系统：/Library/Application Support/Kaspersky Lab/klnagent/Binaries/klnagent

对于 Windows 设备，您可以在安装包的设置中为网络代理的安装指定不同的文件夹。但是对于 Linux 设备，网络代理只能安装在默认目录中。

网络代理安装文件夹还包含用于管理和诊断网络代理操作的实用程序，例如 klmover 和 klnagchk 实用程序。

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。

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

# 管理组

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

管理组内的所有受管理设备都被配置以做如下事情：

- 使用共同的应用程序设置（您可以在组策略中指定）。
- 通过以指定设置创建组任务，对所有应用程序使用通用的操作模式。组任务的例子包括创建和安装公用安装包、更新应用程序数据库和模块、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、Windows 或 macOS 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。一台管理服务器能够管理的设备数量取决于托管管理服务器的设备的配置和 DBMS 限制。

# 未分配的设备

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

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

# 管理员工作站

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

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

您可以将管理员的工作站作为客户端设备包括在管理组中。

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

# 管理 Web 插件

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

您可以从卡巴斯基网站下载管理 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卡巴斯基应用程序和设备的界面

- 应用程序事件传输
- Kaspersky Security Center Web Console 显示应用程序的操作数据和事件，以及从客户端设备转发的统计信息

# 政策

*政策*是应用于一个管理群组和其子群组的卡巴斯基应用程序设置集。您可以在管理组的设备上安装多个 Kaspersky 应用程序。Kaspersky Security Center 为管理组中的每个卡巴斯基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卡巴斯基应用程序，只能有一个策略处于活动状态。设备对卡巴斯基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 Linux 允许您创建*策略配置文件*。策略配置文件用于在单一管理组中的设备在不同策略设置下运行时。

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

# 任务

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

特定应用程序的任务仅在安装了该应用程序的管理插件时可以被创建。

任务可以在管理服务器和设备上执行。

以下任务在管理服务器上执行：

- 自动分发报告
- 将更新下载至管理服务器存储库
- 备份管理服务器数据
- 数据库维护

以下类型的任务在设备上执行：

- *本地任务* — 在特定设备上执行的任务。

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

- *组任务* — 在特定组的所有设备上执行的任务。

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

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

您可以为每个应用程序创建不管多少个组任务、全局任务或本地任务。

您可以更改任务设置、查看任务进度、复制、导出、导入和删除任务。

仅当为其创建任务的应用程序在运行时，才能在设备上启动任务。

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

不在任务设置中包括私人数据。例如，避免指定域管理员密码。

# 任务范围

*任务范围*是执行任务的设备集合。范围的类型包括以下：

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

当创建*全局任务*时，您可以使用以下方法指定范围：

- 手动指定特定设备。

  您可以使用 IP 地址（或 IP 范围）或 DNS 名称作为设备地址。您还可以选择由管理服务器检测到的联网设备。

- 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。

- 作为代理服务器加入卡巴斯基安全网络 (KSN)。

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

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

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

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

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

如果管理员手动分配分发点，则可以将它们分配给管理组或网络位置。

带有活动连接配置文件的网络代理不参与广播域检测。

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

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

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

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

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

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

作为分发点的设备必须被保护，包括物理保护，以防范非授权的访问。

# 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。

# 虚拟管理服务器

基于物理管理服务器，可以创建多个虚拟管理服务器，它们与从属管理服务器相似。相比于基于访问控制列表（ACLs）的任意访问模式，虚拟管理服务器模式功能更强大并且提供更高度隔离。除了具有策略和任务的已分配设备的专用管理组结构外，每个虚拟管理服务器还具有自己的未分配设备组、自己的报告集、选定的设备和事件、安装包、移动规则等。虚拟管理服务器的功能范围既可以被服务提供商 (xSP) 用来最大限度地隔离客户，也可以为具有复杂工作流和众多管理员的大型组织所用。

虚拟管理服务器与从属管理服务器非常相似，但是有以下不同点：

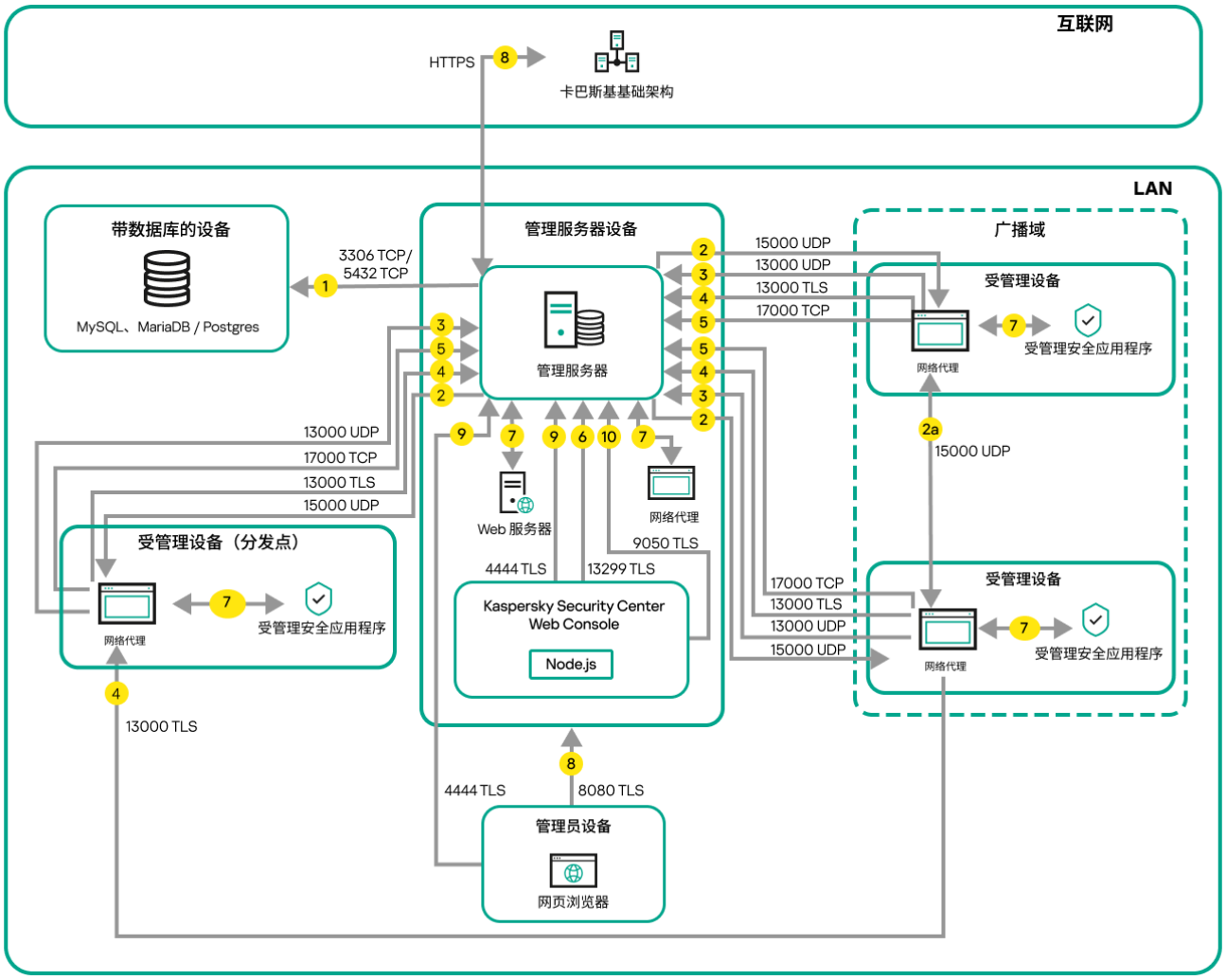
- 虚拟管理服务器缺少多数全局设置和自己的 TCP 端口。
- 虚拟管理服务器没有从属管理服务器。
- 虚拟管理服务器没有其他虚拟管理服务器。
- 物理管理服务器可以查看它所有虚拟管理服务器的设备、组、事件和受管理设备上的对象（隔离区条目、应用程序注册表等等）。
- 虚拟管理服务器仅可以扫描连接了分发点的网络。

# 数据流量和端口使用的 schema

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

# LAN 中的管理服务器和受管理设备

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




局域网 (LAN) 中的管理服务器和受管理设备

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

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

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

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

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

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

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

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

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

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

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

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

   身份和访问管理器 (IAM)组件通过 TLS 端口 13299 连接到管理服务器。

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

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

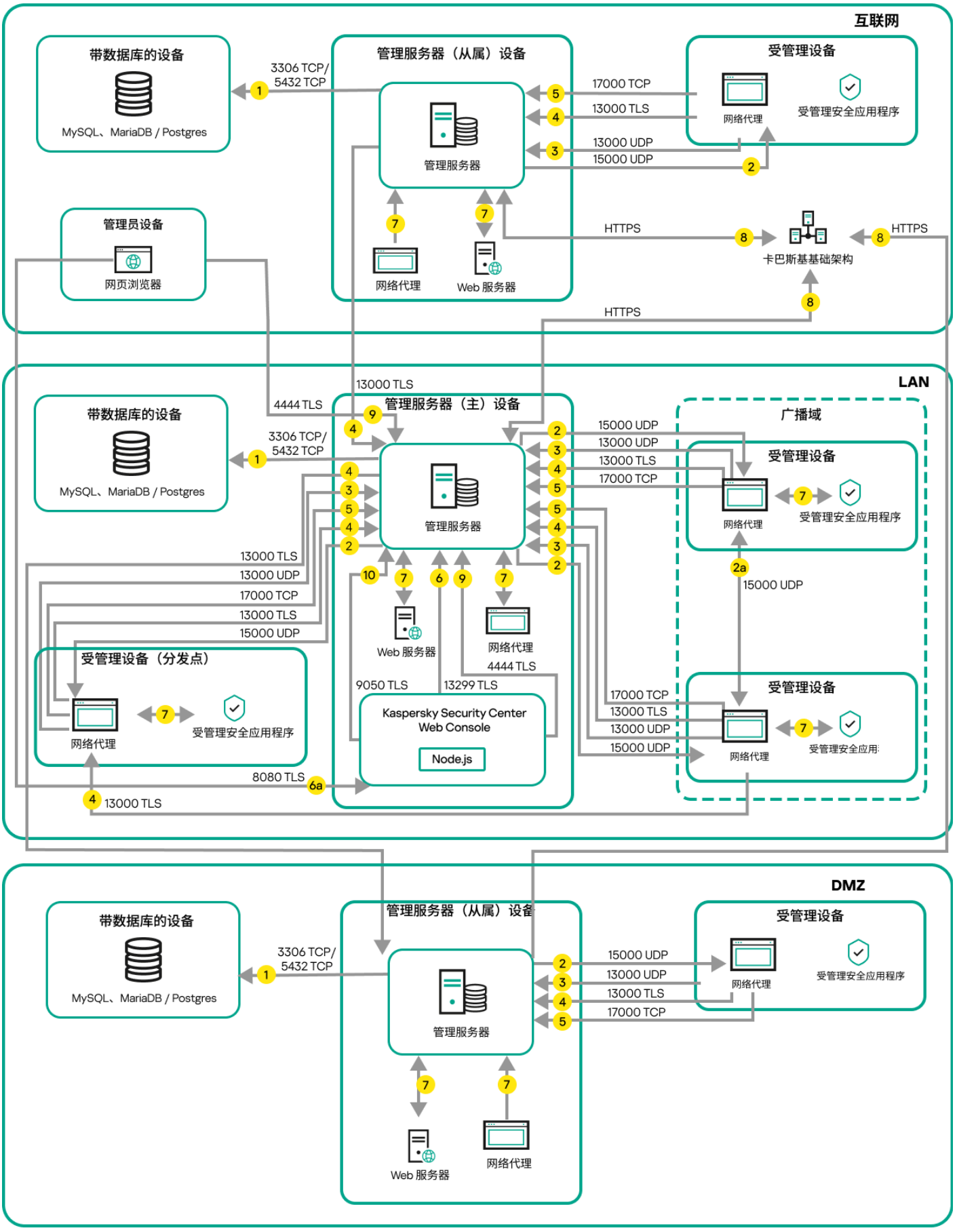
   如果您不想让您的管理服务器拥有互联网连接，您必须手动管理该数据。

9. Kaspersky Security Center Web Console 服务器和浏览器（与 Kaspersky Security Center Web Console 一起使用）将经由 TLS 端口 4444，通过 OpenID Connect 身份验证协议连接到管理服务器。

10. Kaspersky Security Center Web Console 服务器通过 TLS 端口 9050 连接到管理服务器。

# 局域网中的主管理服务器和两个从属管理服务器

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




管理服务器层级：主管理服务器和两个从属管理服务器

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

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

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

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

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

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

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

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

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

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

   身份和访问管理器 (IAM)组件通过 TLS 端口 13299 连接到管理服务器。

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

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

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

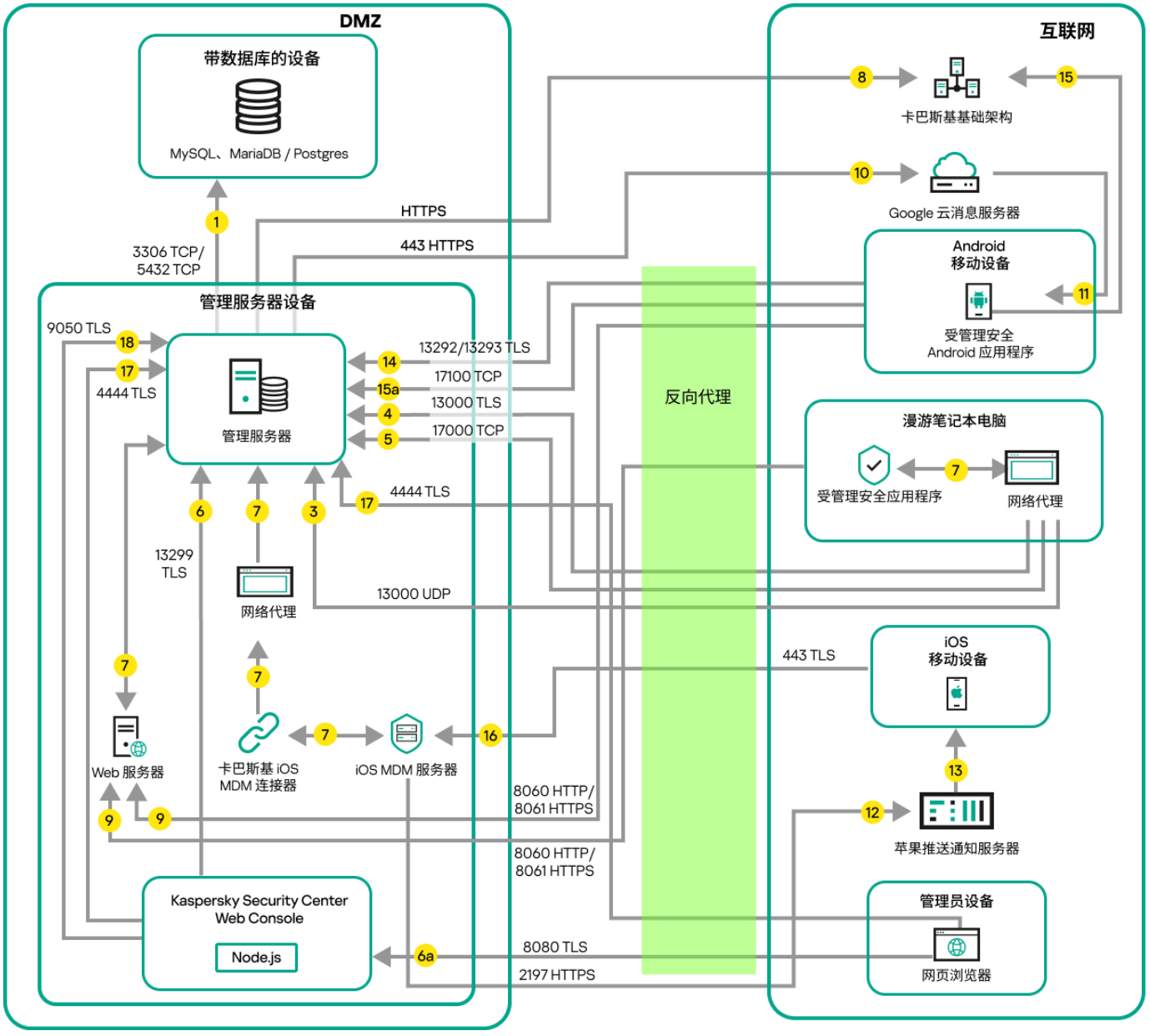
   如果您不想让您的管理服务器拥有互联网连接，您必须手动管理该数据。

9. Kaspersky Security Center Web Console 服务器和浏览器（与 Kaspersky Security Center Web Console 一起使用）将经由 TLS 端口 4444，通过 OpenID Connect 身份验证协议连接到管理服务器。

10. Kaspersky Security Center Web Console 服务器通过 TLS 端口 9050 连接到管理服务器。

# 管理服务器位于 LAN、受管理设备位于互联网、反向代理使用中

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




管理服务器位于局域网；受管理设备通过反向代理连接到管理服务器

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

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

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

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

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

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

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

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

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

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

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

   身份和访问管理器 (IAM)组件通过 TLS 端口 13299 连接到管理服务器。

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

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

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

   如果您不想让您的管理服务器拥有互联网连接，您必须手动管理该数据。

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

10. 仅对 Android 移动设备：来自管理服务器的数据被传输到 Google 服务器。该连接用于通知 Android 移动设备他们需要连接到管理服务器。然后推送通知被发送到移动设备。

11. 仅对 Android 移动设备：来自 Google 服务器的推送通知被发送到移动设备。该连接用于通知移动设备他们需要连接到管理服务器。

12. 仅对 iOS 移动设备：来自 iOS MDM 服务器的数据被发送到 Apple 推送通知服务器。然后推送通知被发送到移动设备。

13. 仅对 iOS 移动设备：推送通知从 Apple 服务器被发送到移动设备。该连接用于通知 iOS 移动设备他们需要连接到 iOS MDM 服务器。

14. 仅对移动设备：来自受管理应用程序的数据通过 TLS 端口 13292 / 13293 被传输到管理服务器（或连接网关）— 直接或通过反向代理。

15. 仅对移动设备：来自移动设备的数据被传输到 Kaspersky 基础架构。

    如果移动设备没有互联网访问，数据通过端口 17100 发送到管理服务器，然后管理服务器将其发送到 Kaspersky 基础架构；然而，该方案很少被应用。

16. 仅针对 iOS 移动设备：来自移动设备的数据通过 TLS 端口 443 传输到 iOS MDM 服务器，该服务器与管理服务器位于同一设备上或位于连接网关上。

17. Kaspersky Security Center Web Console 服务器和浏览器（与 Kaspersky Security Center Web Console 一起使用）将经由 TLS 端口 4444，通过 OpenID Connect 身份验证协议连接到管理服务器。

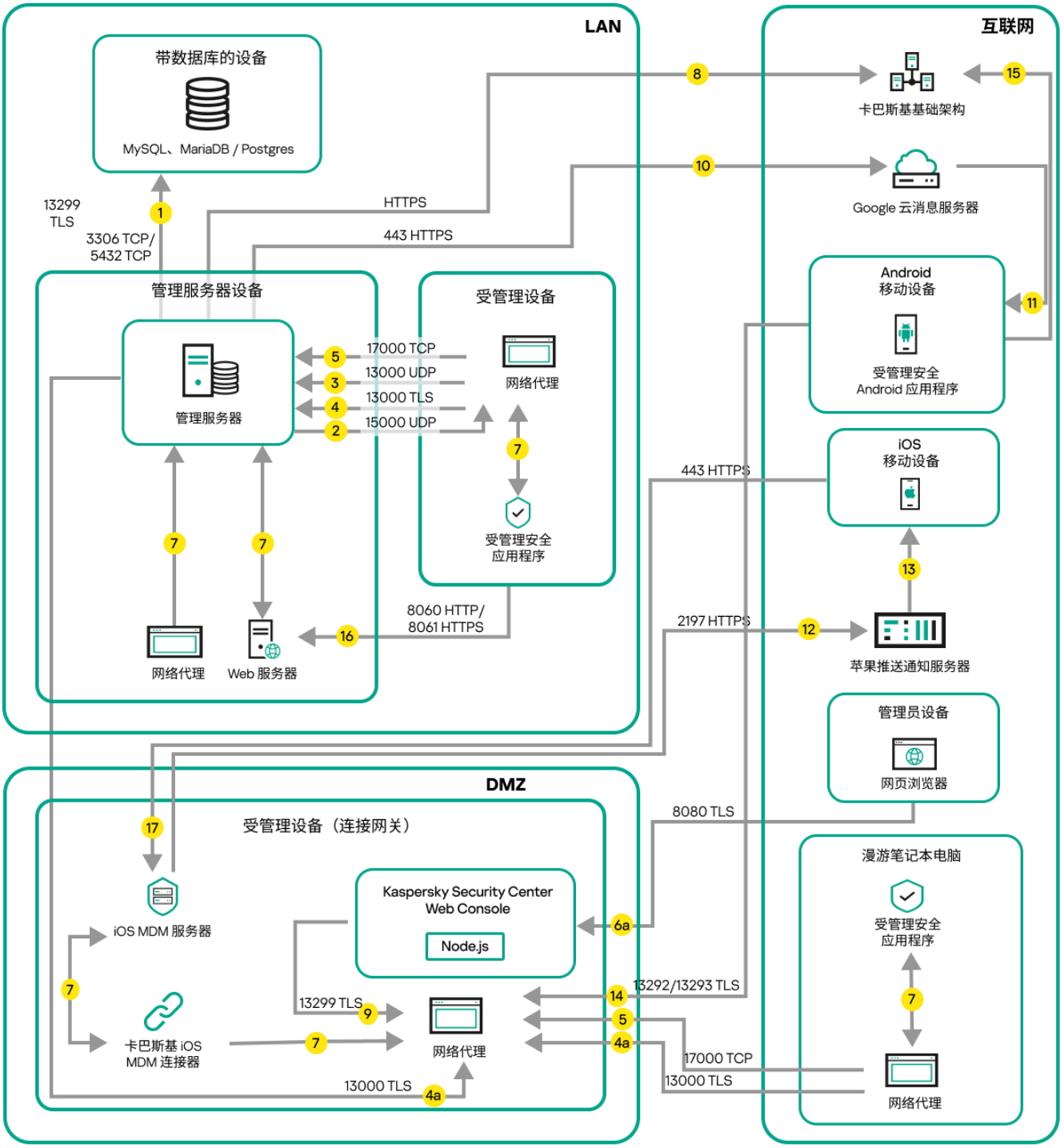
18. Kaspersky Security Center Web Console 服务器通过 TLS 端口 9050 连接到管理服务器。

# 管理服务器位于 LAN、受管理设备位于互联网、连接网关使用中

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

如果您不想让受管理设备直接连接到管理服务器，且不想使用反向代理或企业防火墙，则推荐采用该部署方案。

对于此部署方案，不支持 Identity and Access Manager (IAM) 提供的域身份验证（单点登录）功能。




受管理移动设备通过连接网关连接到管理服务器

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

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

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

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

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

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

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

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

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

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

   漫游设备也通过 TLS 端口 13000 连接到连接网关。

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

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

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

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

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

   如果您不想让您的管理服务器拥有互联网连接，您必须手动管理该数据。

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

10. 仅对 Android 移动设备：来自管理服务器的数据被传输到 Google 服务器。该连接用于通知 Android 移动设备他们需要连接到管理服务器。然后推送通知被发送到移动设备。

11. 仅对 Android 移动设备：来自 Google 服务器的推送通知被发送到移动设备。该连接用于通知移动设备他们需要连接到管理服务器。

12. 仅对 iOS 移动设备：来自 iOS MDM 服务器的数据被发送到 Apple 推送通知服务器。然后推送通知被发送到移动设备。

13. 仅对 iOS 移动设备：推送通知从 Apple 服务器被发送到移动设备。该连接用于通知 iOS 移动设备他们需要连接到 iOS MDM 服务器。

14. 仅对移动设备：来自受管理应用程序的数据通过 TLS 端口 13292 / 13293 被传输到管理服务器（或连接网关）— 直接或通过反向代理。

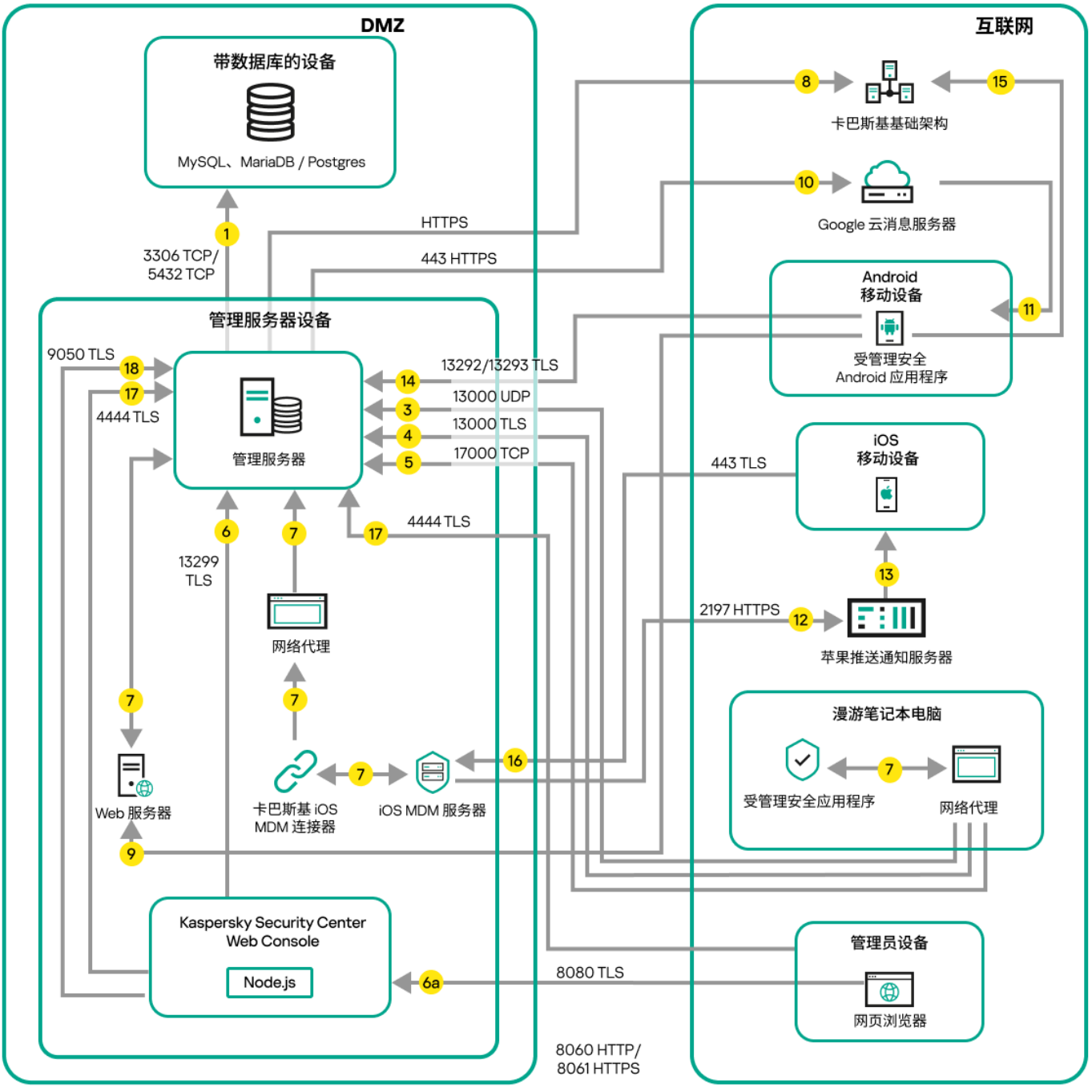
15. 仅对移动设备：来自移动设备的数据被传输到 Kaspersky 基础架构。

> 如果移动设备没有互联网访问，数据通过端口 17100 发送到管理服务器，然后管理服务器将其发送到 Kaspersky 基础架构；然而，该方案很少被应用。

16. 仅针对 iOS 移动设备：来自移动设备的数据通过 TLS 端口 443 传输到 iOS MDM 服务器，该服务器与管理服务器位于同一设备上或位于连接网关上。

# 管理服务器位于 DMZ、受管理设备位于互联网

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




管理服务器位于 DMZ、受管理移动设备位于互联网

在该图像中，未使用连接网关：移动设备直接连接到管理服务器。

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

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

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

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

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

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

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

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

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

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

   身份和访问管理器 (IAM)组件通过 TLS 端口 13299 连接到管理服务器。

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

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

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

   如果您不想让您的管理服务器拥有互联网连接，您必须手动管理该数据。

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

10. 仅对 Android 移动设备：来自管理服务器的数据被传输到 Google 服务器。该连接用于通知 Android 移动设备他们需要连接到管理服务器。然后推送通知被发送到移动设备。FCM 服务也在 443 HTTPS 端口上运行。

11. 仅对 Android 移动设备：来自 Google 服务器的推送通知被发送到移动设备。该连接用于通知移动设备他们需要连接到管理服务器。

12. 仅对 iOS 移动设备：来自 iOS MDM 服务器的数据被发送到 Apple 推送通知服务器。然后推送通知被发送到移动设备。

13. 仅对 iOS 移动设备：推送通知从 Apple 服务器被发送到移动设备。该连接用于通知 iOS 移动设备他们需要连接到 iOS MDM 服务器。

14. 仅对移动设备：来自受管理应用程序的数据通过 TLS 端口 13292 / 13293 被传输到管理服务器（或连接网关）— 直接或通过反向代理。

15. 仅对移动设备：来自移动设备的数据被传输到 Kaspersky 基础架构。

    如果移动设备没有互联网访问，数据通过端口 17100 发送到管理服务器，然后管理服务器将其发送到 Kaspersky 基础架构；然而，该方案很少被应用。

16. 仅针对 iOS 移动设备：来自移动设备的数据通过 TLS 端口 443 传输到 iOS MDM 服务器，该服务器与管理服务器位于同一设备上或位于连接网关上。

17. Kaspersky Security Center Web Console 服务器和浏览器（与 Kaspersky Security Center Web Console 一起使用）将经由 TLS 端口 4444，通过 OpenID Connect 身份验证协议连接到管理服务器。

18. Kaspersky Security Center Web Console 服务器通过 TLS 端口 9050 连接到管理服务器。

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

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

## 交互模式中的惯例

下表提供了方案中使用的转换。

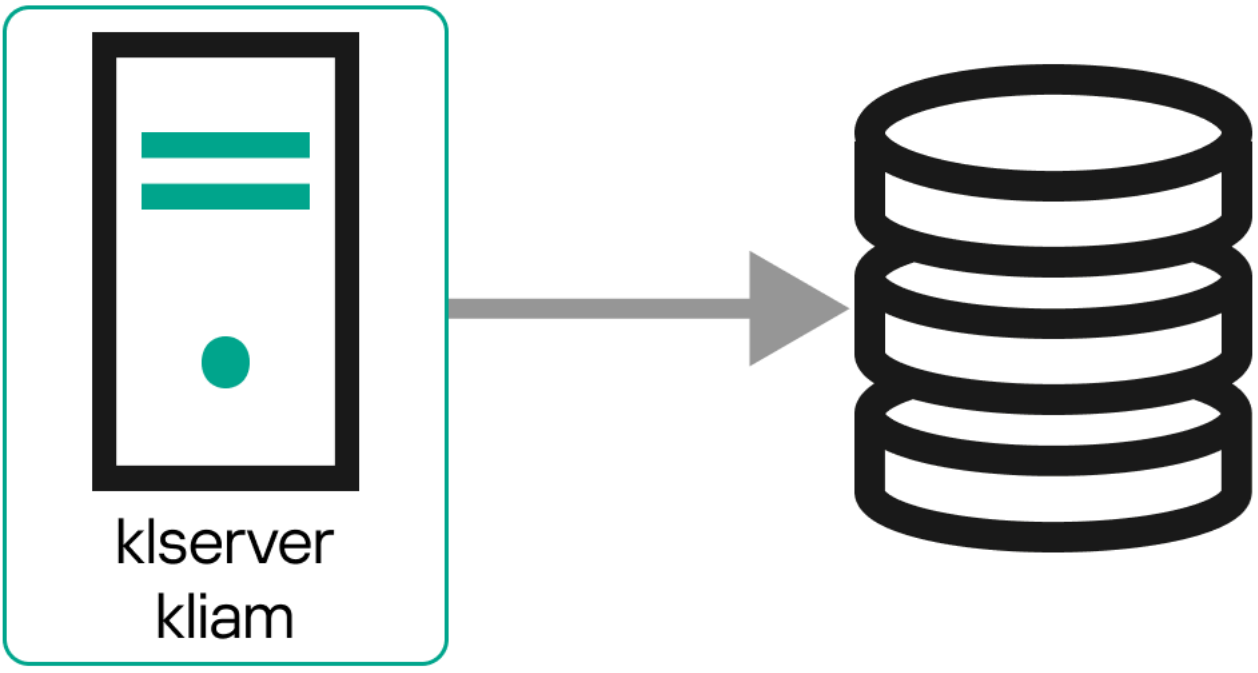
文档约定

| 图标 | 含义 |
| --- | --- |
|  | 管理服务器 |
|  | 从属管理服务器 |
|  | DBMS |
|  | 客户端设备(安装了网络代理和 Kaspersky Endpoint Security 系列应用程序，或 Kaspersky Security Center Linux 可以管理的其他应用程序) |
|  | 连接网关 |
|  | 分发点 |

| | |
|---|---|
|  | 用户设备上的浏览器 |
|  | 运行在设备和打开端口的进程 |
|  | 端口和其号码 |
|  | TCP 流量（箭头方向显示流量方向） |
|  | UDP 流量（箭头方向显示流量方向） |
|  | DBMS 传输 |
|  | DMZ 边界 |

# 管理服务器和 DBMS

管理服务器和 Identity and Access Manager (IAM) 的数据分别存储在同一个 DBMS 中的不同数据库中。



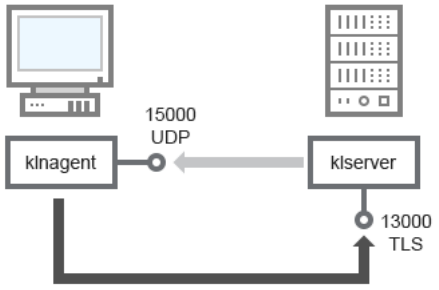

管理服务器、 Identity and Access Manager 和 DBMS

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。
IAM 连接到 DBMS 所用的端口由用户在 Kaspersky Security Center Linux 安装期间指定。

当卸载或者将服务器移动到另一部设备时，管理服务器不会自动移除管理服务器数据库和 IAM 数据库。如有必要，您必须手动移除这些数据库。

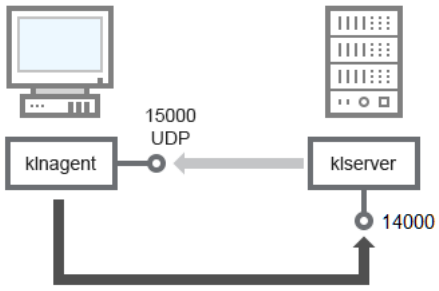
# 管理服务器和客户端设备：管理安全应用程序

管理服务器通过 TLS 端口 13000 从网络代理接收连接（参见下图）。




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

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




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

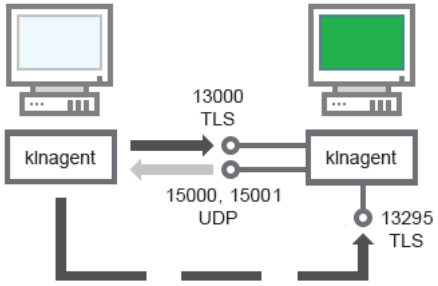
为了澄清方案，参见下图。

管理服务器和客户端设备：管理安全应用程序（流量）

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

# 通过分发点在客户端设备上升级软件

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




通过分发点在客户端设备上升级软件

对于方法描述，参见下表。

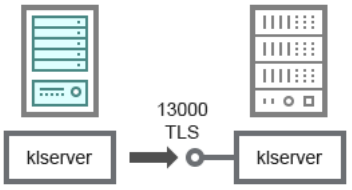
通过分发点升级软件（流量）

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

# 管理服务器层级：主管理服务器和从属管理服务器

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

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



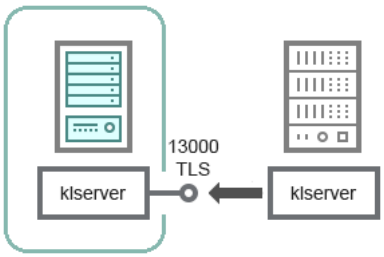

管理服务器层级：主管理服务器和从属管理服务器

对于方法描述，参见下表。

管理服务器层级（流量）

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

# DMZ 中带有从属管理服务器的管理服务器层级




DMZ 中带有从属管理服务器的管理服务器层级

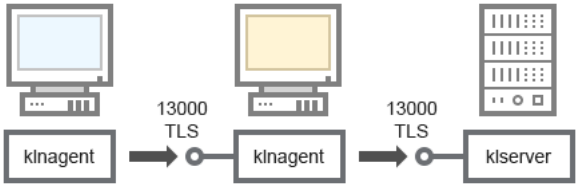
方案显示了管理服务器层级，其中 DMZ 中的从属管理服务器从主管理服务器接收连接（有关方案说明，请参见下表）。当组合两个管理服务器到一个层级，确保端口 13299 在两个管理服务器上都可以访问。Kaspersky Security Center Web Console 通过端口 13299 连接到管理服务器。

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

DMZ 中带有从属管理服务器的管理服务器层级（流量）

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

# 管理服务器、网段连接网关和客户端设备



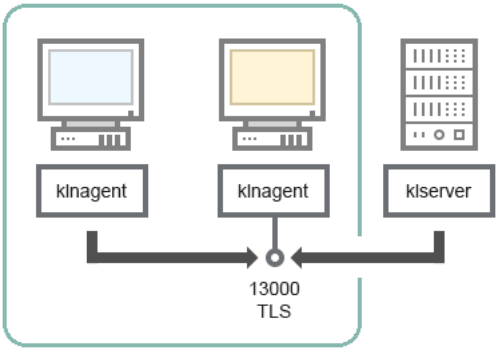

管理服务器、网段连接网关和客户端设备

对于方法描述，参见下表。

管理服务器、网段连接网关和客户端设备（流量）

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

# 管理服务器和 DMZ 中的两台设备：连接网关和客户端设备



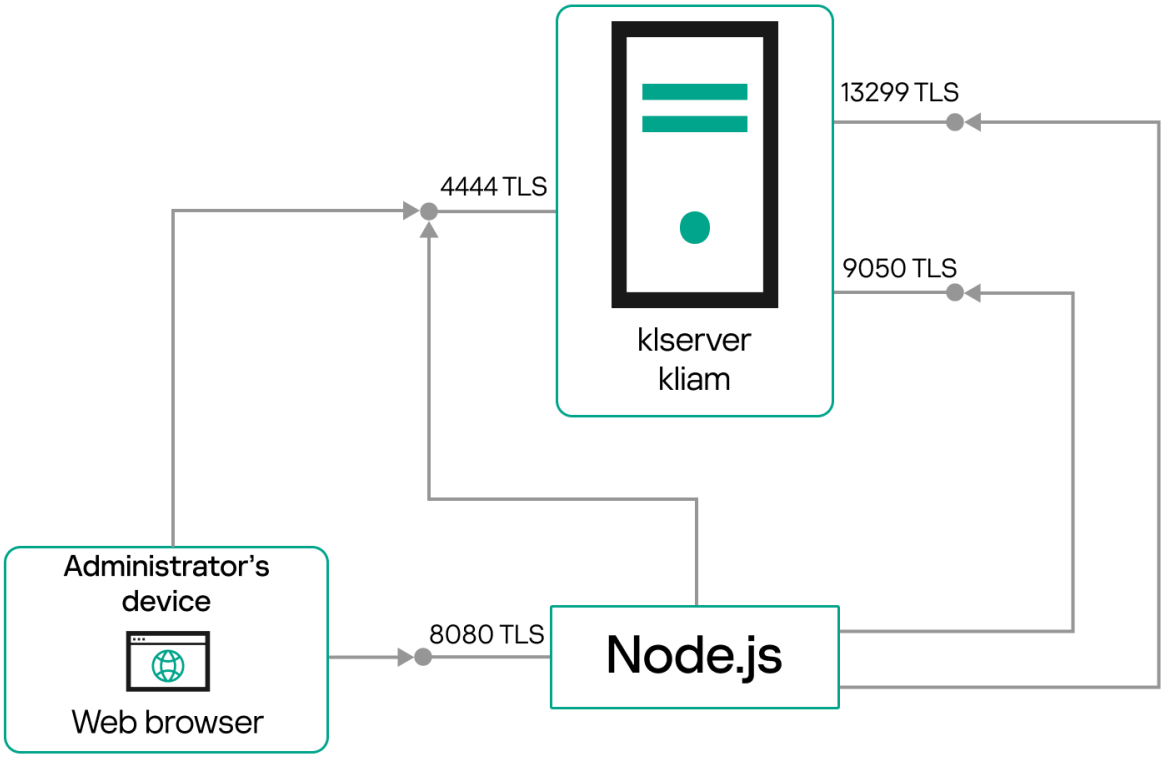

带有连接网关的管理服务器和 DMZ 中的客户端设备

对于方法描述，参见下表。

带有网段连接网关的管理服务器和客户端设备（流量）

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

# 管理服务器和 Kaspersky Security Center Web Console




管理服务器和 Kaspersky Security Center Web Console

对于方法描述，参见下表。

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

| 设备 | 端口号 | 打开端口的进程名称 | 协议 | 端口目的 |
|---|---|---|---|---|
| 管理服务器 | 13299 | klserver | TCP (TLS) | 通过 OpenAPI 接收从 Kaspersky Security Center Web Console 和 Identity and Access Manager (IAM) 到管理服务器的连接 |
| Kaspersky Security Center Web Console 服务器或管理服务器 | 8080 | Node.js：服务器端 JavaScript | TCP (TLS) | 从 Kaspersky Security Center Web Console 接收连接 |
| 管理服务器 | 4444 | kliam | TCP (TLS) | 通过 OpenID Connect 身份验证协议接收从 Kaspersky Security Center Web Console 服务器和浏览器（与 Kaspersky Security Center Web Console 一起使用）到带有 IAM 的管理服务器的连接 |
| 管理服务器 | 9050 | kliam | TCP (TLS) | 接收从 Kaspersky Security Center Web Console 到 IAM 的连接 |

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

# 启动

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

## 先决条件

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

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

## 阶段

主要安装方案分阶段进行：

1. **选择组织保护结构**

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

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

2. **准备使用自定义证书**

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

3. **安装数据库管理系统（DBMS）**

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

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

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

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

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

   > 如果您想在安装后更改DBMS 类型，则必须重新安装 Kaspersky Security Center Linux。您可以导出任务和策略，以便在重新安装后导入。请参阅以下文章：导出任务、导出策略。

### 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，根据网络配置来配置端口并指定连接设置。

### 5 安装 Kaspersky Security Center Linux

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

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

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

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

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

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

### 8 执行初始化设置

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

### 9 发现网络设备

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

### 10 整理设备到管理组

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

确保所有受管理设备被正确分配到适当的管理组，且网络中不再有未分配的设备。

### 11 分配分发点

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

### 12 安装网络代理和安全应用程序到网络设备

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

要远程安装应用程序，运行保护部署向导。

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

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

### 13 部署授权许可密钥到客户端设备

部署授权许可密钥到客户端设备以在这些设备上激活受管理安全应用程序。

### 14 配置 Kaspersky 应用程序策略

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

### 15 监控网络保护状态

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

# 强化指南

Kaspersky Security Center Linux 设计用于在组织网络中集中执行基本的管理和维护任务。该应用程序使管理员可以访问有关组织网络安全级别的详细信息。Kaspersky Security Center Linux 允许您配置使用卡巴斯基应用程序构建的所有保护组件。

Kaspersky Security Center Linux 管理服务器拥有对客户端设备保护管理的完全访问权限，是组织安全系统中最重要的组件。因此，管理服务器需要增加保护方法。

配置之前，请使用管理服务器数据备份任务或 klbackup 实用程序创建 Kaspersky Security Center Linux 管理服务器备份副本并将其保存在安全位置。

强化指南描述了配置 Kaspersky Security Center Linux 及其组件的建议和功能，旨在降低其危害的风险。

强化指南包含以下信息：

- 选择管理服务器架构
- 配置与管理服务器的安全连接
- 配置访问管理服务器的账户
- 管理服务器保护的管理
- 管理客户端设备保护
- 配置受管理应用程序的保护
- 管理服务器维护
- 将信息传输到第三方应用程序
- 第三方信息系统安全建议

# 加固检查清单

## 管理服务器部署

- 在专用物理服务器或虚拟服务器上安装管理服务器。
- 请勿使用专用服务器运行其他服务。
- 请勿在以下位置安装管理服务器（以下简称“服务器”）：
  - 域控制器
  - 终端服务器
  - 用户设备

## 连接安全

- 配置防火墙以限制对服务器设备的所有端口和协议的访问，但服务器所需的端口例外。仅允许受受信任设备访问服务器设备。
- 配置用于将 Kaspersky Security Center Web Console（也称为 Web Console）连接到 Web Console 服务器的服务器端口的IP 地址允许列表。
- 配置防火墙，仅允许受信任设备通过 Web Console 访问服务器。
- 在服务器上配置 TLS 协议版本 1.2 或更高版本。
- 配置防火墙以限制对安装了服务器数据库管理系统的设备的访问。
- 配置服务器与数据库管理系统（MySQL或PostgreSQL）之间的 SSL身份验证。

## 账号与授权

- 为服务器访问启用双重身份验证（TOTP，RFC 6238）。
- 请勿在通过云控制台与服务器建立连接的同一设备上安装身份验证器应用程序。
- 请通过使用令牌、智能卡或其他方法使用多重身份验证 (MFA) 访问服务器设备。
- 为服务器设备创建一个专用管理组，并为其创建特殊安全策略。
- 限制拥有主管理员角色的用户数量。

- 根据用户角色和组角色配置对服务器功能的访问权限。
- 仅允许为单独用户账户远程安装应用程序。
- 对服务器设备上的所有用户进行定期审核。

管理服务器保护的管理

- 在服务器设备上安装安全应用程序。
  - 对于物理服务器 — Kaspersky Endpoint Security
  - 对于虚拟服务器 — Kaspersky Security for Virtualization
- 创建并应用单独策略进行服务器保护（与其他受管理设备的安全策略不同）。
- 启用安全应用程序中所有可用的保护模块。

为受管理应用程序配置策略和任务

- 为以下应用程序创建策略并将其应用于所有受管理设备或包含新受管理设备的组：
  - 网络代理
  - Kaspersky Endpoint Security for Windows/Linux/macOS
  - Kaspersky Endpoint Agent（或其他卡巴斯基应用程序）
- 启用密码保护，防止禁用保护或卸载卡巴斯基应用程序。
- 锁定策略设置（关闭"锁定"），防止在受管理设备上重新分配这些设置。
- 为所有设备创建全盘扫描任务。
- 启用卡巴斯基安全网络 (KSN)并接受最新的KSN 声明。
- 配置设备发现，并为新发现的设备指定默认管理组。
- 限制使用自动规则在管理组之间移动设备。
- 保护分发点免受未经授权的访问。
- 避免在小型网络或高重要性网络中自动分配分发点。

管理服务器维护

- 请勿删除或禁用以下任务：
  - 备份
  - 管理服务器维护
- 定期安装操作系统和第三方软件更新。

事件传输到第三方系统

- 配置安全事件的监控和报告。
- 配置事件导出到 SIEM 系统。
- 为以下内容配置服务器通知：
  - 审计事件
  - 严重事件
  - 故障事件和警告

第三方信息系统安全建议

- 将 CIS 基准安全建议应用于所使用的操作系统、DBMS 和 Hypervisor。
- 对于 Astra Linux，请遵循相应红皮书版本的安全建议。
- 对于 RED OS，请遵循 RED OS 官方文档中的建议。

# 管理服务器部署

管理服务器架构

一般来说，集中式管理架构的选择取决于受保护设备的位置、相邻网络的访问、数据库更新的交付方案等。

在架构开发的初始阶段，我们建议熟悉 Kaspersky Security Center Linux 组件以及他们之间的互动，以及数据流量和端口使用的模式。

基于此信息，您可以形成一个架构指定：

- 管理服务器位置和网络连接
- 管理员工作区的组织以及连接到管理服务器的方法
- 网络代理及防护软件的部署方法
- 使用分发点
- 使用虚拟管理服务器
- 使用管理服务器层级
- 反病毒数据库更新方案
- 其他信息流

## 选择用于安装管理服务器的设备

我们建议将管理服务器安装在组织基础架构的专用服务器上。如果服务器上没有安装其他第三方软件，您可以根据 Kaspersky Security Center Linux 的要求配置安全设置而不依赖于第三方软件的要求。

您可以在物理服务器或虚拟服务器上部署管理服务器。请确保所选设备满足硬件和软件要求。

## 限制将管理服务器安装在域控制器、终端服务器或用户设备上

我们强烈不建议将管理服务器安装在域控制器、终端服务器或用户设备上。

我们建议您提供网络关键节点的功能分离。这种方法允许您在节点出现故障或受到损害时保持不同系统的可操作性。同时，您可以为每个节点创建不同的安全策略。

## 用于安装和运行管理服务器的账户

在部署管理服务器期间，需要创建两个非特权账户。管理服务器中包含的服务将在这些非特权账户下运行。为账户授予权限时，请遵循最低权限原则。避免在“kladmins”组中包含不必要的账户。

您还需要创建一个内部 DBMS 账户。管理服务器使用此内部 DBMS 账户来访问选定的 DBMS。

所需账户及其权利集取决于所选的 DBMS 类型和管理服务器数据库创建方法。

# 连接安全

## TLS 的使用

我们建议禁止与管理服务器的不安全连接。例如，您可以在管理服务器设置中禁止使用 HTTP 的连接。

请注意，默认情况下，管理服务器的几个 HTTP 端口是关闭的。其余端口用于管理服务器 Web 服务器 (8060)。此端口可受管理服务器设备的防火墙设置限制。

## 严格的 TLS 设置

建议使用 1.2 及以后版本的 TLS 协议，限制或禁止不安全的加密算法。

您可以配置管理服务器使用的加密协议 (TLS)。请注意，在发布管理服务器版本时，默认配置加密协议设置以确保数据安全传输。

## 限制访问管理服务器数据库

我们建议限制访问管理服务器数据库。例如，只允许从管理服务器设备进行访问。这可降低管理服务器数据库因已知漏洞而受到损害的可能性。

您可以根据使用的数据库的操作说明配置参数，也可以在防火墙上提供关闭的端口。

## 与外部 DBMS 的安全交互

如果在安装管理服务器期间将 DBMS 安装在单独的设备上（外部 DBMS），我们建议配置与该 DBMS 进行安全交互和身份验证的参数。有关配置 SSL 身份验证的更多信息，请参阅“身份验证 PostgreSQL 服务器”和“场景：身份验证 MySQL 服务器”。

## 配置允许连接到管理服务器的 IP 地址允许列表

默认情况下，Kaspersky Security Center Linux 用户可以从安装了 Kaspersky Security Center Web Console 或者 OpenAPI 应用程序的任何设备登录 Kaspersky Security Center Linux。您可以配置管理服务器，使用户只能从具有允许 IP 地址的设备进行连接。例如，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 Web Console 服务器连接到 Kaspersky Security Center Linux，他或她将无法登录Kaspersky Security Center Linux。

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

默认情况下，Kaspersky Security Center Linux 用户可以从任何设备连接到 Kaspersky Security Center Web Console。在具有 Kaspersky Security Center Web Console 的设备上，您必须配置防火墙（内置于操作系统或第三方防火墙中），以便操作员只能从允许的 IP 地址连接到 Kaspersky Security Center Web Console。

### 轮询期间与域控制器连接的安全性

为了轮询域控制器，管理服务器或 Linux 分发点尝试通过 LDAPS 连接到该域。默认情况下，连接时不需要证书验证。要强制执行证书验证，请将 `KLNAG_LDAP_TLS_REQCERT` 标志设置为 1。此外，您可以使用 `KLNAG_LDAP_SSL_CACERT`标志指定证书颁发机构 (CA) 的自定义路径来访问证书链。

## 账户和身份验证

在执行以下步骤之前，请使用管理服务器数据备份任务或 klbackup 实用程序创建 Kaspersky Security Center Linux 管理服务器备份副本并将其保存在安全位置。

### 通过管理服务器使用双重身份验证

Kaspersky Security Center Linux为**Kaspersky Security Center云控制台的用户提供基于RFC 6238标准（TOTP：基于时间的一次性密码算法）的双重身份验证**。

每次登录Kaspersky Security Center云控制台时，您都需要输入用户名、密码以及额外的一次性安全码。若要接收一次性安全码，您的电脑或移动设备上必须安装双重身份验证应用。

有支持 RFC 6238 标准的软件和硬件验证器（令牌）。例如，软件验证器包括 Google Authenticator、Microsoft Authenticator、FreeOTP。

我们强烈建议不要在与管理服务器建立连接的同一台设备上安装认证应用。您可以在移动设备上安装认证应用。

### 对操作系统使用双重身份验证

为了确保使用双重身份验证进行全面保护，不仅需要保护管理服务器，还需要保护安装管理服务器的设备。

当连接到安装了管理服务器的设备时（通过SSH、RDP或其他协议），我们建议使用多重身份验证（MFA），例如使用令牌、智能卡或其他身份验证方法。

### 限制保存管理员密码

如果您使用 Kaspersky Security Center Web Console，我们不建议在用户设备上安装的浏览器中保存管理员密码。

### 内部用户账户的身份验证

默认情况下，管理服务器内部用户账户的密码必须遵守以下规则：

- 密码的字符长度必须是 8 到 256 位。
- 密码必须包含以下组中三组的字符：
  - 大写字母 (A-Z)
  - 小写字母 (a-z)
  - 数字 (0-9)
  - 特殊字符 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- 密码不可以包含任何空格、Unicode 字符以及“.”和“@”按先后顺序的组合。

默认下，允许的最大密码输入尝试次数是 10。您可以更改允许的密码输入尝试次数。

Kaspersky Security Center Linux 用户可以输入无效密码的次数有限。达到限制后，用户账户被锁定一小时。

### 配置更改内部用户账户密码的选项

我们建议配置以下选项来更改内部用户账户的密码：

- 密码轮换期
- 需要更改密码的初次警告时间
- **用户必须在首次登录时更改密码**选项的值

### 用来防止未经授权修改的账户保护

我们建议启用附加选项来保护管理服务器的内部用户账户免遭未经授权的修改。必须为每个内部用户单独配置此保护。

### 管理服务器的专用管理组

我们建议为管理服务器创建一个专门的管理组。授予该组特殊访问权限并为其创建特殊安全策略。

为避免故意降低管理服务器的安全级别，我们建议限制可以管理专用管理组的账户列表。

### 限制主管理员角色的分配

由 kladduser 实用程序创建的用户在管理服务器或者虚拟管理服务器的访问控制列表 (ACL) 中被分配为主管理员角色。我们建议避免将主管理员角色分配给大量用户。

### 配置对应用程序功能的访问权限

我们建议为每个用户或用户组灵活配置对 Kaspersky Security Center Linux 功能的访问权限。

基于角色的访问控制允许通过使用一组预定义的权限创建标准用户角色并根据用户的职责范围将这些角色分配给用户。

基于角色的访问控制模型的主要优点：

- 易于管理
- 角色层级
- 最小特权方法
- 职责分离

您可以根据职位为某些员工分配内置角色，或创建全新的角色。

在配置角色时，注意与改变管理服务器设备保护状态和远程安装第三方软件相关的权限：

- 对管理组进行管理。
- 管理服务器操作。
- 远程安装。
- 更改用于存储事件和发送通知的参数。
  此权限允许您设置在事件发生时在管理服务器设备上运行脚本或可执行模块的通知。

### 使用单独的账户进行远程安装应用程序

除了访问权限的基本区分外，我们建议限制所有账户（主管理员或其他专用账户除外）进行应用程序远程安装。

我们建议使用单独的账户进行远程安装应用程序。您可以分配角色或者权限给单独账户。

### 定期审核所有用户和用户的操作

我们建议对管理服务器设备上的所有用户进行定期审核。这使您能够应对与可能损害设备相关的某些类型的安全威胁。

另外，您还可以跟踪用户的操作，例如连接到管理服务器和断开连接、连接到管理服务器时出现错误以及对象修改（对于支持修订管理的对象）。

# 管理服务器保护的管理

### 选择管理服务器保护软件

根据管理服务器部署的类型和一般保护策略，选择应用程序来保护管理服务器设备。

如果您在专用设备上部署管理服务器，我们建议选择 Kaspersky Endpoint Security 应用程序来保护管理服务器设备。这可让您应用所有可用技术来保护管理服务器设备，包括行为分析模块。

如果管理服务器安装在基础设施中存在的设备上并且之前曾用于其他任务，我们建议考虑以下保护软件：

- Kaspersky Industrial CyberSecurity for Nodes。我们建议在包含在工业网络中的设备上安装此应用程序。Kaspersky Industrial CyberSecurity for Nodes 是一个应用程序，具有与各种工业软件制造商的兼容性证书。
- 推荐的安全产品。如果管理服务器安装在装有其他软件的设备上，我们建议考虑该软件供应商对安全产品兼容性的建议（可能已经有选择安全解决方案的建议，您可能需要配置信任区域）。

### 为保护应用程序创建单独的安全策略

我们建议为保护管理服务器设备的应用程序创建单独的安全策略。此策略必须不同于客户端设备的安全策略。这可让您为管理服务器指定最合适的安全设置，而不会影响其他设备的保护级别。

我们建议将设备分组，然后将管理服务器设备放入一个单独的组中，您可以为其创建特殊的安全策略。

### 保护模块

如果与管理服务器安装在同一设备上的第三方软件的供应商没有特别建议，我们建议激活并配置所有可用的保护模块（在检查这些保护模块的运行一段时间后）。

### 配置管理服务器设备的防火墙

在管理服务器设备上，我们建议配置防火墙以限制设备数量，管理员可以从这些设备通过 Kaspersky Security Center Web Console 连接到管理服务器。

默认情况下，管理服务器使用端口13299 接收来自 Kaspersky Security Center Web Console 的连接。我们建议限制可以使用该端口管理管理服务器的设备数量。

# 管理客户端设备保护

### 限制将授权许可密钥添加到安装包

安装包存储在管理服务器共享文件夹的 Packages 子文件夹中。如果将授权许可密钥添加到安装包，则所有对此文件夹具有读取权限的用户都可以访问该授权许可密钥（直接或通过管理服务器中嵌入的Web 服务器）。

为避免泄露授权许可密钥，我们不建议将授权许可密钥添加到安装包中。

我们推荐使用将授权许可密钥自动分发到受管理设备，通过受管理应用程序的"添加授权许可密钥"任务进行部署，并手动将激活码或密钥文件添加到设备。

### 在管理组之间移动设备的自动规则

我们建议限制使用自动规则在管理组之间移动设备。

如果您使用自动规则移动设备，这可能会导致策略的传播，这些策略为移动的设备提供比重新定位前的设备更多的权限。

此外，将客户端设备移动到另一个管理组可能会导致策略设置的传播。这些策略设置可能不适合分发给访客和不受信任的设备。

此建议不适用于将设备一次性初始分配给管理组。

### 分发点和连接网关的安全要求

安装了网络代理的设备可以充当分发点并执行以下功能：

- 将从管理服务器收到的更新和安装包分发到组内的客户端设备。
- 在客户端设备上执行第三方软件和卡巴斯基应用程序的远程安装。
- 轮询网络以检测新设备并更新现有设备的信息。分发点可以使用与管理服务器相同的设备检测方法。

在组织的网络上放置分发点用于：

- 降低管理服务器负载
- 流量优化
- 让管理服务器能够访问网络中难以到达的设备

考虑到可用功能，我们建议保护充当分发点的设备免受任何类型的未经授权的访问（包括物理访问）。

## 限制自动分配分发点

为了简化管理并保持网络的可操作性，我们建议使用分发点的自动分配。但是，对于工业网络和小型网络，我们建议您避免自动分配分发点，因为（例如）用于推送远程安装任务的账户的私人信息可以通过操作系统转移到分发点。

对于工业网络和小型网络，您可以手动分配设备作为分发点。

您还可以查看分发点活动报告。

## Kaspersky Security Center Linux 用户设备的安全要求

Kaspersky Security Center Linux 用户的设备必须满足特殊的安全要求。我们建议保护这些设备免受任何类型未经授权的访问（包括物理访问）。

Kaspersky Security Center Linux 用户设备包括以下内容：

- Kaspersky Security Center Linux 用户使用浏览器从其连接到 Kaspersky Security Center Web Console 的设备。
- 通过 OpenAPI 与管理服务器交互的应用程序从其连接到 Kaspersky Security Center Linux 的设备。

## 安装了 Kaspersky Security Center Web Console 的设备的安全要求

安装了 Kaspersky Security Center Web Console 的设备用于管理 Kaspersky Security Center Linux，因此必须对这些设备的安全性应用特殊要求。我们建议保护这些设备免受任何类型未经授权的访问（包括物理访问）。

# 配置受管理应用程序的保护

## 受管理应用程序策略

我们建议为每种类型使用的应用程序和 Kaspersky Security Center Linux 组件（网络代理、Kaspersky Endpoint Security for Windows、Kaspersky Endpoint Security for Linux、Kaspersky Endpoint Agent 等）创建一个策略。此组策略必须应用于所有受管理设备（根管理组）或根据配置的移动规则新的受管理设备将自动移动到其中的单独组。

## 指定用于禁用保护和卸载应用程序的密码

**我们强烈建议启用密码保护，以防止入侵者禁用或卸载卡巴斯基安全应用程序。**在支持密码保护的平台上，您可以为 Kaspersky Endpoint Security、网络代理和其他卡巴斯基应用程序设置密码。启用密码保护后，我们建议通过关闭"锁"来锁定相应设置。

## 指定将客户端设备手动连接到管理服务器的密码（klmover 实用程序）

klmover 实用程序允许您手动将客户端设备连接到管理服务器。klmover 工具位于网络代理安装文件夹。

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

klmover 实用程序需要本地管理员权限。

如果您丢失或忘记了安装在不再受 Kaspersky Security Center 管理的设备上受密码保护的网络代理的密码，则无法使用 klmover 实用程序或命令行删除网络代理。在这种情况下，您必须在安装了受密码保护的网络代理的设备上重新安装操作系统。

在 Windows 设备上启用**使用卸载密码**选项还会为清理工具 (cleaner.exe) 启用密码保护。

## 使用卡巴斯基安全网络

在受管理应用程序的所有策略和管理服务器属性中，我们建议启用卡巴斯基安全网络 (KSN) 的使用并接受 KSN 声明。更新或升级管理服务器时，您可以接受更新后的 KSN 声明。在某些情况下，当法律或其他法规禁止使用云服务时，您可以禁用 KSN。

### 定期扫描受管理设备

对于所有设备组，我们建议创建一个定期运行完整设备扫描的任务。

### 发现新设备

我们建议正确配置设备发现设置：设置与域控制器的集成，并指定用于发现新设备的 IP 地址范围。

出于安全目的，您可以使用包含所有新设备的默认管理组和影响该组的默认策略。

## 管理服务器维护

### 备份管理服务器数据

数据备份允许您在不丢失数据的情况下恢复管理服务器数据。

默认情况下，数据备份任务在管理服务器安装后自动创建并定期执行，从而将备份保存在适当的目录中。
数据备份任务的设置可以更改如下：

- 备份频率增加
- 指定保存副本的特殊目录
- 更改备份副本的密码

如果您将备份副本存储在不同于默认目录的特殊目录中，我们建议限制该目录的访问控制列表 (ACL)。管理服务器账户和管理服务器数据库的账户必须具有此目录的写入权限。

### 管理服务器维护

管理服务器维护允许您降低数据库容量，提高应用程序的运行和操作可靠性。我们建议您至少每周维护一次管理服务器。

管理服务器通过专用任务进行维护。在维护管理服务器时，应用程序执行以下操作：

- 重组数据库索引
- 更新数据库统计信息
- 收缩数据库（如果必要）

### 安装操作系统更新和第三方软件更新

我们强烈建议您定期为管理服务器设备上的操作系统和第三方软件安装软件更新。

客户端设备不需要持续连接到管理服务器，因此在安装更新后重新启动管理服务器设备是安全的。管理服务器停机期间在客户端设备上注册的所有事件都会在连接恢复后发送给它。

## 事件传输到第三方系统

### 监控和报告

为了及时响应安全问题，我们建议配置监控和报告功能。

### 导出事件到 SIEM 系统

为了在重大损害发生之前快速检测安全问题，我们建议在 SIEM 系统中使用事件导出。

### 审计事件的电子邮件通知

Kaspersky Security Center Linux 允许您接收受管理设备上安装的管理服务器和 Kaspersky 应用程序在操作期间发生的事件信息。为了及时响应紧急情况，我们建议配置管理服务器以发送有关其发布的审计事件、关键事件、故障事件和警告的通知。

由于这些事件是系统内事件，因此可以预期它们的数量很少，这非常适用于邮件。

## 第三方信息系统安全建议

### CIS 基准的安全建议

当使用管理服务器和网络代理支持的操作系统、虚拟化平台或数据库服务器版本时，我们建议应用互联网安全中心 (CIS) 的最佳信息安全实践（如有）来微调这些信息系统。

互联网安全中心 (CIS) 是一家致力于提高信息技术领域安全性的非营利组织。特别是，CIS 负责开发和分发安全标准，例如 CIS 控制和 CIS 基准。这些标准是一组用于确保信息系统安全的建议和实践。

CIS 门户网站包含针对管理服务器和网络代理支持的以下信息系统版本提供的相关建议：

- 以下系列的操作系统：
  - 桌面版 Windows
  - 服务器版 Windows
  - Debian
  - Ubuntu
  - CentOS
  - Oracle Linux
  - Red Hat Enterprise Linux
  - SUSE Linux Enterprise Server
  - macOS
- VMware 虚拟化平台
- 数据库服务器：
  - Microsoft SQL Server
  - MySQL
  - MariaDB
  - PostgreSQL

### Astra Linux 操作系统的安全建议

使用 Astra Linux 操作系统时，您应该遵循针对相应版本 Astra Linux 的红皮书中所述的安全建议。

### RED OS 操作系统的安全建议

使用 RED OS 操作系统时，您应该使用 RED OS 官方文档中描述的管理员指南中的安全建议。

# 有关使用卡巴斯基安全应用程序的建议

## 在 Kaspersky Endpoint Security for Windows 中使用 KLAdmin 密码

KLAdmin 账户是可以不受限制地访问 Kaspersky Endpoint Security for Windows 的管理员账户。KLAdmin 账户有权在 Kaspersky Endpoint Security for Windows 中执行任何受密码保护的操作，包括删除应用程序。KLAdmin 账户的权限无法撤销。您可以在Kaspersky Endpoint Security for Windows 策略的属性中设置 KLAdmin 账户的密码。Kaspersky Endpoint Security for Windows 管理员对 KLAdmin 账户密码的安全使用负全部责任。如果您的组织有自己的密码策略，请遵循该策略的指示。密码越长、越复杂，就越可靠。

我们对保护组织免遭 KLAdmin 密码盗窃的建议如下：

- **一般要求**
  请勿使用账户名或部分账户名作为密码。
- **最小密码长度要求**
  创建一个长度至少为 10 个字符的密码。
- **使用多种字符类型的要求**
  设置一个包含不同类别字符的复杂密码：小写和大写字母、数字和特殊字符。
- **密码过期要求**
  将密码的最短有效期设置为 90 天。新密码不得与最近 24 个密码中的任何一个匹配。

# 场景：验证 MySQL 服务器

我们建议您使用 TLS 证书对 MySQL 服务器进行身份验证。您可以使用来自可信证书颁发机构 (CA) 的证书或自签名证书。

管理服务器支持 MySQL 的单向和双向 SSL 身份验证。

## 启用单向 SSL 身份验证

请按照以下步骤为 MySQL 配置单向 SSL 身份验证：

1. **为 MySQL 服务器生成自签名 TLS 证书**
   运行以下命令：

```
openssl genrsa 1024 > ca-key.pem

openssl req -new -x509 -nodes -days 365 -key ca-key.pem -config myssl.cnf > ca-cert.pem

openssl req -newkey rsa:1024 -days 365 -nodes -keyout server-key.pem -config myssl.cnf
> server-req.pem
```

```
openssl x09 -req -in server-req.pem -days 365 -CA ca-cert.pem -CAkey ca-key.pem -
set_serial 01 > server-cert.pem
```

2. **创建服务器标志文件**

   使用 klscflag 实用程序来创建 KLSRV_MYSQL_OPT_SSL_CA 服务器标志并指定证书的路径作为其值。klscflag 实用程序位于安装管理服务器的目录中。默认安装路径为/opt/kaspersky/ksc64/sbin。

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <ca-cert.pem 的路径> -t d
   ```

3. **配置数据库**

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

   ```
   [mysqld]

   ssl-ca=".../mysqlcerts/ca-cert.pem"

   ssl-cert=".../mysqlcerts/server-cert.pem"

   ssl-key=".../mysqlcerts/server-key.pem"
   ```

### 启用双向 SSL 身份验证

请按照以下步骤为 MySQL 配置双向 SSL 身份验证：

1. **创建服务器标志文件**

   使用 klscflag 实用程序来创建服务器标记并指定证书文件的路径作为其值：

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <ca-cert.pem> -t s 的路径

   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CERT -v <server-cert.pem> -t s 的路径

   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_KEY -v <server-key.pem> -t s 的路径
   ```

   klscflag 实用程序位于安装管理服务器的目录中。默认安装路径为/opt/kaspersky/ksc64/sbin。

2. **指定密码（可选）**

   如果 server-key.pem 需要密码，请创建 KLSRV_MARIADB_OPT_TLS_PASPHRASE 标记并指定密码作为其值：

   ```
   klscflag -fset -pv klserver -n KLSRV_MARIADB_OPT_TLS_PASPHRASE -v <密码> -t s
   ```

3. **配置数据库**

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

   ```
   [mysqld]

   ssl-ca=".../mysqlcerts/ca-cert.pem"

   ssl-cert=".../mysqlcerts/server-cert.pem"

   ssl-key=".../mysqlcerts/server-key.pem"
   ```

## 场景：验证 PostgreSQL 服务器

我们建议您使用 TLS 证书对 PostgreSQL 服务器进行身份验证。您可以使用来自可信证书颁发机构 (CA) 的证书或自签名证书。

管理服务器支持 PostgreSQL 的单向和双向 SSL 身份验证。

PostgreSQL 服务器的认证分为几个阶段进行：

1. **为 PostgreSQL 服务器生成证书**

   运行以下命令：

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

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

2. **为管理服务器生成证书**

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

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

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

3. **配置客户端证书身份验证**

   修改 pg_hba.conf 如下：

   ```
   hostssl mydb myuser 192.168.1.0/16 scram-sha-256
   ```

   确保 pg_hba.conf 不包含以`host`开头的记录。

4. **指定 PostgreSQL 证书**

   **单向 SSL 身份验证**

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

   ```
   listen_addresses ='localhost, server-ip'
   ssl = on
   ssl_cert_file = '<psql.crt>'
   ssl_key_file = '<psql.key>'
   ```

   **双向 SSL 身份验证**

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

   ```
   listen_addresses ='localhost, server-ip'
   ssl = on
   ssl_ca_file = '<postgres.crt>'
   ssl_cert_file = '<psql.crt>'
   ssl_key_file = '<psql.key>'
   ```

5. **重新启动 PostgreSQL 守护进程**

   运行以下命令：

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

6. **指定管理服务器的服务器标志**

   **单向 SSL 身份验证**

使用 klscflag 实用程序来创建 KLSRV_POSTGRES_OPT_SSL_CA 服务器标记并指定证书的路径作为其值。

运行命令行，然后将当前目录更改为包含 klscflag 实用程序的目录。klscflag 实用程序位于安装管理服务器的目录中。默认安装路径为/opt/kaspersky/ksc64/sbin。

运行以下命令：

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v <psql.crt 的路径> -t s
```

**双向 SSL 身份验证**

使用 klscflag 实用程序来创建服务器标记并指定证书文件的路径作为其值。

运行命令行，然后将当前目录更改为包含 klscflag 实用程序的目录。klscflag 实用程序位于安装管理服务器的目录中。默认安装路径为/opt/kaspersky/ksc64/sbin。

运行以下命令：

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v <psql.crt 的路径> -t s
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CERT -v <postgres.crt 的路径> -t s
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_KEY -v <postgres.key 的路径> -t s
```

如果 postgres.key 需要密码，请创建 KLSRV_POSTGRES_OPT_TLS_PASSPHRASE 标记并指定密码作为其值：

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_TLS_PASPHRASE -v <密码> -t s
```

7. **重启管理服务器服务**

# 部署准备

本节介绍如何根据组织的需要选择 Kaspersky Security Center Linux 部署、 Kaspersky Security Center Linux 配置和 DBMS 的选项。

在组织的网络上部署 Kaspersky Security Center Linux 组件有多种选择，具体取决于以下标准：

- 设备总数
- 在组织或地理上拆分的单元（本地办公室、分支）
- 由狭窄通道连接的网络拆分网络
- 需要到管理服务器的互联网访问

一台管理服务器最多可支持 50,000 部设备（使用 PostgreSQL 或 Postgres Pro 作为 DBMS）。如果组织网络中的设备总数超过 50,000，必须在网络中部署多个管理服务器，并合并到一个方便集中管理的层级。

如果组织包含大规模有各自管理员的远程本地办公室（分支），则适合在这些办公室部署管理服务器。否则，此类办公室必须被视为通过低吞吐量通道连接的独立网络，请参见“标准配置：由自己管理员运行的多个大规模办公室”一文。

当使用由狭窄通道连接的拆分网络时，可以分配一个或几个网络代理作为分发点来节省流量（参见分发点数量计算表格）。这种情况下，一个拆分网络中的所有设备都从此本地更新中心上获取更新。实际分发点可以从管理服务器（默认情景）和互联网上的卡巴斯基服务器下载更新（参见“标准配置：多个小型远程办公室”一文）。

“Kaspersky Security Center Linux 标准配置”部分提供了 Kaspersky Security Center Linux 标准配置的详细描述。当计划部署时，根据组织架构选择最合适的标准配置。

在部署计划阶段，必须考虑到特别证书 X.509 到管理服务器的分配。X.509 证书到管理服务器的分配可能用在以下情况（部分列表）：

- 通过 SSL 终端代理或使用反向代理检查安全套接层 (SSL)
- 与组织公共密钥基础架构（PKI）的整合
- 在证书字段中指定所需值
- 提供所需的证书加密长度

# 选择 Kaspersky Security Center Linux 的配置

该部分描述了以下用于组织网络中的 Kaspersky Security Center Linux 组件部署的标准配置：

- 单一办公室
- 几个大规模办公室，被地理拆分并由自己的管理员运行
- 多个小办公室，被地理拆分

## 标准配置：单一办公室

可以在组织网络中部署一个或多个管理服务器。管理服务器数量可以基于可用硬件或受管理设备总数来选择。

一台管理服务器最多可支持 50,000 台设备（使用 PostgreSQL 或 Postgres Pro 作为 DBMS）。考虑今后增加受管理设备的数量的可能性：最好连接较少设备到单一管理服务器。

管理服务器可以被部署在内部网络或 DMZ 中，具体取决于管理服务器是否需要互联网连接。

如果使用了多个服务器，建议您合并它们到一个层级。使用管理服务器层级时，允许您避免冗余策略和任务、处理整个受管理设备集合，使其如同被单一管理服务器管理一样：例如，搜索设备、创建设备分类和创建报告。

## 标准配置：由自己管理员运行的几个大规模办公室

如果组织有多个地理位置分散的大规模办公室，则必须考虑在每个办公室部署管理服务器的选项。每个办公室可以部署一台或多台管理服务器，具体取决于可用的客户端设备和硬件的数量。此种情况下，每个办公室可以被视为“标准配置：单一办公室”。为了简化管理，建议将所有管理服务器合并到一个层次结构（可能是多层）中。

如果一些员工带着他们的设备（笔记本电脑）在办公室之间移动，请在网络代理策略中创建网络代理连接配置文件。

## 标准配置：多个小远程办公室

该标准配置适用于总部办公室以及许多可通过互联网与总部办公室联系的远程小型办公室。每个远程办公室可能位于 Network Address Translation (NAT) 之外，例如，两个远程办公室之间无法建立连接，因为它们是隔离的。

总部办公室必须部署一台管理服务器，必须为所有其他办公室分配一个或多个分发点。如果办公室通过互联网连接，最好为分发点创建*将更新下载至分发点存储库*任务，这样它们将从卡巴斯基服务器、本地或网络文件夹直接下载更新，而不是从管理服务器下载。

如果远程办公室的一些设备不能直接访问管理服务器（例如，到管理服务器的访问是通过互联网提供但是一些设备没有互联网连接），分发点必须被切换到连接网关模式。此种情况下，远程办公室设备上的网络代理将被通过网关而不是直接连接到管理服务器，为了后期同步。

作为管理服务器，很可能无法轮询远程办公室网络，最好把该功能转给分发点。

管理服务器将无法发送通知到远程办公室 NAT 以外的受管理设备的端口 15000 UDP。要解决该问题，可以在作为分发点的设备的属性中启用持续连接到管理服务器模式（"**不断开与管理服务器的连接**"复选框）。如果分发点总数不超过 300 则该模式可用。使用推送服务器以确保受管理设备和管理服务器之间存在持续连接。有关详细信息，请参阅以下文章：启用推送服务器。

# 选择企业保护结构

组织保护结构的选择根据以下因素进行定义：

- 组织的网络拓扑。
- 组织结构。
- 负责网络保护的员工的数量及其责任分配。
- 可用于分配以便保护管理组件的硬件资源。
- 可用于分配以便维护组织网络内部保护组件运行的通信通道的吞吐量。
- 在组织网络中执行关键管理操作的时间限制。关键管理操作，包括分发反病毒数据库和修改客户端设备的策略。

在选择保护结构时，建议您首先评估可用来操作集中式保护系统的网络和硬件资源。

要分析网络和硬件基础架构，建议您遵照以下过程：

1. 定义将部署保护的网络的以下设置：
   - 网段数量。
   - 各个网段之间的通信通道的速度。
   - 每个网段中的受管理设备的数量。
   - 可用于分配以便维护保护运行的每个通信通道的吞吐量。
2. 确定为所有受管理设备执行主要管理操作的最大允许时间。

3. 分析来自步骤 1 和步骤 2 的信息以及来自管理系统负载测试的数据。根据分析，回答以下问题：

   - 是否可以用单个管理服务器服务所有客户端，或者是否需要一台管理服务器层级？
   - 需要哪种管理服务器硬件配置以便用在项目 2 中指定的时间限制内处理所有客户端？
   - 是否需要使用分发点来减少通信通道的负载？

在获取上述问题的答案之后，您可以编辑组织保护所允许的一组结构。

在组织的网络中，您可以使用下列标准保护结构之一：

- 一台管理服务器。将所有客户端设备连接至单个管理服务器。管理服务器充当分发点。
- 一个包含分发点的管理服务器。将所有客户端设备连接至单个管理服务器。某些联网的客户端设备作为分发点运行。
- 管理服务器层级。每个网段都分配了单独的管理服务器，作为管理服务器常规层次结构的一部分。主管理服务器充当分发点。
- 包含分发点的管理服务器层级。每个网段都分配了单独的管理服务器，作为管理服务器常规层次结构的一部分。某些联网的客户端设备作为分发点运行。

# 部署保护系统的常规方案

本部分描述了使用 Kaspersky Security Center 的企业网络保护系统的标准部署方案。

系统必须防止任何非授权的访问。我们建议您为您的操作系统安装所有可用更新，然后再安装应用程序到您的设备并物理保护管理服务器和分发点。

您可以使用 Kaspersky Security Center 部署保护系统到企业网络，通过以下部署方案：

- 通过 Kaspersky Security Center Web Console 部署保护系统。

  Kaspersky 应用程序自动安装在客户端设备上，并通过 Kaspersky Security Center 自动连接到管理服务器。

- 使用在 Kaspersky Security Center 中生成的独立安装包手动部署保护系统。

  手动在客户端设备和管理员工作站中安装 Kaspersky 应用程序；在安装网络代理时指定客户端设备与管理服务器的连接设置。

  该部署方法建议在远程安装不可用时使用。

Kaspersky Security Center 不支持使用 Microsoft Active Directory® 组策略进行部署。

# 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。 |
| Tantor（参见支持的版本） | 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。<br>Tantor DBMS 仅在 Astra Linux Special Edition RUSB.10015-01（操作更新 1.8）上受支持。 |

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。

# 提供到管理服务器的互联网访问

以下情况需要到管理服务器的互联网访问：

- 定期更新 Kaspersky 数据库、软件模块和应用程序
- 更新第三方软件

  默认情况下，管理服务器不需要互联网连接就可以在受管理设备上安装 Microsoft 软件更新。例如，受管理设备可以直接从 Microsoft 更新服务器下载 Microsoft 软件更新，也可以从组织的网络中部署了 Microsoft Windows Server Update Services (WSUS) 的 Windows Server 下载。在以下情况下，管理服务器必须连接到互联网：

  - 将管理服务器用作 WSUS 服务器时
  - 要安装除 Microsoft 软件以外的第三方软件的更新
- 修复第三方软件漏洞

管理服务器需要互联网连接才能执行以下任务：

- 针对 Microsoft 软件漏洞生成推荐的修复程序列表。该列表由 Kaspersky 专家创建并定期更新。
- 修复除 Microsoft 软件以外的第三方软件的漏洞。

- 管理漫游用户的设备（便携式电脑）
- 在远程办公室管理设备
- 与位于远程办公室的主管理服务器或从属管理服务器交互
- 管理移动设备

该部分描述了通过互联网提供到管理服务器的访问的典型方法。着眼于提供到管理服务器的互联网访问的每种情况都可能需要一个管理服务器专用证书。

## 互联网访问：本地网络上的管理服务器

如果管理服务器位于组织的内部网络上，则最好通过端口转发使管理服务器的 TCP 端口 13000 可从外部访问。

## 互联网访问：DMZ 中的管理服务器

如果管理服务器位于组织网络的 DMZ 中，则不能访问组织的内部网络。因此，以下限制被应用：

- 管理服务器无法检测新设备。
- 管理服务器无法通过在组织内部网络设备上强制安装来运行网络代理初始化部署。

  这仅应用到网络代理初始化安装上。任何网络代理的后续升级或安全应用程序安装可以被管理服务器运行。

请注意， Kaspersky Security Center Linux 不支持使用 Microsoft Windows 组策略进行部署。

您可以使用位于组织网络上的分发点。要在没有网络代理的设备上运行初始化部署，您首先要在其中一台设备上安装网络代理，然后给它分配分发点状态。结果，在其他设备上的网络代理初始化安装将通过该分发点由管理服务器运行。

要确保将通知成功发送到组织内部网络中受管理设备的端口 15000 UDP，您必须使用分发点覆盖整个网络。在被分配的分发点的属性中，选择**不断开与管理服务器的连接**复选框。因此，管理服务器将建立一个到分发点的持续连接，同时这些分发点能够发送通知到组织内部网络（可以是 IPv4 或 IPv6 网络）中的设备的端口 15000 UDP。

# 安装

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

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

要成功配置 MariaDB x64 服务器以与 Kaspersky Security Center 配合使用，您必须使用除本文中指定的服务器参数之外的默认服务器参数。

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=<实际值不得低于预期 KAV 数据库大小的 80%>
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
sql_mode="STRICT_TRANS_TABLES,NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION"
```

`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。确保将 `innodb_file_per_table` 参数设置为 `1`。

对于 MariaDB 10.1，另外在 [mysqld] 部分输入以下行：

```
innodb_file_format='Barracuda'
innodb_default_row_format=dynamic
innodb_large_prefix=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，优化器附加组件 `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。

增加 MariaDB systemd 服务可打开的文件（文件描述符）的默认限制，以确保在高负载下保持稳定。

*要增加文件描述符的限制：*

1. 执行以下命令：

   ```
   sudo systemctl edit mariadb.service
   ```

2. 请在 `[Service]` 部分的 `LimitNOFILE` 参数中指定文件描述符的限制：

   ```
   LimitNOFILE=1048576
   ```

3. 运行以下命令以确保参数指定正确：

   ```
   sudo systemd-analyze verify mariadb.service
   ```

4. 运行以下命令重新加载 systemd 进程：

   ```
   sudo systemctl daemon-reload
   ```

5. 运行以下命令重新启动 MariaDB 服务：

   ```
   sudo systemctl restart mariadb.service
   ```

   文件描述符的限制已增加。

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

要成功配置 PostgreSQL 或 Postgres Pro 服务器以与 Kaspersky Security Center Linux 配合使用，您必须使用除本文中指定的服务器参数之外的默认服务器参数。

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

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

在 Linux ALT 操作系统上，默认路径为 `/var/lib/pgsql/data/postgresql.conf`

PostgreSQL 和 Postgres Pro 的推荐参数：

- `max_connections = 151`

  如果您使用集群 Postgres DBMS，请在所有 DBMS 服务器以及集群配置中指定 `max_connections` 参数。

- `shared_buffers` = N

  N = 数据库管理系统 (DBMS) 预计 RAM 容量的 25%。如果 DBMS 与管理服务器安装在同一设备上，则计算应基于分配给 DBMS 的 RAM，而不是设备的总 RAM。

  如果 RAM 小于 1 GB，则保留默认值。

- `temp_buffers = 24MB`

- `work_mem = 16MB`

- `maintenance_work_mem = 128MB`

- `max_stack_depth` = 最大堆栈大小（执行"`ulimit -s`"命令以获取此值，单位为 KB）减去 1 MB 安全余量

- `max_parallel_workers_per_gather = 0`

- `standard_conforming_strings` = on

如果您使用 Postgres Pro 15.7 或 Postgres Pro 15.7.1，请禁用 `enable_compound_index_stats` 参数：

`enable_compound_index_stats = off`

更新配置文件后，重新加载配置或重新启动DBMS服务器。

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

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

有关如何配置高可用性 DBMS 集群的详细信息，请参阅以下文章：为 Kaspersky Security Center Linux 准备高可用性 DBMS 集群。

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

要成功配置 MySQL x64 服务器以与 Kaspersky Security Center 配合使用，您必须使用除本文中指定的服务器参数之外的默认服务器参数。

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=<实际值不得低于预期 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)
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。确保将 `innodb_file_per_table` 参数设置为 `1`。

# 准备高可用性 DBMS 集群以与 Kaspersky Security Center Linux 配合使用

Kaspersky Security Center Linux 支持以下高可用性集群：

- Platform V Pangolin
- Postgres Pro 内置高可用性
- Patroni（可选配 HAProxy 负载均衡器）

复制类型必须设置为同步。

如果您使用的是 PostgreSQL 的 Patroni 模板 3.3.1 或更早版本，请确保`synchronous_standby_names`参数已正确应用。要检查是否使用了同步复制，请在主要节点上运行以下查询：

```
SELECT application_name, client_addr, client_hostname, client_port, sync_state
FROM pg_stat_replication;
```

如果任何节点的`sync_state`列显示的值不是`sync`或者`potential`，则集群使用了异步复制，而异步复制不受支持。要解决此问题，请执行以下任一操作：

- 将 Patroni 更新到 3.3.2 或更高版本。
- 在 Patroni 配置文件中，找到`bootstrap`部分的`dcs`子部分并将`synchronous_mode`参数设置为`true`：

  ```
  bootstrap:
  dcs:
  <...>
  synchronous_mode: true
  ```

建议的高可用性 DBMS 集群最低配置必须至少包含三个节点。

*要准备高可用性 DBMS 集群以与 Kaspersky Security Center Linux 配合使用：*

1. 配置与 Kaspersky Security Center Linux 配合使用的 PostgreSQL 或 Postgres Pro 服务器。
2. 如果您希望管理服务器自动发现集群节点的地址，以便您只需在安装程序期间指定主要节点或副本节点的 DNS 名称或 IP 地址，请执行以下步骤：

   a. 通过向`postgresql`部分添加以下行，在所有高可用性 DBMS集群节点上，修改配置文件 /etc/pangolin-manager/postgres.yml（如果您使用 Platform V Pangolin）或 /etc/postgresql/<版本>/main/postgresql.conf（如果您使用 Postgres Pro 内置高可用性集群）：

   ```
   log_hostname=1
   ```

   对于其他配置文件参数，您可以使用PostgreSQL 和 Postgres Pro 的推荐参数值。

   b. 编辑配置文件后，在所有高可用性 DBMS集群节点上重启 DBMS 集群服务。

   c. 确保数据库用户拥有`pg_read_all_stats`特权。您可以通过运行以下命令授予此权限：

   ```
   GRANT pg_read_all_stats TO "%1";
   ```

其中`%1`是数据库用户的名称。

用户名在管理服务器安装程序期间在`KLSRV_UNATT_DBMS_LOGIN`参数中指定。

d. 为 IAM 数据库配置负载均衡器。请参阅您所选负载均衡器的文档。

高可用性 DBMS 集群已准备好与 Kaspersky Security Center Linux 协同工作。

# 安装 Kaspersky Security Center Linux

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

安装之前，您必须执行以下操作：

- 安装用于 Kaspersky Security Center Linux 的 DBMS。您可以选择其中一个受支持的 DBMS。对于如何安装所选 DBMS 的信息，请参考其文档。

  如果 Linux 操作系统的发行版不包含受支持的 DBMS，您可以从第三方软件包存储库安装 DBMS。

  安装 DBMS 后，请按照相应的说明进行操作：

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

    配置使用 PostgreSQL 和 Postgres Pro 的 DBMS 账户

    如果您希望管理服务器自动发现集群节点的地址，以便您只需在安装期间指定主要节点或副本节点的 DNS 名称或 IP 地址，请确保您已执行以下文章中的步骤 2：为使用 Kaspersky Security Center Linux 准备高可用性 DBMS 集群。

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

    配置使用 MySQL 和 MariaDB 的 DBMS 账户

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

    配置使用 MySQL 和 MariaDB 的 DBMS 账户

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

  如果您使用操作系统 RED OS 7.3.4 或更高版本或者 MSVSPHERE 9.2 或更高版本，请安装 libxcrypt-compat 包以确保管理服务器正确运行。

- 确保 DNS 服务器在网络上可用。

- 从卡巴斯基网站下载安装文件。选择与您设备上安装的 Linux 发行版相对应的安装文件 — ksc64_<version_number>_amd64.deb 或 ksc64-<version_number>.x86_64.rpm。

要安装 Kaspersky Security Center Linux，您必须在拥有 root 权限的账户下运行以下说明中提供的命令。

*要安装 Kaspersky Security Center Linux：*

1. 创建组“kladmins”以及非特权账户“ksc”和“ksciam”。这些账户必须是 ‘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`

`adduser ksciam`

`gpasswd -a ksciam kladmins`

`usermod -g kladmins ksciam`

2. 在数据库管理系统 (DBMS) 服务器上，为 IAM 创建一个数据库。数据库名称必须与您为使用 Kaspersky Security Center Linux 而安装的数据库名称不同。卸载或将服务器移动到其他设备时，管理服务器不会自动删除 IAM 数据库，您必须手动删除数据库。

   - 对于 PostgreSQL，请运行以下命令：

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
     ```

   - 对于 MariaDB，请运行以下命令：

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
     ```

3. 如果您使用高可用性 DBMS 集群，请执行以下步骤：

   a. 授予 'ksc' 用户`pg_read_all_stats`权限：

   ```
   GRANT pg_read_all_stats TO "ksc";
   ```

   b. 在所有高可用性数据库管理系统 (DBMS) 集群节点上，修改配置文件 /etc/pangolin-manager/postgres.yml（如果您使用 Platform V Pangolin）或 /etc/postgresql/main/postgresql.conf（如果您使用Postgres Pro 内置高可用性集群）。如果在将集群连接到 Kaspersky Security Center Linux时仅指定主要节点或副本节点的 DNS 名称或 IP 地址，请将以下行添加到`postgresql`部分：

   ```
   log_hostname: '1'
   ```

   c. 编辑配置文件 /etc/pangolin-manager/postgres.yml 后，在所有高可用性 DBMS 集群节点（除仲裁节点外）上重启 DBMS 集群服务，操作如下：

   ```
   systemctl restart pangolin-manager.service
   ```

   或

   ```
   systemctl restart postgresql-<version>
   ```

4. 如有必要，增加可为用于管理服务器服务功能的账户打开的文件（文件描述符）的默认限制。为此，打开 /etc/security/limits.conf 文件，然后指定文件描述符的软限制和硬限制，如下所示：

```
ksc  soft  nofile  <max_number_of_opened_files>
ksc  hard  nofile  <max_number_of_opened_files>
```

默认情况下，文件描述符的限制在安装期间指定。软文件限制为 32,768 个文件，硬文件限制为 131,072 个文件。

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

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

6. 运行 Kaspersky Security Center Linux 配置：

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

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

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

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

8. 出现提示时，输入以下设置：

   a. 选择“**标准**”作为管理服务器安装模式。

   b. 输入管理服务器的 DNS 名称或静态 IP 地址。其他设备将使用该地址连接到管理服务器。

   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 台受管理设备，则输入“1”。
   - 如果有 101 到 1000 台受管理设备，则输入“2”。
   - 如果有超过 1000 台受管理设备，则输入“3”。

   此设置用于自动随机延迟任务启动以优化网络负载。下方列表显示了计算延迟的间隔：

   - 1 至 100 个受管理设备，值 1。不使用延迟。
   - 101 至 1000 个受管理设备，值 2。延迟 5 分钟。
   - 超过 1000 个受管理设备，价值 3。延迟 10 分钟。

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

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

i. 输入安装了 DBMS 的设备的 DNS 名称或 IP 地址。127.0.0.1 默认用于本地 DBMS 安装。

要使用高可用性故障转移集群，请执行以下操作之一：

- 按以下格式输入所有节点的 DNS 名称或 IP 地址和端口：

```
<fqdn1>:<port>,<fqdn2>:<port>,<...><fqdnX>:<port>;
```

- 仅指定主要节点或副本节点的 DNS 名称或 IP 地址。

j. 输入数据库端口号。该端口用于与管理服务器通信。如果您在步骤 8.h 中输入了所有高可用性集群节点的 DNS 名称或 IP 地址和端口，则跳过此步骤。

默认情况下，使用以下端口：

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

k. 输入数据库名称。

l. 输入用于访问数据库的数据库管理员账户的登录名。

m. 输入用于访问数据库的数据库管理员账户的密码。

n. 如果您安装了 PostgreSQL 或 Postgres Pro，则可以指定管理服务器要使用的数据库架构。为此，请指定架构名称。

> 架构名称区分大小写：必须仅使用小写字母。

如果您不想使用自定义架构，请按 ENTER 键，将使用默认架构。

o. 输入 IAM Server FQDN。如果您未指定此变量，则使用安装了管理服务器的设备的 DNS 名称。

您必须指定您在步骤 8a 中输入的管理服务器 DNS 名称。

p. 输入用于启动 IAM 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“ksciam”账户。

q. 选择您安装的与 IAM 服务一起使用的 DBMS：

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

r. 输入 IAM 服务要使用的 IAM DBMS 地址。

要使用高可用性集群，请执行以下操作之一：

- 按以下格式输入所有节点的 DNS 名称或 IP 地址和端口：

```
<fqdn1>:<port>,<fqdn2>:<port>,<...><fqdnX>:<port>;
```

- 仅指定负载均衡器的 DNS 名称或 IP 地址。

s. 输入 IAM DBMS 端口号。该端口用于与 IAM 服务通信。如果您在步骤 8.p 中输入了所有高可用性集群节点的 DNS 名称或 IP 地址和端口，则跳过此步骤。

默认情况下，使用以下端口：

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

t. 输入 IAM 服务要使用的 IAM 数据库名称。IAM 服务使用的数据库名称应与管理服务器使用的数据库名称不同。

u. 输入用于访问 IAM 数据库的数据库账户的登录名。

v. 输入用于访问 IAM 数据库的数据库账户的密码。

等待服务被添加并自动启动：

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

w. 如果您安装了 PostgreSQL 或 Postgres Pro，则可以指定 IAM 要使用的数据库架构。为此，请指定架构名称。

如果您不想使用自定义模式，请按 ENTER 键，系统将使用 public 模式。

> 架构名称区分大小写：必须仅使用小写字母。
> 请勿指定保留的 iam 架构名称：client、iam、ksc、locker、pat、scope、voltron。

x. 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 256 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 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

如果跳过此步骤，您可以稍后使用以下命令创建新用户：

```
/opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <password>
```

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

网络代理安装

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。

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`
- `systemctl status kliam_srv.service`

# 以静默模式安装 Kaspersky Security Center Linux

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

安装前：

- 安装用于 Kaspersky Security Center Linux 的 DBMS。您可以选择其中一个受支持的 DBMS。对于如何安装所选 DBMS 的信息，请参考其文档。

  如果 Linux 操作系统的发行版不包含受支持的 DBMS，您可以从第三方软件包存储库安装 DBMS。

  安装 DBMS 后，请按照相应的说明进行操作：

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

    配置使用 PostgreSQL 和 Postgres Pro 的 DBMS 账户

    如果您希望管理服务器自动发现集群节点的地址，以便您只需在安装期间指定主要节点或副本节点的 DNS 名称或 IP 地址，请确保您已执行以下文章中的步骤 2：为使用 Kaspersky Security Center Linux 准备高可用性 DBMS 集群。

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

    配置使用 MySQL 和 MariaDB 的 DBMS 账户

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

    配置使用 MySQL 和 MariaDB 的 DBMS 账户

- 确保安装了 DBMS 的设备上不存在以下名称的 DBMS 用户账户：
  - client
  - iam
  - ksc
  - locker
  - pat
  - scope
  - voltron
- 确保您要安装 Kaspersky Security Center Linux 的设备运行支持的 Linux 分类。

  > 如果您使用操作系统 RED OS 7.3.4 或更高版本或者 MSVSPHERE 9.2 或更高版本，请安装 libxcrypt-compat 包以确保管理服务器正确运行。

- 从卡巴斯基网站下载安装文件。选择与您设备上安装的 Linux 发行版相对应的安装文件 — ksc64_[version_number]_amd64.deb 或 ksc64-[version_number].x86_64.rpm。

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

1. 阅读最终用户授权许可协议。只有在您理解并接受最终用户授权许可协议的条款后，才执行下面的步骤。
2. 创建一个组“kladmins”和非特权账户“ksc”和'ksciam'，这些账户必须是“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`

`adduser ksciam`

`gpasswd -a ksciam kladmins`

`usermod -g kladmins ksciam`

3. 在数据库管理系统 (DBMS) 服务器上，为 IAM 创建一个数据库。数据库名称必须与您为使用 Kaspersky Security Center Linux 而安装的数据库名称不同。卸载或将服务器移动到其他设备时，管理服务器不会自动删除 IAM 数据库，您必须手动删除数据库。

   - 对于 PostgreSQL，请运行以下命令：

     `sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"`

   - 对于 MariaDB，请运行以下命令：

     `sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"`

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. 在 root 或用户环境中设置 `KLAUTOANSWERS` 环境变量的值，该值包含应答文件的完整名称（包括路径），例如，使用以下命令：

   `export KLAUTOANSWERS=/tmp/ksc_install/answers.txt`

6. 以静默模式运行 Kaspersky Security Center Linux 安装 — 根据您的 Linux 发行版，运行以下命令之一：

   在根环境中：

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

   在用户环境中：

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

7. 创建一个使用 Kaspersky Security Center Web Console 的用户。为此，请在具有 root 权限的账户下运行以下命令：

   `/opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <密码>`，其中，密码必须至少包含 8 个字符。

8. 安装Kaspersky Security Center云控制台。

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

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

| | | | |
|---|---|---|---|
| KLSRV_UNATT_PORT_SRV_SSL | 否 | 管理服务器 SSL 端口号。可选默认值是 13000。 | 端口号 |
| KLSRV_UNATT_PORT_KLOAPI | 否 | 用于使用OpenAPI的端口号。此端口也用于接收来自 Kaspersky Security Center Web Console 的连接。可选，默认值为 13299。 | 端口号 |
| KLSRV_UNATT_PORT_GUI | 否 | 用于使用 klakaut 实用程序的端口号。可选默认值是 13291。klakaut 实用程序及其帮助系统位于 Kaspersky Security Center Linux 的安装文件夹中。<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。 | 端口号 |
| KLSRV_UNATT_NETRANGETYPE | 否 | 您要管理的设备的大概数量。此设置用于优化网络负载。可选默认值是 1。 | 1 适用于 1 到 100 个受管理设备。<br>2 适用于 101 到 1,000 个受管理设备。<br>3 适用于超过 1,000 个受管理设备。 |
| KLSRV_UNATT_DBMS_TYPE | 是 | 数据库管理系统类型：MySQL（MariaDB）或 Postgres。 | mysql<br>或<br>postgres |
| KLSRV_UNATT_DBMS_INSTANCE | 是 | 数据库服务器 IP 地址。<br>要使用 PostgreSQL、Postgres Pro 内置高可用性集群或者 Platform V Pangolin DBMS 集群，请按照以下格式输入所有节点的 DNS 名称或 IP 地址和端口：<br><fqdn1>:<port>,<fqdn2>:<port>,<...><br><fqdnX>:<port>;<br>或者，如果想使用 Platform V Pangolin DBMS 集群，您可以在指定 DBMS 地址时仅指定主要节点或副本节点的 DNS 名称或 IP 地址。 | IP 地址 |
| KLSRV_UNATT_DBMS_PORT | 是 | 数据库服务器端口。MySQL (MariaDB) 的默认值为 3306；Postgres 的默认值为 5432。 | 3306<br>或<br>5432 |
| KLSRV_UNATT_DB_NAME | 是 | 数据库名称。数据库名称必须与 KLSRV_UNATT_DB_IAM_NAME 变量中指定的 IAM 数据库名称不同。 | 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_DBMS_SCHEMA | 否 | 自定义 DBMS 架构。<br>如果您未指定自定义架构，管理服务器将使用默认架构。<br>架构名称区分大小写：必须仅使用小写字母。<br>只有在使用 PostgreSQL 或 Postgres Pro 作为 DBMS 时，才能指定自定义架构。否则，该变量将被忽略。 | database_schema |
| KLSRV_UNATT_IAM_ADDRESS | 是 | 用户浏览器将被 OpenIDConnect 重定向到此地址。<br>输入 IAM Server FQDN。您必须使用在 KLSRV_UNATT_SERVERADDRESS 参数中指定的管理服务器 DNS 名称。 | FQDN |
| KLSRV_UNATT_KLIAMUSER | 是 | 用于启动 IAM 服务的账户名称。该账户必须是 KLSRV_UNATT_KLADMINSGROUP 变量中指定的安全组的成员。 | ksciam |
| KLSRV_UNATT_DBMS_IAM_TYPE | 是 | IAM 数据库管理系统类型：MySQL (MariaDB) 或 Postgres。 | mysql<br>或者<br>postgres |

| | | | |
|---|---|---|---|
| KLSRV_UNATT_DBMS_IAM_INSTANCE | 是 | IAM 数据库服务器地址。<br>要使用 PostgreSQL、Postgres Pro 内置高可用性集群或者 Platform V Pangolin DBMS 集群，请按照以下格式输入所有节点的 DNS 名称或 IP 地址和端口：<br>`<fqdn1>:<port>,<fqdn2>:<port>,<...> <fqdnX>:<port>;`<br>或者，如果想使用 Platform V Pangolin DBMS 集群，您可以在指定 DBMS 地址时仅指定主节点或副本节点的 DNS 名称或 IP 地址。 | IP 地址 |
| KLSRV_UNATT_DBMS_IAM_PORT | 是 | IAM 数据库服务器端口。MySQL (MariaDB) 的默认值为 3306；Postgres 的默认值为 5432。 | 3306<br>或者<br>5432 |
| KLSRV_UNATT_DBMS_IAM_LOGIN | 是 | 有权访问 IAM 数据库的用户的用户名。<br>如果 IAM 数据库类型为 MySQL (MariaDB) 并具有以下两个设置：<br>• `gtid_mode=ON`<br>• `gtid_purged=ON\|AUTO`<br>确保指定的用户具有以下 DBMS 权限之一：<br>• `RELOAD`<br>• `FLUSH_TABLES` | |
| KLSRV_UNATT_DBMS_IAM_PASSWORD | 是 | 有权访问 IAM 数据库的用户的密码。 | |
| KLSRV_UNATT_DBMS_IAM_SCHEMA | 否 | 自定义 DBMS 架构。<br>如果您未指定自定义架构，IAM 将使用公共架构。<br>只有在使用 PostgreSQL 或 Postgres Pro 作为 DBMS 时，才能指定自定义架构。否则，该变量将被忽略。<br>架构名称区分大小写：必须仅使用小写字母。<br>请勿指定保留的 iam 架构名称：`client, iam, ksc, locker, pat, scope, voltron`。 | `database_schema` |
| KLSRV_UNATT_DB_IAM_NAME | 是 | IAM 数据库名称。IAM 数据库的名称必须与 `KLSRV_UNATT_DB_NAME` 变量中指定的数据库名称不同。<br>指定手动创建的空数据库。 | `iamdb` |
| 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。该账户必须是 `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。该账户必须是 `KLSRV_UNATT_KLADMINSGROUP` 变量中指定的安全组的成员。 | `ksc` |
| 如果要将管理服务器部署为 Kaspersky Security Center Linux 故障转移集群，应答文件必须包含以下附加变量： | | | |
| KLFOC_UNATT_EXT_RESOURCE_MANAGEMENT | 否 | 故障转移集群配置。如果应答文件中省略了该参数，则使用默认值。<br>可能值：<br>`0` — 故障转移集群，其节点位于单个数据中心中（默认值）。<br>`2` — 地理分布式故障转移集群，其节点位于不同的数据中心中。 | `0`<br>或<br>`2` |
| KLFOC_UNATT_NODE | 是 | 节点编号（1 或 2）。 | `1`<br>或<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>或者<br>ExternalLoadBalancer |
| 如果 KLFOC_UNATT_CONN_MODE 变量的值为 VirtualAdapter，则答案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 Linux

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

安装前：

- 安装数据库管理系统。
- 下载kaspersky_astra_pub_key.gpg 应用程序密钥。
- 从卡巴斯基网站下载 ksc64_[version_number]_amd64.deb 安装文件。

在具有 root 权限的账户下，以高度完整性和零机密性运行本说明中提供的命令。

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

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

   ```
   DIGSIG_ELF_MODE=1
   ```

2. 在命令行中，运行以下命令来安装兼容包：

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

3. 为应用程序密钥创建一个目录：

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

4. 将应用程序密钥放在上一步创建的目录中：

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

5. 针对系统的所有内核更新初始 RAM 文件系统映像：

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

   重新启动系统。

6. 创建组“kladmins”以及非特权账户“ksc”和“ksciam”。这些账户必须是 '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
# adduser ksciam
# gpasswd -a ksciam kladmins
# usermod -g kladmins ksciam
```

7. 运行 Kaspersky Security Center Linux 安装：
   ```
   # apt install /<path>/ksc64_[ 版本号 ]_amd64.deb
   ```

8. 运行 Kaspersky Security Center Linux 配置：
   ```
   # /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

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

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

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

10. 出现提示时，输入以下设置：

    a. 输入管理服务器的 DNS 名称或静态 IP 地址。

    b. 输入管理服务器端口号。默认情况下使用端口 14000。

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

    d. 评估您要管理的设备的大概数量：

    - 如果有 1 到 100 台受管理设备，则输入“1”。
    - 如果有 101 到 1000 台受管理设备，则输入“2”。
    - 如果有超过 1000 台受管理设备，则输入“3”。

    此设置用于自动随机延迟任务启动以优化网络负载。下方列表显示了计算延迟的间隔：

    - 1 至 100 个受管理设备，值 1。不使用延迟。
    - 101 至 1000 个受管理设备，值 2。延迟 5 分钟。
    - 超过 1000 个受管理设备，价值 3。延迟 10 分钟。

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

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

i. 输入安装了数据库的设备的 IP 地址。

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

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

k. 输入数据库名称。

l. 输入用于访问数据库的数据库管理员账户的登录名。

m. 输入用于访问数据库的数据库管理员账户的密码。

n. 输入 IAM 服务器 DNS 名称。
您必须指定在步骤 10a 中输入的管理服务器 DNS 名称。

o. 输入用于启动 kliam 服务的账户名。该账户必须是输入的安全组的成员。

p. 选择您安装的与 IAM 服务一起使用的 DBMS：

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

q. 输入 IAM 服务要使用的 DBMS 地址。

r. 输入数据库端口号。该端口用于与 IAM 服务通信。默认情况下，使用以下端口：

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

s. 输入 IAM 服务要使用的数据库名称。IAM 服务使用的数据库名称应与管理服务器使用的数据库名称不同。

t. 输入用于访问 IAM 数据库的数据库根账户的登录名。

u. 输入用于访问 IAM 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`
- `kliam_srv`

v. 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 256 个字符。
- 密码必须包含以下组中三组的字符：
  - 大写字母 (A-Z)
  - 小写字母 (a-z)
  - 数字 (0-9)
  - 特殊字符 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

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

服务验证

使用以下命令检查服务是否正在运行：

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

# 安装 Kaspersky Security Center Web Console

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

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

使用与您设备上安装的 Linux 发行版对应的以下安装文件之一：

- 对于 Debian：ksc-web-console-<内部版本号>.x86_64.deb
- 对于基于 RPM 的操作系统：ksc-web-console-<内部版本号>.x86_64.rpm

您通过从 Kaspersky 网站下载来接收安装文件。

*要安装 Kaspersky Security Center Web Console：*

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

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

3. 创建包含参数的响应文件以连接 Kaspersky Security Center Web Console 到管理服务器：`/etc/ksc-web-console-setup.json`。

   **包含最小参数集的响应文件示例**

   响应文件的参数集取决于 Kaspersky Security Center Web Console 连接的管理服务器的版本：

   - 16 或更高版本的管理服务器

     登录管理服务器版本 16 或更高版本所需的最小参数集的响应文件示例：

     ```
     {
         "address": "ksc-web-console.example.com",
         "port": 8080,
         "trusted":  {
             "Administration Server v16": {
                 "iamHost": "ksc16.example.com",
                 "iamOAuthPort": 4444,
                 "iamProxyPort": 9050,
                 "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
                 "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
                 "kscPort": 13299,
                 "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
             }
         },
         "certDomain":"ksc-web-console.example.com",
         "acceptEula": true
     }
     ```

   - 15.4 或更早版本的管理服务器

     登录管理服务器版本 15.4 或更早版本所需的最小参数集的响应文件示例：

     ```
     {
         "address": "ksc-web-console.example.com",
         "port": 8080,
         "trusted":  {
              "Administration Server v15.4": {
                  "kscHost": "ksc.example.com",
                  "kscPort": 13299,
                  "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
              }
         },
         "certDomain":"ksc-web-console.example.com",
         "acceptEula": true
     }
     ```

   您可以将 Kaspersky Security Center Web Console 安装在与管理服务器相同或不同的设备上。如果将 Kaspersky Security Center Web Console 安装在不同的设备上，则 Kaspersky Security Center Web Console 地址（由 `address` 指定）和管理服务器地址（由 `iamHost` 或 `kscHost` 指定）不同。如果将 Kaspersky Security Center Web Console 与管理服务器安装在同一设备上，则这些参数具有相同的值。

   `iamHost` 值必须与您在安装管理服务器时指定的 IAM 地址匹配。若要获取指定的 IAM 地址，请在安装了管理服务器的设备上运行以下命令：

   ```
   grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
   ```

有关详细信息，请参阅文章：Kaspersky Security Center Web Console 安装参数。

您可以将多个不同版本的管理服务器添加到受信任服务器列表中。在此情况下，服务器可以使用不同的身分验证方法。

我们建议您指定 1024 以上的端口号。如果您希望 Kaspersky Security Center Web Console 在 1024 以下的端口上运行，安装后必须确保已获取 setcap 实用程序，然后运行以下命令：

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

如果您没有 setcap 实用程序，则可以安装该实用程序。**单击此链接查看命令。**

对于 Debian 和 Ubuntu 操作系统，运行以下命令之一：

- `sudo apt-get install libcap2-bin`
- `sudo apt install libcap2-bin`

对于 SUSE Linux Enterprise Server 和 Red Hat Enterprise Linux，请运行以下命令：

- `sudo zypper install libcap-progs`

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

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

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

   - 要通过 .deb 文件安装或升级 Kaspersky Security Center Web Console，请运行以下命令：
     `sudo apt-get install ksc-web-console-<内部版本号>.x86_64.deb`
   - 要从 .rpm 文件安装 Kaspersky Security Center Web Console，运行以下命令之一：
     `sudo yum install ksc-web-console-<内部版本号>.x86_64.rpm`

     或

     `sudo alien -i ksc-web-console-<内部版本号>.x86_64.rpm`
   - 要从先前版本的 Kaspersky Security Center Web Console 升级，请运行以下命令之一：
     - 对于运行基于 RPM 的操作系统的设备：
       `sudo yum install ksc-web-console-<内部版本号>.x86_64.rpm`
     - 对于运行基于 Debian 的操作系统的设备：
       `sudo apt-get install ksc-web-console-<内部版本号>.x86_64.deb`

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

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

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

如果管理服务器通用证书被备份中的另一个证书替换，或者被使用 klsetsrvcert 实用程序替换，则必须移除，然后重新安装 Kaspersky Security Center Web Console。否则，登录 Web Console 将受到限制。
如果重新安装后无法登录 Web Console，请检查 IAM Server 配置。

## Kaspersky Security Center Web Console 安装参数

对于在运行 Linux 的设备上安装 Kaspersky Security Center Web Console 服务器，您必须创建响应文件 – 一个包含连接 Kaspersky Security Center Web Console 到管理服务器的参数的 .json 文件。您必须命名该文件为 ksc-web-console-setup.json 并将其放置到 /etc/ksc-web-console-setup.json 目录中。

响应文件的参数集取决于 Kaspersky Security Center Web Console 连接的管理服务器版本。

- 16 或更高版本的管理服务器

  管理服务器版本 16 或更高版本包含身份和访问管理器（IAM），该管理器在 Kaspersky Security Center云控制台中提供单点登录（SSO）的域身份验证。即使您不使用单点登录 (SSO)，如果 Kaspersky Security Center Web Console 要连接到管理服务器，响应文件也必须包含与 IAM 组件交互所需的参数。

  以下是用于安装 Web Console 的响应文件示例，该控制台将连接到版本 16 或更高版本的管理服务器。在该示例中， Web Console 和管理服务器安装在不同设备上：

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "defaultLangId": 1049,
    "enableLog": true,
    "trusted":  {
        "Administration Server v16": {
    "iamHost": "ksc16.example.com",
    "iamOAuthPort": 4444,
    "iamProxyPort": 9050,
    "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
    "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
    "kscPort": 13299,
    "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "acceptEula": true,
    "certPath": "/root/server.crt",
    "keyPath": "/root/key-without-passphrase.pem",
    "webConsoleAccount": "Group1:User1",
    "managementServiceAccount": "Group1:User2",
    "serviceWebConsoleAccount": "Group1:User3",
    "pluginAccount": "Group1:User4",
    "natsMessageQueueAccount": "Group1:User6"
}
```

- 15.4 或更早版本的管理服务器

  管理服务器15.4 或更早版本仅支持通过指定内部用户或域用户的用户名和密码进行身份验证。

  以下是用于安装 Web Console 的响应文件示例，该控制台将连接到版本 15.4 或更早版本的管理服务器。

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "defaultLangId": 1049,
    "enableLog": true,
    "trusted":  {
        "Administration Server v15.4": {
    "kscHost": "ksc.example.com",
    "kscPort": 13299,
    "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "acceptEula": true,
```

```
    "certPath": "/root/server.crt",
    "keyPath": "/root/key-without-passphrase.pem",
    "webConsoleAccount": "Group1:User1",
    "managementServiceAccount": "Group1:User2",
    "serviceWebConsoleAccount": "Group1:User3",
    "pluginAccount": "Group1:User4",
    "natsMessageQueueAccount": "Group1:User6"
}
```

webConsoleAccount、managementServiceAccount、serviceWebConsoleAccount、pluginAccount, natsMessageQueueAccount、certPath 和 keyPath 参数是可选的。您可以在响应文件中省略这些参数。

如果要使用自定义证书，请同时指定certPath和keyPath参数。如果您不指定参数或仅指定一个参数，Web 浏览器会不断通知您您的连接不是私密的。

出于安全原因，不建议指定webConsoleAccount、managementServiceAccount、serviceWebConsoleAccount、pluginAccount和natsMessageQueueAccount参数。
如果您决定指定这些参数，请确保自定义用户账户属于同一安全组。当未指定这些参数时，Kaspersky Security Center Web Console 安装程序会创建一个默认安全组，然后在该组中创建具有默认名称的用户账户。
webConsoleAccount、managementServiceAccount、serviceWebConsoleAccount、pluginAccount和natsMessageQueueAccount参数不得彼此分开使用：请为所有这些参数指定值，或者不为其中任何参数指定值。

您可以将 Kaspersky Security Center Web Console 安装在与管理服务器相同或不同的设备上。如果将 Kaspersky Security Center Web Console 安装在不同的设备上，则 Kaspersky Security Center Web Console 地址（由 address 指定）和管理服务器地址（由 iamHost 或 kscHost 指定）不同。如果将 Kaspersky Security Center Web Console 与管理服务器安装在同一设备上，则这些参数具有相同的值。

iamHost值必须与安装管理服务器时指定的 IAM 地址匹配。若要获取指定的 IAM 地址，请在管理服务器主机上运行以下命令：

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

我们建议您指定 1024 以上的端口号。如果您希望 Kaspersky Security Center 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
```

如果您没有 setcap 实用程序，则可以安装该实用程序。**单击此链接查看命令**。

对于 Debian 和 Ubuntu 操作系统，运行以下命令之一：

- sudo apt-get install libcap2-bin
- sudo apt install libcap2-bin

对于 SUSE Linux Enterprise Server 和 Red Hat Enterprise Linux，请运行以下命令：

- sudo zypper install libcap-progs

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

下表描述了可以在响应文件中指定的参数。

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

| 参数 | 描述 | 可用值 |
| --- | --- | --- |
| `address` | 安装 Kaspersky Security Center Web Console 的设备的地址（FQDN 或主机名）（必填）。<br>如果您在 Kaspersky Security Center 服务器上安装 Kaspersky Security Center Web Console，请使用安装 Kaspersky Security Center Linux时指定的地址。<br>如果您在不同的设备上安装 Kaspersky Security Center Web Console，请指定 Web 浏览器用于连接到 Kaspersky Security Center Web Console 服务器的设备地址（FQDN 或主机名）。 | 字符串值。<br>例如：`"ksc.example.com"` |
| `port` | Kaspersky Security Center Web Console 用于接收来自 Web 浏览器的连接的端口（必需）。 | 数字值。<br>推荐值为 8080（ Linux ALT 操作系统除 |
| `defaultLangId` | 用户界面语言（默认，`1033`）。<br>如有必要，您可以更改 Kaspersky Security Center Web Console 界面的语言。 | 语言数码：<br>• 德语：`1031`<br>• 英语：`1033`<br>• 西班牙语：`1034`<br>• 西班牙语（墨西哥）：`2058`<br>• 法语：`1036`<br>• 意大利语：`1040`<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：`2052`<br>• 繁体中文：`1028`<br>如果没有指定值，则使用 English (en-U |
| `enableLog` | 是否要启用 Kaspersky Security Center Web Console 跟踪日志记录。<br>我们建议您仅在卡巴斯基技术支持专家要求时才更改该参数的默认值。 | 布尔值：<br>• `true`—日志记录已启用。<br>• `false`—日志记录已禁用。 |

| 参数 | 描述 | 可用值 |
| --- | --- | --- |
| `trusted` | Kaspersky Security Center Web Console 可以连接到的受信任管理服务器的地址列表。您可以将多个不同版本的管理服务器添加到受信任服务器列表中。<br>对于 16 或更高版本的管理服务器：<br>• 将显示在登录窗口中的管理服务器名称。<br>• `iamHost` 是管理服务器的地址（FQDN 或主机名），其中包含 IAM 组件（从 Kaspersky Security Center Linux 版本 16 开始），Kaspersky Security Center Web Console 连接到该管理服务器。`iamHost` 值必须与安装管理服务器时指定的 IAM 地址匹配。若要获取指定的 IAM 地址，请在管理服务器主机上运行以下命令：`grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml`<br>• `iamOAuthPort` 是用于通过 OpenID Connect 身份验证协议交换身份验证令牌的端口（默认值为 4444）。此端口用于 Kaspersky Security Center Web Console 服务器和管理服务器之间的通讯，以及浏览器（与 Kaspersky Security Center Web Console 配合使用）和管理服务器之间的通讯。<br>• `iamProxyPort` 是用于将 Kaspersky Security Center Web Console 服务器连接到管理服务器的端口（默认值为 9050）。<br>• `iamCertPath` 是IAM 证书的路径。IAM 证书在首次运行管理服务器时自动创建。证书位于安装管理服务器的设备上。证书的默认路径：/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem。自签名 IAM 证书会自动轮换。<br>• `iamPATPath` 是将 Kaspersky Security Center Web Console 注册为 IAM 中的 OAuth 客户端时所用令牌的路径。该文件会在您首次运行管理服务器时自动生成。令牌位于安装管理服务器的设备上。令牌的默认路径：var/opt/kaspersky/klnagent_srv/iam/initial_token.txt。该令牌永久有效，无需轮换。<br>• `kscPort` 是用于通过 OpenAPI 将 Kaspersky Security Center Web Console 连接到管理服务器的端口（默认值为 13299）。<br>• `kscCertPath` 是管理服务器证书的路径。证书位于安装管理服务器的设备上。证书的默认路径：/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer。<br>对于 15.4 或更高版本的管理服务器：<br>• 将显示在登录窗口中的管理服务器名称。<br>• `kscHost` 是 Kaspersky Security Center Web Console 连接到的管理服务器的地址（FQDN 或主机名称）。<br>• `kscPort` 是用于将 Kaspersky Security Center Web Console 服务器连接到管理服务器的 OpenAPI 端口（默认值为 13299）。<br>• `kscCertPath` 是管理服务器证书的路径。证书位于安装管理服务器的设备上。证书的默认路径：/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer。<br>将 Kaspersky Security Center Web Console 安装到管理服务器设备以外的其他设备上时，请将已安装管理服务器的设备中的管理服务器证书文件（由 `kscCertPath` 指定）、IAM 证书文件（由 `iamCertPath` 指定）和令牌文件（由 `iamPATPath` 指定）复制到目标设备中。在 Web Console 安装程序的响应文件中指定这些文件的本地路径。 | JSON 文件中的一部分采用以下格式：<br>`"trusted": { "Administration Server v16": { "iamHost": "ksc-iam.example.com", "iamOAuthPort": 4444, "iamProxyPort": 9050, "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/init "kscPort": 13299, "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cer }, "Administration Server v15.4": { "kscHost": "ksc.example.com", "kscPort": 13299, "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cer } }`<br>您可以指定任何管理服务器名称，而不 `Administration Server v16` 和 `Adm Server v15.4`。 |
| `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 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 此选项）。<br>如果未指定任何值，Kaspersky Securit Console 安装程序会向您显示 EULA 并 接受 EULA 的条款。 |
| `certDomain` | 如果您想要生成新的自签名证书，请使用此参数指定用于将 Web 浏览器连接到 Kaspersky Security Center Web Console 的 FQDN。 | 字符串值。 |

| 参数 | 描述 | 可用值 |
| --- | --- | --- |
| certPath | 使用该参数指定在您的基础架构中受信任且满足自定义证书要求的 Kaspersky Security Center Web Console 自定义证书的路径。<br>您只能为一个证书或一个证书链指定一个私钥（keyPath）。 | 字符串值。<br>Kaspersky Security Center Web Conso 书。<br>在要安装 Kaspersky Security Center W 备上，指定 PEM 格式的证书文件的路径<br>示例：/root/server.crt |
| keyPath | 使用该参数指定与certPath参数中指定的 Kaspersky Security Center Web Console 定义证书关联的私钥路径。 | 字符串值。<br>带有私钥的文件不得被加密。<br>在要安装 Kaspersky Security Center W 备上，指定 PEM 格式的密钥文件的路径<br>示例：/root/key-without-passph |
| webConsoleAccount | 运行 Kaspersky Security Center Web Console 服务的账户名称。 | 以下格式的字符串值："< 组名称 >:< 用<br>例如："Group1:User1"。<br>如果未指定任何值，Kaspersky Security Console 安装程序会使用默认名称 user_management_%uid% 创建一个新 |
| managementServiceAccount | 运行 Kaspersky Security Center Web Console 管理服务的账户名称。 | 以下格式的字符串值："< 组名称 >:< 用<br>示例："Group1:User2"。<br>如果未指定任何值，Kaspersky Security 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："< 组名称 >:< 用<br>示例："Group1:User3"。<br>如果未指定任何值，Kaspersky Security Console 安装程序会使用默认名称 user_svc_nodejs_%uid% 创建一个新 |
| 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："< 组名称 >:< 用<br>示例："Group1:User4"。<br>如果未指定任何值，Kaspersky Security Console 安装程序会使用默认名称 user_web_plugin_%uid% 创建一个新 |
| natsMessageQueueAccount | 运行Kaspersky Security Center Web Console NATS服务的账户名称。 | 以下格式的字符串值："< 组名称 >:< 用<br>示例："Group1:User6"。<br>如果未指定任何值，Kaspersky Security Console 安装程序会使用默认名称 user_message_queue_%uid% 创建一 |

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

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

*要安装 Kaspersky Security Center Web Console：*

1. 确保您要安装 Kaspersky Security Center Web Console 的设备运行支持的 Linux 分类。
2. 阅读最终用户授权许可协议 (EULA)。如果 Kaspersky Security Center Linux 分发包不包含带有 EULA 文本的 TXT 文件，您可以从 卡巴斯基网站 下载文件。如果您不接受授权许可协议的条款，不要安装应用程序。
3. 创建一个响应文件，其中包含用于将 Kaspersky Security Center Web Console 连接到管理服务器的参数：/etc/ksc-web-console-setup.json。

**包含最小参数集的响应文件示例**

响应文件的参数集取决于 Kaspersky Security Center Web Console 连接的管理服务器的版本：

- 16 或更高版本的管理服务器

  登录管理服务器版本 16 或更高版本所需的最小参数集的响应文件示例：

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
        "Administration Server v16": {
            "iamHost": "ksc16.example.com",
            "iamOAuthPort": 4444,
            "iamProxyPort": 9050,
            "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
            "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
            "kscPort": 13299,
            "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

- 15.4 或更早版本的管理服务器

  登录管理服务器版本 15.4 或更早版本所需的最小参数集的响应文件示例：

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

您可以将 Kaspersky Security Center Web Console 安装在与管理服务器相同或不同的设备上。如果将 Kaspersky Security Center Web Console 安装在另一台设备上，则 Kaspersky Security Center Web Console 地址（由 `address` 指定）和管理服务器地址（由 `iamHost` 或 `kscHost` 指定）不同。如果将 Kaspersky Security Center Web Console 与管理服务器安装在同一设备上，则这些参数具有相同的值。

`iamHost`值必须与您在安装管理服务器时指定的 IAM 地址匹配。若要获取指定的 IAM 地址，请在安装了管理服务器的设备上运行以下命令：

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

有关详细信息，请参阅文章：Kaspersky Security Center Web Console 安装参数。

您可以将多个不同版本的管理服务器添加到受信任服务器列表中。在此情况下，服务器可以使用不同的身分验证方法。

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

```
DIGSIG_ELF_MODE=1
```

5. 在命令行中，运行以下命令来安装兼容包：

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

6. 为应用程序密钥创建一个目录：

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

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

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

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

8. 更新 RAM 磁盘：

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

重新启动系统。

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

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

```
sudo apt-get install ksc-web-console-<build_number>.x86_64.deb
```

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

```
sudo apt-get install ksc-web-console-<build_number>.x86_64.deb
```

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

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

```
sudo systemctl restart KSC*
```

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

# 使用脚本安装Kaspersky Security Center for Linux

`ksc_fast_install.py`脚本可让您部署 Kaspersky Security Center Linux，并执行其组件的初始设置：管理服务器和 Web Console，包括 DBMS 和所需的支持包。

该脚本从参数文件读取参数。使用参数的默认值。如有必要，您可以更改这些值。

### 如何使用脚本

运行时，该脚本会：

- 检查是否满足以下条件：
  - 您拥有执行脚本所需的权限。
  - 该脚本与操作系统和DBMS兼容。
  - 已接受EULA和隐私策略。
    如果您未在参数文件中接受它们，则在运行脚本后系统会提示您接受。
  - 管理服务器和云控制台的硬件要求。
    这些要求在《容量大小指南》中定义。
- 安装DBMS（如果尚未安装）并配置其参数
- 创建卡巴斯基安全管理中心数据库，配置操作系统凭据
- 安装管理服务器和云控制台
- 为您提供用于登录云控制台的登录名和密码。
  在关闭命令行终端之前，请以任何方便的方式保存凭据。如果丢失凭据，您必须通过运行以下命令添加新的用户帐户：`/opt/kaspersky/ksc64/sbin/kladduser -n <用户>`

如果一个或多个条件未得到满足，或发生错误，脚本将终止，并显示相应通知。

> 该脚本不包括系统强化操作。为降低 Kaspersky Security Center 遭入侵的风险，请考虑遵循强化指南中的建议。
> 基于脚本的安装方法适用于在未安装 Kaspersky Security Center Linux 的设备上部署 Kaspersky Security Center Linux 16.3 及更高版本。
> 运行该脚本需要 Python 3.6 及更高版本。

仅当当前设备未安装 Kaspersky Security Center Linux 时，才能进行部署。

您不能使用该脚本升级到 Kaspersky Security Center Linux 的新版本，也不能在已部署 Kaspersky Security Center Linux 故障转移集群的情况下使用该脚本。

`ksc_fast_install.py` 脚本支持在表中所述的操作系统版本和 DBMS 上安装 Kaspersky Security Center Linux。

| 操作系统版本 | DBMS |
| --- | --- |
| Ubuntu Server 26.04 LTS | PostgreSQL 18 |
| RED OS 8 | PostgreSQL 16 |
| Astra Linux特别版RUSB.10015-01（版本1.8.5） | PostgreSQL 15 |
| CentOS Stream 10 | PostgreSQL 18 |

该脚本不支持自定义数据库架构。

如何通过脚本进行部署

**先决条件**

运行脚本之前，请确保已完成以下操作：

- 通过执行以下命令之一更新您的操作系统：`dnf update` 或 `apt update`
- 通过执行以下命令获取超级用户权限：`sudo -i`
- 通过执行以下命令授予脚本运行权限：`chmod +x ./ksc_fast_install.py`
- 通过执行以下命令确保您的操作系统软件仓库中提供受支持的 DBMS：`sudo apt policy postgresql`

*要通过运行脚本部署Kaspersky Security Center for Linux，请执行以下操作：*

1. 从 Kaspersky 网站 下载以下内容：
   - 用于管理服务器和 Web Console 的 .deb 或 .rpm 分发包。
   - “KSC 安装脚本”压缩文件。

     使用脚本时，请选择与操作系统软件包管理器兼容的管理服务器和 Web Console 分发包。

     该压缩文件包含以下文件：
     - `ksc_fast_install.py` 脚本文件。
     - 参数文件。

       默认文件名为`params.txt`。如果要重命名该文件，请确保在命令行终端中运行脚本时通过`--params`参数指定了新名称。
     - 包含管理服务器 EULA 和隐私策略的文件。
     - Kaspersky Security Center Web Console EULA 文件。
     - 包含 EULA 哈希值的文件。
2. 将所有下载的文件放在同一个本地目录中。
3. 如有必要，请配置参数文件。

   **单击此处查看参数文件示例及其参数说明**

   ```
   # Required parameters:

   #klfi_server_eula_accepted=N

   #klfi_nwc_eula_accepted=N
   ```

```
#klfi_pp_accepted=N

# Optional parameters:

#klfi_klserver_db=KAV

#klfi_klserver_dbuser=klserver

#klfi_klserver_address=

#klfi_kliam_db=KAV_IAM

#klfi_kliam_dbuser=kliam

#klfi_kliam_address=

#klfi_sys_group_kladmin=kladmins

#klfi_sys_user_klserver=klsrvuser

#klfi_sys_user_kliam=kliamuser

#klfi_sys_user_svc=klsvcuser

#klfi_nwc_port=8080

#klfi_display_name=

#klfi_netsize=M
```

`klfi_server_eula_accepted=N`、`klfi_nwc_eula_accepted=N` 和 `klfi_pp_accepted=N` 参数是必填参数，并且始终存在于参数文件中。其他参数为可选参数。

对于必填参数：

- 如果您在未取消注释行的情况下更改默认值，系统将提示您接受 EULA 和隐私策略。
- 如果指定了 `Y` 或 `N` 以外的值，则无论是否已取消注释该行，系统都会提示您接受 EULA 和隐私策略。
- 如果您取消注释该行但未更改默认值 `N`，脚本将无法运行。
- 如果您取消注释该行并将值设置为 `Y`，脚本将不会提示您。

| 参数及其默认值 | 参数描述和其他可能值（如有） |
| --- | --- |
| `klfi_server_eula_accepted=N` | 管理服务器最终用户授权许可协议。<br>可能值：<br>• `Y` – 已接受 EULA。<br>• `N` – 未接受 EULA。 |
| `klfi_nwc_eula_accepted=N` | Kaspersky Security Center Web Console 最终用户授权许可协议。<br>可能值：<br>• `Y` – 已接受 EULA。<br>• `N` – 未接受 EULA。 |

| | |
|---|---|
| `klfi_pp_accepted=N` | 隐私政策。<br>可能值：<br>• `Y` – 已接受隐私策略。<br>• `N` – 未接受隐私策略。 |
| `klfi_klserver_db=KAV` | 管理服务器数据库名称。<br>该名称必须不同于 `klfi_kliam_db` 参数中指定的 IAM 数据库名称。 |
| `klfi_kliam_db=KAV_IAM` | IAM 数据库名称。<br>该名称必须不同于 `klfi_klserver_db` 参数中指定的管理服务器数据库名称。 |
| `klfi_klserver_dbuser=klserver` | 管理服务器数据库用户的名称。 |
| `klfi_kliam_dbuser=kliam` | IAM 数据库用户的名称。 |
| `klfi_klserver_address=FQDN` | 管理服务器 FQDN 或当前设备名称。<br>如果未指定参数值，脚本会自动确定 FQDN 或运行脚本的设备名称。<br>如果脚本无法确定这些值，则安装将结束并报错。 |
| `klfi_kliam_address=FQDN` | IAM 服务器 FQDN 或当前设备名称。<br>如果未指定参数值，脚本会自动确定 FQDN 或运行脚本的设备名称。<br>如果脚本无法确定这些值，则安装将结束并报错。 |
| `klfi_sys_group_kladmin=kladmins` | 服务的安全组名称。 |
| `klfi_sys_user_klserver=klsrvuser` | 用于启动管理服务器服务的账户名。 |
| `klfi_sys_user_kliam=kliamuser` | 用于启动 IAM 服务的账户名称。 |
| `klfi_sys_user_svc=klsvcuser` | 用于启动其他服务的账户名。 |
| `klfi_nwc_port=8080` | 用于连接到 Kaspersky Security Center Web Console 的端口。 |
| `klfi_display_name=FQDN` | 将显示在登录窗口中的管理服务器名称。 |

| | |
|---|---|
| `klfi_netsize=M` | 您要管理的设备的大概数量。<br>每项估算都考虑了运行 Kaspersky 应用程序所需的资源。该计算涵盖了在单个设备上同时运行管理服务器、网络代理、Kaspersky Security Center Web Console 和 Kaspersky Endpoint Security for Linux。<br>这些计算不包括管理服务器备份的存储空间。使用外部文件资源作为挂载点，以便将备份存储在单独的设备上，或增加可用磁盘空间以满足备份存储需求。<br>建议为操作系统安装额外增加 4–6 GB RAM 和 20 GB 可用磁盘空间。<br>按网络规模估算硬件资源：<br>• `S` –1 到 1000 台受管理设备。<br>  • CPU–8 核<br>  • RAM–16 GB<br>  • `/var` 目录的可用磁盘空间–70 GB，300 IOPS 或更高<br>• `M` –1001 到 10000 台受管理设备。<br>  • CPU–12 核<br>  • RAM–24 GB<br>  • `/var` 目录的可用磁盘空间–340 GB，300 IOPS 或更高<br>• `L` –10001 到 30000 台受管理设备。<br>  • CPU–20 核<br>  • RAM–40 GB<br>  • `/var` 目录的可用磁盘空间–490 GB，300 IOPS 或更高<br>• `XL` –30001 到 50000 台受管理设备。<br>  • CPU–28 核<br>  • RAM–54 GB<br>  • `/var` 目录的可用磁盘空间–640 GB，300 IOPS 或更高 |

参数文件中的各行均已注释。如果要配置这些值，请删除要取消注释的行开头的 #符号。

`klfi_server_eula_accepted`、`klfi_nwc_eula_accepted` 和 `klfi_pp_accepted` 参数是必填参数，其默认值为 `N`。如果您在未更改参数文件中的这些值的情况下运行脚本，系统将提示您接受 EULA 和隐私策略。

4. 运行脚本。

脚本执行完毕后，会显示一条关于Kaspersky Security Center for Linux组件已成功部署的通知，以及用于登录云控制台的登录名和密码。

如果不满足基于脚本的安装条件、在参数文件中指定了未知参数，或者某个参数重复多次，脚本将返回错误，并显示相应通知。

如果在资源发现步骤中，脚本错误地检测到 RAM 不足，请在安装期间禁用动态 RAM 使用。

如果在安装Kaspersky Security Center for Linux组件或DBMS时发生错误，脚本将回滚更改，然后终止。

### 安装失败时回滚

如果在安装Kaspersky Security Center for Linux组件或DBMS时发生错误，脚本会自动执行回滚。在错误发生前安装的组件或DBMS会被删除。

操作系统软件包的升级和支持软件包的安装不会回滚。

如果手动终止脚本，已成功完成的步骤不会回滚。如有必要，您可以重新运行脚本，安装将从中断的步骤继续。

要恢复安装，您必须在命令行终端中使用 `rollback` 参数运行脚本：`python3 ksc_fast_install.py rollback`

# Kaspersky Security Center Linux 故障转移集群部署

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

Kaspersky Security Center Linux 故障转移集群支持两种配置：

- 节点位于单个数据中心的故障转移集群节点；
- 节点位于不同数据中心的地理分布式故障转移集群。

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

> 使用 syslog 功能进行故障排除。

### 切换条件

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

- 由于软件或硬件故障，主动节点损坏。
- 由于维护活动，主动节点暂时停止。
- 至少一个 Kaspersky Security Center Linux 服务（或进程）故障或意外终止。Kaspersky Security Center Linux 服务包括以下各项：klnagent_klfoc、kladminserver_klfoc、klactprx_klfoc、klwebsrv_klfoc。
- 活动节点与文件服务器上的存储之间的网络连接已中断或终止（仅适用于位于单个数据中心中的集群）。

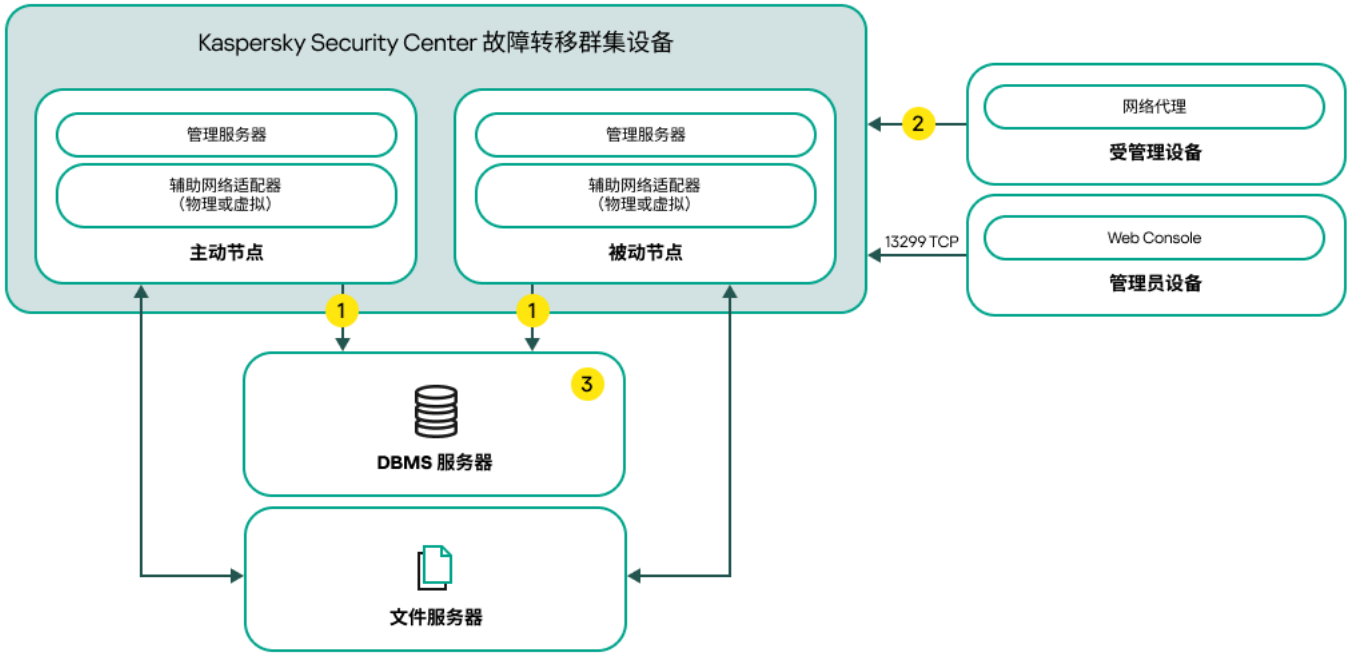
# Kaspersky Security Center Linux 故障转移集群。部署方案

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

- 部署在单个数据中心内的 Kaspersky Security Center Linux 故障转移集群：
  - 一个使用从属网络适配器和安装在专用设备上的 DBMS 的方案。
  - 一个使用第三方负载均衡器和安装在专用设备上的 DBMS 的方案。
- 跨多个数据中心部署的地理分布式 Kaspersky Security Center Linux 故障转移集群。

Kaspersky Security Center Linux 故障转移集群。

一个使用从属网络适配器和安装在专用设备上的 DBMS 的方案




一个使用从属网络适配器和安装在专用设备上的 DBMS 的方案

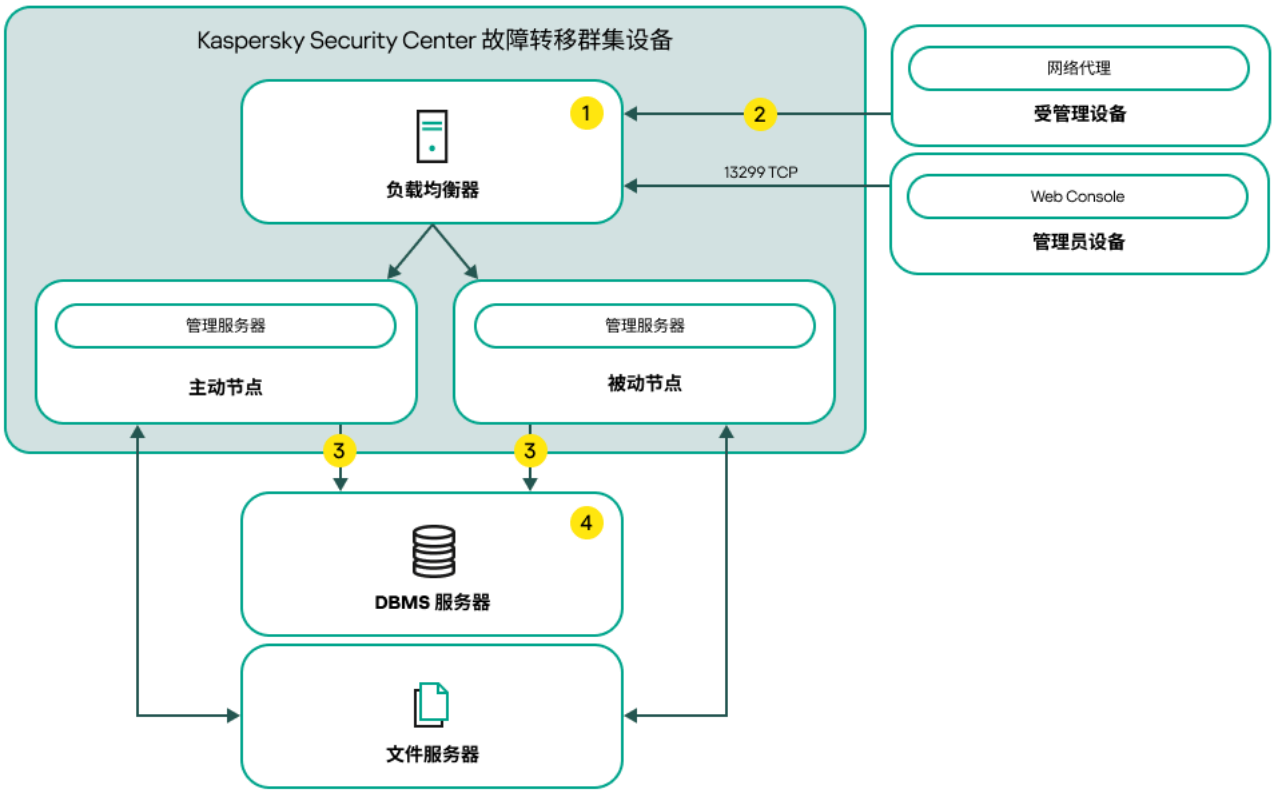
方案图例：

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 打开已安装管理服务器的设备上的以下端口，连接到受管理设备：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。

一个使用第三方负载均衡器和安装在专用设备上的 DBMS 的方案




一个使用第三方负载均衡器和安装在专用设备上的 DBMS 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。

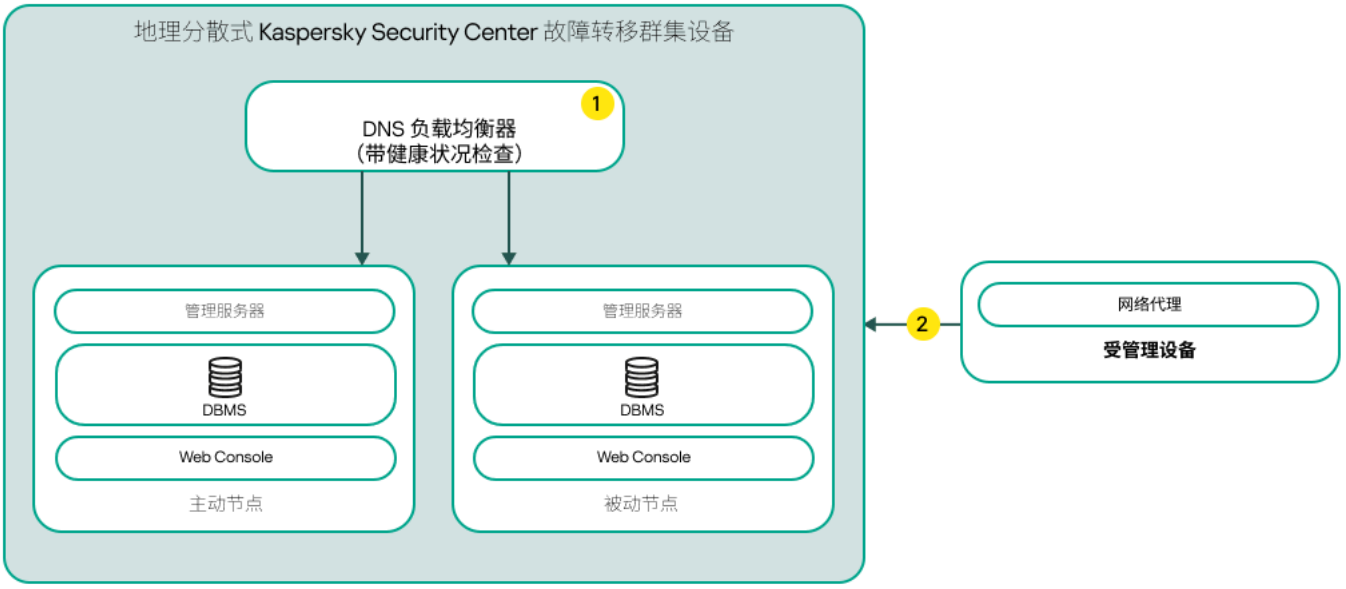
2 打开已安装管理服务器的设备上的以下端口，连接到受管理设备：TCP 13000、UDP 13000 和 TCP 17000。

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。

地理分布式 Kaspersky Security Center Linux 故障转移集群

这种部署方案可以确保所有组件的高可用性。在此方案中，管理服务器、数据库管理系统和 Kaspersky Security Center Web Console 安装在两个集群节点上。




地理分布式 Kaspersky Security Center Linux 故障转移集群的部署方案

1 在安装地理分布式 Kaspersky Security Center Linux 故障转移集群之前必须在您的一端部署的带有健康检查功能的 DNS 均衡器。

DNS 均衡器会定期检查集群节点的状态。当通过域名访问集群时，DNS 均衡器总是返回活动节点的 IP 地址。

2 打开已安装管理服务器的设备上的以下端口，连接到受管理设备：TCP 13000、UDP 13000 和 TCP 17000。

# Kaspersky Security Center Linux 故障转移集群。

本节包含有关部署在单个数据中心内的 Kaspersky Security Center Linux 故障转移集群的一般信息，以及在网络中准备和部署 Kaspersky Security Center Linux 故障转移集群的说明。

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

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

Kaspersky 应用程序部署分阶段进行：

> 建议遵循此场景中所述的步骤顺序。

1. **检查硬件要求**

   确保您拥有满足故障转移集群要求的硬件。

2. **选择部署方案**

   选择部署方案。这会影响部署的后续阶段。

3. **为 Kaspersky Security Center Linux 服务准备用户账户**

   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 `kladmins` 组。运行以下命令：

      ```
      sudo groupadd kladmins
      ```

      ```
      sudo groupmod -g <new_GID> kladmins
      ```

      确保该组在所有三台设备上具有相同的 GID。运行以下命令：

      ```
      getent group kladmins
      ```

      如果 GID 不匹配，您可以使用以下命令指定 GID：

      ```
      sudo groupmod -g <new_GID> kladmins
      ```

   2. 创建 `ksc` 用户账户。将用户账户分配到 `kladmins` 组中。运行以下命令：

      ```
      sudo adduser ksc
      ```

      ```
      sudo usermod -u <new_UID> ksc
      ```

      ```
      sudo gpasswd -a ksc kladmins
      ```

      ```
      sudo usermod -g kladmins ksc
      ```

      确保用户账户在所有三台设备上具有相同的 UID。运行以下命令：

      ```
      getent passwd ksc
      ```

      如果 UID 不匹配，您可以使用以下命令指定 UID：

      ```
      sudo usermod -u <new_UID> ksc
      ```

   3. 创建 `rightless` 用户账户。将用户账户分配到 `kladmins` 组中。运行以下命令：

      ```
      sudo adduser rightless
      ```

      ```
      sudo usermod -u <new_UID> rightless
      ```

      ```
      sudo gpasswd -a rightless kladmins
      ```

      ```
      sudo usermod -g kladmins rightless
      ```

      确保用户账户在所有三台设备上具有相同的 UID。运行以下命令：

      ```
      getent passwd rightless
      ```

      如果 UID 不匹配，您可以使用以下命令指定 UID：

      ```
      sudo usermod -u <new_UID> rightless
      ```

   4. 创建 `ksciam` 用户账户。将用户账户分配到 `kladmins` 组中。运行以下命令：

`sudo adduser ksciam`

`sudo usermod -u <new_UID> ksciam`

`sudo gpasswd -a ksciam kladmins`

`sudo usermod -g kladmins ksciam`

确保用户账户在所有三台设备上具有相同的 UID。运行以下命令：

`getent passwd ksciam`

如果 UID 不匹配，您可以使用以下命令指定 UID：

`sudo usermod -u <new_UID> ksciam`

5. 若有必要，需为用于运行 Kaspersky Security Center Linux 服务相关功能的账户，提高其可打开文件（文件描述符）的默认限制。为此，打开 /etc/security/limits.conf 文件，然后指定文件描述符的软限制和硬限制，如下所示：

   `ksc soft nofile <最大打开文件数>`

   `ksc hard nofile <最大打开文件数>`

   默认情况下，文件描述符的限制在安装期间指定。软文件限制为 32,768 个文件，硬文件限制为 131,072 个文件。

### 4 文件服务器准备

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

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

### 5 DBMS 安装

安装用于 Kaspersky Security Center Linux 的 DBMS。您可以选择其中一个受支持的 DBMS。对于如何安装所选 DBMS 的信息，请参考其文档。

如果 Linux 操作系统的发行版不包含受支持的 DBMS，您可以从第三方软件包存储库安装 DBMS。

安装 DBMS 后，请按照相应的说明进行操作：

- 配置与 Kaspersky Security Center Linux 配合使用的 PostgreSQL 或 Postgres Pro 服务器
- 配置与 Kaspersky Security Center Linux 配合使用的 MariaDB x64 服务器

IAM 创建一个数据库。卸载或将服务器移动到其他设备时，管理服务器不会自动删除 IAM 数据库，因此您必须手动删除数据库。

- 对于 PostgreSQL，请运行以下命令：

  `sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"`

- 对于 MariaDB，请运行以下命令：

  `sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"`

在安装了 DBMS 的设备上，配置将作为主动节点和被动节点运行的设备的连接。

### 6 准备主动和被动节点

准备两台具有相同硬件和软件的设备，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

7. **Kaspersky Security Center Linux 安装**

   在两个节点上均以故障转移集群模式安装 Kaspersky Security Center Linux。

   您必须先在想将其作为主动节点的设备上安装 Kaspersky Security Center Linux，然后在被动节点上安装。

   操作说明：在 Kaspersky Security Center Linux 故障转移集群节点上安装 Kaspersky Security Center Linux。

8. **Kaspersky Security Center Web Console 安装**

   在非集群节点的单独设备上安装 Kaspersky Security Center Web Console。

   在应答文件中将故障转移集群指定为管理服务器地址。

   管理服务器证书位于以下路径：/mnt/KlFocDataShare_klfoc/1093/cert/klserver.cer

   将证书文件复制到正在安装 Kaspersky Security Center Web Console 的设备上。在应答文件中指定证书的本地路径。

9. **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，您可以运行以下命令来启动切换到被动节点：

   `/opt/kaspersky/ksc64/sbin/klfoc -failover --stp klfoc`

   使用以下命令验证两个节点上的故障转移集群管理服务是否处于 `Active: active (running)` 状态：

   `systemctl status klfocsvc_klfoc`

   使用以下命令验证活动节点上的其他故障转移集群服务是否处于 `Active: active (running)` 状态。在被动节点上，这些故障转移集群服务必须处于 `Active: inactive (dead)` 或 `Active: failed (Result: signal)` 状态。

   - `systemctl status klnagent_klfoc`
   - `systemctl status kladminserver_klfoc`
   - `systemctl status klactprx_klfoc`
   - `systemctl status klwebsrv_klfoc`

Kaspersky Security Center Linux 故障转移集群已部署。

## Kaspersky Security Center Linux 故障转移集群。硬件和软件要求

我们建议您在主动节点和被动节点、安装有DBMS的设备以及文件服务器上安装Kaspersky Endpoint Security for Linux。要同时安装 Kaspersky Security Center Linux 故障转移集群和 Kaspersky Endpoint Security for Linux，必须在节点和文件服务器要求的基础上增加 1.5 GB RAM、15% CPU，并且至少具有 300 IOPS。

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。

主动节点和被动节点的最低配置

| 硬件 | 参数值 |
| --- | --- |
| CPU | 2 核，2500 MHz |
| RAM | 6 GB |
| 磁盘空间 | 10 GB，150 IOPS 或更高 |
| 网络接口控制器 | 1 Gbps |

- 支持 CIFS/SMB 协议 2.0 或更高版本的文件服务器。您必须提供一台专用设备来用作文件服务器。

  文件服务器的配置

  | 硬件 | 参数值 |
  | --- | --- |
  | CPU | 16 核，2500 MHz |
  | RAM | 32 GB |
  | 磁盘空间 | 500 GB，500 IOPS 或更高 |
  | 网络接口控制器 | 10 Gbps |

  确保在文件服务器与主动和被动节点之间提供了高网络带宽。

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

## 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

   根据您的 Linux 发行版，通过运行相应的命令安装 nfs-utils 包或 nfs-kernel-server 包：

   ```
   sudo yum install nfs-utils
   sudo apt install nfs-kernel-server
   ```

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

   确保以下文件夹不存在：

   - `/mnt/KlFocStateShare`
   - `/mnt/KlFocDataShare_klfoc`

   如果存在其中任意一个文件夹，请递归删除该文件夹。

   运行以下命令：

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

`sudo mkdir -p /mnt/KlFocDataShare_klfoc`

`sudo chown ksc:kladmins /mnt/KlFocStateShare`

`sudo chown ksc:kladmins /mnt/KlFocDataShare_klfoc`

`sudo chmod -R 770 /mnt/KlFocStateShare /mnt/KlFocDataShare_klfoc`

`sudo sh -c "echo /mnt/KlFocStateShare *\(rw,sync,no_subtree_check,no_root_squash\) >> /etc/exports"`

`sudo sh -c "echo /mnt/KlFocDataShare_klfoc *\(rw,sync,no_subtree_check,no_root_squash\) >> /etc/exports"`

`sudo exportfs -a`

`sudo systemctl start rpcbind`

`sudo systemctl start nfs-server`

通过运行以下命令启用自动启动：

`sudo systemctl enable rpcbind`

您可以指定自定义文件夹，但最好使用建议的文件夹名称以方便使用在线帮助。

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

在继续之前，请确保您已完成"场景：部署卡巴斯基故障转移集群"中的先前步骤。

准备两台设备作为 Kaspersky Security Center Linux 故障转移集群的主动和被动节点。

通用文件夹配置

*配置通用文件夹：*

1. 根据您的 Linux 发行版，通过运行相应的命令在每个节点上安装 nfs-utils 包或 nfs-kernel-server 包：

   `yum install nfs-utils`

   `apt install nfs-kernel-server`

2. 通过运行以下命令创建挂载点：

   `mkdir -p /mnt/KlFocStateShare`

   `mkdir -p /mnt/KlFocDataShare_klfoc`

3. 匹配挂载点和共享文件夹：

   `sudo sh -c "echo <文件服务器>:/mnt/KlFocStateShare /mnt/KlFocStateShare nfs vers=4,soft,timeo=50,retrans=2,auto,user,rw 0 0 >> /etc/fstab"`

   `sudo sh -c "echo <文件服务器>:/mnt/KlFocDataShare_klfoc /mnt/KlFocDataShare_klfoc nfs vers=4,noauto,user,rw,exec 0 0 >> /etc/fstab"`

   其中，`{文件服务器}` 是具有共享文件夹的文件服务器的 FQDN。

4. 通过运行以下命令挂载共享文件夹：

   `mount /mnt/KlFocStateShare`

`mount /mnt/KlFocDataShare_klfoc`

5. 确保访问共享文件夹的权限属于 ksc:kladmins。

   运行以下命令：

   `ls -la /mnt/`

网络适配器配置

从属网络适配器可以是物理或虚拟适配器。如果您选择了带有辅助网络适配器的部署方案，请在两个节点上执行相应的步骤：

- 使用基于物理网络适配器（MACVLAN 技术）的虚拟辅助网络适配器：

  1. 安装 iputils-arping 包。根据您的 Linux 发行版，运行以下命令之一：

     - `yum install iputils`

     或者

     - `apt install iputils-arping`

  2. 为确保使用 NetworkManager 管理物理网络适配器，请运行以下命令：

     `nmcli device status`

     如果命令输出显示物理网络适配器未受到管理，请配置 NetworkManager 来管理物理网络适配器。确切的配置步骤取决于您的 Linux 发行版。

  3. 若要辨识接口，请使用以下命令：

     `ip a`

  4. 要创建配置文件，请运行以下命令：

     `nmcli connection add type macvlan dev <`物理接口`> mode bridge ifname <`虚拟接口`> ipv4.addresses <`地址掩码`> ipv4.method manual autoconnect no`

- 使用物理辅助网络适配器或通过虚拟机监控程序创建虚拟 TAP 设备。在这种情况下，请禁用 NetworkManager 软件。

  1. 将辅助网络适配器连接到节点。

  2. 安装 iputils-arping 包。根据您的 Linux 发行版，运行以下命令之一：

     - `yum install iputils`

     或者

     - `apt install iputils-arping`

  3. 要删除目标接口的 NetworkManager 连接，请运行以下命令：

     `nmcli con del <`连接名称`>`

     要检查与目标接口的连接，请运行以下命令：

     `nmcli con show`

  4. 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>`

5. 重启 NetworkManager：

   `systemctl reload NetworkManager`

   为确保目标接口不再受管理，请运行以下命令：

   `nmcli dev status`

加载均衡器配置

如果您选择了带有负载均衡器的部署方案，请按照以下说明进行配置。

*配置负载均衡器：*

1. 准备一个安装了 nginx 或其他负载均衡器的专用 Linux 设备。
2. 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。
3. 在 nginx 服务器上，根据以下文章的说明打开所有管理服务器端口：Kaspersky Security Center Linux 使用的端口。

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。

故障转移集群节点的可用性应由到管理服务器的主连接端口的可用性决定。被动节点不接受任何外部连接，直到发生切换。

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

在继续之前，请确保您已完成"场景：部署卡巴斯基故障转移集群"中的先前步骤。

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

根据安装在您的设备上的 Linux 发行版，您需要使用以下安装文件之一：

- ksc64_[version_number]_amd64.deb
- ksc64-[version_number].x86_64.rpm

您通过从 Kaspersky 网站下载来接收安装文件。

如果使用 RED OS 版本 7.3.4 或更高版本，或者 MSVSPHERE 版本 9.2 或更高版本，则必须在两个节点上都安装 libxcrypt-compat 包。

在活动节点上安装

*在活动节点上安装 Kaspersky Security Center Linux：*

1. 确保您要安装 Kaspersky Security Center Linux 的设备运行支持的 Linux 分类。
2. 如果使用从属网络适配器，请在被提示时输入其名称。您可以输入以下命令来显示所有网络接口：

   ```
   ip addr
   ```

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

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

4. 运行 Kaspersky Security Center Linux 配置：

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

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

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

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

6. 选择“**主集群节点**”作为管理服务器安装模式。
7. 出现提示时，指定以下设置：

   a. 输入状态共享挂载点的本地路径：`/mnt/KlFocStateShare`

   b. 输入数据共享挂载点的本地路径：`/mnt/KlFocDataShare_klfoc`

   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. 输入从属网络适配器的 FQDN/IP 地址或外部负载均衡器的 FQDN/IP 地址。

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

   g. 评估您要管理的设备的大概数量：

   - 如果有 1 到 100 台受管理设备，则输入“1”。
   - 如果有 101 到 1000 台受管理设备，则输入“2”。
   - 如果有超过 1000 台受管理设备，则输入“3”。

此设置用于自动随机延迟任务启动以优化网络负载。下方列表显示了计算延迟的间隔：

- 1 至 100 个受管理设备，值 1。不使用延迟。
- 101 至 1000 个受管理设备，值 2。延迟 5 分钟。
- 超过 1000 个受管理设备，价值 3。延迟 10 分钟。

h. 输入服务的安全组名称。默认情况下，使用 kladmins 组。

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

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

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

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

l. 输入安装了数据库的设备的 DNS 名称或 IP 地址。

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

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

n. 输入数据库名称。

o. 输入用于访问数据库的数据库管理员账户的登录名。

p. 输入用于访问数据库的数据库管理员账户的密码。

q. 输入 IAM Server FQDN。
您必须指定在步骤 7e 中输入的管理服务器 DNS 名称。

r. 输入用于启动 IAM 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“ksciam”账户。

s. 选择您安装的与 IAM 服务一起使用的 DBMS：

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

t. 输入 IAM 服务要使用的 IAM DBMS 地址。

u. 输入 IAM DBMS 端口号。该端口用于与 IAM 服务通信。默认情况下，使用以下端口：

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

v. 输入 IAM 服务要使用的 IAM 数据库名称。IAM 服务使用的数据库名称应与管理服务器使用的数据库名称不同。

w. 输入用于访问 IAM 数据库的数据库账户的登录名。

x. 输入用于访问 IAM 数据库的数据库账户的密码。

8. 等待服务被添加并自动启动：

- klfocsvc_klfoc
- kladminserver_klfoc
- klwebsrv_klfoc
- klactprx_klfoc
- klnagent_klfoc
- kliam_klfoc

9. 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 256 个字符。

如果跳过此步骤，可以稍后通过运行以下命令来创建账户：

```
/opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <密码>
```

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

在辅助（被动）节点上安装

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

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

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

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

3. 运行 Kaspersky Security Center Linux 配置：

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

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

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

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

5. 选择"**辅助集群节点**"作为管理服务器安装模式。

6. 出现提示时，输入状态共享挂载点的本地路径：`/mnt/KlFocStateShare`

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

服务验证

使用以下命令验证故障转移集群管理服务是否处于 `Active: active (running)` 状态：

```
systemctl status klfocsvc_klfoc
```

使用以下命令验证其他故障转移集群服务是否处于 `Active: inactive (dead)` 状态：

- `systemctl status klnagent_klfoc`
- `systemctl status kladminserver_klfoc`
- `systemctl status klactprx_klfoc`
- `systemctl status klwebsrv_klfoc`
- `systemctl status kliam_klfoc`

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

## 手动启动和停止集群节点

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

启动和停止整个故障转移集群以进行维护

*要启动或停止整个故障转移集群：*

在主动节点上，运行以下命令之一：

- 要停止集群，请运行：`/opt/kaspersky/ksc64/sbin/klfoc -stopcluster --stp klfoc`
- 要启动集群，请运行：`/opt/kaspersky/ksc64/sbin/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。
10. 要确保当前节点为主动节点，请运行以下命令来检查服务是否正在运行：

    `systemctl status klnagent_klfoc.service`

    `systemctl status kladminserver_klfoc.service`

    `systemctl status klactprx_klfoc.service`

    `systemctl status klwebsrv_klfoc.service`

    `systemctl status kliam_klfoc.service`

    这些服务在主动节点上运行，而不是在被动节点上运行。

该节点维护完毕并连接到故障转移集群。

## 重新安装故障转移集群节点

*要重新安装故障转移集群节点：*

1. 创建管理服务器的备份。
2. 将活动节点切换到维护模式。
3. 有必要保留当前操作系统，请执行以下步骤。
   如果要更换设备或操作系统，请跳过此步骤。

   a. 要停止故障转移集群，请运行以下命令：
   `klfoc -stopcluster --stp klfoc`

   b. 要强制停止故障转移集群服务，请运行以下命令：
   `sudo systemctl stop klfocsvc_klfoc`
   `systemctl status kl*klfoc*`

   c. 要卸载故障转移集群目录，请运行以下命令：
   `sudo umount /mnt/KlFocDataShare_klfoc`
   `sudo umount /mnt/KlFocStateShare`

   d. 要卸载 Kaspersky Security Center Linux，请根据您的 Linux 发行版运行以下任一命令：

   - `sudo dpkg --remove ksc64`

或

- `sudo yum remove ksc64`

e. 针对被动节点执行以下说明中的所有步骤：

1. 为 Kaspersky Security Center Linux 故障转移集群准备节点。
2. 在 Kaspersky Security Center Linux 故障转移集群节点上安装 Kaspersky Security Center Linux。

4. 退出维护模式。从“手动启动和停止集群节点”说明的第 6 步（停止故障转移集群）继续。

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

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

Kaspersky Security Center Web Console 不支持在集群节点上进行安装。我们建议在单独的服务器上安装 Kaspersky Security Center Web Console。

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

1. 执行 Kaspersky Security Center Web Console 安装的步骤 1 和步骤 2。
2. 在第 3 步，在响应文件中指定`trusted`安装参数，以允许 Kaspersky Security Center Web Console 连接到 Kaspersky Security Center Linux 故障转移集群。

   `trusted` **安装参数**的组成部分

   如果您使用域身份验证和单点登录连接到 Kaspersky Security Center Linux 故障转移集群，请按如下方式指定受信任的安装参数：如果您将 Kaspersky Security Center Web Console 连接到管理服务器版本 16 或更高版本，则将使用Identity and Access Manager (IAM)提供的域身份验证和单点登录 (SSO)。在此情况下，请按如下方式指定 `trusted` 安装参数：

```
"trusted":  {
  "<管理服务器名称>": {
    "iamHost": "ksc-iam.example.com",
    "iamOAuthPort": 4444,
    "iamProxyPort": 9050,
    "iamCertPath": "<共享数据文件夹>/iam/main_certificate.pem",
    "iamPATPath": "<共享数据文件夹>/iam/initial_token.txt",
    "kscPort": 13299,
    "kscCertPath": "<共享数据文件夹>/1093/cert/klserver.cer"
  }
}
```

其中：

- < 管理服务器名称 > 是将显示在 Kaspersky Security Center Web Console 登录窗口中的 Kaspersky Security Center Linux 故障转移集群名称。

- `iamHost` 是安装管理服务器和 IAM 的设备的地址。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 FQDN 或主机名称作为 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均衡器的 FQDN 或主机名称。

  `iamHost` 值必须与安装管理服务器时指定的 IAM 地址匹配。若要获取指定的 IAM 地址，请在管理服务器主机上运行以下命令：

  ```
  grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
  ```

- `iamOAuthPort` 是用于通过 OpenID Connect 身份验证协议交换身份验证令牌的端口（默认值为 4444）。此端口用于 Kaspersky Security Center Web Console 服务器和管理服务器之间的通讯，以及浏览器（与 Kaspersky Security Center Web Console 配合使用）和管理服务器之间的通讯。

- `iamProxyPort` 是用于将 Kaspersky Security Center Web Console 服务器连接到管理服务器的端口（默认值为 9050）。

- `iamCertPath` 是 IAM 证书的路径。IAM 证书会在您首次运行管理服务器时自动创建。证书位于安装管理服务器的设备上。证书的默认路径为：< 共享数据文件夹 >`/iam/main_certificate.pem`。该证书位于 Kaspersky Security Center Linux 故障转移集群的共享数据存储中。自签名 IAM 证书会自动轮换。

- `iamPATPath` 是将 Kaspersky Security Center Web Console 注册为 IAM 中的 OAuth 客户端时所用令牌的路径。该文件会在您首次运行管理服务器时生成。令牌位于安装管理服务器的设备上。令牌的默认路径：<共享数据文件夹>/iam/initial_token.txt。该令牌位于 Kaspersky Security Center Linux 故障转移集群的共享数据存储中。该令牌永久有效，无需轮换。

- `kscPort` 是 Kaspersky Security Center Web Console 用于连接到管理服务器的 OpenAPI 端口（默认值为 13299）。

- `kscCertPath` 是位于 Kaspersky Security Center Linux 故障转移集群的共享数据存储中的管理服务器证书。证书文件的默认路径为：< 共享数据文件夹 >`\1093\cert\klserver.cer`。

  将管理服务器证书文件（由 `kscCertPath` 指定）、IAM 证书文件（由 `iamCertPath` 指定）和令牌文件（由 `iamPATPath` 指定）从共享数据存储复制到安装 Kaspersky Security Center Web Console 的设备。指定管理服务器证书的本地路径。

如果将 Kaspersky Security Center Web Console 连接到管理服务器版本 15.4 或更早版本，则将使用指定域用户或内部用户的名称和密码进行身份验证。在这种情况下，请按如下方式指定受信任的安装参数：

```
"trusted":  {
  "<管理服务器名称>": {
    "kscHost": "ksc.example.com",
    "kscPort": 13299,
    "kscCertPath": "<共享数据文件夹>/1093/cert/klserver.cer"
  }
}
```

其中：

- < 管理服务器名称 > 是将显示在 Kaspersky Security Center Web Console 登录窗口中的 Kaspersky Security Center Linux 故障转移集群名称。
- `kscHost` 是管理服务器地址（FQDN 或主机名）。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地址。
- `kscPort` 是 Kaspersky Security Center Web Console 用于连接到管理服务器的 OpenAPI 端口（默认值为 13299）。
- `kscCertPath` 是位于 Kaspersky Security Center Linux 故障转移集群的共享数据存储中的管理服务器证书。证书文件的默认路径为：< 共享数据文件夹 >`\1093\cert\klserver.cer`。将证书文件从共享数据存储复制到安装 Kaspersky Security Center Web Console 的设备。指定管理服务器证书的本地路径。

3. 继续 Kaspersky Security Center Web Console 的标准安装。

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

# 地理分布式 Kaspersky Security Center Linux 故障转移集群

本节包含有关地理分布式 Kaspersky Security Center Linux 故障转移集群的一般信息，以及针对以下配置在您的网络中准备和部署地理分布式故障转移集群的说明：

- 运行安装有 PostgreSQL 数据库管理系统的 Ubuntu 的集群节点
- 运行安装有 Platform V Pangolin 数据库管理系统的 SberLinux 的集群节点

## 运行安装有 PostgreSQL数据库管理系统的 Ubuntu 的地理分布式集群

按照此方案，您可以准备基础设施并部署地理分布式 Kaspersky Security Center Linux 故障转移集群。

先决条件

- 部署具有健康检查功能的高可用性 DNS 均衡器。
- 确保主动和被动集群节点是两个硬件和软件配置完全相同的设备。
  - 硬件要求：
    - CPU — 16 核，2500 MHz
    - RAM：32 GB
    - 磁盘空间 — 500 GB，IOPS 300 或更高
    - 网络接口控制器 — 1 Gbps

- 软件要求：
  - 操作系统：Ubuntu Server 24.04 LTS (Noble Numbat) 64 位
  - DBMS：PostgreSQL 17 64 位

阶段

部署在单个数据中心内的 Kaspersky Security Center Linux 故障转移集群无法升级为地理分布式故障转移集群。

地理分布式 Kaspersky Security Center Linux 故障转移集群的部署分阶段进行：

1. **准备故障转移集群节点的文件系统**

   在两个集群节点上都准备文件系统。准备工作包括创建 LVM 逻辑卷和配置目录作为挂载点。

2. **配置复制集群文件系统**

   安装 DRBD 实用程序并配置 DRBD 资源，以便在故障转移集群节点之间进行数据复制。之后，在主动集群节点上创建复制文件系统。

3. **在故障转移集群节点上安装和配置 Corosync 和 Pacemaker**

   安装 Corosync 和 Pacemaker 以提供集群通讯和资源管理以实现高可用性。

4. **安装和配置 PostgreSQL DBMS**

   在集群节点上安装并配置 PostgreSQL。

5. **在故障转移集群节点上安装 Kaspersky Security Center Linux**

   在集群节点上安装 Kaspersky Security Center Linux，然后配置集群节点之间的加密。

6. **在故障转移集群节点上安装 Kaspersky Security Center Web Console**

   在两个故障转移集群节点上都安装 Kaspersky Security Center Web Console 以实现高可用性。

## 准备集群节点的文件系统

作为准备部署地理分布式 Kaspersky Security Center Linux 故障转移集群的第一步，您必须在两个集群节点上都设置文件系统。准备工作包括创建 LVM 逻辑卷和配置目录作为挂载点。在两个集群节点上执行以下步骤。

*准备集群节点的文件系统：*

1. 为管理服务器数据和数据库创建一个 LVM 逻辑卷：

   ```
   lvcreate -L <volume size> -n klfocdata <volume group name>
   ```

   创建一个单独的 LVM 逻辑卷用于存储应答文件：

   ```
   lvcreate -L <volume size> -n klfocstate <volume group name>
   ```

其中：

- `volume group name`是 LVM 使用的卷组名称。
- `klfocdata` 和 `klfocstate` 是逻辑卷名称。这些逻辑卷是在卷组内创建的。
  为了保持一致性，我们建议使用这些卷名称，但您也可以根据需要指定自定义名称。
- [[volume size]] 卷的大小。我们建议为管理服务器数据和数据库分配至少 500 GB 的空间。存储应答文件的卷只需要少量空间。

2. 创建用作逻辑卷挂载点的目录。
   - 对于管理服务器数据和数据库：

     ```
     mkdir -p /mnt/KlFocDataShare_klfoc
     ```

   - 对于响应文件：

     ```
     mkdir -p /mnt/KlFocStateShare_klfoc
     ```

为了保持一致性，我们建议使用 [[/mnt/KlFocDataShare_klfoc]] 和 [[/mnt/KlFocStateShare_klfoc]] 目录，不过如果需要，您可以指定自定义名称。

集群节点的文件系统已准备就绪。之后，您需要配置复制集群文件系统。

## 配置复制集群文件系统

安装和配置 DRBD

*DRBD* 是用于数据复制的第三方软件（专门用于上一步中准备的数据卷和挂载点）。

准备好集群节点的文件系统后，您必须安装 DRBD 实用程序并配置 DRBD 资源，以便在集群节点之间进行数据复制。在两个集群节点上执行以下步骤。

*在集群节点上安装和配置 DRBD：*

1. 安装 DRBD 实用程序：

   ```
   apt update
   apt install -y drbd-utils
   ```

   我们建议使用 DRBD 9.2.6 或更高版本，因为它提供内置的流量加密功能。
   DRBD 流量也可以使用您自己的 VPN 解决方案进行加密。

2. 为文件系统准备期间创建的每个逻辑卷创建 DRBD 资源配置文件（`klfocdata` 和 `klfocstate`）。
   所有配置文件必须放置在 [[/etc/drbd.d/]] 中。
   - 资源 `klfocdata`（管理服务器数据和数据库）
     对 klfocdata 资源使用异步复制（协议 A）。根据您的环境配置所有其他参数。

**配置文件示例**

```
resource klfocdata {
    protocol A;
    net {
        after-sb-0pri    discard-least-changes;
        after-sb-1pri    call-pri-lost-after-sb;
        after-sb-2pri    call-pri-lost-after-sb;
    }
    syncer {
        rate 110M;
    }
    # Hostname of the active node
    on db1 {
        device    /dev/drbd0;
        disk      /dev/<volume group name>/klfocdata;
        address   <disk IP address>;
        meta-disk internal;
    }
    # Hostname of the passive node
    on db2 {
        device    /dev/drbd0;
        disk      /dev/<volume group name>/klfocdata;
        address   <disk IP address>;
        meta-disk internal;
    }
}
```

- 资源 `klfocstate`（应答文件）

  使用同步复制（协议 C）创建 klfocstate 资源。根据您的环境配置所有其他参数。

  **配置文件示例**

```
resource klfocstate {
    protocol C;
    net {
        after-sb-0pri    discard-least-changes;
        after-sb-1pri    call-pri-lost-after-sb;
        after-sb-2pri    call-pri-lost-after-sb;
    }
    syncer {
        rate 110M;
    }
    # Hostname of the active node
    on db1 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
    # Hostname of the passive node
    on db2 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
}
```

3. 初始化两个资源的 DRBD 元数据：

```
drbdadm create-md klfocdata
drbdadm create-md klfocstate
```

4. 启动所有已配置资源上的 DRBD：

```
drbdadm up all
```

DRBD 已在两个集群节点上安装和配置。

在主动集群节点上创建复制文件系统

在两个集群节点上都安装和配置 DRBD 后，在主动集群节点上创建复制文件系统。在主动集群节点上执行以下步骤。

*要在主动集群节点上创建复制文件系统：*

1. 将两个 DRBD 资源提升为主角色：

```
drbdadm primary --force klfocdata
drbdadm primary --force klfocstate
```

2. 格式化 DRBD 设备，以便为集群节点上的复制卷做好准备：

```
mkfs.ext4 /dev/drbd0
mkfs.ext4 /dev/drbd2
```

3. 配置文件系统参数：

```
tune2fs -m 0 /dev/drbd0
tune2fs -m 0 /dev/drbd2
```

4. 将 DRBD 设备挂载到之前创建的目录：

```
mount -o noatime /dev/drbd0 /mnt/KlFocDataShare_klfoc
mount -o noatime /dev/drbd2 /mnt/KlFocStateShare_klfoc
```

如果安装了 multipathd 服务，则必须将其配置为在两个集群节点上都忽略设备[[/dev/drbd*]]。

5. 验证复制状态：

```
drbdadm status
```

正确的文件系统配置输出：

```
klfocdata role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate
klfocstate role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate
```

主动集群节点上的复制文件系统已配置。之后，您必须在集群节点上安装并配置 Corosync 和 Pacemaker。

## 在集群节点上安装和配置 Corosync 和 Pacemaker

Corosync 和 Pacemaker 提供集群通讯和资源管理，以实现高可用性。它们确保在发生故障时服务自动迁移到健康的节点，从而最大限度地减少停机时间。

*在集群节点上安装和配置 Corosync 和 Pacemaker：*

1. 在两个集群节点上，安装所需的软件包：

```
sudo apt install pacemaker -y
sudo apt install crmsh -y
sudo apt install resource-agent-extra -y
```

2. 根据官方文档，在两个集群节点上配置 Corosync 和 Pacemaker。 。这包括启用自动启动、生成和分发身份验证密钥以及配置 authkey 文件的访问权限。

   为确保设置正确，请在集群节点之一上运行以下命令：

```
crm status
```

   预期输出应显示集群状态并列出所有活动节点，以确认 Corosync 正在正常运行且节点之间正在通讯。

3. 在两个集群节点上，配置 Pacemaker 集群的基本设置：

```
crm configure property stonith-enabled="false"
crm configure property symmetric-cluster="false"
crm configure rsc_defaults resource-stickiness="110"
crm configure rsc_defaults migration-threshold=3
crm configure property no-quorum-policy=ignore
```

4. 在两个集群节点上，禁用由 Corosync 管理的脚本的启动：

```
systemctl disable drbd.service
```

5. 在集群节点之一上，在 Pacemaker 中创建基于 DRBD 的资源。

   - klfocdata 的 DRBD 资源

     a. 为 DRBD 卷 `klfocdata` 创建集群资源，使集群能够自动管理其状态并监控其健康状况：

```
crm configure primitive drbd_klfocdata ocf:linbit:drbd params drbd_resource="klfocdata" \
op monitor interval="60s" op start interval="0" timeout="240s" op stop interval="0" \
timeout="240s" op monitor role=Master interval="10s" op monitor role=Slave interval="30s"
```

     b. 基于已创建的资源 [[drbd_klfocdata]] 创建集群管理资源 [[ms_drbd_klfocdata]]：

```
crm configure ms ms_drbd_klfocdata drbd_klfocdata meta master-max="1" master-node-max="1" \
clone-max="2" clone-node-max="1" notify="true"
```

     c. 为 DRBD 卷 [[fs_klfocdata]] 创建挂载点，指定设备、目标目录、文件系统类型和挂载选项：

```
crm configure primitive fs_klfocdata ocf:heartbeat:Filesystem params device="/dev/drbd0" \
directory="/mnt/KlFocDataShare_klfoc" fstype="ext4" options="data=journal"
```

- klfocstate 的 DRBD 资源

  a. 为 DRBD 卷 `klfocstate` 创建集群资源，使集群能够自动管理其状态并监控其健康状况：

  ```
  crm configure primitive drbd_klfocstate ocf:linbit:drbd params drbd_resource="klfocstate" \
  op monitor interval="60s" op start interval="0" timeout="240s" op stop interval="0" \
  timeout="240s" op monitor role=Master interval="10s" op monitor role=Slave interval="30s"
  ```

  b. 基于已创建的资源 [[drbd_klfocstate]] 创建集群管理资源 ms_drbd_klfocstate：

  ```
  crm configure ms ms_drbd_klfocstate drbd_klfocstate meta master-max="1" master-node-max="1" \
  clone-max="2" clone-node-max="1" notify="true"
  ```

  c. 为 DRBD 卷 [[fs_klfocstate]] 创建挂载点，指定设备、目标目录、文件系统类型和挂载选项：

  ```
  crm configure primitive fs_klfocstate ocf:heartbeat:Filesystem params device="/dev/drbd2" \
  directory="/mnt/KlFocStateShare_klfoc" fstype="ext4" options="noatime"
  ```

6. 在两个集群节点上，禁用 DRBD 服务的自动启动：

```
systemctl disable drbd.service
```

Corosync 和 Pacemaker 已在集群节点上安装和配置。之后，您必须安装 DBMS并创建管理服务器数据库和 IAM 数据库。

## 安装和配置 PostgreSQL DBMS

在集群节点上安装和配置 Corosync 和 Pacemaker 后，您必须在两个集群节点上都安装 DBMS。

*安装和配置 DBMS：*

1. 在两个集群节点上，安装 PostgreSQL 17 x64 或更高版本。
   对于如何安装 PostgreSQL 的信息，请参考其文档。

2. 确保安装了 DBMS 的集群节点上不存在以下名称的 DBMS 用户账户：

   - client
   - iam
   - ksc
   - locker
   - pat
   - scope
   - voltron

3. 在两个集群节点上，停止 DBMS，然后禁用 DBMS 服务的自动启动：

```
sudo systemctl stop postgresql
sudo systemctl disable postgresql
```

4. 在主动集群节点上，将 DBMS 目录复制到`/mnt/KlFocDataShare_klfoc/dbms`目录：

```
rsync -av /var/lib/postgresql/17/main/ /mnt/KlFocDataShare_klfoc/dbms
mv /var/lib/postgresql/17/main /var/lib/postgresql/17/main.bk
```

5. 在主动集群节点上，将 PostgreSQL 配置文件复制到 [[/mnt/KlFocDataShare_klfoc/dbms]] 目录：

```
sudo cp /etc/postgresql/17/main/pg_hba.conf /mnt/KlFocDataShare_klfoc/dbms
sudo cp /etc/postgresql/17/main/pg_ident.conf /mnt/KlFocDataShare_klfoc/dbms
```

6. 在两个集群节点上，打开配置文件[[/etc/postgresql/17/main/postgresql.conf]]，然后设置目录 [[/mnt/KlFocDataShare_klfoc/dbms]]作为数据库数据目录。

   此外，指定配置文件路径（`/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf` 和`/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf`），并移除`include_dir`参数：

```
data_directory = '/mnt/KlFocDataShare_klfoc/dbms'
hba_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf'
ident_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf'
listen_addresses = '*'
```

7. 在配置文件`/etc/postgresql/17/main/postgresql.conf`中，调整数据库管理系统配置以满足 Kaspersky Security Center Linux 要求。

8. 创建 PostgreSQL 服务资源：

```
crm configure primitive klfocsvc_dbms ocf:heartbeat:pgsql \
params pgctl="/usr/lib/postgresql/17/bin/pg_ctl" \
psql="/usr/bin/psql" \
pgdata="/mnt/KlFocDataShare_klfoc/dbms" \
config="/etc/postgresql/17/main/postgresql.conf" \
socketdir="/var/run/postgresql" \
op start timeout=60s \
op stop timeout=60s \
op monitor interval=30s timeout=60s
```

9. 将 PostgreSQL 资源添加到`group_klfoc`集群组：

```
crm configure edit klfoc_group
```

10. 在列表末尾追加 PostgreSQL 资源名称`klfocsvc_dbms`，例如：

```
group klfoc_group {
...
klfocsvc_dbms
}
```

11. 在主动集群节点上，为 IAM 创建一个数据库。数据库名称必须与您为使用 Kaspersky Security Center Linux 而安装的数据库名称不同。卸载或将服务器移动到其他设备时，管理服务器不会自动删除 IAM 数据库，您必须手动删除数据库。

```
sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
```

数据库管理系统已安装并配置。管理服务器数据库和 IAM 数据库已创建。之后，您需要在集群节点上安装 Kaspersky Security Center Linux。

## 在地理分布式故障转移集群节点上安装 Kaspersky Security Center Linux

Kaspersky Security Center Linux 通过使用应答文件以静默模式安装在地理分布式集群节点上，也就是说，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。

先决条件：

- 完成所有准备步骤：
  - 准备集群节点的文件系统
  - 配置复制集群文件系统
  - 在集群节点上安装和配置 Corosync 和 Pacemaker
  - 安装和配置 PostgreSQL DBMS
- 确保集群节点运行 Ubuntu Server 24.04 LTS (Noble Numbat) x64。
- 从卡巴斯基网站下载安装文件 [[ksc64_[version_number]_amd64.deb]]。

在活动节点上安装

*在活动节点上以静默模式安装 Kaspersky Security Center Linux：*

1. 阅读最终用户授权许可协议。只有在您理解并接受最终用户授权许可协议的条款后，才执行下面的步骤。
2. 创建组“`kladmins`”和非特权账户“`ksc`”与'`ksciam`'，这些账户必须是“`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
adduser ksciam
gpasswd -a ksciam kladmins
usermod -g kladmins ksciam
```

3. 在目录 [[/mnt/KlFocDataShare_klfoc/]] 中创建一个目录，用于存放 Kaspersky Security Center Linux 文件：

```
mkdir /mnt/KlFocDataShare_klfoc/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。

在用于 Kaspersky Security Center Linux 静默模式安装的参数列表中，指定地理分布式集群部署所需的以下参数：

- `KLFOC_UNATT_EXT_RESOURCE_MANAGEMENT=2`
  设置值 [[2]] 以部署地理分布式集群。
- `KLSRV_UNATT_SERVERADDRESS=<DNS balancer address>`和`KLSRV_UNATT_IAM_ADDRESS=<DNS balancer address>`
  必须已部署带有健康检查功能的 DNS 均衡器。这些参数的值必须相同，并且设置为 DNS 均衡器的 FQDN。

5. 用以下命令在包含应答文件全称（例如，包括路径）的根或用户环境中设置 `KLAUTOANSWERS` 环境变量的值：

```
export KLAUTOANSWERS=/tmp/ksc_install/answers.txt
```

6. 运行以下命令以静默模式启动 Kaspersky Security Center Linux 安装：
   - 在根环境中：

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

   - 在用户环境中：

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

7. 禁用 klfocsvc_klfoc.service 服务的自动启动：

```
systemctl disable klfocsvc_klfoc.service
```

8. Kaspersky Security Center Linux 安装完成后，停止主动集群节点。
9. 将所有集群资源迁移到被动节点。
   您可以使用命令[[crm node standby]]（并使用[[crm node online]]把它带回来）。

在被动节点上安装

*在被动节点上安装 Kaspersky Security Center Linux：*

1. 运行 Kaspersky Security Center Linux 安装：

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

2. 运行 Kaspersky Security Center Linux 配置：

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

3. 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：

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

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

4. 选择被动集群节点作为管理服务器安装模式。

5. 出现提示时，输入状态共享挂载点的本地路径：`/mnt/KlFocStateShare_klfoc`。

6. 禁用 klfocsvc_klfoc.service 服务的自动启动：

```
systemctl disable klfocsvc_klfoc.service
```

7. 创建`klfocsvc_klfoc`服务资源：

```
crm configure primitive klfocsvc_klfoc systemd:klfocsvc_klfoc \
op start timeout="900s" interval="0" \
op stop timeout="900s" interval="0" \
op monitor interval="30s" timeout="90s"
```

8. 添加`klfocsvc_klfoc`资源到`group_klfoc`组：

```
crm configure edit klfoc_group
```

9. 在组行末尾追加[[klfocsvc_klfoc]]，例如：

```
group klfoc_group {
...
klfocsvc_klfoc
}
```

10. 验证活动节点上的所有资源是否都处于启动状态。

```
crm status
```

配置集群节点之间的加密

*要配置集群节点之间的加密，*

如果您在配置复制集群文件系统期间安装了 DRBD 版本 9.2.6 或更高版本，请根据 DRBD 官方文档 配置集群节点之间的加密。

或者，您可以使用自己的 VPN 解决方案对集群节点之间的流量进行加密。

地理分布式 Kaspersky Security Center Linux 故障转移集群已安装。之后，您必须在两个集群节点上都安装 Kaspersky Security Center Web Console 。

## 运行安装有 Platform V Pangolin 数据库管理系统的 SberLinux 的地理分布式集群

按照此方案，您可以准备基础设施并部署地理分布式 Kaspersky Security Center Linux 故障转移集群。

先决条件

- 部署具有健康检查功能的高可用性 DNS 均衡器。
- 确保主动和被动集群节点是两个硬件和软件配置完全相同的设备。
  - 硬件要求：
    - CPU — 16 核，2500 MHz
    - RAM：32 GB
    - 磁盘空间 — 500 GB，IOPS 300 或更高
    - 网络接口控制器 — 1 Gbps
  - 软件要求：
    - 操作系统：Platform V SberLinux OS Server (SLO) 9.5.1 64 位
    - DBMS: Platform V Pangolin 6.5.1 64 位

阶段

> 部署在单个数据中心内的 Kaspersky Security Center Linux 故障转移集群无法升级为地理分布式故障转移集群。

地理分布式 Kaspersky Security Center Linux 故障转移集群的部署分阶段进行：

1. **准备故障转移集群节点的文件系统**

   在两个集群节点上都准备文件系统。准备工作包括创建 LVM 逻辑卷和配置目录作为挂载点。

2. **配置复制集群文件系统**

   安装 DRBD 实用程序并配置 DRBD 资源，以便在故障转移集群节点之间进行数据复制。之后，在主动集群节点上创建复制文件系统。

3. **在故障转移集群节点上安装和配置 Corosync 和 Pacemaker**

   安装 Corosync 和 Pacemaker 以提供集群通讯和资源管理以实现高可用性。

4. **安装和配置 Platform V Pangolin 数据库管理系统**

   在集群节点上安装和配置 Platform V Pangolin。

5. **在故障转移集群节点上安装 Kaspersky Security Center Linux**

   在集群节点上安装 Kaspersky Security Center Linux，然后配置集群节点之间的加密。

### 6 在故障转移集群节点上安装 Kaspersky Security Center Web Console

在两个故障转移集群节点上都安装 Kaspersky Security Center Web Console 以实现高可用性。

## 准备集群节点的文件系统

作为准备部署地理分布式 Kaspersky Security Center Linux 故障转移集群的第一步，您必须在两个集群节点上都设置文件系统。准备工作包括创建 LVM 逻辑卷和配置目录作为挂载点。在两个集群节点上执行以下步骤。

*准备集群节点的文件系统：*

1. 为管理服务器数据和数据库创建一个 LVM 逻辑卷：

   ```
   lvcreate -L <volume size> -n klfocdata <volume group name>
   ```

   创建一个单独的 LVM 逻辑卷用于存储应答文件：

   ```
   lvcreate -L <volume size> -n klfocstate <volume group name>
   ```

   其中：

   - `volume group name` 是 LVM 使用的卷组名称。
   - `klfocdata` 和 `klfocstate` 是逻辑卷名称。这些逻辑卷是在卷组内创建的。

     为了保持一致性，我们建议使用这些卷名称，但您也可以根据需要指定自定义名称。
   - [[volume size]] 卷的大小。我们建议为管理服务器数据和数据库分配至少 500 GB 的空间。存储应答文件的卷只需要少量空间。

2. 创建用作逻辑卷挂载点的目录。

   - 对于管理服务器数据和数据库：

     ```
     mkdir -p /mnt/KlFocDataShare_klfoc
     ```

   - 对于响应文件：

     ```
     mkdir -p /mnt/KlFocStateShare_klfoc
     ```

   为了保持一致性，我们建议使用 [[/mnt/KlFocDataShare_klfoc]] 和 [[/mnt/KlFocStateShare_klfoc]] 目录，不过如果需要，您可以指定自定义名称。

集群节点的文件系统已准备就绪。之后，您需要配置复制集群文件系统。

## 配置复制集群文件系统

安装和配置 DRBD

*DRBD* 是用于数据复制的第三方软件（专门用于上一步中准备的数据卷和挂载点）。

准备好集群节点的文件系统后，您必须安装 DRBD 实用程序并配置 DRBD 资源，以便在集群节点之间进行数据复制。在两个集群节点上执行以下步骤。

*在集群节点上安装和配置 DRBD：*

1. 按如下方式安装 DRBD 实用程序：

   a. 在两个节点上都启用 EPEL 和 ELRepo 存储库：

   ```
   dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
   dnf install https://www.elrepo.org/elrepo-release-9.el9.elrepo.noarch.rpm
   ```

   b. 输出所有可用的 kmod-drbd9x 软件包版本，并筛选为 el9_6 平台构建的软件包列表（例如，使用 Platform V SberLinux OS Server (SLO) 9.6）：

   ```
   dnf search --showduplicates kmod-drbd9x | grep el9_6
   ```

   c. 在两个节点上都安装列表中的最新可用版本。Platform V SberLinux OS Server (SLO) 9.6 的示例：

   ```
   dnf install kmod-drbd9x-9.2.14-1.el9_6.elrepo.x86_64
   dnf install drbd drbd-utils drbd-udev drbd-pacemaker drbd-selinux
   modprobe drbd
   ```

   如果将来出现更新的版本，请相应地替换版本字符串。

   我们建议使用 DRBD 9.2.6 或更高版本，因为它提供内置的流量加密功能。
   DRBD 流量也可以使用您自己的 VPN 解决方案进行加密。

2. 为文件系统准备期间创建的每个逻辑卷创建 DRBD 资源配置文件（`klfocdata` 和 `klfocstate`）。
   所有配置文件必须放置在 [[/etc/drbd.d/]] 中。

   - 资源 `klfocdata`（管理服务器数据和数据库）
     对 klfocdata 资源使用异步复制（协议 A）。根据您的环境配置所有其他参数。
     **配置文件示例**

     ```
     resource klfocdata {
         protocol A;
         net {
             after-sb-0pri    discard-least-changes;
             after-sb-1pri    call-pri-lost-after-sb;
             after-sb-2pri    call-pri-lost-after-sb;
         }
         syncer {
             rate 110M;
         }
         # Hostname of the active node
         on db1 {
             device    /dev/drbd0;
             disk      /dev/<volume group name>/klfocdata;
             address   <disk IP address>;
             meta-disk internal;
         }
         # Hostname of the passive node
         on db2 {
             device    /dev/drbd0;
             disk      /dev/<volume group name>/klfocdata;
             address   <disk IP address>;
             meta-disk internal;
         }
     }
     ```

   - 资源 `klfocstate`（应答文件）

使用同步复制（协议 C）创建 klfocstate 资源。根据您的环境配置所有其他参数。

**配置文件示例**

```
resource klfocstate {
    protocol C;
    net {
        after-sb-0pri    discard-least-changes;
        after-sb-1pri    call-pri-lost-after-sb;
        after-sb-2pri    call-pri-lost-after-sb;
    }
    syncer {
        rate 110M;
    }
    # Hostname of the active node
    on db1 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
    # Hostname of the passive node
    on db2 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
}
```

3. 初始化两个资源的 DRBD 元数据：

```
drbdadm create-md klfocdata
drbdadm create-md klfocstate
```

4. 启动所有已配置资源上的 DRBD：

```
drbdadm up all
```

DRBD 已在两个集群节点上安装和配置。

在主动集群节点上创建复制文件系统

在两个集群节点上都安装和配置 DRBD 后，在主动集群节点上创建复制文件系统。在主动集群节点上执行以下步骤。

*要在主动集群节点上创建复制文件系统：*

1. 将两个 DRBD 资源提升为主角色：

```
drbdadm primary --force klfocdata
drbdadm primary --force klfocstate
```

2. 格式化 DRBD 设备，以便为集群节点上的复制卷做好准备：

```
mkfs.ext4 /dev/drbd0
mkfs.ext4 /dev/drbd2
```

3. 配置文件系统参数：

```
tune2fs -m 0 /dev/drbd0
tune2fs -m 0 /dev/drbd2
```

4. 将 DRBD 设备挂载到之前创建的目录：

```
mount -o noatime /dev/drbd0 /mnt/KlFocDataShare_klfoc
mount -o noatime /dev/drbd2 /mnt/KlFocStateShare_klfoc
```

如果安装了 multipathd 服务，则必须将其配置为在两个集群节点上都忽略设备[[/dev/drbd*]]。

5. 验证复制状态：

```
drbdadm status
```

正确的文件系统配置输出：

```
klfocdata role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate
klfocstate role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate
```

主动集群节点上的复制文件系统已配置。之后，您必须在集群节点上安装并配置 Corosync 和 Pacemaker。

## 在集群节点上安装和配置 Corosync 和 Pacemaker

Corosync 和 Pacemaker 提供集群通讯和资源管理，以实现高可用性。它们确保在发生故障时服务自动迁移到健康的节点，从而最大限度地减少停机时间。

*在集群节点上安装和配置 Corosync 和 Pacemaker：*

1. 在两个集群节点上，安装所需的软件包：

```
dnf install pcs
dnf install drbd-pacemaker
```

2. 根据官方文档，在两个集群节点上配置 Corosync 和 Pacemaker。 。这包括启用自动启动、生成和分发身份验证密钥以及配置 authkey 文件的访问权限。

为确保设置正确，请在集群节点之一上运行以下命令：

```
crm status
```

预期输出应显示集群状态并列出所有活动节点，以确认 Corosync 正在正常运行且节点之间正在通讯。

3. 在两个集群节点上，配置 Pacemaker 集群的基本设置：

```
pcs property set stonith-enabled=false
pcs property set symmetric-cluster=false
pcs resource defaults resource-stickiness=110
pcs resource defaults migration-threshold=3
pcs property set no-quorum-policy=ignore
```

4. 在两个集群节点上，禁用由 Corosync 管理的脚本的启动：

```
systemctl disable drbd.service
```

5. 在集群节点之一上，在 Pacemaker 中创建基于 DRBD 的资源。

- klfocdata 的 DRBD 资源

  a. 为 DRBD 卷 `klfocdata` 创建集群资源，使集群能够自动管理其状态并监控其健康状况：

  ```
  pcs resource create drbd_klfocdata ocf:linbit:drbd \
  drbd_resource="klfocdata" \
  op monitor interval=60s \
  op start interval=0 timeout=240s \
  op stop interval=0 timeout=240s \
  op monitor role=Master interval=10s \
  op monitor role=Slave interval=30s \
  ```

  b. 基于已创建的资源 [[drbd_klfocdata]] 创建集群管理资源 [[ms_drbd_klfocdata]]：

  ```
  pcs resource clone drbd_klfocdata promotable=true
  master-max=1
  clone-max=2
  clone-node-max=1 notify=true
  ```

  c. 为 DRBD 卷 [[fs_klfocdata]] 创建挂载点，指定设备、目标目录、文件系统类型和挂载选项：

  ```
  pcs resource create fs_klfocdata ocf:heartbeat:Filesystem \
  device="/dev/drbd0" \
  directory="/mnt/KlFocDataShare_klfoc" \
  fstype="ext4" \
  options="data=journal"
  ```

- klfocstate 的 DRBD 资源

  a. 为 DRBD 卷 `klfocstate` 创建集群资源，使集群能够自动管理其状态并监控其健康状况：

  ```
  pcs resource create drbd_klfocstate ocf:linbit:drbd \
  drbd_resource=klfocstate \
  op monitor interval=60s \
  op start interval=0 timeout=240s \
  op stop interval=0 timeout=240s \
  op monitor role=Promoted interval=10s \
  op monitor role=Unpromoted interval=30s \
  ```

b. 基于已创建的资源 [[drbd_klfocstate]] 创建集群管理资源 ms_drbd_klfocstate：

```
pcs resource clone drbd_klfocstate promotable=true \
master-max=1 \
clone-max=2 \
clone-node-max=1 \
notify=true
```

c. 为 DRBD 卷 [[fs_klfocstate]] 创建挂载点，指定设备、目标目录、文件系统类型和挂载选项：

```
pcs resource create fs_klfocstate ocf:heartbeat:Filesystem \
device="/dev/drbd2" \
directory="/mnt/KlFocStateShare_klfoc" \
fstype="ext4" \
options="noatime"
```

6. 在两个集群节点上，禁用 DRBD 服务的自动启动：

```
systemctl disable drbd.service
```

Corosync 和 Pacemaker 已在集群节点上安装和配置。之后，您必须安装 DBMS并创建管理服务器数据库和 IAM 数据库。

## 安装和配置 Platform V Pangolin 数据库管理系统

在集群节点上安装和配置 Corosync 和 Pacemaker 后，您必须在两个集群节点上都安装 DBMS。

*安装和配置 DBMS：*

1. 在两个集群节点上，安装 Platform V Pangolin 6.5.1 x64 或更高版本。

   对于如何安装 Platform V Pangolin 的信息，请参考其文档。

2. 确保安装了 DBMS 的集群节点上不存在以下名称的 DBMS 用户账户：

   - client
   - iam
   - ksc
   - locker
   - pat
   - scope
   - voltron

3. 在主动集群节点上，将 DBMS 目录复制到`/mnt/KlFocDataShare_klfoc/dbms`目录：

```
sudo rsync -av  /pgdata/06/data/ /mnt/KlFocDataShare_klfoc/dbms
sudo mv /pgdata/06/data/ /pgdata/06/data.bk/
```

4. 在两个集群节点上，打开配置文件`/mnt/KlFocDataShare_klfoc/dbms/postgresql.conf`，然后设置目录`/mnt/KlFocDataShare_klfoc/dbms`作为数据库数据目录。

   此外，指定配置文件路径（`/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf`和`/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf`），并移除`include_dir`参数：

```
data_directory = '/mnt/KlFocDataShare_klfoc/dbms'
hba_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf'
ident_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf'
listen_addresses = '*'
```

5. 创建数据库管理系统服务资源：

```
pcs resource create klfocsvc_dbms pgsql \
pgctl="/usr/pangolin-6.5/bin/pg_ctl"  psql="/usr/bin/psql" pgdata="/mnt/KlFocDataShare_klfoc/dbms"
config="/mnt/KlFocDataShare_klfoc/dbms/postgresql.conf" socketdir="/tmp" \
op start timeout=60s interval=0s \
op stop timeout=60s interval=0s \
op monitor interval=30s timeout=60s \
op promote timeout=120s interval=0s \
op demote timeout=120s interval=0s \
meta target-role=Started
```

6. 在两个集群节点上，禁用 DBMS 服务的自动启动：

```
sudo systemctl disable pangolin.service
```

7. 添加数据库管理系统资源`klfocsvc_dbms`到`group_klfoc`集群组：

```
pcs resource group add group_klfoc klfocsvc_dbms
```

8. 在列表末尾追加 DBMS 资源名称`klfocsvc_dbms`，例如：

```
group klfoc_group {
...
klfocsvc_dbms
}
```

9. 在主动集群节点上，为 IAM 创建一个数据库。数据库名称必须与您为使用 Kaspersky Security Center Linux 而安装的数据库名称不同。卸载或将服务器移动到其他设备时，管理服务器不会自动删除 IAM 数据库，您必须手动删除数据库。

```
sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
```

数据库管理系统已安装并配置。管理服务器数据库和 IAM 数据库已创建。之后，您需要在集群节点上安装 Kaspersky Security Center Linux。

## 在地理分布式故障转移集群节点上安装 Kaspersky Security Center Linux

Kaspersky Security Center Linux 通过使用应答文件以静默模式安装在地理分布式集群节点上，也就是说，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。

先决条件：

- 完成所有准备步骤：
  - 准备集群节点的文件系统
  - 配置复制集群文件系统
  - 在集群节点上安装和配置 Corosync 和 Pacemaker
  - 安装和配置 Platform V Pangolin 数据库管理系统
- 确保集群节点运行 Platform V SberLinux 操作系统服务器 (SLO) 9.5.1 x64。
- 从卡巴斯基网站下载安装文件 [[ksc64_[version_number]_amd64.deb]]。

在活动节点上安装

*在活动节点上以静默模式安装 Kaspersky Security Center Linux：*

1. 阅读最终用户授权许可协议。只有在您理解并接受最终用户授权许可协议的条款后，才执行下面的步骤。
2. 创建组“`kladmins`”和非特权账户“`ksc`”与'`ksciam`'，这些账户必须是“`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
adduser ksciam
gpasswd -a ksciam kladmins
usermod -g kladmins ksciam
```

3. 在目录 [[/mnt/KlFocDataShare_klfoc/]] 中创建一个目录，用于存放 Kaspersky Security Center Linux 文件：

```
mkdir /mnt/KlFocDataShare_klfoc/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。

   在用于 Kaspersky Security Center Linux 静默模式安装的参数列表中，指定地理分布式集群部署所需的以下参数：

   - `KLFOC_UNATT_EXT_RESOURCE_MANAGEMENT=2`

     设置值 [[2]] 以部署地理分布式集群。

   - `KLSRV_UNATT_SERVERADDRESS=<DNS balancer address>`和`KLSRV_UNATT_IAM_ADDRESS=<DNS balancer address>`

     必须已部署带有健康检查功能的 DNS 均衡器。这些参数的值必须相同，并且设置为 DNS 均衡器的 FQDN。

5. 用以下命令在包含应答文件全称（例如，包括路径）的根或用户环境中设置 `KLAUTOANSWERS` 环境变量的值：

```
export KLAUTOANSWERS=/tmp/ksc_install/answers.txt
```

6. 运行以下命令以静默模式启动 Kaspersky Security Center Linux 安装：

   - 在根环境中：

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

   - 在用户环境中：

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

7. 禁用 klfocsvc_klfoc.service 服务的自动启动：

   ```
   systemctl disable klfocsvc_klfoc.service
   ```

8. Kaspersky Security Center Linux 安装完成后，停止主动集群节点。

9. 将所有集群资源迁移到被动节点。
   您可以使用命令`pcs node standby`（并使用`pcs node online`把它带回来）。

在被动节点上安装

*在被动节点上安装 Kaspersky Security Center Linux：*

1. 运行 Kaspersky Security Center Linux 安装：

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

2. 运行 Kaspersky Security Center Linux 配置：

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

3. 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：

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

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

4. 选择被动集群节点作为管理服务器安装模式。

5. 出现提示时，输入状态共享挂载点的本地路径：`/mnt/KlFocStateShare_klfoc`。

6. 禁用 klfocsvc_klfoc.service 服务的自动启动：

   ```
   systemctl disable klfocsvc_klfoc.service
   ```

7. 创建`klfocsvc_klfoc`服务资源：

```
crm configure primitive klfocsvc_klfoc systemd:klfocsvc_klfoc \
op start timeout="900s" interval="0" \
op stop timeout="900s" interval="0" \
op monitor interval="30s" timeout="90s"
```

8. 添加`klfocsvc_klfoc`资源到`group_klfoc`组：

```
pcs resource group add group_klfoc klfocsvc_klfoc
```

9. 在组行末尾追加[[klfocsvc_klfoc]]，例如：

```
group klfoc_group {
...
klfocsvc_klfoc
}
```

10. 验证活动节点上的所有资源是否都处于启动状态。

```
pcs status
```

配置集群节点之间的加密

*要配置集群节点之间的加密，*

如果您在配置复制集群文件系统期间安装了 DRBD 版本 9.2.6 或更高版本，请根据 DRBD 官方文档配置集群节点之间的加密。

或者，您可以使用自己的 VPN 解决方案对集群节点之间的流量进行加密。

地理分布式 Kaspersky Security Center Linux 故障转移集群已安装。之后，您必须在两个集群节点上都安装 Kaspersky Security Center Web Console 。

## 在地理分布式故障转移集群节点上安装 Kaspersky Security Center Web Console

对于地理分布式 Kaspersky Security Center Linux 故障转移集群部署，必须支持 Kaspersky Security Center Web Console 高可用性。要实现这一点，必须在两个集群节点上都安装 Kaspersky Security Center Web Console 。

*要安装 Kaspersky Security Center Web Console：*

1. 在两个节点上都创建一个使用 Kaspersky Security Center Web Console 的用户。为此，请在具有 root 权限的账户下运行以下命令：

```
/opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <password>
```

其中，密码必须至少包含 8 个字符。

2. 在两个节点上，阅读最终用户授权许可协议 (EULA)。如果 Kaspersky Security Center Linux 分发包不包含带有 EULA 文本的 TXT 文件，您可以从 卡巴斯基网站 下载文件。如果您不接受授权许可协议的条款，不要安装应用程序。

3. 在两个节点上，创建包含用于将 Kaspersky Security Center Web Console 连接到管理服务器的参数的响应文件：`/etc/ksc-web-console-setup.json`。

**包含最小参数集的响应文件示例**

响应文件的参数集取决于 Kaspersky Security Center Web Console 连接的管理服务器的版本：

- 16 或更高版本的管理服务器

  登录管理服务器版本 16 或更高版本所需的最小参数集的响应文件示例：

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
        "Administration Server v16": {
            "iamHost": "ksc16.example.com",
            "iamOAuthPort": 4444,
            "iamProxyPort": 9050,
            "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
            "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
            "kscPort": 13299,
            "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

- 15.4 或更早版本的管理服务器

  登录管理服务器版本 15.4 或更早版本所需的最小参数集的响应文件示例：

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

您可以将 Kaspersky Security Center Web Console 安装在与管理服务器相同或不同的设备上。如果将 Kaspersky Security Center Web Console 安装在不同的设备上，则 Kaspersky Security Center Web Console 地址（由 `address` 指定）和管理服务器地址（由 `iamHost` 或 `kscHost` 指定）不同。如果将 Kaspersky Security Center Web Console 与管理服务器安装在同一设备上，则这些参数具有相同的值。

`iamHost`值必须与您在安装管理服务器时指定的 IAM 地址匹配。若要获取指定的 IAM 地址，请在安装了管理服务器的设备上运行以下命令：

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

有关详细信息，请参阅文章：Kaspersky Security Center Web Console 安装参数。

您可以将多个不同版本的管理服务器添加到受信任服务器列表中。在此情况下，服务器可以使用不同的身分验证方法。

我们建议您指定 1024 以上的端口号。如果您希望 Kaspersky Security Center Web Console 在 1024 以下的端口上运行，安装后必须确保已获取 setcap 实用程序，然后运行以下命令：

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

如果您没有 setcap 实用程序，则可以安装该实用程序。**单击此链接查看命令。**

对于 Debian 和 Ubuntu 操作系统，运行以下命令之一：

- `sudo apt-get install libcap2-bin`
- `sudo apt install libcap2-bin`

对于 SUSE Linux Enterprise Server 和 Red Hat Enterprise Linux，请运行以下命令：

- `sudo zypper install libcap-progs`

4. 在两个节点上，使用具有 root 权限的账户运行安装文件。

```
sudo apt-get install ksc-web-console-<build number>.x86_64.deb
```

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

5. 在集群节点之一上，为 KSCWebConsole 服务创建一个 Pacemaker 资源，使 KSCWebConsole 成为 Pacemaker 管理的服务：

```
crm configure primitive ksc_webconsole systemd:KSCWebConsole \
op monitor interval=30s timeout=60s \
op start timeout=120s \
op stop timeout=120s \
meta target-role=Stopped
```

6. 在两个节点上，停止 KSCWebConsole 服务并禁用其自动启动：

```
sudo systemctl stop KSCWebConsole
sudo systemctl disable KSCWebConsole
```

7. 在一个集群节点上，添加`ksc_webconsole`资源到`group_klfoc`组：

```
crm configure edit klfoc_group
```

8. 在组行末尾追加`ksc_webconsole`，在`klfocsvc_dbms`之后，例如：

```
group klfoc_group {
...
klfocsvc_dbms
ksc_webconsole
}
```

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

# 使用 DBMS 的账户

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

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

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

请勿手动更改管理服务器数据库和 IAM 数据库，包括修改值、删除或添加架构、表和索引。任何非由管理服务器自身执行的数据库更改都会立即或稍后（例如，升级到新版本后或从备份副本还原时）中断管理服务器的正常运行。只有在收到卡巴斯基技术支持的明确指示后，才允许编辑数据库。

下表包含有关在安装和启动管理服务器之前应授予账户的 DBMS 权限的信息。

## MySQL 和 MariaDB

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

- 架构权限：
  - 管理服务器数据库：ALL（不包括 GRANT OPTION）。
  - 系统方案（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。

有关如何将数据从共享表空间移动到每表一个文件表空间的详细信息，请参阅在 MySQL 和 MariaDB DBMS 中将数据从共享表空间移动到每表一个文件表空间。

### 配置管理服务器数据恢复的权限

您授予内部 DBMS 账户的权限足以从备份中恢复管理服务器数据。

## PostgreSQL 或 Postgres Pro

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

Postgres 角色的权限

| 自动创建数据库 | | 手动创建数据库 |
|---|---|---|
| *Postgres* 用户不需要额外权限。 | 新角色的权限：CREATEDB。 | 对于新角色：<br>• 针对管理服务器数据库的权限：ALL。<br>• 针对公共架构中所有表的权限：ALL。<br>• 针对公共架构中所有序列的权限：ALL。 |

当使用 Postgres 高可用性集群（版本 14 或更高版本）作为数据库时，数据库用户必须具有`pg_read_all_stats`权限。您可以通过运行以下命令授予此权限：

```
GRANT pg_read_all_stats TO "%1";
```

其中`%1`是数据库用户的名称。

用户名在管理服务器安装程序期间在`KLSRV_UNATT_DBMS_LOGIN`参数中指定。

### 配置管理服务器数据恢复的权限

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

# 配置使用 MySQL 和 MariaDB 的 DBMS 账户

先决条件

在为 DBMS 账户分配权限之前，请执行以下操作：

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

请勿手动更改管理服务器数据库和 IAM 数据库，包括修改值、删除或添加架构、表和索引。任何非由管理服务器自身执行的数据库更改都会立即或稍后（例如，升级到新版本后或从备份副本还原时）中断管理服务器的正常运行。只有在收到卡巴斯基技术支持的明确指示后，才允许编辑数据库。

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 kscdbadmin 的用户并为 kscdbadmin 指定密码 */
   CREATE USER 'kscdbadmin' IDENTIFIED BY '<密码>';
   ```

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 kscdbadmin */
   GRANT USAGE ON *.* TO 'kscdbadmin';
   GRANT ALL ON kav.* TO 'kscdbadmin';
   GRANT SELECT, SHOW VIEW ON mysql.* TO 'kscdbadmin';
   ```

```
GRANT SELECT, SHOW VIEW ON sys.* TO 'kscdbadmin';
GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'kscdbadmin';
GRANT PROCESS ON *.* TO 'kscdbadmin';
GRANT SUPER ON *.* TO 'kscdbadmin';
```

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，请从脚本中排除以下命令：`GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'kscdbadmin'`。

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 'kscdbadmin';
```

5. 为 IAM 创建一个 DBMS 账户。执行以下命令：

```
/* 创建一个名为 iamdbadmin 的用户并为 iamdbadmin 指定密码 */
CREATE USER 'iamdbadmin' 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 'iamdbadmin'@'%' IDENTIFIED WITH mysql_native_password BY '< 密码 >';
  ```

- 要更改现有 DBMS 账户的身份验证，执行以下命令：

  ```
  ALTER USER 'iamdbadmin'@'%' IDENTIFIED WITH mysql_native_password BY '< 密码 >';
  ```

6. 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：

```
/* 授予权限给 iamdbadmin */
GRANT USAGE ON *.* TO 'iamdbadmin';
GRANT ALL ON iamdb.* TO 'iamdbadmin';
GRANT SELECT, SHOW VIEW ON mysql.* TO 'iamdbadmin';
GRANT SELECT, SHOW VIEW ON sys.* TO 'iamdbadmin';
GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'iamdbadmin';
GRANT PROCESS ON *.* TO 'iamdbadmin';
GRANT SUPER ON *.* TO 'iamdbadmin';
```

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，请从脚本中排除以下命令：`GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'iamdbadmin'`。

7. 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 'iamdbadmin';
```

8. 要手动创建管理服务器数据库，请执行以下命令（在此命令中，管理服务器数据库名称为*kav*）：

   ```
   CREATE DATABASE kav
   ```

   使用您在创建 DBMS 账户的脚本中指定的相同数据库名称。

9. 要手动创建 IAM 数据库，请运行以下脚本（在此命令中，IAM 数据库名称为*iam*）：

   ```
   CREATE DATABASE iam
   ```

   卸载或将服务器移动到其他设备时，管理服务器不会自动删除 IAM 数据库，您必须手动删除数据库。

10. 安装管理服务器。

安装完成后，将创建管理服务器数据库，管理服务器进入就绪状态。

# 配置使用 PostgreSQL 和 Postgres Pro 的 DBMS 账户

先决条件

在为 DBMS 账户分配权限之前，请执行以下操作：

1. 确保您以本地管理员账户登录系统。
2. 安装 PostgreSQL 和 Postgres Pro 的使用环境。
3. 配置与 Kaspersky Security Center Linux 配合使用的 PostgreSQL 或 Postgres Pro 服务器。

请勿手动更改管理服务器数据库和 IAM 数据库，包括修改值、删除或添加架构、表和索引。任何非由管理服务器自身执行的数据库更改都会立即或稍后（例如，升级到新版本后或从备份副本还原时）中断管理服务器的正常运行。只有在收到卡巴斯基技术支持的明确指示后，才允许编辑数据库。

配置要安装管理服务器的 DBMS 账户

*要配置用于安装管理服务器的 DBMS 账户：*

1. 运行 Postgres 的使用环境。
2. 使用 *Postgres*数据库中的*Postgres*登录。
3. 创建一个新的 Postgres 角色（在本例中，该角色是*kscdbadmin*）：

   ```
   CREATE USER "kscdbadmin" WITH PASSWORD '<password>';
   ```

4. 创建管理服务器数据库（在本例中，管理服务器数据库名称为 kav）：

   ```
   CREATE DATABASE "kav" ENCODING 'UTF8' OWNER "kscdbadmin";
   ```

我们建议您将按照本说明步骤 3 创建的 Postgres 角色指定为数据库所有者（在本例中，该角色为 *kscdbadmin*）。

**指定其他用户为数据库所有者**

如果需要指定另一个 Postgres 角色，请以该所有者（或超级用户）角色连接到数据库，并运行以下命令：

```
GRANT ALL PRIVILEGES ON DATABASE "kav" TO "kscdbadmin";
GRANT USAGE ON SCHEMA public TO "kscdbadmin";
GRANT CREATE ON SCHEMA public TO "kscdbadmin";
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "kscdbadmin";
GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "kscdbadmin";
```

确保数据库所有者角色拥有 CONNECT 和 TEMPORARY 权限。

如果出现错误 "New encoding (UTF8) is incompatible with the encoding of the template database"，请使用以下命令创建数据库：
`CREATE DATABASE "kav" ENCODING 'UTF8' OWNER "kscdbadmin" TEMPLATE template0;`
而不是：
`CREATE DATABASE "kav" ENCODING 'UTF8' OWNER "kscdbadmin";`

5. 为 IAM 创建一个新的 Postgres 角色（在本例中，Postgres 角色是 `iamdbadmin`）：

```
CREATE USER "iamdbadmin" WITH PASSWORD '<password>';
```

6. 创建一个 IAM 数据库（在本例中，IAM 数据库名称是 `iam`）：

```
CREATE DATABASE "iam" ENCODING 'UTF8' OWNER "iamdbadmin";
```

我们建议您将按照本说明步骤 5 创建的 Postgres 角色指定为数据库所有者（在本例中，该角色为 *iamdbadmin*）。

**指定其他用户为 IAM 数据库所有者**

如果需要指定另一个 Postgres 角色，请以该所有者（或超级用户）角色连接到数据库，并运行以下命令：

```
GRANT ALL PRIVILEGES ON DATABASE "iam" TO "iamdbadmin";
GRANT USAGE ON SCHEMA public TO "iamdbadmin";
GRANT CREATE ON SCHEMA public TO "iamdbadmin";
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "iamdbadmin";
GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "iamdbadmin";
```

确保数据库所有者角色拥有 CONNECT 和 TEMPORARY 权限。

如果出现错误“新编码 (UTF8) 与模板数据库的编码不兼容”，请使用以下命令创建数据库：
`CREATE DATABASE "iam" ENCODING 'UTF8' OWNER "iamdbadmin" TEMPLATE template0;`
而不是：
`CREATE DATABASE "iam" ENCODING 'UTF8' OWNER "iamdbadmin";`

卸载或将服务器移动到其他设备时，管理服务器不会自动删除 IAM 数据库，您必须手动删除数据库。

7. 安装管理服务器。

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

# 在 MySQL 或 MariaDB DBMS 中将数据从共享表空间移动到每个表一个文件的表空间

对于 MySQL 和 MariaDB DBMS，您可以通过以下方式存储数据：

- 作为共享表空间，当所有用户数据库的数据存储在单个文件中（通常在`ibdata1`文件中）时。
- 作为每个表一个文件的表空间，为每个表创建一个单独的数据空间作为单独的文件。

使用共享表空间会增加表空间碎片的风险。由于无法执行`SHRINK`操作，共享表空间中的文件可能会占用大约 90% 的磁盘空间。这会对磁盘子系统的性能产生负面影响。因此，选择每个表一个文件的表空间很有用。

本文介绍如何将数据从共享表空间移动到每个表一个文件的表空间。如果其他应用程序也使用 MySQL 或 MariaDB DBMS，则必须将这些应用程序的数据库移动到每个表独享文件的表空间。

> 仅当您将 MySQL 或 MariaDB DBMS 用于管理服务器时，才建议执行此过程。
> 将数据从共享表空间移动到每个表一个文件的表空间可能会增加磁盘子系统的负载。

## 先决条件

在开始之前，请确保：

- 您通过运行数据备份任务或klbackup 实用程序创建了管理服务器数据的备份副本。
- 您创建了其他应用程序的备份副本，这些应用程序的数据库由 MySQL 或 MariaDB DBMS（如有）管理。
- 在安装了 DBMS 的设备上，在带有数据库的分区中，有一个可用磁盘空间。

所需磁盘空间是当前数据库总大小（`ibdata1`文件的当前大小）的 150%。

## 过程

*要将数据从共享表空间移动到每个表一个文件的表空间：*

1. 停止 Kaspersky Security Center 管理服务器服务和其他使用您要为其执行此过程的 DBMS 实例的应用程序。
2. 根据 DBMS 版本，以超级用户身份登录到您的 DBMS，然后在任何方便的应用程序中运行 `fix_tablespace.sql` 脚本。

   您可以单击这些链接查看 `fix_tablespace.sql` 脚本：

   **查看适用于 MySQL 5.7 和 MariaDB 10.1+ 的脚本**

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
```

```
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;
    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';' );
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;
        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

**查看适用于 MySQL 8.0+ 的脚本**

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;
    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';' );
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` TABLESPACE =
innodb_file_per_table;' );
        PREPARE stmt2 FROM @`strSQL`;
        EXECUTE stmt2;
        DEALLOCATE PREPARE stmt2;
        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

您不得停止脚本执行。
如果没有发生 DBMS 错误，但您终止了脚本执行，请再次运行脚本，或者停止执行此过程的步骤，重新启动 DBMS 服务，然后从备份中恢复管理服务器数据。

3. 在 my.cnf 文件的`[mysqld]`部分中，将`innodb_file_per_table`参数设置为`1`。

4. 重新启动 MySQL 或 MariaDB 服务。

5. 启动 Kaspersky Security Center 管理服务器服务。

数据被从共享表空间移动到每个表一个文件表空间。

# 用于 Kaspersky Security Center Linux 的证书

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

## 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 Web Console 证书
- Identity and Access Manager 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。使用自定义证书时，证书文件必须包含完整的公钥链，包括所有中间证书，直至根证书颁发机构 (CA)。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 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：

- 当 Kaspersky Security Center Web Console 连接到管理服务器时对其进行身份验证。
- 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 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。

在管理服务器证书被替换为备用或自定义证书后，请在响应文件中指定新证书，然后使用此文件重新安装 Kaspersky Security Center Web Console。否则，Kaspersky Security Center Web Console 将无法连接到管理服务器。

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 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 Web Console 证书

Kaspersky Security Center 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。

Identity and Access Manager 证书

Identity and Access Manager 证书（IAM 证书）用于以下目的：

- 当用户的浏览器通过 OAuth 协议连接到管理服务器时对其进行身份验证。
- 当 Kaspersky Security Center Web Console 连接到管理服务器时对其进行身份验证。

IAM 证书在首次运行管理服务器时自动创建。证书存储在管理服务器设备的以下目录中：/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem（对于 Kaspersky Security Center 故障转移集群：<共享数据文件夹>/iam/main_certificate.pem）。在创建用于安装 Kaspersky Security Center Web Console 的响应文件时，必须使用 `iamCertPath` 参数指定 IAM 证书的路径。

IAM 证书的有效期为 365 天。Kaspersky Security Center 会在当前证书到期前 48 小时自动生成通用备用 IAM 证书。备用证书随后用于无缝替换过期的 IAM 证书。

任何 IAM 证书的最长有效期不得超过 397 天。

如有必要，您可以分配自定义 IAM 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。

在 IAM 证书被替换为备用证书或自定义证书后，请在响应文件中指定新证书，然后使用此文件重新安装 Kaspersky Security Center Web Console。否则，Kaspersky Security Center Web Console 将无法连接到管理服务器。

当您登录 Kaspersky Security Center Web Console 时，浏览器会被重定向到管理服务器登录页面（https://<管理服务器地址>:4444）进行身份验证。浏览器和管理服务器之间的流量使用 TLS 协议和 IAM 证书加密。

浏览器可能会提醒您与管理服务器的连接不是私密连接，以及 IAM 证书无效。出现此警告是因为 IAM 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 IAM 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 IAM 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 Linux 中使用的自定义证书的要求

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

| 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<br>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。<br>证书必须包含有效的“主题备用名称（SAN）”，其中包含管理服务器的回环地址：<br>• 对于 IPv4：127.0.0.1<br>• 对于 IPv6：0:0:0:0:0:0:0:1 | 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。 |
| 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 容器包括完整的公钥链。<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 Web Console 证书 | 扩展密钥用法：服务器身份验证，客户端身份验证。<br>从中指定证书的 PEM 容器包括完整的公钥链。<br>证书的使用者可选名称 (SAN) 存在；即， `subjectAltName` 字段的值有效。该值必须与安装管理服务器时指定的 IAM 地址匹配。若要获取指定的 IAM 地址，请在管理服务器主机上运行以下命令：<br>`grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml`<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 Web Console 不支持加密证书。 |
| Identity and Access Manager 证书（IAM 证书） | 扩展密钥用法：服务器身份验证。<br>从中指定证书的 PEM 容器包括完整的公钥链。<br>证书必须有效并支持客户端身份验证。<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 Web Console 不支持加密证书。 |

# 重新颁发 Kaspersky Security Center 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 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 Web Console 证书。

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

打开 Kaspersky Security Center Web Console 时，浏览器会通知您与 Kaspersky Security Center Web Console 连接不是私有，并且 Kaspersky Security Center 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 Linux 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 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 Web Console 证书：*

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

- 如果要使用相同的 Kaspersky Security Center Web Console 安装文件，请删除 Kaspersky Security Center Web Console，然后安装相同的 Kaspersky Security Center 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 Web Console 证书的有效期将增加 397 天。

## 替换 Kaspersky Security Center Web Console 证书

默认下，当您安装 Kaspersky Security Center Web Console Server（也叫 Kaspersky Security Center 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 Web Console 的证书：*

1. 打开安装 Kaspersky Security Center Web Console 时创建的响应文件。
   如果您想，您可以创建新的响应文件。
2. 在该文件中，指定以下路径：
   - 使用`certPath`参数访问 Kaspersky Security Center Web Console 自定义证书文件
   - 使用`keyPath`参数访问与 Kaspersky Security Center Web Console 自定义证书关联的私钥。

   > 您必须指定这两条路径。否则，Web 浏览器会不断通知您您的连接不是私密的。
3. 通过指定新响应文件来重新安装 Kaspersky Security Center Web Console。执行以下操作之一：
   - 如果要使用相同的 Kaspersky Security Center Web Console 安装文件，请删除 Kaspersky Security Center Web Console，然后安装相同的 Kaspersky Security Center 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 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 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 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 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

以下条件必须得到满足：

- 新证书必须以 PKCS#12 格式创建（例如，通过组织的 PKI）。
- 对于新证书，必须满足下表中列出的要求。

  在下表中，请注意要求“CA: true”，这意味着新证书必须由受信任的证书颁发机构（CA）颁发。具有要求"CA: true"的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。

管理服务器证书的要求

| 证书类别 | 要求 |
| --- | --- |
| 普通证书，普通备用证书（“C”，“CR”） | 最小密钥长度：2048<br>基本限制：<br>• 路径长度限制：无<br>路径长度约束值可以是不同于“无”的整数，但不能小于 1。<br>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 (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。<br>证书必须包含有效的“主题备用名称（SAN）”，其中包含管理服务器的回环地址：<br>• 对于 IPv4：127.0.0.1<br>• 对于 IPv6：0:0:0:0:0:0:0:1 |

| 证书类别 | 要求 |
| --- | --- |
| 移动证书，移动备用证书（“M”，“MR”） | 最小密钥长度：2048<br>基本限制：<br>• CA：true<br>• 路径长度限制：无<br>如果通用证书的路径长度限制值不小于 1，则路径长度限制值可能是不同于“无”的整数。<br>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 (EKU)：服务器身份验证。EKU 可选，但如果您的证书包含它，则必须在 EKU 中指定服务器身份验证数据。 |
| 自动生成的用户证书的证书 CA（“MCA”） | 最小密钥长度：2048<br>基本限制：<br>• CA：true<br>• 路径长度限制：无<br>如果普通证书的路径长度限制值不小于 1，则路径长度限制值可能是不同于“无”的整数。<br>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 (EKU)：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。

3. **在 Kaspersky Security Center Web Console 的设置中指定新证书**

   替换证书后，请在响应文件中指定该证书，然后使用此文件更新 Kaspersky Security Center Web Console。否则，Kaspersky Security Center Web Console 将无法连接到管理服务器。

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

为避免失去对设备的控制，请参阅场景：在继续操作之前指定自定义管理服务器证书。

*要替换管理服务器证书：*

从命令提示符运行以下实用程序：

```
/opt/kaspersky/ksc64/sbin/klsetsrvcert [-t <certificate type> {-i <path to new certificate> [-p <password>] [-o <validation parameters>] | -g <dns name>}][-f <replacement time>][-r <root certificates>][-l <log file path>]
```

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 | 值 |
| --- | --- |
| -t < 证书类型 > | 要替换的证书类型。< 证书类型 > 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 < 更换时间 > | 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 < 新证书路径 > | 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 < 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 > | 系统将为指定的 DNS 名称（通用名称和主题备用名称）创建一个新证书。 |
| -r < 根证书 > | 受信任的根证书颁发机构列表，格式 PEM。 |
| -l < 日志文件路径 > | 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 <新证书路径> -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 <新证书路径> -p <密码> -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。

问答

**替换管理服务器通用证书后还需要哪些其他步骤?**

1. 确保**满足自定义证书的要求**。

   如果您使用的是自定义证书而不是自签名证书，则在将 Kaspersky Security Center Linux 升级到更高版本之前，必须确保证书包含主题备用名称 (SAN)。如果没有，在升级 Kaspersky Security Center Linux 之前替换证书至关重要。否则，升级后您将无法登录 Web Console。

   *要确保证书包含 SAN：*

   1. 在安装了管理服务器的设备上，执行命令：

      - 对于 Linux 设备：

        ```
        sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
        ```

      - 对于 Windows 设备：

        ```
        certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
        ```

   2. 请确保命令输出中包含“使用者备用名称”，并且名称包含管理服务器设备的地址。

   3. 如果缺少“使用者备用名称”，请使用 klsetsrvcert 实用程序将自定义证书替换为符合要求的证书。

2. 确保 IAM 服务器配置文件包含当前管理服务器地址。如果没有，请将地址添加到配置文件中。

3. 重新安装 Web Console以避免出现以下错误：
   *管理服务器使用了不受信任的证书。请通过指定有效证书重新配置应用程序，或联系主管理员。*

# 使用 klmover 实用程序将网络代理连接到管理服务器

您可以使用 klmover 实用程序恢复不受控设备与管理服务器之间的连接（例如，在管理服务器发生故障后，如果无法从备份中恢复）。

*要恢复连接，请从命令行运行 klmover 实用程序：*

- 对于 Linux：
  - 对于 32 位系统：`/opt/kaspersky/klnagent/bin/klmover [-address <服务器地址>] [-pn <端口号>] [-ps <SSL 端口号>] [-nossl] [-cert <证书文件路径>]`
  - 对于 64 位系统：`/opt/kaspersky/klnagent64/bin/klmover [-address <服务器地址>] [-pn <端口号>] [-ps <SSL 端口号>] [-nossl] [-cert <证书文件路径>]`
- 对于 Windows：
  - 对于 32 位系统：`<路径>\klmover.exe [-address <服务器地址>] [-pn <端口号>] [-ps <SSL 端口号>] [-nossl] [-cert <证书文件路径>]`
  - 对于 64 位系统：`<路径>\klmover.exe [-address <服务器地址>] [-pn <端口号>] [-ps <SSL 端口号>] [-nossl] [-cert <证书文件路径>]`
- 对于 macOS：

  `/Library/Application Support/Kaspersky Lab/klnagent/Binaries/klmover [-address <服务器地址>] [-pn <端口号>] [-ps <SSL 端口号>] [-nossl] [-cert <证书文件路径>]`

其中<路径>是网络代理的默认安装路径或者您在网络代理安装包的设置中指定的安装路径。

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

如果您丢失或忘记了安装在不再受 Kaspersky Security Center 管理的设备上受密码保护的网络代理的密码，则无法使用 klmover 实用程序或命令行删除网络代理。在这种情况下，您必须在安装了受密码保护的网络代理的设备上重新安装操作系统。

klmover 实用程序需要本地管理员权限。

在 Windows 设备上启用**使用卸载密码**选项还会为清理工具 (cleaner.exe) 启用密码保护。

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 | 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。 |

| 参数 | 值 |
| --- | --- |
| `-cert < 证书文件路径 >` | 访问管理服务器时使用指定的证书文件作为身份验证。 |
| `-nauninstpwd < 密码 >` | 使用此参数指定网络代理卸载密码。<br>该参数不是必需的。 |

# 重新颁发 Web 服务器证书

发布后续下载到受管理设备的网络代理安装包以及发布 iOS MDM 配置文件、iOS 应用和 Kaspersky Endpoint Security for Mobile 安装包都需要在 Kaspersky Security Center Linux 中使用的 Web 服务器证书。根据当前的应用程序配置，可以使用不同的证书作为 Web 服务器证书（有关详细信息，请参阅"关于 Kaspersky Security Center Linux 证书"）。

在开始升级应用程序之前，您可能需要重新颁发 Web 服务器证书以满足您组织的特定安全要求或保持受管理设备的持续连接。Kaspersky Security Center Linux 提供了两种重新颁发 Web 服务器证书的方式；两种方法之间的选择取决于您是否通过移动协议（即，通过使用移动证书）连接和管理移动设备。

如果您从未在管理服务器属性窗口的"**Web 服务器**"部分中将您自己的自定义证书指定为 Web 服务器证书，则移动证书将用作 Web 服务器证书。在这种情况下，通过重新颁发移动协议本身来重新颁发 Web 服务器证书。

*要在已通过移动协议管理移动设备的情况下重新颁发 Web 服务器证书：*

1. 生成自定义证书，并准备好在 Kaspersky Security Center Linux 中使用。请检查您的自定义证书是否符合 Kaspersky Security Center Linux 的要求。如有必要，请修改证书。
2. 在主菜单中，单击管理服务器名称。

   管理服务器属性窗口将打开。
3. 在"**常规**"选项卡上，选择"**Web 服务器**"部分。
4. 在"**通过 HTTP**"子部分中，选择"**从文件上传证书**"选项，然后单击"**更改证书**"按钮。
5. 在打开的窗口中，在"**证书格式**"字段中选择您的证书类型：
   - 如果选择了"**PKCS #12 容器**"，则单击"**证书**"字段旁边的"**浏览**"按钮，然后指定硬盘驱动器上的证书文件。如果证书文件受密码保护，请在"**密码**"字段中输入密码。
   - 如果选择了"**X.509 证书**"，则单击"**私钥**"字段旁边的"**浏览**"按钮，然后指定硬盘驱动器上的私钥。如果私钥受密码保护，请在"**密码**"字段中输入密码。
6. 单击"**保存**"按钮，然后单击"**确定**"。

   窗口将被关闭。
7. 如有必要，在"**Web 服务器 HTTPS 端口**"字段中更改 Web 服务器的 HTTPS 端口号，然后单击"**保存**"按钮。

Web 服务器证书已重新颁发。

*要在未通过移动协议管理移动设备的情况下重新颁发 Web 服务器证书：*

1. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**证书**”部分。
3. 如果您计划继续使用 Kaspersky Security Center 颁发的证书，请执行以下操作：
   a. 选择“**通过管理服务器发布的证书**”选项，然后单击“**浏览**”按钮。
   b. 在打开的窗口中，在“**连接地址**”和“**激活条款**”设置组中选择相关选项，然后单击“**确定**”。

或者，如果您计划使用自己的自定义证书，请执行以下操作：

a. 请检查您的自定义证书是否符合Kaspersky Security Center Linux 的要求。如有必要，请修改证书。

b. 选择“**其他证书**”选项，单击“**管理证书**”按钮，然后在打开的窗口中单击“**浏览**”按钮。

c. 在打开的窗口中，在“**证书格式**”字段中选择您的证书类型：

- 如果选择了“**PKCS #12 容器**”，则单击“**证书**”字段旁边的“**浏览**”按钮，然后指定硬盘驱动器上的证书文件。如果证书文件受密码保护，请在“**密码**”字段中输入密码。
- 如果选择了“**X.509 证书**”，则单击“**私钥**”字段旁边的“**浏览**”按钮，然后指定硬盘驱动器上的私钥。如果私钥受密码保护，请在“**密码**”字段中输入密码。

d. 单击“**保存**”按钮，然后单击“**确定**”。

移动证书已重新颁发以用作 Web 服务器证书。

# 将默认 IAM 证书更改为自定义证书

*要更改默认 IAM 证书：*

1. 生成自定义证书，并准备好在 Kaspersky Security Center Linux 中使用。请检查您的自定义证书是否符合Kaspersky Security Center Linux 的要求。
2. 确保 kladmins 组有权访问 IAM 证书文件。
3. 定位 IAM 配置文件：`/var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml`
   在此文件中，将 IAM证书文件的路径添加到`server_iam`部分：
   - `certificates.main.cert`: 主证书文件的路径。
   - `certificates.main.key`: 主证书私钥的路径。私钥不得使用密码保护。
4. 定位 Web Console 配置文件：`/etc/ksc-web-console-setup.json`
   在此文件中，将 `iamCertPath` 字段值设置为主证书的公钥。
5. 通过运行以下命令重启 kliam 服务：
   ```
   sudo service kliam_srv restart
   ```

6. 重新安装 Web Console。

   重新安装后， Web Console 将使用自定义 IAM 证书。

*要更改备用 IAM 证书：*

1. 定位 IAM 配置文件： `/var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml`

   在此文件中，指定 IAM 证书文件的路径：

   - `server_iam.certificates.reserve.cert`：主证书文件的路径。
   - `server_iam.certificates.reserve.key`：主证书私钥的路径。私钥不得使用密码保护。

2. 通过运行以下命令重启 kliam 服务：

   ```
   sudo systemctl restart kliam_srv.service
   ```

   主证书文件过期后，将使用备用 IAM 证书。

## 将管理服务器地址添加到 IAM 服务器配置中

在升级、迁移或搬迁过程中更改通用管理服务器证书（“C”）后，您需要在 IAM 服务器配置文件中指定管理服务器地址，以确保 IAM 服务器和管理服务器之间进行正确的证书验证。

*要将管理服务器地址添加到 IAM 服务器配置中：*

1. 通过运行以下命令，从通用管理服务器证书（“C”）获取主题备用名称 (SAN) 值：

   ```
   sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
   ```

2. 根据命令输出，执行以下操作之一：

   - 如果输出结果显示缺少该值，请检查**自定义证书的要求**。

     如果您使用的是自定义证书而不是自签名证书，则在将 Kaspersky Security Center Linux 升级到更高版本之前，必须确保证书包含主题备用名称 (SAN)。如果没有，在升级 Kaspersky Security Center Linux 之前替换证书至关重要。否则，升级后您将无法登录 Web Console。

     *要确保证书包含 SAN：*

     1. 在安装了管理服务器的设备上，执行命令：

        - 对于 Linux 设备：

          ```
          sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
          ```

        - 对于 Windows 设备：

          ```
          certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
          ```

     2. 请确保命令输出中包含“使用者备用名称”，并且名称包含管理服务器设备的地址。

     3. 如果缺少“使用者备用名称”，请使用 klsetsrvcert 实用程序将自定义证书替换为符合要求的证书。

     如果证书不符合要求，请使用 klsetsrvcert 实用程序替换先前管理服务器上的通用管理服务器证书。之后，重复升级、迁移或搬迁过程。

- 如果该值与 Kaspersky Security Center Linux 安装期间指定的值匹配（在安装向导的“**输入 IAM 服务器 DNS 名称**”步骤中，或者对于静默安装，在`KLSRV_UNATT_IAM_ADDRESS`参数中），则不需要进一步操作。IAM 服务器和管理服务器将正确交互。

- 如果该值包含环回地址（127.0.0.1 和/或 0:0:0:0:0:0:0:1），请在配置文件中使用其中一个。建议使用 127.0.0.1。

3. 按以下格式将管理服务器通用证书中的一个 SAN 地址值添加到 IAM 服务器配置文件中的`server_iam`块中：`ksc_address: "<SAN_address>"`。

   您可以使用文本编辑器（例如 vi）修改 IAM 服务器配置文件。以下命令会在 vi 文本编辑器中打开该文件：

   ```
   vi /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
   ```

   IAM 服务器配置文件中 server_iam 块的示例：

   ```
   server_iam:
       iam_address: "ksc.example.com"
       server_display_name: "ksc.example.com"
       ksc_address: "oldksc.example.internal"
       ksc_ca: "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
   ```

   请确保使用与示例中相同的空格。

4. 检查`ksc_address`参数中的网络名称解析为管理服务器的 IP 地址。为此，您可以使用管理服务器上的 Ping 实用程序。

   如果解析出的地址不同，请确保旧的管理服务器从网络断开连接，并且不存在任何包含旧 IP 地址的 DNS 记录。如果无法解析该地址，请使用企业 DNS 中的 DNS 记录进行映射，或者在管理服务器的主机文件中添加条目。

5. 运行以下命令重启 IAM 服务器服务以应用配置更改：

   ```
   sudo systemctl restart kliam_srv.service
   ```

管理服务器地址被从管理服务器通用证书添加到 IAM 服务器配置文件。

## 故障解决

IAM 服务器上的配置问题可能会导致登录 Web Console 时出现错误。下表描述了可能的错误及其解决方法。

| 错误 | 描述 | 解决 |
| --- | --- | --- |
| 您的请求目前无法处理。请稍候然后重试。 | 除了升级或恢复 Kaspersky Security Center Linux 后的数据初始化过程之外，如果使用指定的网络地址连接到管理服务器失败，也可能出现此错误。 | 请使用 Ping 实用程序检查网络名称解析到的 IP 地址。 |
| 管理服务器使用了不受信任的证书。请通过指定有效证书重新配置应用程序，或联系主管理员。 | 如果 IAM 服务器配置文件中的地址值与管理服务器通用证书的“使用者备用名称 (SAN)”属性中的值不匹配，则可能会出现此错误。 | 请按照上述说明操作。 |
| 用户名或密码不正确。 | 除了凭证不正确之外，如果网络上存在另一个同名的管理服务器，也可能出现此错误。 | 请检查指定的地址是否解析到当前管理服务器的 IP 地址。 |

# 定义共享文件夹

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

共享文件夹在网络代理部署中偶尔使用。

共享文件夹必须禁用大小写敏感。

# 登录到 Kaspersky Security Center Web Console 并登出

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

您可以使用以下方法登录 Kaspersky Security Center Web Console：

- 通过使用域身份验证（单点登录）

  此方法用于在连接到管理服务器版本 16 及更高版本的 Kaspersky Security Center Web Console 中进行安全身份验证。如果您要使用域身份验证，必须在 Kaspersky Security Center Web Console 安装过程中，为与 Identity and Access Manager (IAM) 之间的交互指定额外参数。

- 通过指定域用户的名称和密码

  使用域用户账户登录之前，请轮询域控制器以获取域用户列表。然后，您必须指定域用户名和密码才能登录管理服务器。此方法仅支持通过 Microsoft Active Directory 进行身份验证。

- 通过指定内部用户的名称和密码

您想要用于登录 Kaspersky Security Center Web Console 的用户账户必须已分配角色。登录前，请确保域账户或内部用户账户已被分配角色。否则，将会出现登录错误。

## 通过使用域身份验证（单点登录）进行登录

*要使用域身份验证登录 Kaspersky Security Center Web Console，请执行以下操作：*

1. 在浏览器中，转到 https://< `Kaspersky Security Center Web Console` 地址>:<端口号>。

   将显示管理服务器选择页面。

2. 如果您添加若干个受信任的服务器，在管理服务器列表选择您要连接的管理服务器。

   如果您只添加了一个管理服务器，则不会显示管理服务器列表。

   浏览器将重定向到 https://<管理服务器地址>:4444。

3. 配置 Kerberos 域身份验证。

4. 执行以下操作之一：

   - 单击**使用域身份验证**按钮。
   - 如果服务器上创建了一个或多个虚拟管理服务器，并且您要使用域身份验证登录到虚拟服务器：

     a. 单击**显示虚拟服务器选项**。

     b. 输入您在创建虚拟服务器时指定的虚拟管理服务器名称。

     c. 单击**使用域身份验证**按钮。

5. 指定移动设备上的身份验证应用程序生成的一次性安全码。

   首次登录时，请为您的帐户配置双重身份验证。如果您无法配置双重身份验证，请联系在常规功能**常规功能**用户权限**用户权限修改对象**ACL权限且已配置双重身份验证的用户，将您的帐户添加到双重身份验证允许列表中。

登录后，将显示 Kaspersky Security Center Web Console 主页，其中包含您上次使用的语言和主题。您可以通过Kaspersky Security Center云控制台导航并使用其操作Kaspersky Security Center Linux。

通过指定域或内部用户的名称和密码进行登录

*要通过指定用户名和密码登录Kaspersky Security Center云控制台：*

1. 在浏览器中，转到 https://< `Kaspersky Security Center`云控制台地址>:<端口号>。

   将显示管理服务器选择页面。

2. 如果您添加若干个受信任的服务器，在管理服务器列表选择您要连接的管理服务器。

   如果您只添加了一个管理服务器，则不会显示管理服务器列表。

   浏览器将重定向到 https://<管理服务器地址>:4444。

3. 执行以下操作之一：

   - 要使用域用户账户登录管理服务器，请输入域用户的用户名和密码。

     您可以采用以下格式之一输入域用户的用户名：

     - 用户名`@dns.domain`
     - `NTDOMAIN\`用户名

     使用域用户账户登录之前，请轮询域控制器以获取域用户列表。

   - 要通过指定管理员的用户名和密码登录管理服务器，请输入内部用户的用户名和密码。

- 如果服务器上创建了一个或多个虚拟管理服务器，并且您要登录到虚拟服务器：

  a. 单击**显示虚拟服务器选项**。

  b. 输入您在创建虚拟服务器时指定的虚拟管理服务器名称。

  c. 输入拥有虚拟管理服务器权限的管理员的用户名和密码。

4. 单击**登录**按钮。

5. 指定移动设备上的身份验证应用程序生成的一次性安全码。

   首次登录时，请为您的帐户配置双重身份验证。如果您无法配置双重身份验证，请联系在常规功能**常规功能**用户权限**用户权限修改对象**ACL权限且已配置双重身份验证的用户，将您的帐户添加到双重身份验证允许列表中。

6. 如果为您的账户启用了强制更改密码或密码已过期，则会显示密码更改窗口。设置新密码以登录 Kaspersky Security Center Web Console。

登录后，将显示 Kaspersky Security Center Web Console 主页，其中包含您上次使用的语言和主题。您可以通过 Kaspersky Security Center Web Console 导航并使用其操作 Kaspersky Security Center Linux。

注销

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

在上方窗格中，单击您的账户名称以转到账户菜单，然后选择“**登出**”。

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

# Kaspersky Security Center Web Console 界面

Kaspersky Security Center Linux 通过 Kaspersky Security Center Web Console 界面进行管理。

Kaspersky Security Center Web Console 窗口包含以下项目：

- 主菜单位于窗口左侧
- 窗口上部区域中的上方窗格
- 工作区在窗口右侧

## 主菜单

主菜单包含以下部分：

- **管理服务器**。显示您当前连接到的管理服务器的名称。您可以通过单击管理服务器名称来打开管理服务器属性。
- **控制台导航**。显示主菜单地图。大部分显示的部分可以被添加到书签或设置为主页。默认**控制台导航**被设为主页。您可以更改这些设置。
- **监控**。提供基础架构、保护状态和统计信息的总览。
- **资产管理**。包含用于设备和硬件管理以及卡巴斯基应用程序政策的工具。
- **任务**。包含用于创建和运行任务的工具。
- **用户和角色**。可让您管理用户和角色，通过为用户分配角色来配置用户权限，以及将策略配置文件与角色关联。
- **存储库**。可让您访问应用程序存储库。
- **软件管理**。可让您管理卡巴斯基和第三方应用程序，以及安装包和补丁。
- **操作**。包含多种操作，包括应用程序授权许可、查看和管理加密驱动器和加密事件。
- **发现和部署**。可让您轮询网络以发现客户端设备，以及手动或自动将设备分发到管理组。这部分还包含快速启动向导和保护部署向导。
- **Marketplace**。包含有关全系列卡巴斯基业务解决方案的信息，可让您选择所需的解决方案，然后继续在卡巴斯基网站上购买这些解决方案。
- **设置**。可让您备份网页插件的当前状态，以便以后能够恢复保存的状态。包含您与界面外观相关的个人设置，例如界面语言或主题。

如有需要，可单击屏幕底部的 V 形符号 (<<)，将主菜单最小化为图标形式。

## 上方窗格

上方窗格始终显示在所有控制台区域中，且无法隐藏。

窗格左侧包含应用程序名称和徽标。如果单击应用程序名称或徽标，将打开 Kaspersky Security Center Web Console 主页。

窗格右侧显示以下内容：

- 通知图标 (🔔)。如果单击该图标，将打开一个包含通知的窗格。
- 您账户的菜单。包含指向 Kaspersky Security Center Linux 帮助的链接。您还可以退出 Kaspersky Security Center Linux，修改您自己账户的密码，并查看 Kaspersky Security Center Web Console 版本和已安装的管理 Web 插件的列表。

工作区域

工作区会显示您选择在 Kaspersky Security Center Web Console 界面窗口的各个部分中查看的信息。它还包含可用于配置信息显示方式的控制元素。

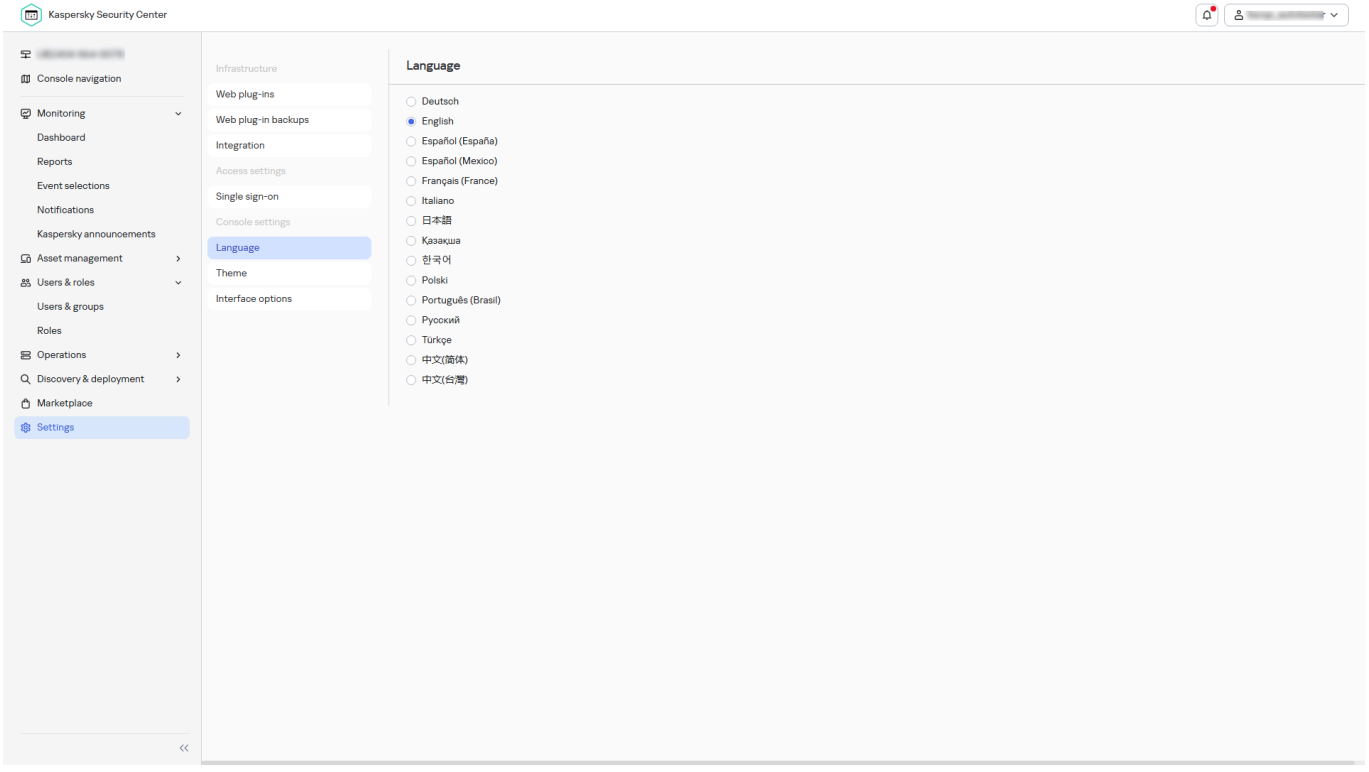
我们建议使用单个浏览器选项卡来操作 Kaspersky Security Center Web Console。

# 更改 Kaspersky Security Center Web Console 界面的语言

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

*要更改界面语言：*

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




更改 Kaspersky Security Center Web Console 界面的语言

# 更改 Kaspersky Security Center Web Console 主页

登录 Kaspersky Security Center Web Console后，主页将显示。

默认**控制台导航**部分被设为主页。如果需要的话，您可以更改主页。

*更改主页：*

1. 在**控制台导航**部分，将鼠标光标悬停在您想要设置为主页的项目上。
2. 主页 (⌂) 图标显示后，单击图标。

   主页被更改，屏幕上显示相应的消息，被选为主页的项目标记有主页 (⌂) 图标。

> **市场** 和**设置** 部分不能设置为主页。

## 添加和移除书签

您可以将频繁使用的 Kaspersky Security Center Web Console 部分添加到书签并从主菜单中的"**书签**"部分快速访问它们。

> 如果您没有向书签添加如何元素，**书签**部分将不显示在主菜单中。

您只能向书签添加显示页面的部分。例如，如果您转到**资产管理** → **资产(设备)**，一个包含设备表的页面会打开，意味着您可以将该部分添加到书签。如果在主菜单中选择该部分后显示一个窗口或者没有显示任何元素，则您无法将该部分添加到书签。

*要将一个部分添加到书签：*

1. 在主菜单中，将鼠标光标悬停在要固定的部分上。
2. 书签 (🔖) 显示后，单击图标。

   该部分显示在**书签**部分。

*要从书签移除一个部分：*

1. 在主菜单中，转到"**书签**"部分。
2. 将鼠标光标悬停在要移除的部分上，然后单击书签 (🔖) 图标。

   该部分被从书签中移除。

您也可以在"**控制台导航**"部分中通过将鼠标光标悬停在上面并单击书签 (🔖) 图标添加或将其从书签中移除。所选项将用书签 (🔖) 图标进行标记并显示在主菜单的"**书签**" 部分。如果您想将该项从书签中移除，请单击书签 (🔖) 图标。

> **书签** 部分仅显示在主菜单中。它从不显示在**控制台导航**页面上。

# 移除 Kaspersky Security Center Web Console

在以下情况下，您可能需要移除 Kaspersky Security Center Web Console 服务器（也称为Kaspersky Security Center Web Console）：

- 使用其他通用证书从备份恢复数据。
- 重新颁发管理服务器通用证书。
- 将 Web Console 证书替换为自定义证书。
- 设备上不再使用 Kaspersky Security Center Web Console。

*要移除 Kaspersky Security Center Web Console：*

1. 根据您的 Linux 发行版，执行以下命令之一：
   - `sudo dnf remove ksc-web-console`
   - `sudo apt remove ksc-web-console`
2. 执行以下命令检查结果：

   `sudo systemctl status KSC*`

   命令输出中一定没有“Kaspersky Security Center Web Console” 。

如果您想恢复 Kaspersky Security Center Web Console，请按照文章中的说明将其安装到设备上：安装 Kaspersky Security Center Web Console。

# 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。
- 设置以电子邮件通知管理服务器和受管理应用程序运行期间发生的事件。
- 为工作站和服务器创建保护策略，以及为受管理设备的顶级层级创建恶意软件扫描任务、更新下载任务和数据备份任务。

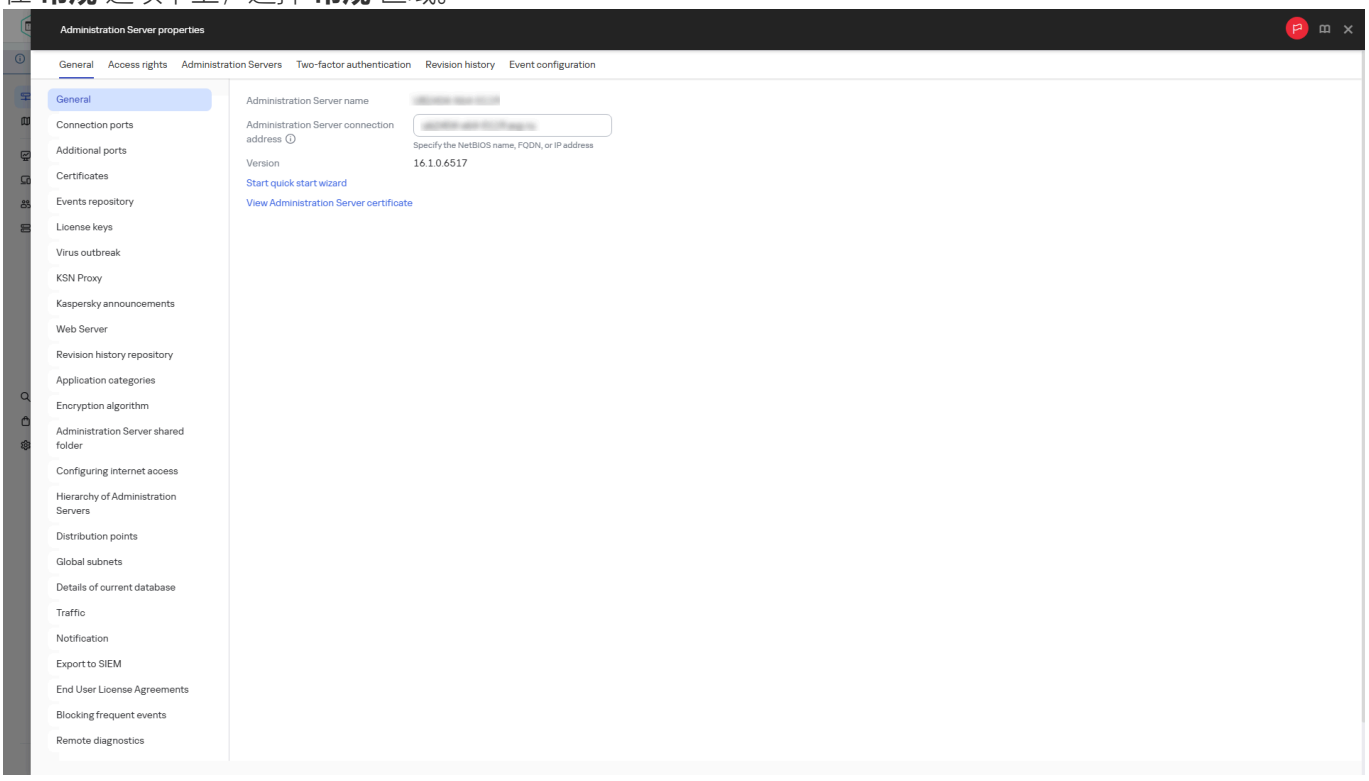
  > 快速启动向导仅为其“**资产(设备)**”文件夹不包含任何策略的应用程序创建策略。如果已经为受管理设备的顶级层级创建具有相同名称的任务，则快速启动向导不会创建同名任务。

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

*要手动启动快速启动向导：*

1. 在主菜单中，单击管理服务器名称。
   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。




管理服务器属性窗口

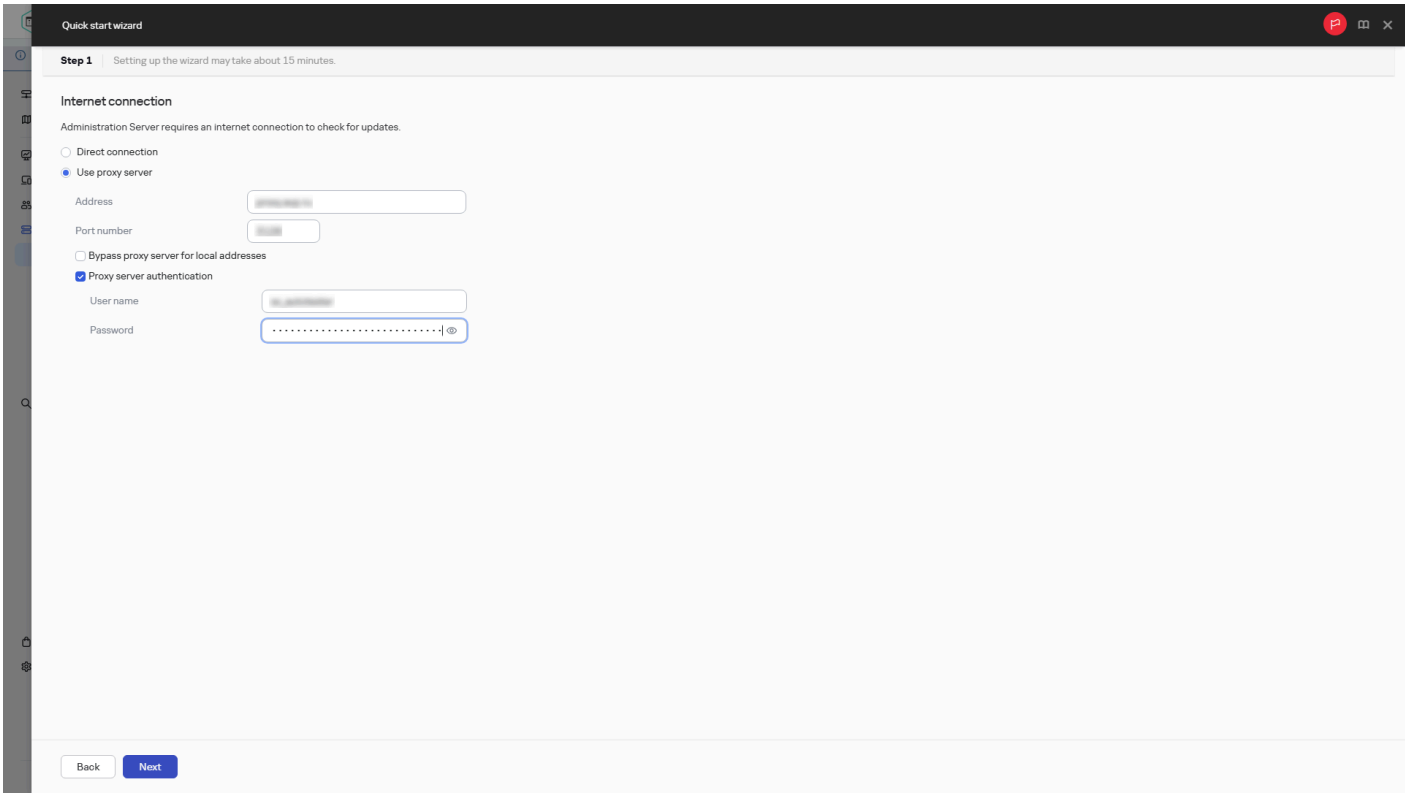
3. 单击**开始快速启动向导**。

向导提示您执行管理服务器初始化配置。遵照向导的说明操作。使用“**下一步**”按钮继续向导操作。

# 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：




互联网连接设置

- **地址**

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

- **端口号**

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

- **对本地地址不使用代理服务器**

  将不会使用代理服务器连接本地网络的设备。

- **代理服务器身份验证**

  如果选择该选框，您可以在输入字段中为代理服务器身份验证指定凭证。

  如果选中“**使用代理服务器**”复选框，则该输入字段可用。

- **用户名**

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

- **密码**

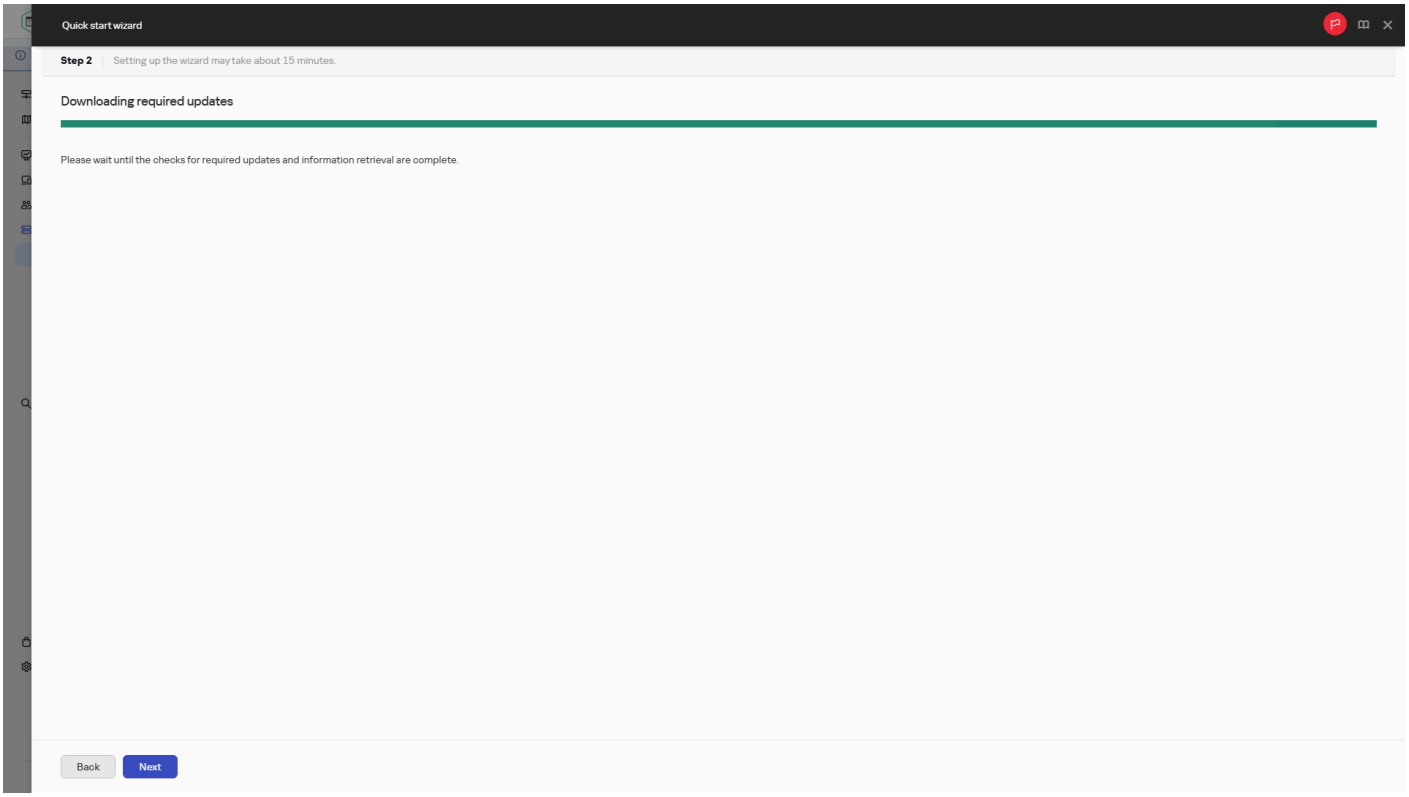
  建立代理服务器连接的账户所属的用户所设置的密码（如果选中“**代理服务器身份验证**”复选框，则该字段可用）。

  要查看输入的密码，单击并按住“**显示**”按钮足够长时间。

您可以稍后从快速启动向导单独配置互联网访问。

# 步骤 2：下载所需更新

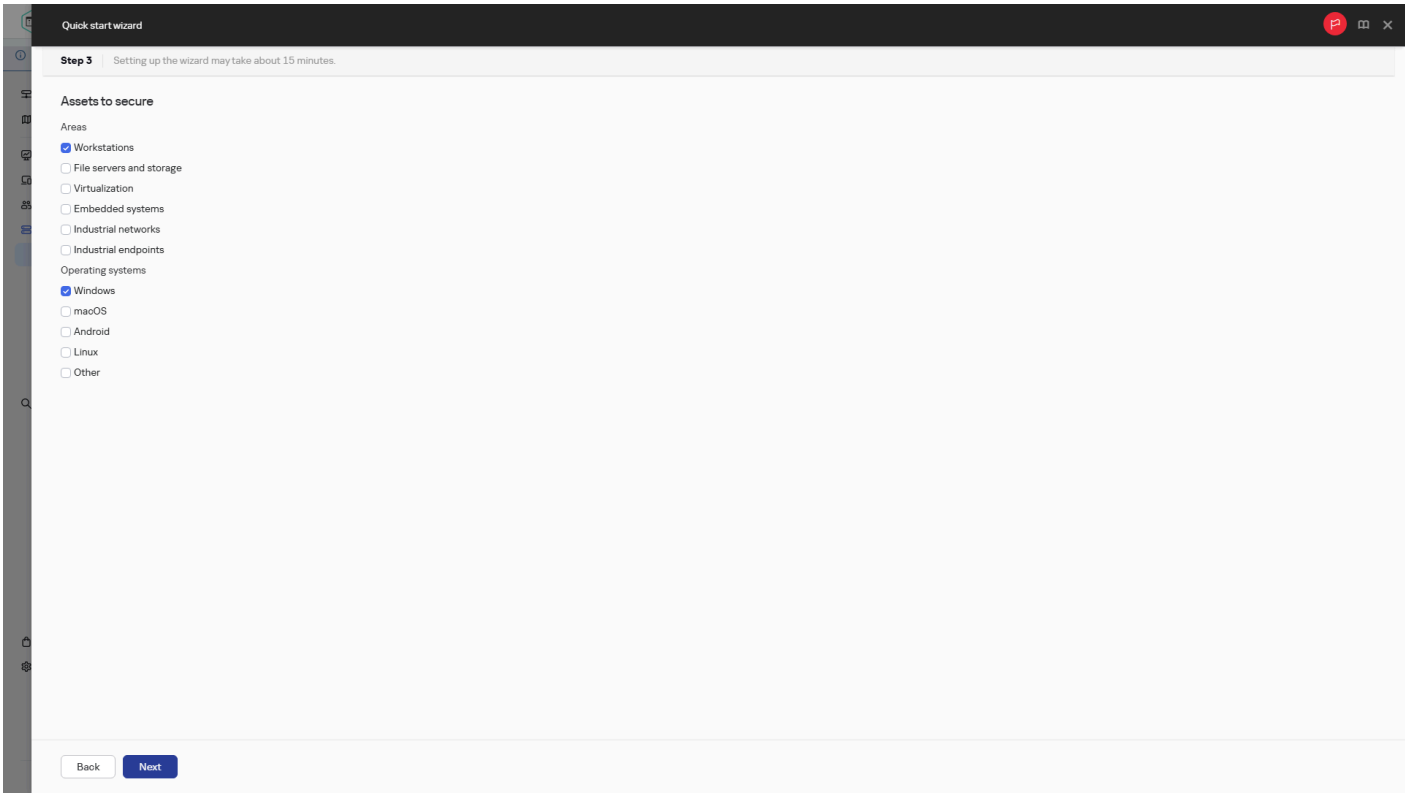
所需更新将从 Kaspersky 服务器自动下载。




正在下载所需更新

# 步骤 3：选择要保护的资产

选择网络中正在使用的保护区域和操作系统。选择这些选项时，将为 Kaspersky 服务器上的应用程序管理插件和分发包指定过滤器，您可以下载这些插件和分发包以将其安装在网络中的客户端设备上。




选择要保护的资产

选择选项：

- **范围**

  您可以选择以下保护范围：

  - **工作站**
  - **文件服务器和存储**
  - **虚拟化**
  - **嵌入式系统**
  - **工业网络**
  - **工业端点**

- **操作系统**

  您可以选择以下平台：

  - Microsoft Windows
  - macOS

- Android
- Linux
- 其他

有关支持的操作系统的更多信息，请参阅“Kaspersky Security Center Web Console 的硬件和软件要求”。

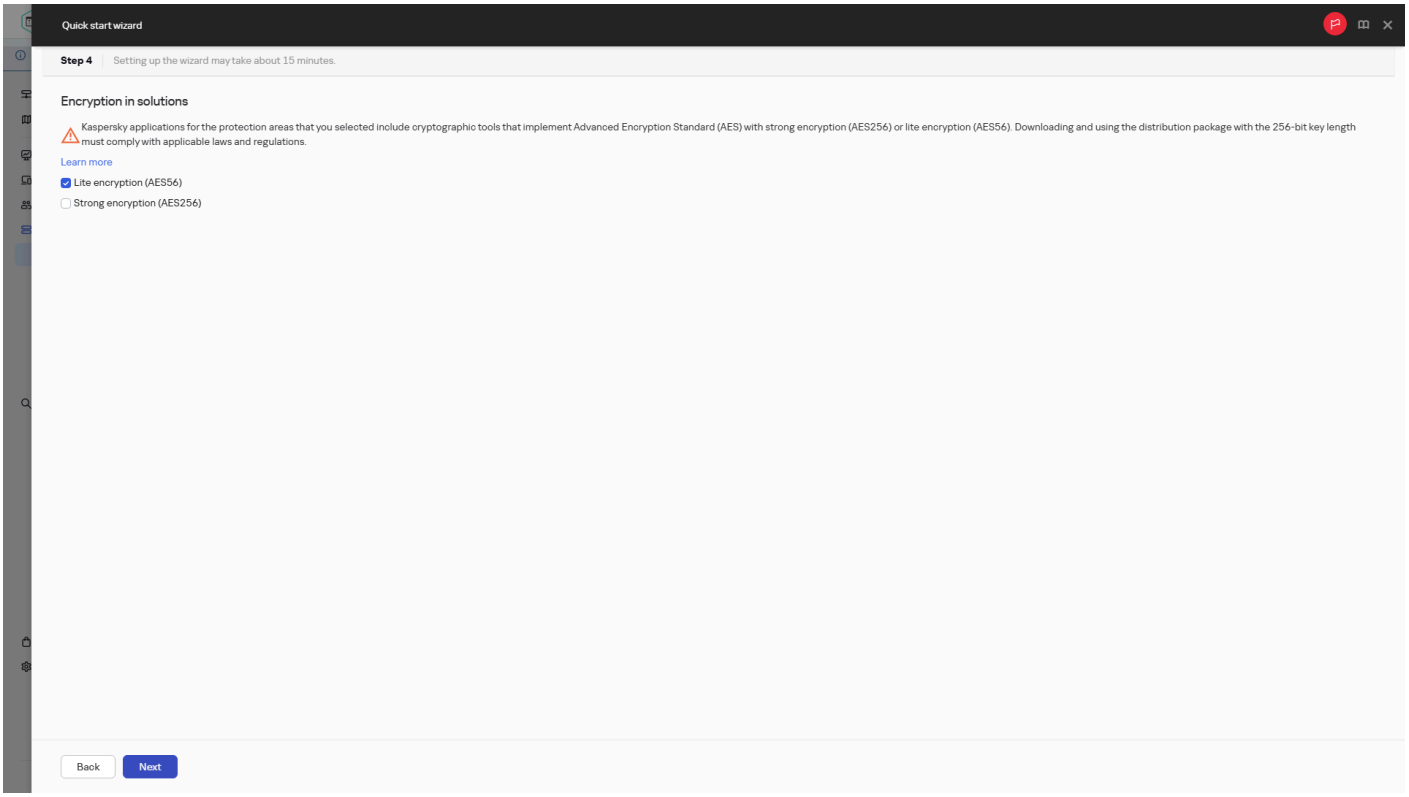
您可以稍后从可用包列表中选择卡巴斯基应用程序包，是从快速启动向导单独配置。为了简化对所需包的搜索，您可以通过各种标准筛选可用包列表。

# 步骤 4：选择解决方案中的加密

只有选择“工作站”作为保护范围并选择“**工作站**”作为平台时，才显示“**加密进行中**”窗口。

Kaspersky Endpoint Security for Windows 包括用于存储在 Windows 客户端设备上的信息的加密工具。这些加密工具采用以 256 位或 56 位密钥长度实现的高级加密标准 (AES)。

必须按照适用的法律法规下载和使用密钥长度为 256 位的分发包。要下载可满足组织需求的有效 Kaspersky Endpoint Security for Windows 分发包，请参考组织的客户端设备所在国家/地区的法律。




选择解决方案中的加密

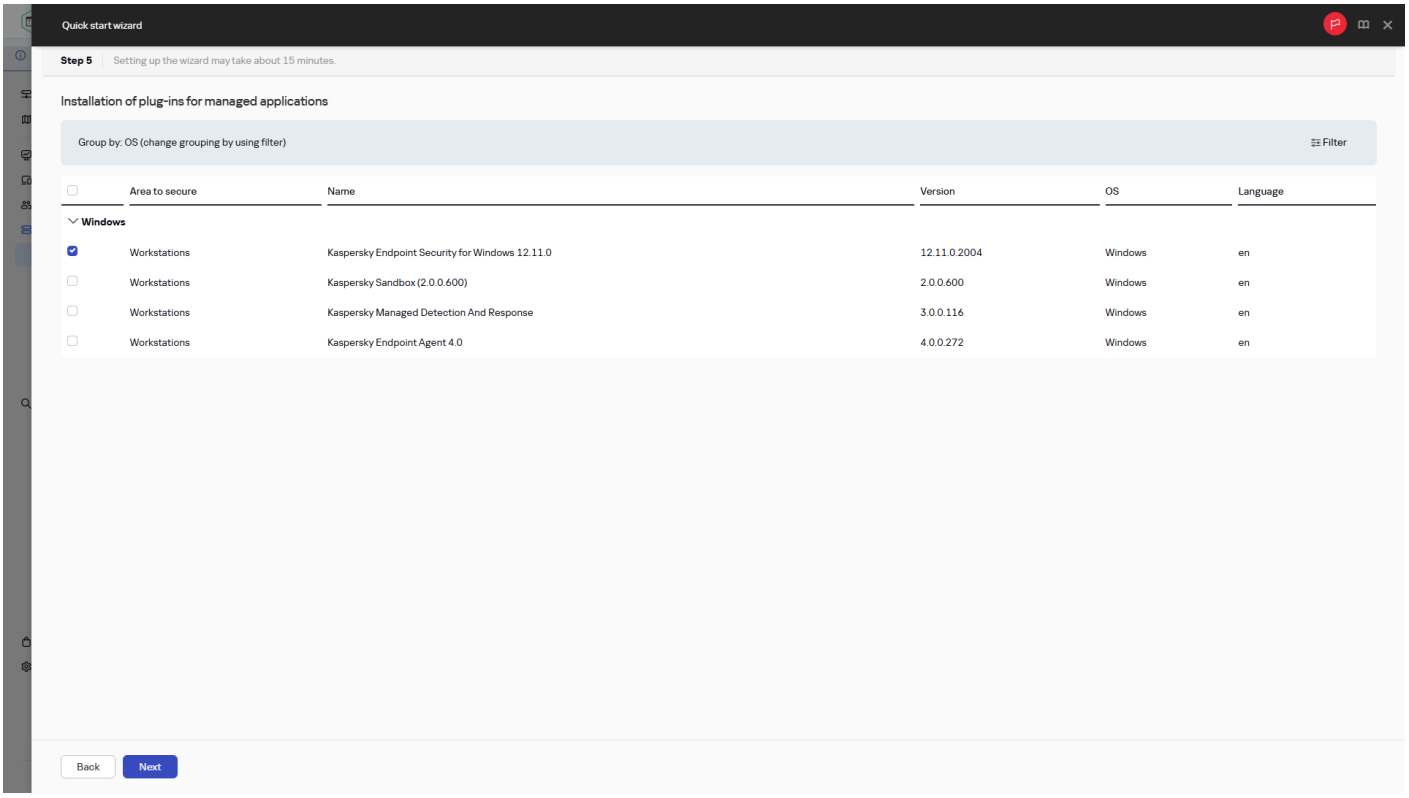
在“**加密进行中**”窗口，选择以下加密类型之一：

- 轻度加密。此加密类型使用 56 位密钥长度。
- 强加密。此加密类型使用 256 位密钥长度。

您可以稍后使用所需的加密类型为 Kaspersky Endpoint Security for Windows 选择分发包，单独从快速启动向导执行。

# 步骤 5：配置受管理应用程序的插件安装

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




受管理应用程序插件安装

插件列表包括以下多列：

- **保护范围**

  选定的要保护的区域会显示在此列中。

- **类型**

  插件类型会显示在此列中。

- **名称**

  将根据您在上一步中选择的保护区域和平台来选择插件。

- **版本**

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

- **最新版本**

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

- **操作系统**

  此列会显示插件操作系统。

- **语言**

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

选择插件后，单击“**下一步**”开始安装。

您可以手动为卡巴斯基应用程序安装管理插件，单独从快速启动向导执行。

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

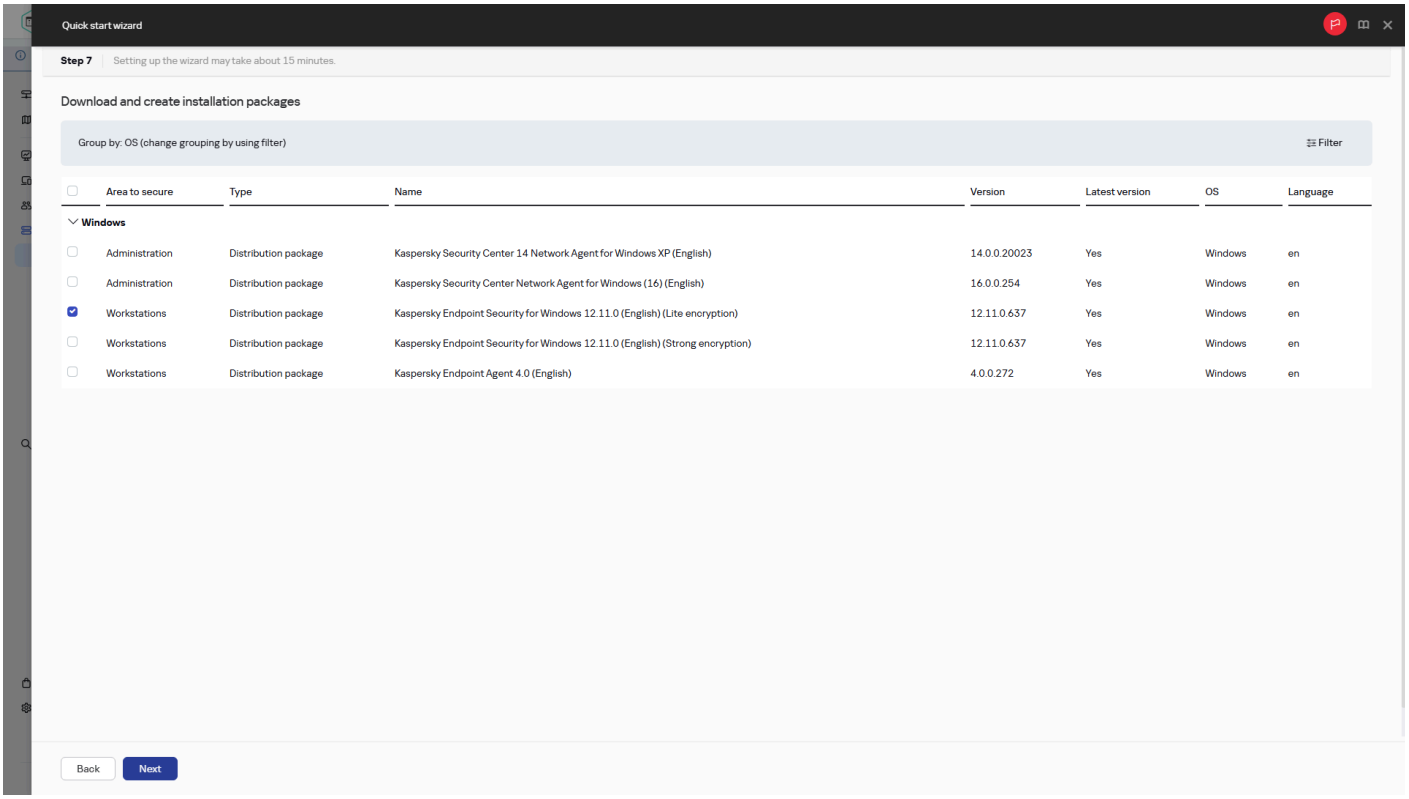
安装所有选定插件后，快速启动向导会自动带您继续下一步。

# 步骤 6：下载分发包并创建安装包

选择要下载的分发包。

受管理应用程序的分发可能需要安装 Kaspersky Security Center Linux 的特定最低版本。

选择 Kaspersky Endpoint Security for Windows 的加密类型之后，将显示两种加密类型的分发包列表。列表中选中了具有所选加密类型的分发包。您可以选择任意加密类型的分发包。分发包语言与 Kaspersky Security Center Linux 语言相对应。如果不存在 Kaspersky Security Center Linux 语言的应用程序分发包，则选择英文分发包。



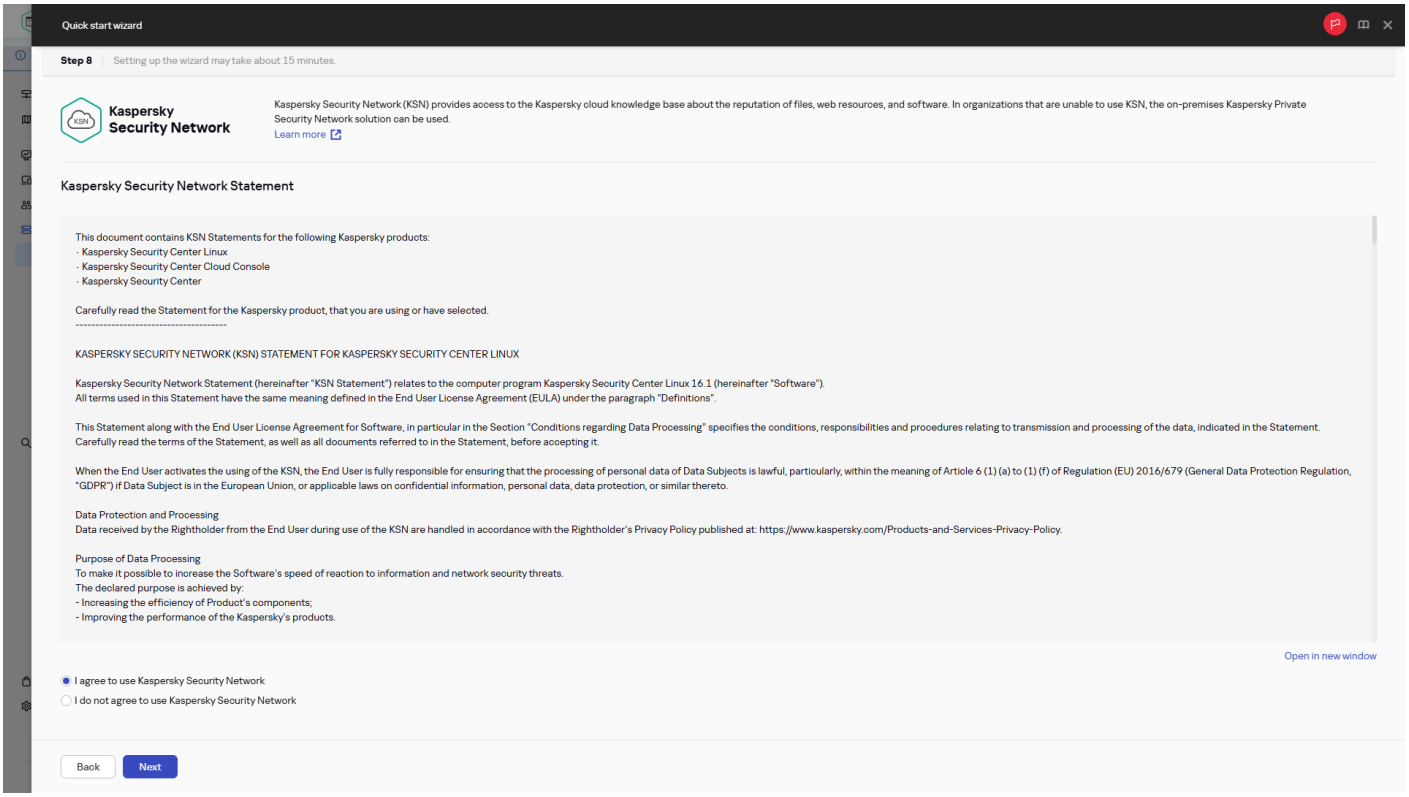

下载分发包并创建安装包

要完成某些分发包的下载，您必须接受 EULA。当您单击“**接受**”按钮时，将显示 EULA 文本。要继续进行向导的下一步，您必须接受 EULA 的条款和条件以及 Kaspersky 隐私策略的条款和条件。如果您不接受条款和条件，则将取消分发包的下载。

在您接受 EULA 的条款和条件以及 Kaspersky 隐私策略的条款和条件之后，将继续下载分发包。稍后，您可以使用安装包在客户端设备上部署 Kaspersky 应用程序。

# 步骤 7：配置卡巴斯基安全网络

指定设置以转发 Kaspersky Security Center Linux 操作信息到卡巴斯基安全网络知识库。




配置卡巴斯基安全网络

您可以选择以下选项之一：

- **我同意使用卡巴斯基安全网络**

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

- **我不同意使用卡巴斯基安全网络**

  Kaspersky Security Center Linux 和受管理应用程序将不向卡巴斯基安全网络提供任何信息。

  如果选择此选项，则将禁用卡巴斯基安全网络。

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

# 步骤 8：选择应用程序激活方法

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

- **通过输入您的激活码**

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

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

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

  如果启用此选项，授权许可密钥将自动部署到受管理设备。

  如果禁用此选项，则可以稍后在主菜单的 **操作** → **授权许可** → **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。

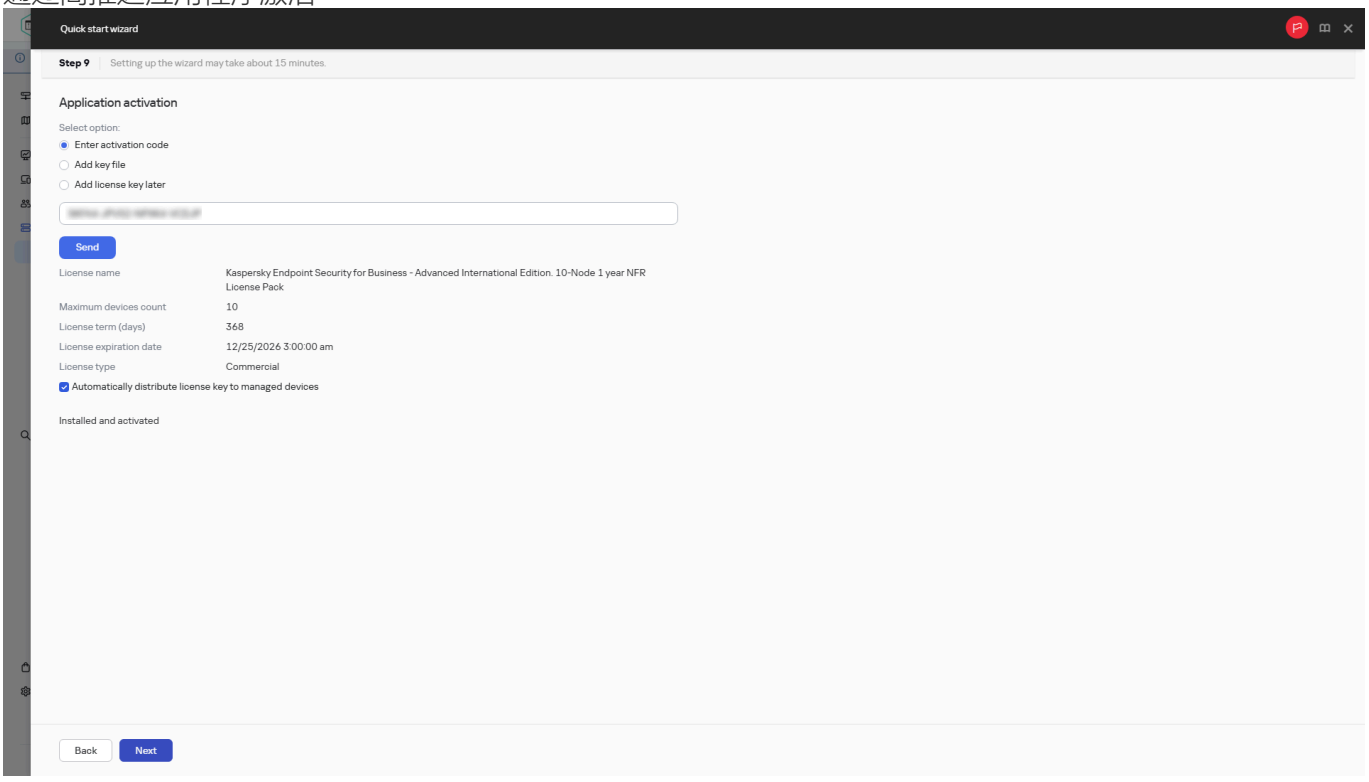
  若使用密钥文件激活程序，您无需连接至 Kaspersky 激活服务器。

  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** → **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



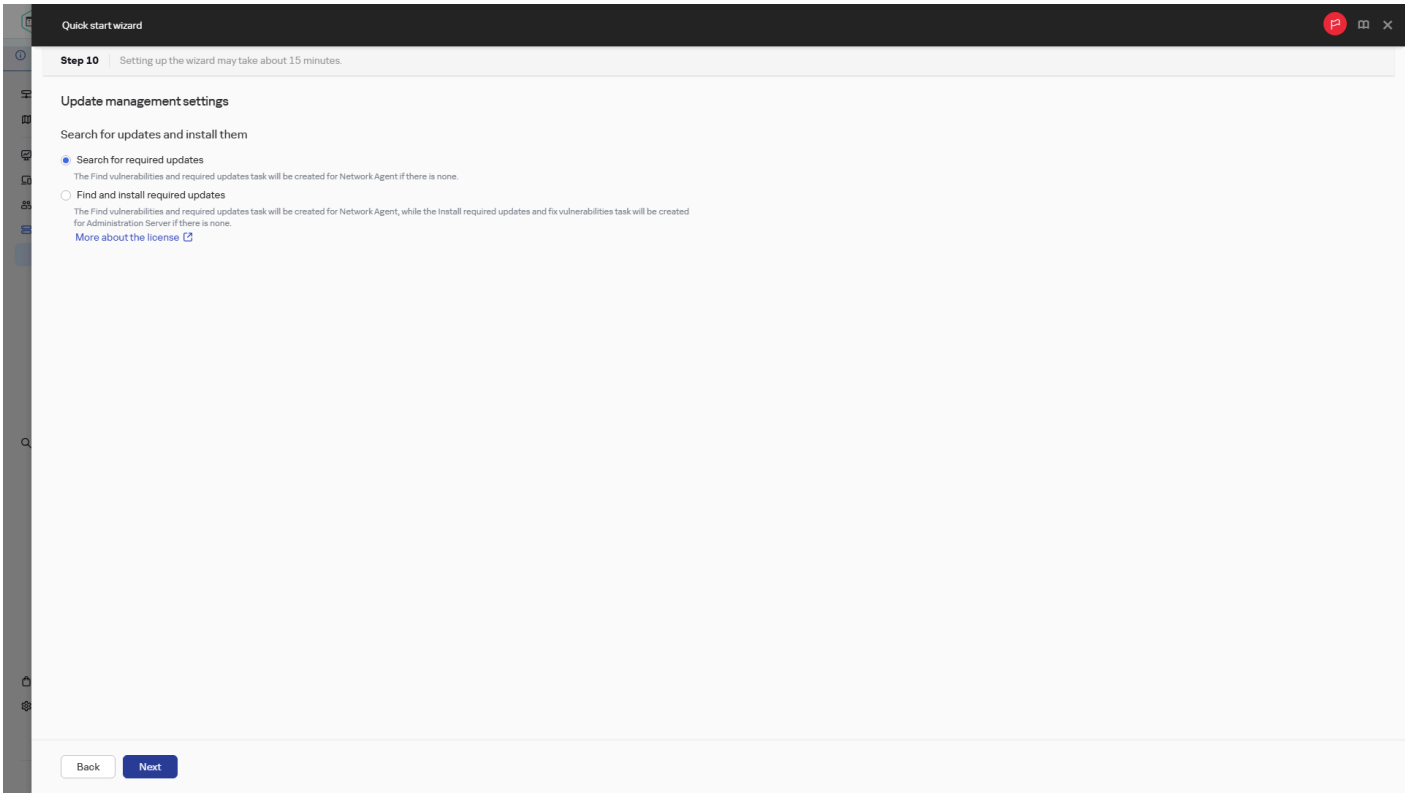

选择应用程序激活方法

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

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

# 步骤 9：指定第三方更新管理设置

如果您没有漏洞和补丁管理授权许可，并且“*查找漏洞和所需更新*”任务已经存在，则快速启动向导中不会显示“**更新管理设置**”步骤。




第三方更新管理设置

对于第三方软件更新，选择以下选项之一：

- **搜索所需更新**

  如果您没有*查找漏洞和所需更新*任务，系统会自动创建该任务。
  默认情况下已选中该选项。

- **查找并安装所需更新**

  如果没有“*查找漏洞和所需更新*”和“*安装所需更新并修复漏洞*”任务，它们会自动创建。

  此选项仅在“漏洞和补丁管理”授权许可下可用。

对于 Windows Update 更新，选择“**使用域策略中定义的更新源”。**

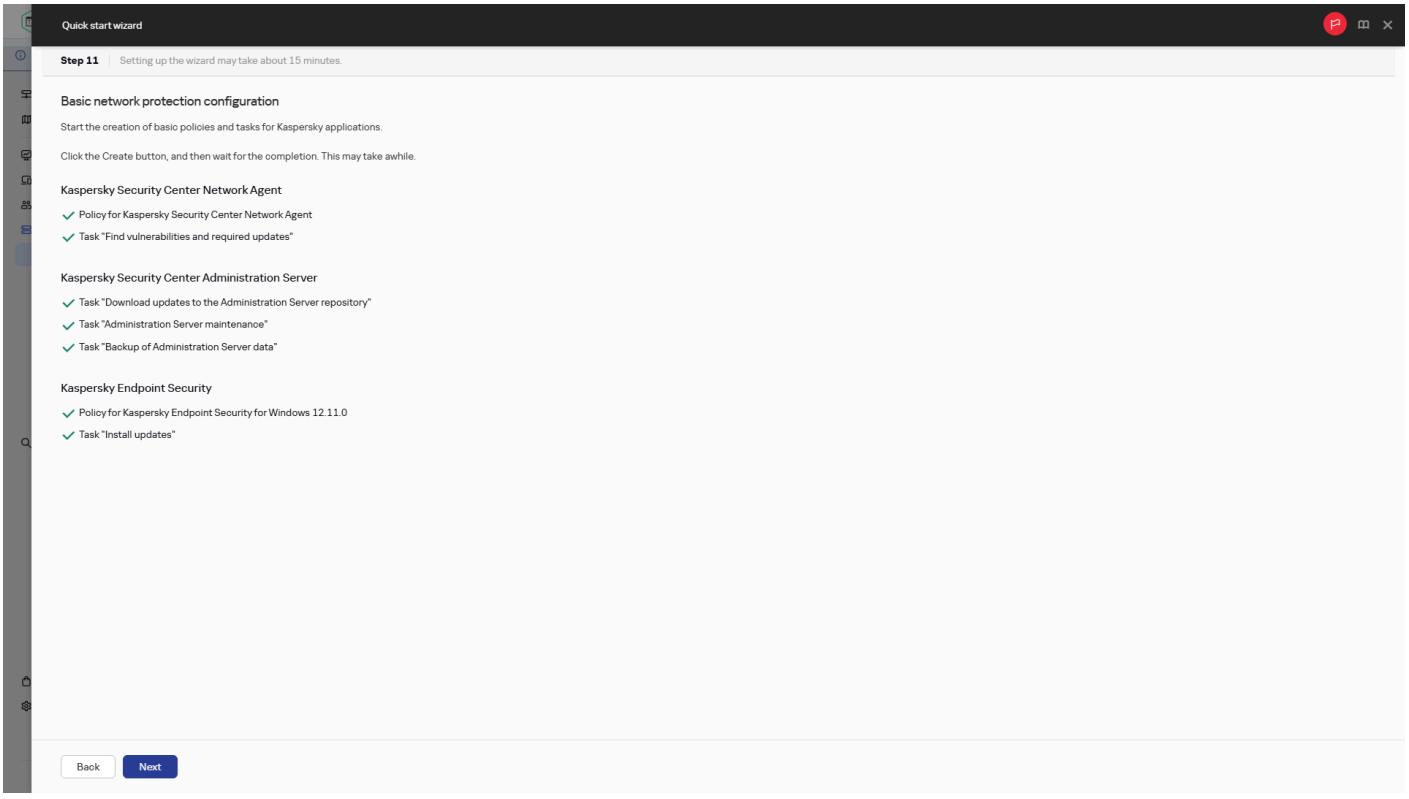
客户端设备将根据域策略设置下载 Windows Update 更新。如果没有网络代理策略，它会自动创建。

您可以从快速启动向导中单独创建“*查找漏洞和所需更新*”和“*安装所需更新并修复漏洞*”任务。

# 步骤 10：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。

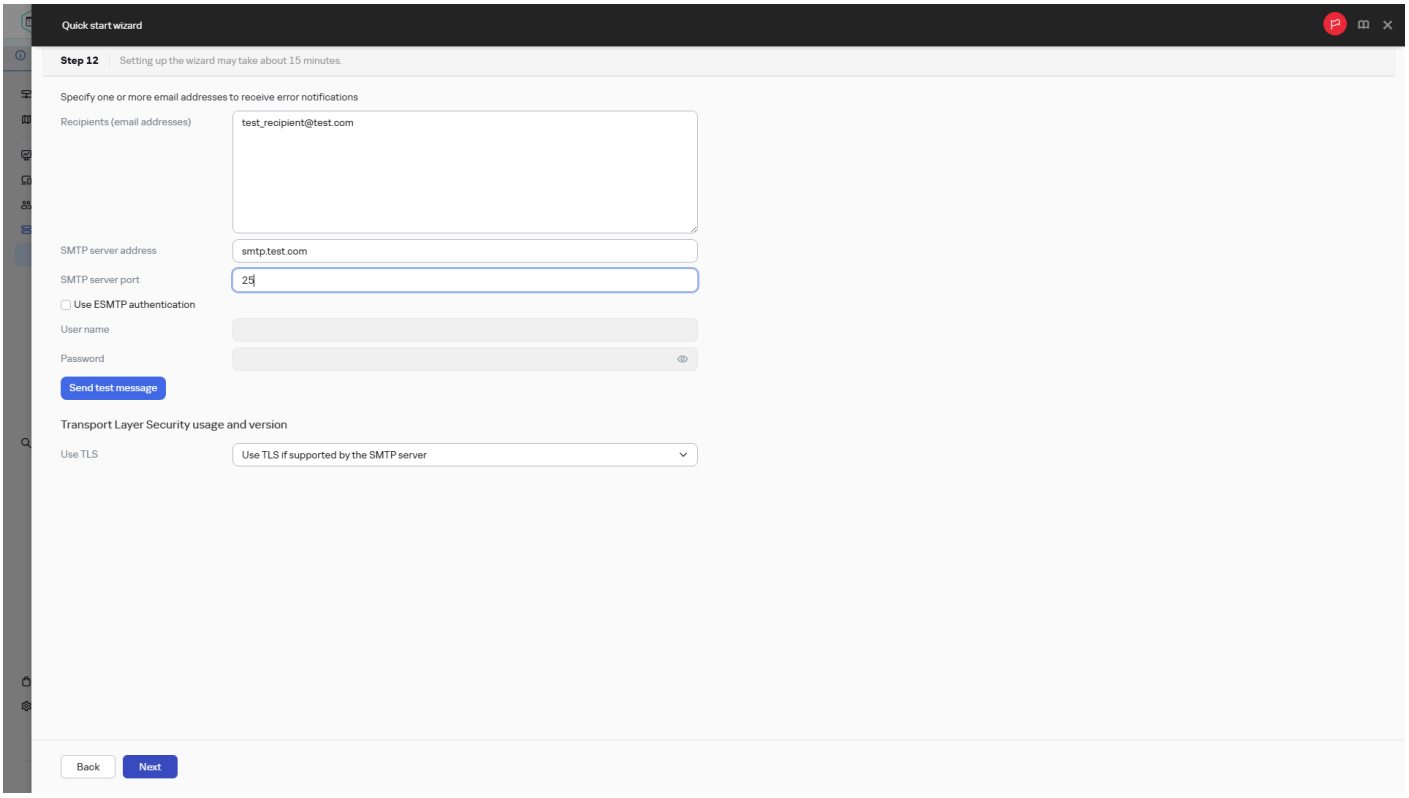
等待策略和任务完成创建，然后转到向导的下一步。




创建基本的网络保护配置

# 步骤 11：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。




配置邮件通知

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。

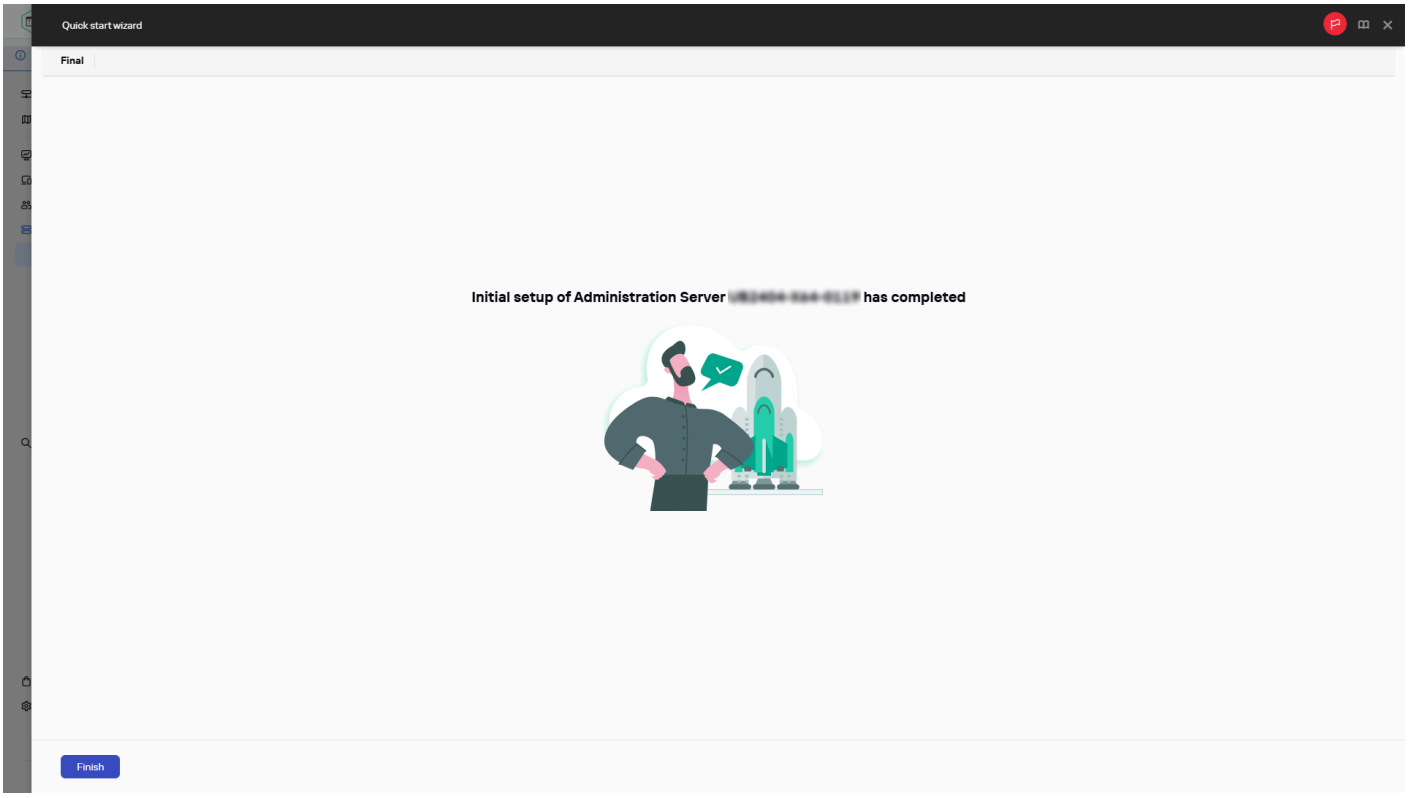
- **使用 ESMTP 身份验证**

  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 12：关闭快速启动向导

要关闭向导，请单击“**完成**”按钮。




快速启动向导的最后一步

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

# 保护部署向导

要安装卡巴斯基应用程序，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**软件管理→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，*

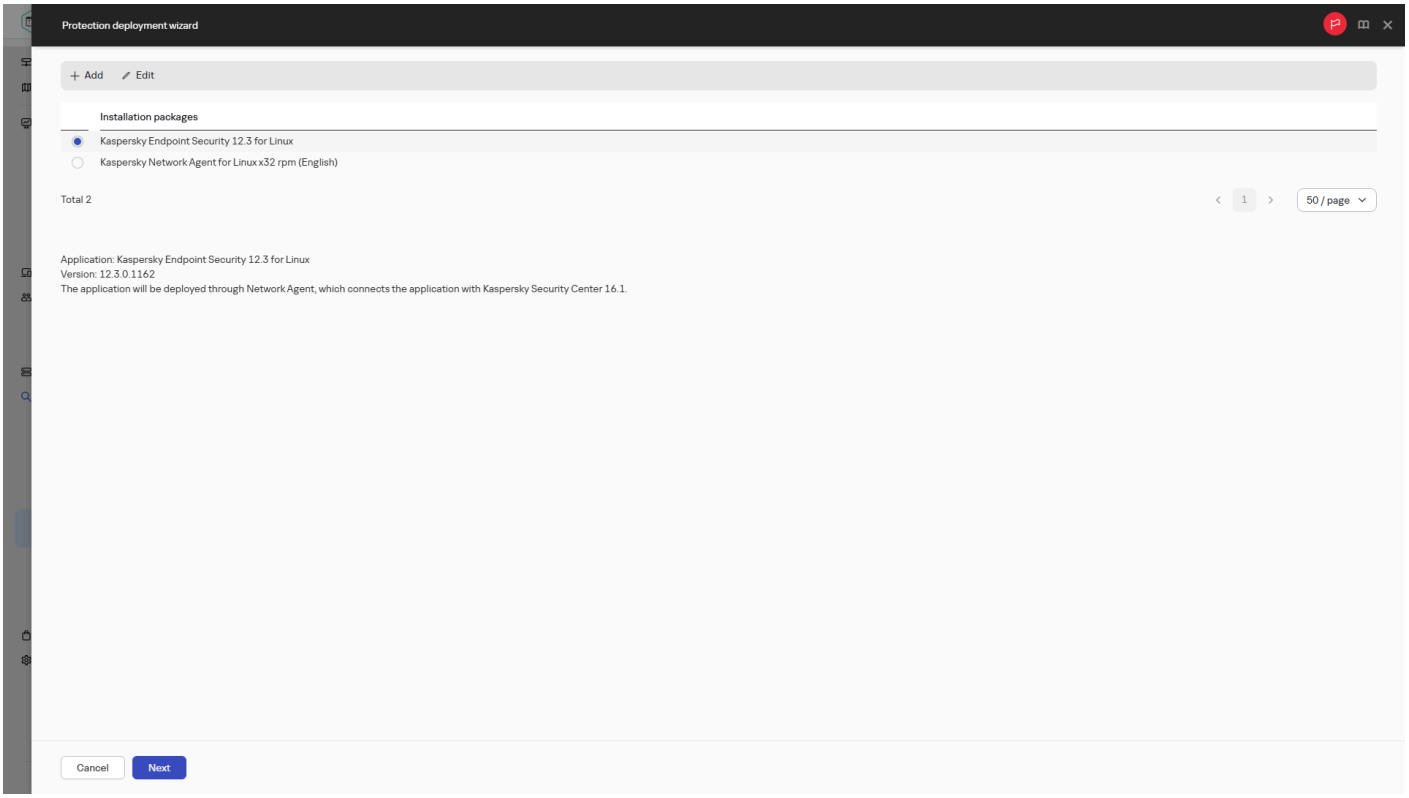
在主菜单中，转到“**发现和部署**”→“**部署和分配**”→“**保护部署向导**”。

保护部署向导启动。使用“**下一步**”按钮继续向导操作。

# 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。




选择安装包

# 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：

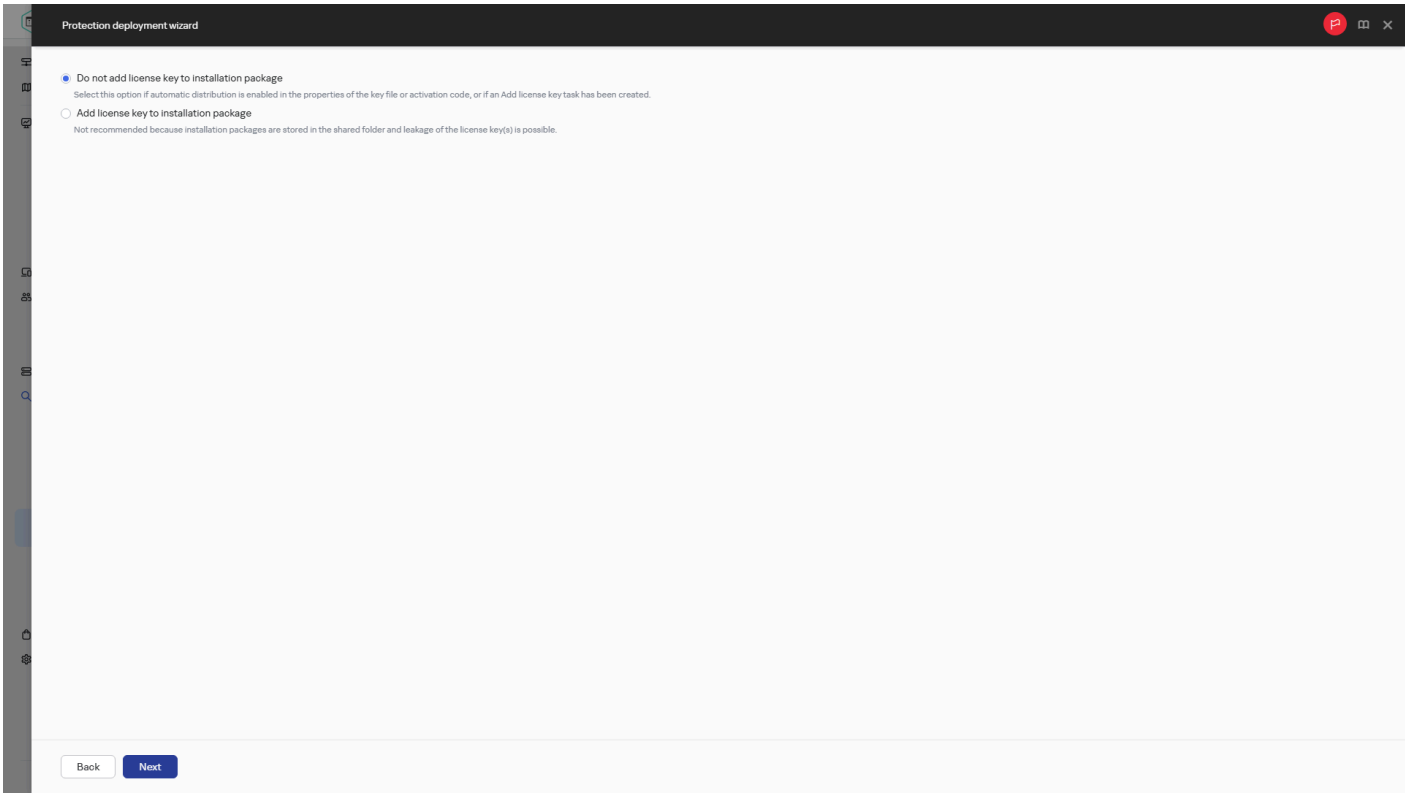
  - 如果自动分发在密钥属性中启用。
  - 如果**添加密钥**任务已创建。

- **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。

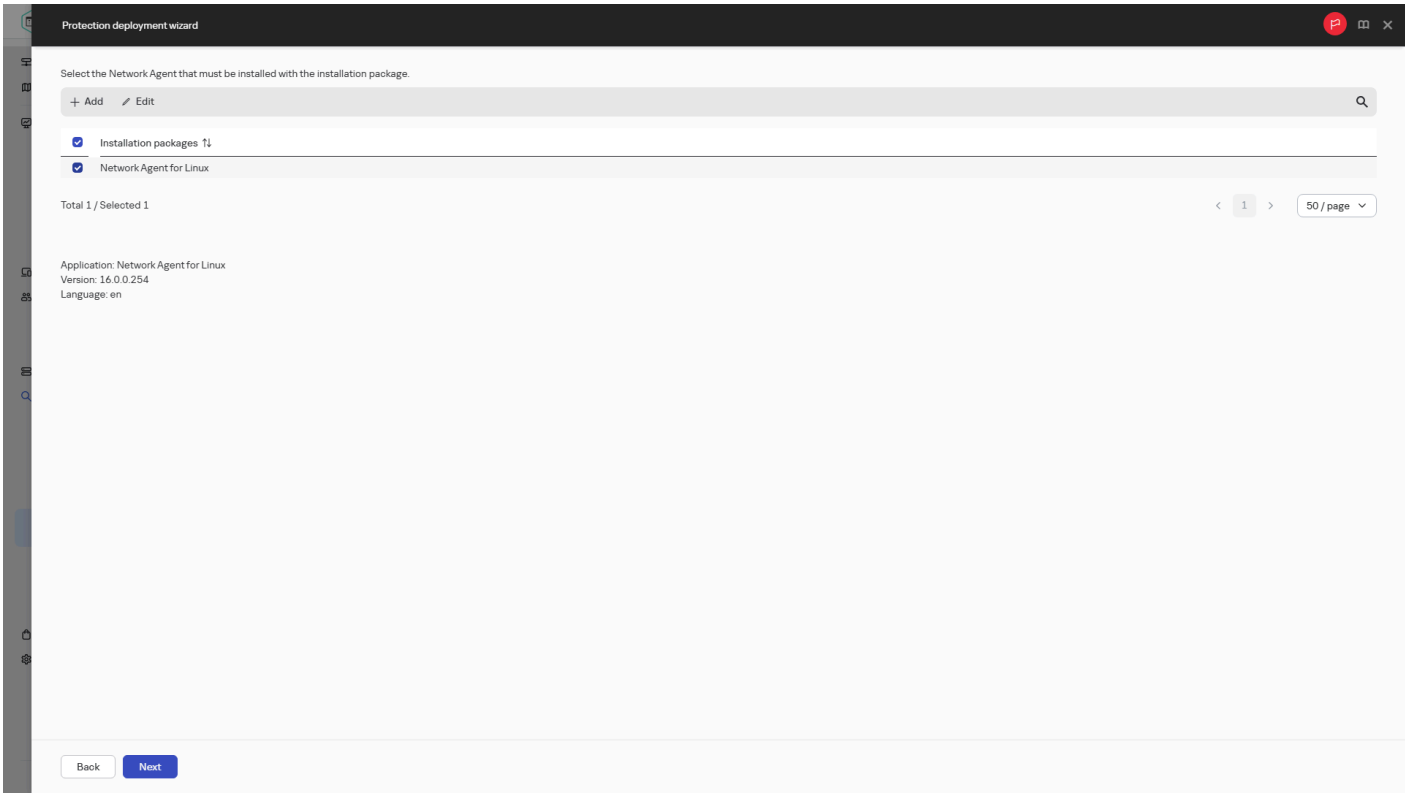



选择密钥文件或激活码的分发方式

# 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。




选择网络代理版本

# 步骤 5：选择设备

指定要安装应用程序的设备列表：

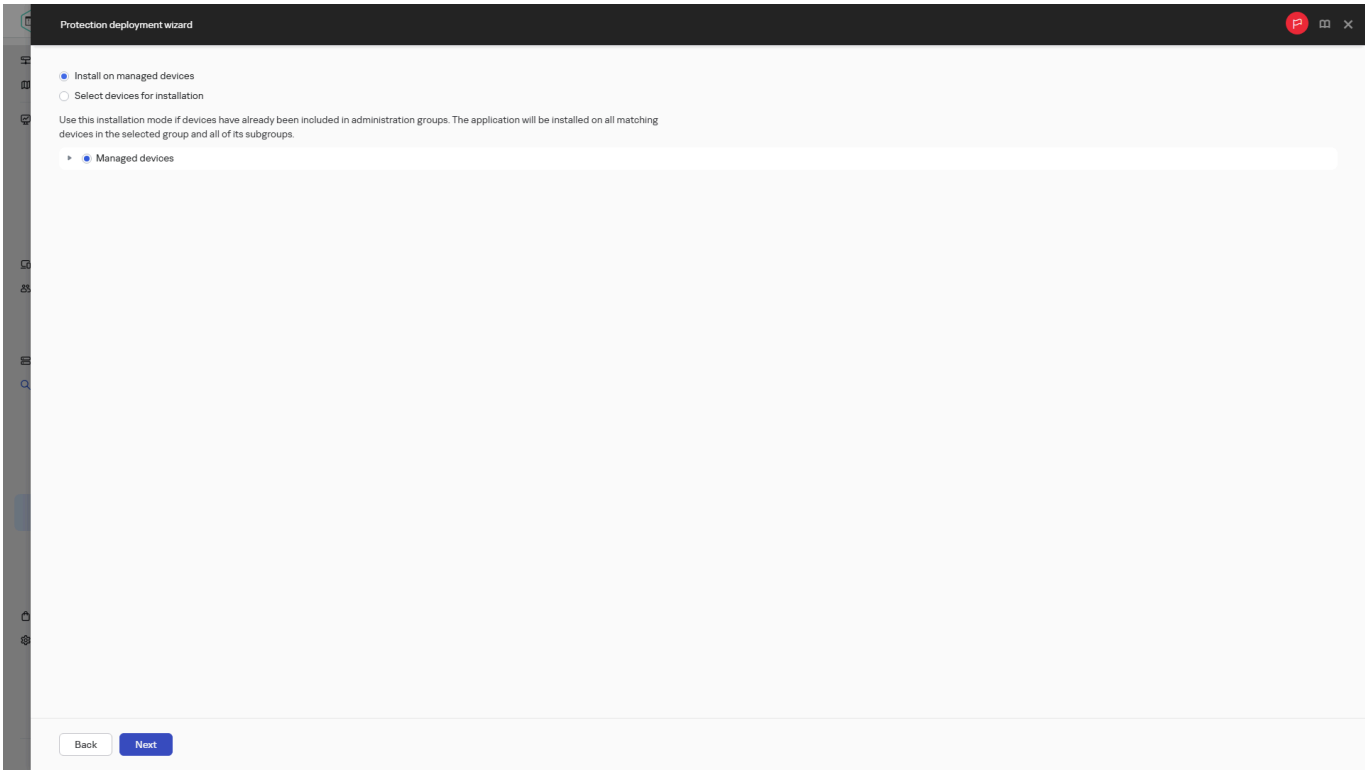
- **安装到受管理设备**

  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。




指定要在上面安装应用程序的设备列表

# 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。

- **通过管理服务器使用操作系统资源**

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

  默认情况下已启用该选项。

定义附加设置：

- **如果已经安装应用程序则不再重新安装**

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

  如果禁用此选项，仍将安装应用程序。

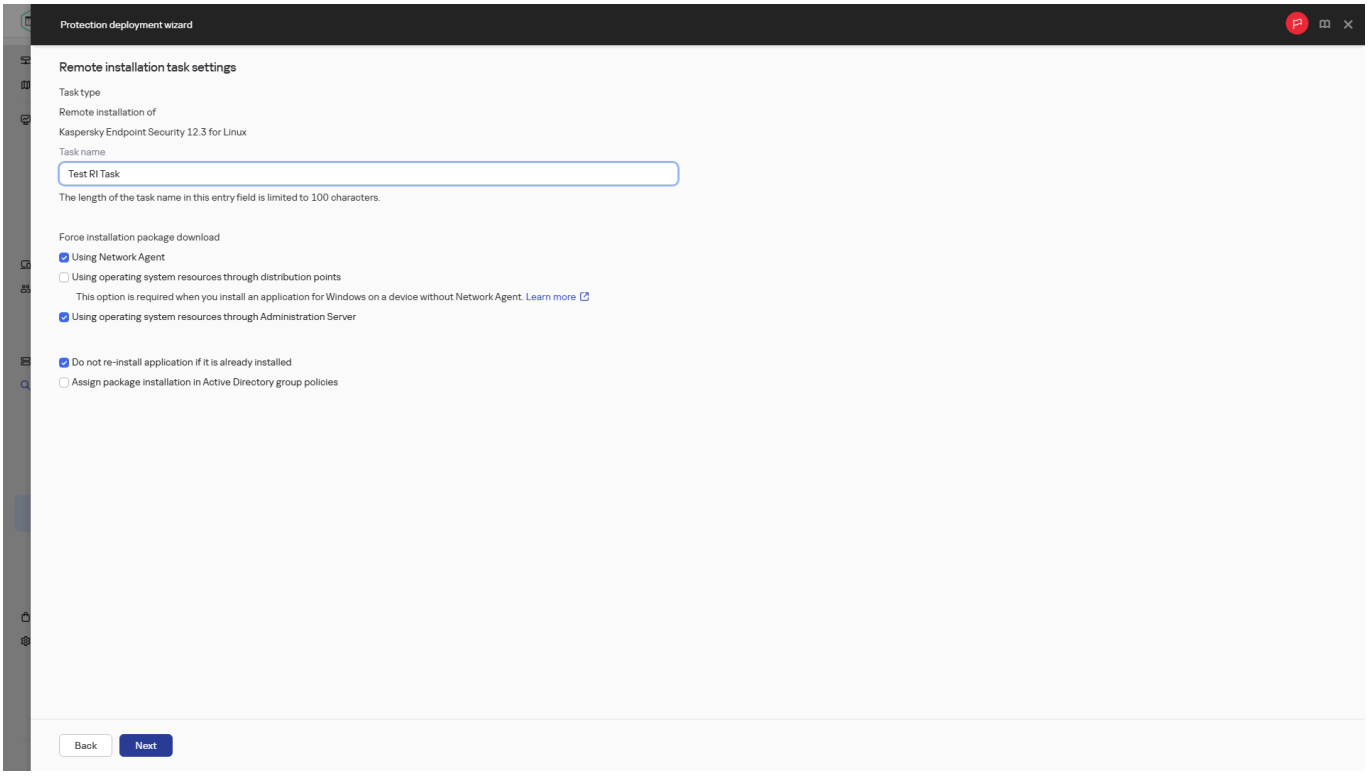
  默认情况下已启用该选项。

- **在 Active Directory 组策略中指定安装包的安装**

  如果启用此选项，安装包将使用 Active Directory 组策略进行安装。

  如果选择网络代理安装包，则该选项可用。

  默认情况下已禁用该选项。




指定远程安装任务设置

# 步骤 7：重启管理

如果安装应用程序时操作系统必须重启，指定要执行的操作：

- **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。

- **提示用户操作**

  客户端设备屏幕上将显示重启提醒，提示用户手动重启设备。可以为该选项定义一些高级设置：用户消息文本、消息显示频率以及强制重启（不需要用户确认）的时间间隔。该选项适用于用户必须可以选择最方便的时间进行重启的工作站。

  默认情况下已选定该选项。

  - **重复提示间隔(分钟)**

    如果启用该选项，应用程序以指定频率提示用户重启操作系统。

    默认情况下已启用该选项。默认时间间隔为 5 分钟。可用值介于 1 和 1 440 分钟之间。

    如果禁用该选项，提示仅显示一次。

  - **在该时间后重启(分钟)**

    提示用户之后，应用程序在指定时间间隔后强制操作系统重启。

    默认情况下已启用该选项。默认延时是 30 分钟。可用值介于 1 和 1 440 分钟之间。

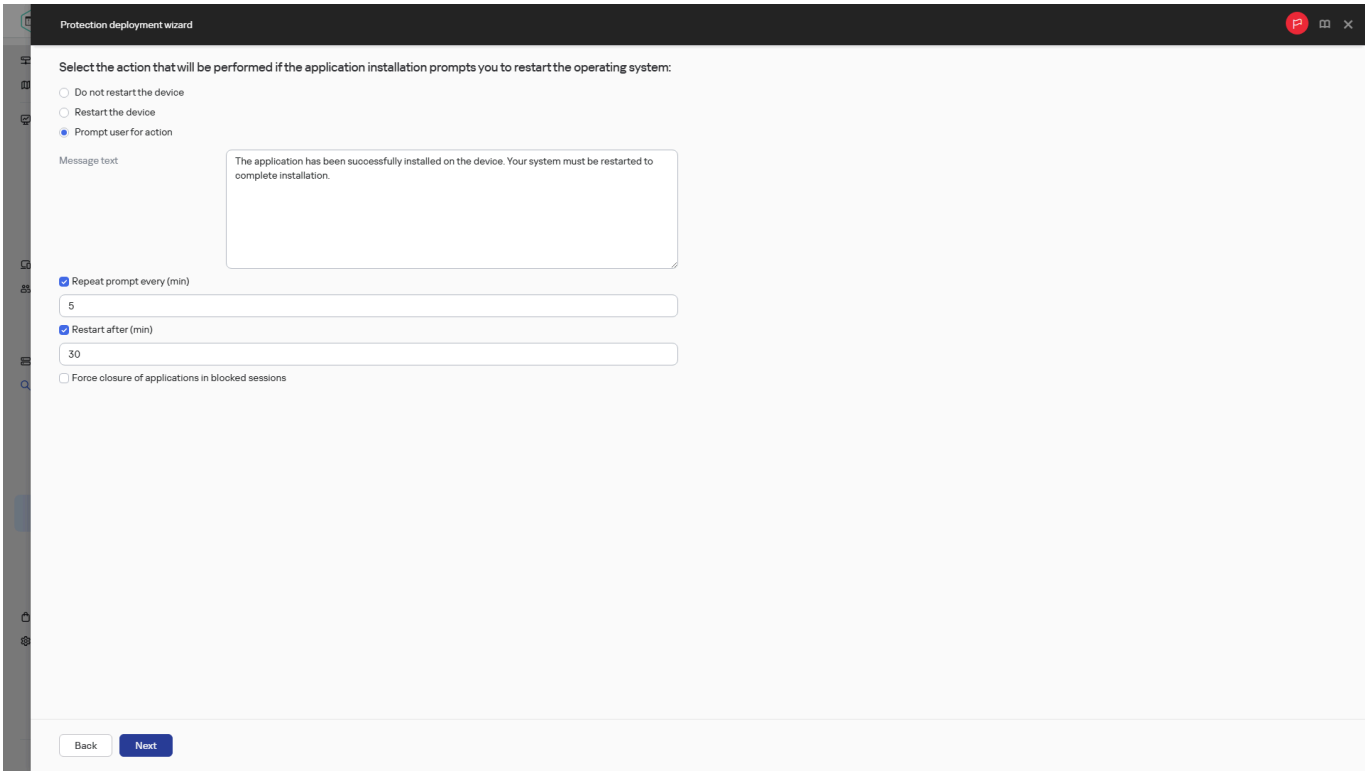
- **强行关闭锁定会话中的应用程序**

  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。




选择操作系统重启选项

# 步骤 8：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 9：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。

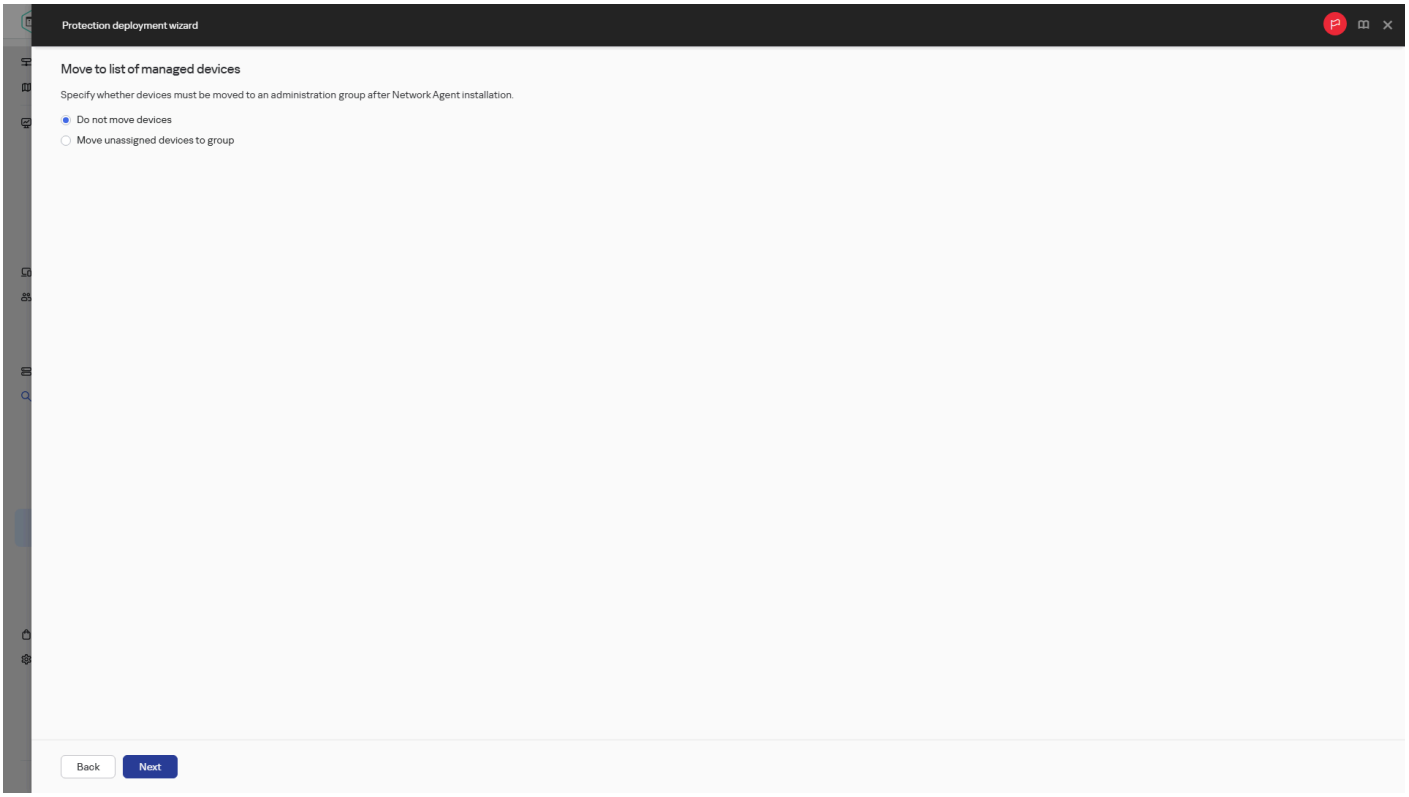
- **不移动设备**

  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。




选择将设备移动到管理组的选项

# 步骤 10：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。

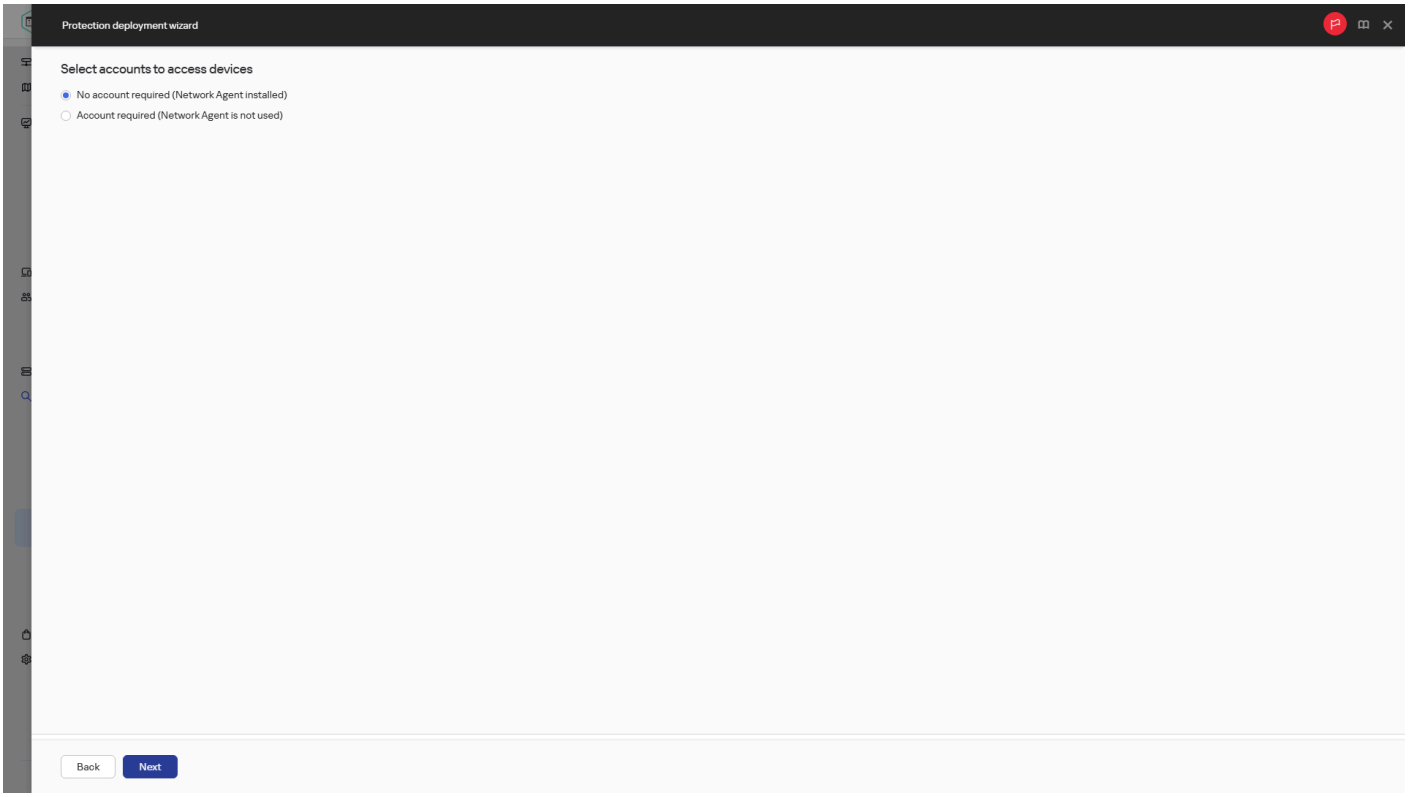
  - **本地或域账户**。如果该选项被选中，请指定将运行应用程序安装程序的用户账户。单击**添加**按钮，选择**本地或域账户**，然后指定用户账户凭据。

    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 Linux 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 Linux 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>"
    ```




选择访问设备的账户

# 步骤 11：开始安装

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

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

单击“**确定**”完成保护部署向导的最后一步。

# 升级 Kaspersky Security Center Linux

您可以在安装了早期版本管理服务器（从版本 13 开始）的设备上安装管理服务器版本 16.3。当升级至版本16.3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。

## 先决条件

- 在开始升级之前，创建管理服务器数据的备份副本。
- 将管理服务器从16或更早版本升级到16.1或更高版本时，将启用双重身份验证。有关更多信息，请参阅关于帐户的双重身份验证。

  为了确保用户可以使用配置的双重身份验证密钥使用现有帐户登录云控制台，并且OpenAPI自动化脚本在升级后继续工作，您必须执行以下步骤：

  - 为所有用户启用双重身份验证
  - 管理员必须为其自己的帐户配置双重身份验证
  - 从双重身份验证中排除所需的账户

    如有需要，请将用于通过OpenAPI运行脚本的集成帐户添加到排除项列表中。
- 确保您使用的是管理服务器16.3版支持的操作系统和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。
- 将管理服务器从 15.4或更早版本升级到 16 或更高版本时，请在 DBMS 服务器上为IAM创建一个数据库。数据库名称必须与您为 Kaspersky Security Center Linux 安装的数据库名称不同。

  - 对于 PostgreSQL，请运行以下命令：

    ```
    sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
    ```
  - 对于 MariaDB，请运行以下命令：

    ```
    sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
    ```
- 将管理服务器从15.4或更早版本升级到16或更高版本时，请准备包含IAM新参数的应答文件。有关所需参数的列表，请参阅文章以静默模式安装Kaspersky Security Center Linux。添加`KLAUTOANSWERS`环境变量，并将其值设置为应答文件的路径。
- 确保 kliam 进程用于 OpenID Connect 协议身份验证的端口可用。默认情况下为 4444。请参阅以下文章中的`trusted`参数说明：Kaspersky Security Center Web Console 安装参数。

## 阶段

1. **升级管理服务器**

您可以使用以下方法之一升级管理服务器的版本：

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

> 升级期间，严禁管理服务器和其他应用程序同时使用 DBMS。

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

2. **运行postinstall.pl脚本（可选步骤）。**

如果应答文件不包含 IAM 参数或者未找到应答文件，则升级期间终端中会显示一条消息，要求您运行 postinstall.pl 脚本。

在方案的该步骤，执行以下操作：

1. 在管理服务器操作系统中，创建一个名为“ksciam”的非特权用户账户，该帐户必须是“kladmins”组的成员：

```
adduser ksciam

gpasswd -a ksciam kladmins

usermod -g kladmins ksciam
```

2. 在具有 root 权限的账户下，运行 /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl 脚本来配置升级后的管理服务器。出现提示时，输入以下设置：
    1. 输入 IAM Server FQDN。您必须使用安装 Kaspersky Security Center Linux 时指定的管理服务器 DNS 名称。
    2. 输入用于启动 IAM 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“ksciam”账户。
    3. 选择您安装的与 IAM 服务一起使用的 DBMS：
        - 如果您安装了 MySQL 或 MariaDB，请输入 1。
        - 如果您安装了 PostgreSQL 或 Postgres Pro，请输入 2。
    4. 输入 IAM 服务要使用的 IAM DBMS 地址。
    5. 输入 IAM DBMS 端口号。该端口用于与 IAM 服务通信。默认情况下，使用以下端口：
        - 端口 3306 用于 MySQL 或 MariaDB
        - 端口 5432 用于 PostgreSQL 或 Postgres Pro
    6. 输入 IAM 服务要使用的 IAM 数据库名称。IAM 服务使用的数据库名称应与管理服务器使用的数据库名称不同。

3. **将Kaspersky Security Center云控制台升级到新版本。**

4. **（可选）将设备上的网络代理升级到新版本。**

5. **确保双重身份验证允许列表仅包含必须有权访问管理服务器的用户账户。**

查看双重身份验证允许列表，并从中删除任何其他帐户。

请注意，如果您将管理服务器升级到版本 16.3，则无法创建网络代理版本 15 或早期版本的新安装包。但是，先前创建的安装包仍然可用。

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。

# 将 Kaspersky Security Center Linux 从 16 版本或更高版本进行升级

本节介绍将 Kaspersky Security Center Linux 从版本 16 或更高版本升级到最新版本的以下选项：

- 使用安装文件进行升级
- 通过备份进行升级
- 在 Kaspersky Security Center Linux 故障转移集群节点上升级

# 使用安装文件将 Kaspersky Security Center Linux 从 16 或更高版本进行升级

要将管理服务器从版本 16 升级到版本 16 或者更高版本升级到最新版本，您可以使用 Kaspersky Security Center Linux 安装文件在早期版本的基础上安装新版本。

*要使用安装文件将 Kaspersky Security Center Linux从 16 或更高版本升级到最新版本：*

1. 从卡巴斯基网站下载包含版本 16.3 的完整软件包的 Kaspersky Security Center Linux 安装文件：
   - 对于运行基于 RPM 的操作系统的设备—`ksc64-<version number>.x86_64.rpm`
   - 对于运行基于 Debian 的操作系统的设备—`ksc64_<version number>_amd64.deb`
2. 开始升级 Kaspersky Security Center Linux。在命令行终端中执行以下命令：
   - 对于运行基于 RPM 的操作系统的设备：

     ```
     sudo yum install ./ksc64-<version number>.x86_64.rpm
     ```

   - 对于运行基于 Debian 的操作系统的设备：

     ```
     sudo apt-get install ./ksc64_<version number>_amd64.deb
     ```

   命令成功执行后，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` 脚本以配置升级后的管理服务器：

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

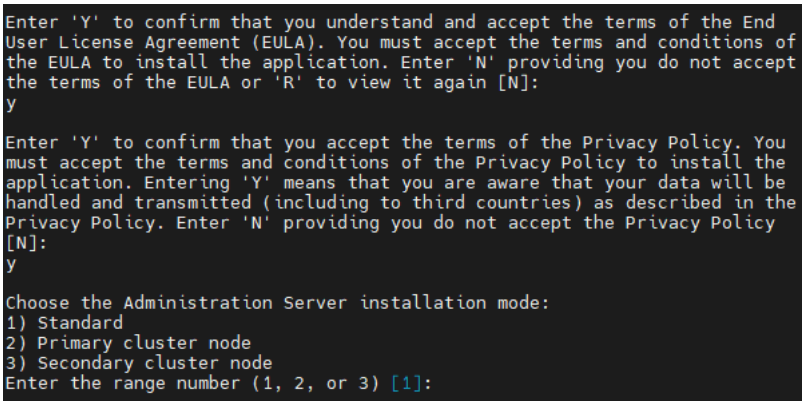
4. 阅读命令行终端中显示的授权许可协议和隐私策略。如果您同意授权许可协议和隐私策略的所有条款：

   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`”以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. 将 Kaspersky Security Center Web Console 升级到新版本。

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

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

   完成远程安装任务后，网络代理版本将升级。
   在基于 Linux 的资产上运行以下命令以删除不再需要的依赖项：

- 对于基于 Debian 的资产，运行以下命令之一：

```
sudo apt-get -y autoremove
sudo apt -y autoremove
```

- 对于基于 RPM 的资产，运行以下命令之一：

```
sudo dnf autoremove
sudo yum autoremove
```

# 通过备份将 Kaspersky Security Center Linux 从 16 版本或更高版本进行升级。

要将管理服务器从版本 16 或者更高版本升级到最新版本，您可以创建管理服务器数据的备份并在安装新版本的 Kaspersky Security Center Linux 后恢复此数据。如果安装期间出现问题，您可以使用升级前创建的管理服务器数据备份恢复先前版本的管理服务器。

*要通过备份将 Kaspersky Security Center Linux 从 16 或更高版本升级到最新版本：*

1. 在升级前，使用旧版本的应用程序备份管理服务器数据。
2. 卸载旧版本的 Kaspersky Security Center Linux。
3. 在之前安装了管理服务器的设备上安装 Kaspersky Security Center Linux 版本 16.3。
   如果备份副本中的数据库架构与管理服务器或 IAM 当前使用的数据库架构不同，数据将还原到当前架构。
   如果备份副本中使用 public 架构，则必须满足以下条件：
   - 数据库中存在 public 数据库架构。
   - 您可以使用管理服务器或 IAM 用于访问数据库的 DBMS 帐户修改 public 数据库架构。

   否则，数据还原将以错误结束。
4. 从升级前创建的备份中恢复管理服务器数据。
5. 安装 Kaspersky Security Center Web Console。
   如果之前安装了 Kaspersky Security Center Web Console，请使用相同的响应文件重新安装它。
   使用管理员的内部用户账户登录 Kaspersky Security Center Web Console。
   恢复管理服务器数据后，数据初始化过程通常需要 15 分钟，但时间取决于硬件性能和管理服务器数据的大小。在此期间，Kaspersky Security Center Web Console 可能无法连接并显示错误。
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。
   在基于 Linux 的资产上运行以下命令以删除不再需要的依赖项：
   - 对于基于 Debian 的资产，运行以下命令之一：

     ```
     sudo apt-get -y autoremove
     sudo apt -y autoremove
     ```
   - 对于基于 RPM 的资产，运行以下命令之一：

     ```
     sudo dnf autoremove
     sudo yum autoremove
     ```

# 在 Kaspersky Security Center Linux 故障转移集群节点上将 Kaspersky Security Center Linux 从版本 16 或者更高版本进行升级

您可以在每个已安装管理服务器版本 16 或更高版本的 Kaspersky Security Center Linux 故障转移集群节点上安装最新版本的管理服务器管理服务器。当升级至最新版本时，上一管理服务器版本的所有数据和设置都将被保留下来。

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

*若要在 Kaspersky Security Center Linux 故障转移集群节点上将 Kaspersky Security Center Linux 从版本 16 或者更高版本进行升级：*

1. 从卡巴斯基网站下载包含版本 16.3 的完整软件包的 Kaspersky Security Center Linux 安装文件：
   - 对于运行基于 RPM 的操作系统的设备—`ksc64-<version number>-<build number>.x86_64.rpm`
   - 对于运行基于 Debian 的操作系统的设备—`ksc64_<version number>-<build number>_amd64.deb`
2. 停止集群。
3. 在集群的活动节点上，在命令行终端中运行以下命令进行升级：
   - 对于运行基于 RPM 的操作系统的设备：

     ```
     sudo yum install ./ksc64-<version number>-<build number>.x86_64.rpm
     ```

   - 对于运行基于 Debian 的操作系统的设备：

     ```
     sudo apt-get install ./ksc64_<version number>-<build number>_amd64.deb
     ```

   命令成功执行后，将创建 `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` 脚本。相关消息显示在终端中。
4. 运行 `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` 脚本以配置升级后的管理服务器：

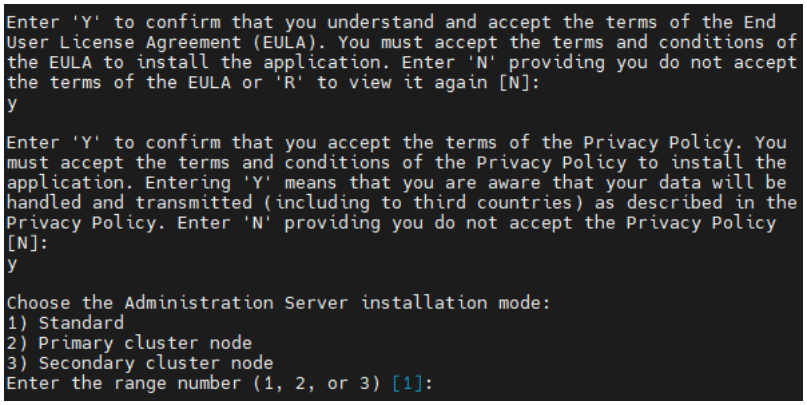
   ```
   sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

5. 阅读命令行终端中显示的授权许可协议和隐私策略。如果您同意授权许可协议和隐私策略的所有条款：
   a. 输入“`Y`”以确认您已完全阅读、理解并接受 EULA 的条款和条件。
   b. 再次输入“`Y`”以确认您已完全阅读、理解并接受描述数据处理的隐私策略。

   在您输入两次“`Y`”后，将继续在您的设备上安装应用程序。

6. 通过输入“2”选择要升级的节点。

   下图显示了最后两个步骤。




接受 EULA 和隐私策略的条款，并在命令行终端中选择安装模式

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

7. 在被动节点上执行步骤 3–5。

   在第 6 步，输入“3”以选择节点。

8. 启动集群。

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

9. 对于安装了早期版本网络代理的设备，请创建并运行新版本网络代理远程安装任务。

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

   完成远程安装任务后，网络代理版本将升级。

   在基于 Linux 的资产上运行以下命令以删除不再需要的依赖项：

   - 对于基于 Debian 的资产，运行以下命令之一：

     ```
     sudo apt-get -y autoremove
     sudo apt -y autoremove
     ```

   - 对于基于 RPM 的资产，运行以下命令之一：

     ```
     sudo dnf autoremove
     sudo yum autoremove
     ```

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

# 将 Kaspersky Security Center Linux 从 15.4 版本或更早版本进行升级

本节介绍将 Kaspersky Security Center Linux 从 15.4 或更早版本升级到 16 或更高版本的以下选项：

- 使用安装文件进行升级
- 通过备份进行升级
- 在 Kaspersky Security Center Linux 故障转移集群节点上升级

Kaspersky Security Center Linux 从 15.4 或更早版本升级到 16 或更高版本的每个升级选项都包括在 DBMS 服务器上创建和配置IAM 数据库、创建非特权“ksciam”帐户来运行 IAM 服务以及将此帐户添加到“kladmins”安全组的步骤。

# 使用安装文件将 Kaspersky Security Center Linux 从 15.4 或更早版本进行升级

要将管理服务器从版本 13—15.4 升级到版本 16 或者更高版本，您可以使用 Kaspersky Security Center Linux 安装文件在早期版本的基础上安装新版本。

开始之前， **查看自自定义证书的要求**。

如果您使用的是自定义证书而不是自签名证书，则在将 Kaspersky Security Center Linux 升级到更高版本之前，必须确保证书包含主题备用名称 (SAN)。如果没有，在升级 Kaspersky Security Center Linux 之前替换证书至关重要。否则，升级后您将无法登录 Web Console。

*要确保证书包含 SAN：*

1. 在安装了管理服务器的设备上，执行命令：
   - 对于 Linux 设备：

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout
     -ext subjectAltName
     ```

   - 对于 Windows 设备：

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. 请确保命令输出中包含“使用者备用名称”，并且名称包含管理服务器设备的地址。
3. 如果缺少“使用者备用名称”，请使用 klsetsrvcert 实用程序将自定义证书替换为符合要求的证书。

*要使用安装文件将 Kaspersky Security Center Linux 从 15.4 或更早版本升级到最新版本：*

1. 从卡巴斯基网站下载包含版本 16.3 的完整软件包的 Kaspersky Security Center Linux 安装文件：
   - 对于运行基于 RPM 的操作系统的设备—`ksc64-<version number>.x86_64.rpm`
   - 对于运行基于 Debian 的操作系统的设备—`ksc64_<version number>_amd64.deb`
2. 在 DBMS 服务器上，创建一个 IAM 数据库。IAM 名称必须与管理服务器使用的数据库名称不同。
   - 对于 PostgreSQL，请运行以下命令：

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
     ```

   - 对于 MariaDB，请运行以下命令：

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
     ```

3. 创建一个名为“ksciam”的非特权帐户，将其添加到“kladmins”安全组，然后将“kladmins”组设置为“ksciam”帐户的主组。为此，请依次运行以下命令：

   ```
   sudo adduser ksciam
   sudo gpasswd -a ksciam kladmins
   sudo usermod -g kladmins ksciam
   ```

4. 开始升级 Kaspersky Security Center Linux。在命令行终端中执行以下命令：
   - 对于运行基于 RPM 的操作系统的设备：

     ```
     sudo yum install ./ksc64-<版本号>.x86_64.rpm
     ```

   - 对于运行基于 Debian 的操作系统的设备：

     ```
     sudo apt-get install ./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。
5. 运行 `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` 脚本来配置升级的管理服务器。

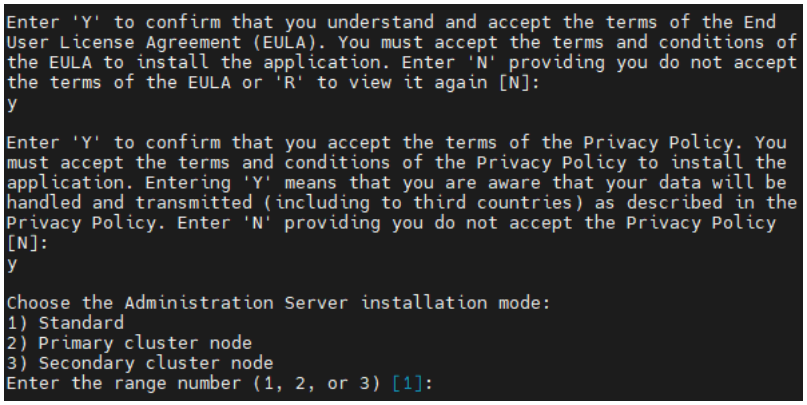
   ```
   sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

6. 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。

7. 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

8. 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。出现提示时，输入以下设置：

   a. 输入 IAM Server FQDN。

      您必须使用安装 Kaspersky Security Center Linux 时指定的管理服务器 DNS 名称。

   b. 输入用于启动 IAM 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“ksciam”账户。

   c. 选择您安装的与 IAM 服务一起使用的 DBMS：

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

   d. 输入 IAM 服务要使用的 IAM DBMS 地址。

   e. 输入 IAM DBMS 端口号。该端口用于与 IAM 服务通信。默认情况下，使用以下端口：

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

   f. 输入 IAM 服务要使用的 IAM 数据库名称。IAM 服务使用的数据库名称应与管理服务器使用的数据库名称不同。

   g. 输入 IAM 服务要使用的 DBMS 登录名和密码。

   h. 如果您安装了 PostgreSQL 或 Postgres Pro，则可以指定 IAM 要使用的数据库架构。为此，请指定架构名称。

      如果您不想使用自定义架构，请按 `ENTER`，将使用 public 架构。

      > 架构名称区分大小写：必须仅使用小写字母。
      > 请勿指定保留的 iam 架构名称：`client, iam, ksc, locker, pat, scope, voltron`。

9. 将 Kaspersky Security Center Web Console 升级到新版本。

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

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

完成远程安装任务后，网络代理版本将升级。

在基于 Linux 的资产上运行以下命令以删除不再需要的依赖项：

- 对于基于 Debian 的资产，运行以下命令之一：

```
sudo apt-get -y autoremove
sudo apt -y autoremove
```

- 对于基于 RPM 的资产，运行以下命令之一：

```
sudo dnf autoremove
sudo yum autoremove
```

# 通过备份将 Kaspersky Security Center Linux 从 15.4 或更早版本进行升级。

要将管理服务器从 14.2—15.4 版本升级到版本 16 或更高版本，您可以创建管理服务器数据的备份，并在安装新版本的 Kaspersky Security Center Linux 后将其恢复。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。

先决条件

1. **请检查自定义证书的要求**。

   如果您使用的是自定义证书而不是自签名证书，则在将 Kaspersky Security Center Linux 升级到更高版本之前，必须确保证书包含主题备用名称 (SAN)。如果没有，在升级 Kaspersky Security Center Linux 之前替换证书至关重要。否则，升级后您将无法登录 Web Console。

   *要确保证书包含 SAN：*

   1. 在安装了管理服务器的设备上，执行命令：

      - 对于 Linux 设备：

        ```
        sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
        ```

      - 对于 Windows 设备：

        ```
        certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
        ```

   2. 请确保命令输出中包含“使用者备用名称”，并且名称包含管理服务器设备的地址。

   3. 如果缺少“使用者备用名称”，请使用 klsetsrvcert 实用程序将自定义证书替换为符合要求的证书。

2. 使用旧版本的应用程序备份管理服务器数据。

升级过程

*要通过备份将 Kaspersky Security Center Linux 从 15.4 或更早版本升级到最新版本：*

1. 卸载旧版本的 Kaspersky Security Center Linux。
2. 在 DBMS 服务器上，创建一个 IAM 数据库。IAM 名称必须与管理服务器使用的数据库名称不同。
   - 对于 PostgreSQL，请运行以下命令：

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
     ```

   - 对于 MariaDB，请运行以下命令：

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
     ```

3. 创建一个名为“ksciam”的非特权帐户，将其添加到“kladmins”安全组，然后将“kladmins”组设置为“ksciam”帐户的主组。为此，请依次运行以下命令：

   ```
   sudo adduser ksciam
   sudo gpasswd -a ksciam kladmins
   sudo usermod -g kladmins ksciam
   ```

4. 在之前安装了管理服务器的设备上安装 Kaspersky Security Center Linux 版本 16.3。
   如果备份副本中的数据库架构与管理服务器或 IAM 当前使用的数据库架构不同，数据将还原到当前架构。
   如果备份副本中使用 public 架构，则必须满足以下条件：
   - 数据库中存在 public 数据库架构。
   - 您可以使用管理服务器或 IAM 用于访问数据库的 DBMS 帐户修改 public 数据库架构。

   否则，数据还原将以错误结束。
5. 从升级前创建的备份中恢复管理服务器数据。
6. 配置管理服务器和 IAM 服务器的证书验证。
7. 安装 Kaspersky Security Center Web Console。
   如果之前安装了 Kaspersky Security Center Web Console，请使用相同的响应文件重新安装它。
   使用管理员的内部用户账户登录 Kaspersky Security Center Web Console。
   恢复管理服务器数据后，数据初始化过程通常需要 15 分钟，但时间取决于硬件性能和管理服务器数据的大小。在此期间，Kaspersky Security Center Web Console 可能无法连接并显示错误。
8. 对于安装了更早版本网络代理的设备，创建并运行用于远程安装新版本网络代理的任务。

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

   完成远程安装任务后，网络代理版本将升级。

在基于 Linux 的资产上运行以下命令以删除不再需要的依赖项：

- 对于基于 Debian 的资产，运行以下命令之一：

```
sudo apt-get -y autoremove
sudo apt -y autoremove
```

- 对于基于 RPM 的资产，运行以下命令之一：

```
sudo dnf autoremove
sudo yum autoremove
```

# 在 Kaspersky Security Center Linux 故障转移集群节点上将 Kaspersky Security Center Linux 从版本 15.4 或者更早版本进行升级

您可以在每个已安装管理服务器版本 14—15.4 的Kaspersky Security Center Linux 故障转移集群节点上安装管理服务器版本 16 或更高版本。当升级时，上一管理服务器版本的所有数据和设置都将被保留下来。

开始之前，**查看自自定义证书的要求**。

如果您使用的是自定义证书而不是自签名证书，则在将 Kaspersky Security Center Linux 升级到更高版本之前，必须确保证书包含主题备用名称 (SAN)。如果没有，在升级 Kaspersky Security Center Linux 之前替换证书至关重要。否则，升级后您将无法登录 Web Console。

*要确保证书包含 SAN：*

1. 在安装了管理服务器的设备上，执行命令：

   - 对于 Linux 设备：

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout
     -ext subjectAltName
     ```

   - 对于 Windows 设备：

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. 请确保命令输出中包含“使用者备用名称”，并且名称包含管理服务器设备的地址。

3. 如果缺少“使用者备用名称”，请使用 klsetsrvcert 实用程序将自定义证书替换为符合要求的证书。

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

*若要在 Kaspersky Security Center Linux 故障转移集群节点上将 Kaspersky Security Center Linux 从版本 15.4 或者更早版本进行升级：*

1. 从卡巴斯基网站下载包含版本 16.3 的完整软件包的 Kaspersky Security Center Linux 安装文件：
   - 对于运行基于 RPM 的操作系统的设备——`ksc64-<version number>-<build number>.x86_64.rpm`
   - 对于运行基于 Debian 的操作系统的设备——`ksc64_<version number>-<build number>_amd64.deb`
2. 停止集群。
3. 在 DBMS 服务器上，创建一个 IAM 数据库。IAM 名称必须与管理服务器使用的数据库名称不同。
   - 对于 PostgreSQL，请运行以下命令：

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
     ```

   - 对于 MariaDB，请运行以下命令：

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
     ```

4. 创建一个名为“ksciam”的非特权帐户，将其添加到“kladmins”安全组，然后将“kladmins”组设置为“ksciam”帐户的主组。为此，请依次运行以下命令：

   ```
   sudo adduser ksciam
   sudo gpasswd -a ksciam kladmins
   sudo usermod -g kladmins ksciam
   ```

5. 在集群的活动节点上，在命令行终端中运行以下命令之一以开始升级：
   - 对于运行基于 RPM 的操作系统的设备：

     ```
     sudo yum install ./ksc64-<版本号>-<内部版本号>.x86_64.rpm
     ```

   - 对于运行基于 Debian 的操作系统的设备：

     ```
     sudo apt-get install ./ksc64_<版本号>-<内部版本号>_amd64.deb
     ```

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

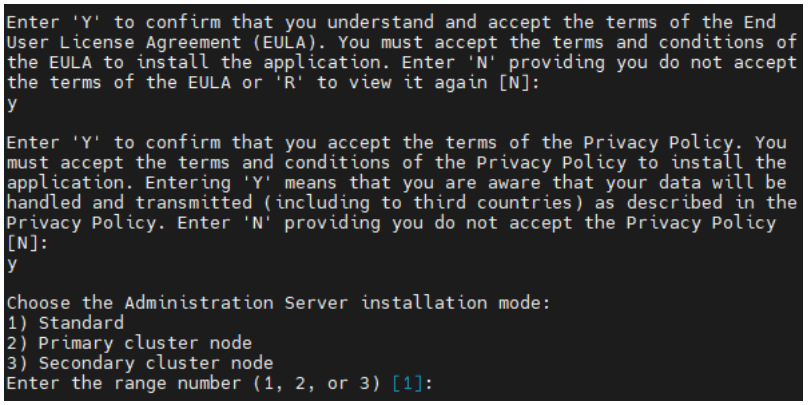
   ```
   sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

7. 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。

8. 通过输入“2”选择要升级的节点。

   下图显示了最后两个步骤。




接受 EULA 和隐私策略的条款，并在命令行终端中选择安装模式

9. 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。出现提示时，输入以下设置：

   a. 输入 IAM Server FQDN。

      您必须使用安装 Kaspersky Security Center Linux 时指定的管理服务器 DNS 名称。

   b. 输入用于启动 IAM 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“ksciam”账户。

   c. 选择您安装的与 IAM 服务一起使用的 DBMS：

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

   d. 输入 IAM 服务要使用的 IAM DBMS 地址。

   e. 输入 IAM DBMS 端口号。该端口用于与 IAM 服务通信。默认情况下，使用以下端口：

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

   f. 输入 IAM 服务要使用的 IAM 数据库名称。IAM 服务使用的数据库名称应与管理服务器使用的数据库名称不同。

   g. 输入 IAM 服务要使用的 DBMS 登录名和密码。

10. 在被动节点上执行步骤 5。

    在第 6 步，输入“3”以选择节点。

11. 启动集群。

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

12. 对于安装了早期版本网络代理的设备，请创建并运行新版本网络代理远程安装任务。

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

完成远程安装任务后，网络代理版本将升级。

在基于 Linux 的资产上运行以下命令以删除不再需要的依赖项：

- 对于基于 Debian 的资产，运行以下命令之一：

```
sudo apt-get -y autoremove
sudo apt -y autoremove
```

- 对于基于 RPM 的资产，运行以下命令之一：

```
sudo dnf autoremove
sudo yum autoremove
```

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

# 升级 Kaspersky Security Center Web Console

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

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

使用与您设备上安装的 Linux 发行版对应的以下安装文件之一：

- 对于基于 Debian 的操作系统: 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

您通过从 Kaspersky 网站下载来接收安装文件。

*要升级 Kaspersky Security Center Web Console：*

1. 确保您要安装 Kaspersky Security Center Web Console 的设备运行以下一种受支持的 Linux 分类。
2. 阅读并接受最终用户授权许可协议 (EULA)。如果 Kaspersky Security Center Linux 分发包不包含带有 EULA 文本的 TXT 文件，您可以从 卡巴斯基网站 下载文件。如果您不接受授权许可协议的条款，请勿使用安装文件升级 Kaspersky Security Center Web Console。
3. 使用您在安装 Kaspersky Security Center Web Console 之前准备的相同响应文件。响应文件名称为 ksc-web-console-setup.json，文件位置为 /etc/ksc-web-console-setup.json。

如果您在安装 Kaspersky Security Center Web Console 时指定了 `webConsoleAccount`、`managementServiceAccount`、`serviceWebConsoleAccount`、`pluginAccount` 和 `natsMessageQueueAccount` 参数的值，请确保响应文件中指定了所有这些参数。

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

**包含最小参数集的响应文件示例**

响应文件的参数集取决于 Kaspersky Security Center Web Console 连接的管理服务器的版本：

- 16 或更高版本的管理服务器

  登录管理服务器版本 16 或更高版本所需的最小参数集的响应文件示例：

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
        "Administration Server v16": {
            "iamHost": "ksc16.example.com",
            "iamOAuthPort": 4444,
            "iamProxyPort": 9050,
            "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
            "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
            "kscPort": 13299,
            "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

- 15.4 或更早版本的管理服务器

  登录管理服务器版本 15.4 或更早版本所需的最小参数集的响应文件示例：

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

您可以将 Kaspersky Security Center Web Console 安装在与管理服务器相同或不同的设备上。如果将 Kaspersky Security Center Web Console 安装在另一台设备上，则 Kaspersky Security Center Web Console 地址（由 `address` 指定）和管理服务器地址（由 `iamHost` 或 `kscHost` 指定）不同。如果将 Kaspersky Security Center Web Console 与管理服务器安装在同一设备上，则这些参数具有相同的值。

`iamHost`值必须与您在安装管理服务器时指定的 IAM 地址匹配。若要获取指定的 IAM 地址，请在安装了管理服务器的设备上运行以下命令：

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

有关详细信息，请参阅文章：Kaspersky Security Center Web Console 安装参数。

您可以将多个不同版本的管理服务器添加到受信任服务器列表中。在此情况下，服务器可以使用不同的身分验证方法。

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

`trusted` **安装参数**的组成部分

如果您使用域身份验证和单点登录连接到 Kaspersky Security Center Linux 故障转移集群，请按如下方式指定受信任的安装参数：如果您将 Kaspersky Security Center Web Console 连接到管理服务器版本 16 或更高版本，则将使用Identity and Access Manager (IAM)提供的域身份验证和单点登录 (SSO)。在此情况下，请按如下方式指定 `trusted` 安装参数：

```
"trusted":  {
  "<管理服务器名称>": {
    "iamHost": "ksc-iam.example.com",
    "iamOAuthPort": 4444,
    "iamProxyPort": 9050,
    "iamCertPath": "<共享数据文件夹>/iam/main_certificate.pem",
    "iamPATPath": "<共享数据文件夹>/iam/initial_token.txt",
    "kscPort": 13299,
    "kscCertPath": "<共享数据文件夹>/1093/cert/klserver.cer"
  }
}
```

其中：

- < 管理服务器名称 > 是将显示在 Kaspersky Security Center Web Console 登录窗口中的 Kaspersky Security Center Linux 故障转移集群名称。
- `iamHost` 是安装管理服务器和 IAM 的设备的地址。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 FQDN 或主机名称作为 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均衡器的 FQDN 或主机名称。

  `iamHost` 值必须与安装管理服务器时指定的 IAM 地址匹配。若要获取指定的 IAM 地址，请在管理服务器主机上运行以下命令：

  ```
  grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
  ```

- `iamOAuthPort` 是用于通过 OpenID Connect 身份验证协议交换身份验证令牌的端口（默认值为 4444）。此端口用于 Kaspersky Security Center Web Console 服务器和管理服务器之间的通讯，以及浏览器（与 Kaspersky Security Center Web Console 配合使用）和管理服务器之间的通讯。
- `iamProxyPort` 是用于将 Kaspersky Security Center Web Console 服务器连接到管理服务器的端口（默认值为 9050）。
- `iamCertPath` 是 IAM 证书的路径。IAM 证书会在您首次运行管理服务器时自动创建。证书位于安装管理服务器的设备上。证书的默认路径为：< 共享数据文件夹 >`/iam/main_certificate.pem`。该证书位于 Kaspersky Security Center Linux 故障转移集群的共享数据存储中。自签名 IAM 证书会自动轮换。
- `iamPATPath` 是将 Kaspersky Security Center Web Console 注册为 IAM 中的 OAuth 客户端时所用令牌的路径。该文件会在您首次运行管理服务器时生成。令牌位于安装管理服务器的设备上。令牌的默认路径：<共享数据文件夹>/iam/initial_token.txt。该令牌位于 Kaspersky Security Center Linux 故障转移集群的共享数据存储中。该令牌永久有效，无需轮换。
- `kscPort` 是 Kaspersky Security Center Web Console 用于连接到管理服务器的 OpenAPI 端口（默认值为 13299）。
- `kscCertPath` 是位于 Kaspersky Security Center Linux 故障转移集群的共享数据存储中的管理服务器证书。证书文件的默认路径为：< 共享数据文件夹 >`\1093\cert\klserver.cer`。

  将管理服务器证书文件（由 `kscCertPath` 指定）、IAM 证书文件（由 `iamCertPath` 指定）和令牌文件（由 `iamPATPath` 指定）从共享数据存储复制到安装 Kaspersky Security Center Web Console 的设备。指定管理服务器证书的本地路径。

如果将 Kaspersky Security Center Web Console 连接到管理服务器版本 15.4 或更早版本，则将使用指定域用户或内部用户的名称和密码进行身份验证。在这种情况下，请按如下方式指定受信任的安装参数：

```
"trusted":  {
  "<管理服务器名称>": {
    "kscHost": "ksc.example.com",
    "kscPort": 13299,
    "kscCertPath": "<共享数据文件夹>/1093/cert/klserver.cer"
  }
}
```

其中：

- < 管理服务器名称 > 是将显示在 Kaspersky Security Center Web Console 登录窗口中的 Kaspersky Security Center Linux 故障转移集群名称。
- `kscHost` 是管理服务器地址（FQDN 或主机名）。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地址。
- `kscPort` 是 Kaspersky Security Center Web Console 用于连接到管理服务器的 OpenAPI 端口（默认值为 13299）。
- `kscCertPath` 是位于 Kaspersky Security Center Linux 故障转移集群的共享数据存储中的管理服务器证书。证书文件的默认路径为：< 共享数据文件夹 >`\1093\cert\klserver.cer`。将证书文件从共享数据存储复制到安装 Kaspersky Security Center Web Console 的设备。指定管理服务器证书的本地路径。

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

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

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

   - 对于运行基于 RPM 的操作系统的设备：
     ```
     sudo yum install ksc-web-console-<build_number>.x86_64.rpm
     ```
   - 对于运行基于 Debian 的操作系统的设备：
     ```
     sudo apt-get install ksc-web-console-<build_number>.x86_64.deb
     ```

   这将开始解包安装文件。请等待安装完成。

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

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

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

该文描述了如何升级 Kaspersky Security Center Web Console 服务器 (也叫 Kaspersky Security Center Web Console) 到 Astra Linux 特别版操作系统。

*要升级 Kaspersky Security Center Web Console：*

1. 确保您要安装 Kaspersky Security Center Web Console 的设备运行以下一种受支持的 Linux 分类。

2. 阅读并接受最终用户授权许可协议 (EULA)。如果 Kaspersky Security Center Linux 分发包不包含带有 EULA 文本的 TXT 文件，您可以从 卡巴斯基网站 下载文件。如果您不接受授权许可协议的条款，请勿使用安装文件升级 Kaspersky Security Center Web Console。

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

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

   **包含最小参数集的响应文件示例**

   响应文件的参数集取决于 Kaspersky Security Center Web Console 连接的管理服务器的版本：

   - 16 或更高版本的管理服务器

     登录管理服务器版本 16 或更高版本所需的最小参数集的响应文件示例：

     ```
     {
         "address": "ksc-web-console.example.com",
         "port": 8080,
         "trusted":  {
             "Administration Server v16": {
                 "iamHost": "ksc16.example.com",
                 "iamOAuthPort": 4444,
                 "iamProxyPort": 9050,
                 "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
                 "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
                 "kscPort": 13299,
                 "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
             }
         },
         "certDomain":"ksc-web-console.example.com",
         "acceptEula": true
     }
     ```

   - 15.4 或更早版本的管理服务器

     登录管理服务器版本 15.4 或更早版本所需的最小参数集的响应文件示例：

     ```
     {
         "address": "ksc-web-console.example.com",
         "port": 8080,
         "trusted":  {
              "Administration Server v15.4": {
                  "kscHost": "ksc.example.com",
                  "kscPort": 13299,
                  "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
              }
         },
         "certDomain":"ksc-web-console.example.com",
         "acceptEula": true
     }
     ```

   您可以将 Kaspersky Security Center Web Console 安装在与管理服务器相同或不同的设备上。如果将 Kaspersky Security Center Web Console 安装在另一台设备上，则 Kaspersky Security Center Web Console 地址（由 `address` 指定）和管理服务器地址（由 `iamHost` 或 `kscHost` 指定）不同。如果将 Kaspersky Security Center Web Console 与管理服务器安装在同一设备上，则这些参数具有相同的值。

   `iamHost` 值必须与您在安装管理服务器时指定的 IAM 地址匹配。若要获取指定的 IAM 地址，请在安装了管理服务器的设备上运行以下命令：

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

有关详细信息，请参阅文章：Kaspersky Security Center Web Console 安装参数。

您可以将多个不同版本的管理服务器添加到受信任服务器列表中。在此情况下，服务器可以使用不同的身分验证方法。

4. 确保在 `/etc/digsig/digsig_initramfs.conf` 文件中，`DIGSIG_ELF_MODE` 参数按如下方式指定：

   ```
   DIGSIG_ELF_MODE=1
   ```

5. 确保已安装 `astra-digsig-oldkeys` 兼容性软件包。

   如果未安装此软件包，请运行以下命令：

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

6. 为应用程序密钥创建一个目录（如果不存在）：

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

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

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

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

8. 更新 RAM 磁盘：

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

   重新启动系统。

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

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

   ```
   sudo apt-get install ksc-web-console-<版本号>.x86_64.deb
   ```

   这将开始解包安装文件。请等待安装完成。

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

    ```
    sudo systemctl restart KSC*
    ```

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

# 迁移到 Kaspersky Security Center Linux

通过使用管理服务器数据备份（使用klbackup 实用程序）和迁移向导，可以从 Kaspersky Security Center Windows 迁移到 Kaspersky Security Center Linux。

借助下表，您可以比较使用管理服务器数据备份和迁移向导进行迁移的主要功能和限制，以便为组织选择更合适的方案。

迁移方法比较

| 参数 | 管理服务器数据备份 | 迁移向导 |
| --- | --- | --- |
| 迁移过程 | 创建 Kaspersky Security Center Windows 管理服务器数据的完整备份并将其恢复到 Kaspersky Security Center Linux 管理服务器上 | 选择并导出管理服务器数据进行迁移，将这些数据导入 Kaspersky Security Center Linux 管理服务器，并将受管理设备切换至 Kaspersky Security Center Linux 管理之下 |
| 迁移方法的特点 | • 迁移所有管理服务器数据<br>• 迁移任意数量的受管理设备<br>• 用于获取 Kaspersky Security Center Windows 管理服务器数据的完整副本并将其传输到 Kaspersky Security Center Linux 管理服务器 | • 部分迁移管理服务器数据<br>• 可以选择要迁移的对象<br>• 要迁移的管理组或子组最多可包含 10,000 个设备<br>• 用于部分传输管理服务器数据，仅包括迁移范围内的组对象；迁移范围之外的组对象必须手动恢复 |
| 迁移范围 | 管理服务器数据的完整传输，受管理设备数量不受限制 | • 管理组结构<br>• 管理组中包含的受管理设备（**不超过 10,000 台设备**）<br>• 分配给迁移设备的标签<br>• 网络代理和受管理应用程序的全局任务（不适用于管理服务器）<br>• 网络代理和受管理应用程序的组任务<br>• 受管理应用程序的策略<br>• 报告模板<br>• 用户角色<br>• 内部用户和安全组<br>• 含有手动添加内容的自定义应用程序类别<br>• 自定义设备分类 |
| 未迁移范围 | — | • 管理服务器的全局任务<br>• 保存在管理服务器上的事件<br>• 远程安装的应用程序分发包的存储库<br>• 管理服务器证书<br>• 管理服务器和受管理应用程序使用的授权许可密钥<br>• 虚拟管理服务器<br>• 网络代理策略设置<br>• 设备移动规则<br>• 设备自动标记规则<br>• 分发点<br>• 管理服务器上保存的卡巴斯基应用程序设置 |
| 支持迁移的 Kaspersky Security Center 版本 | • 任何受支持的 Kaspersky Security Center Windows 版本<br>• Kaspersky Security Center Linux 版本 15.2 或更高版本 | • Kaspersky Security Center Windows 版本 14.2 或更高版本<br>• Kaspersky Security Center Linux 版本 15 或更高版本 |
| 可以进行迁移的 DBMS | • Microsoft SQL Server → MySQL、MariaDB<br>• Microsoft SQL Server → PostgreSQL、Postgres Pro （仅适用于从已安装补丁的 Kaspersky Security Center Windows 版本 14.2 或更高版本迁移至 Kaspersky Security Center Linux 版本 15.3 或更高版本）<br>• MySQL → MySQL、MariaDB<br>• MariaDB → MySQL、MariaDB<br>• PostgreSQL → PostgreSQL<br>Postgres Pro → Postgres Pro（仅适用于从Kaspersky Security Center Windows 版本 15.1 或更高版本迁移到 Kaspersky Security Center Linux 版本 16 或更高版本） | 在受支持的 DBMS之间无限制迁移 |

# 使用管理服务器数据备份迁移到 Kaspersky Security Center Linux

您可以使用数据备份将 Kaspersky Security Center Windows 管理服务器数据迁移至 Kaspersky Security Center Linux。迁移之前，请确保Kaspersky Security Center Windows 的必要功能在 Kaspersky Security Center Linux 中受支持。

为了清楚起见，我们提供了一个教程视频，介绍如何使用备份将管理服务器数据迁移到Kaspersky Security Center Linux。

限制

- 迁移可以在以下 DBMS 之间进行：
  - Microsoft SQL Server → MySQL、MariaDB
  - Microsoft SQL 服务器 → PostgreSQL、 Postgres Pro
  - MySQL → MySQL、MariaDB
  - MariaDB → MySQL、MariaDB
  - PostgreSQL → PostgreSQL
  - Postgres Pro → Postgres Pro
- 支持将存储在 Microsoft SQL Server、MySQL 或 MariaDB 数据库中的管理服务器数据从任何受支持的 Kaspersky Security Center Windows 版本 迁移到 Kaspersky Security Center Linux 版本 15.2 或更高版本。
- 当从 Kaspersky Security Center Windows 版本 15.1 或更高版本迁移到 Kaspersky Security Center Linux 版本 16 或更高版本时，支持将存储在 PostgreSQL 数据库中的管理服务器数据迁移至 PostgreSQL 或 Postgres Pro。
- 当从 Kaspersky Security Center Windows 版本 14.2 或更高版本迁移到Kaspersky Security Center Linux 版本 15.3 或更高版本时，支持将存储在 Microsoft SQL Server 数据库中的管理服务器数据迁移至 PostgreSQL 或 Postgres Pro。

  为支持迁移到 PostgreSQL 或 Postgres Pro，您必须向卡巴斯基技术支持提出请求并安装以下补丁之一：
  - 对于 Kaspersky Security Center 14.2 Windows：14.2.0.26967-pf5
  - 对于基于 Kaspersky Security Center 14.2 Windows 的 Kaspersky Secure Mobility Management：14.2.0.48079-pf5
  - 对于 Kaspersky Security Center 15.1 Windows：15.1.0.20748-pf2

    将 Kaspersky Security Center Windows 更新至版本 15.1.0.22239 后，也可以迁移到 PostgreSQL 或 Postgres Pro。

- 如果您使用 MySQL 或 MariaDB 作为 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux 的 DBMS，则`lower_case_table_names`参数必须与当前和新的 DBMS 匹配。

  在创建数据备份之前，请检查`lower_case_table_names`参数。随后，在为 Kaspersky Security Center Linux 安装 MySQL 或 MariaDB 时，必须将此参数的值设置为与 Windows 版一致。

## 先决条件

开始之前，**查看自自定义证书的要求**。

如果您使用的是自定义证书而不是自签名证书，则在将 Kaspersky Security Center Linux 升级到更高版本之前，必须确保证书包含主题备用名称 (SAN)。如果没有，在升级 Kaspersky Security Center Linux 之前替换证书至关重要。否则，升级后您将无法登录 Web Console。

*要确保证书包含 SAN：*

1. 在安装了管理服务器的设备上，执行命令：

   - 对于 Linux 设备：

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout
     -ext subjectAltName
     ```

   - 对于 Windows 设备：

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. 请确保命令输出中包含“使用者备用名称”，并且名称包含管理服务器设备的地址。

3. 如果缺少“使用者备用名称”，请使用 klsetsrvcert 实用程序将自定义证书替换为符合要求的证书。

## 阶段

使用管理服务器数据备份进行分阶段迁移：

1. **检查您是否拥有管理员的内部用户账户，以便可以登录管理服务器**

   管理员账户将用于登录 Kaspersky Security Center Linux 管理服务器。如果您没有此账户，并且仅在本地 Windows 账户或域账户下登录，则恢复备份后将无法登录 Kaspersky Security Center Linux 管理服务器。Kaspersky Security Center Linux 管理服务器不支持使用本地 Windows 账户登录。可以使用域账户登录，但可能需要对管理服务器进行额外配置。

   如果您没有管理员账户，则必须在使用 kladduser 实用程序恢复备份副本后创建此账户。

2. **创建 Kaspersky Security Center Windows 管理服务器数据的最新备份副本**

   根据 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux 使用的 DBMS 类型，执行以下操作之一：

   - 对于将 MySQL 或 MariaDB 迁移到 MySQL 或 MariaDB：在安装了管理服务器的设备上使用klbackup 实用程序 或数据备份任务 创建备份副本。

   - 要将 PostgreSQL 迁移到 PostgreSQL 和将 Postgres Pro 迁移到 Postgres Pro：在已安装管理服务器的设备上使用 klbackup 实用程序 或数据备份任务 来创建备份副本。

- 对于将 Microsoft SQL Server 迁移到 MySQL 或 MariaDB：使用 klbackup 实用程序来创建备份副本，并启用“**迁移到 MySQL/MariaDB 格式**”选项。
- 对于将 Microsoft SQL Server 迁移到 PostgreSQL 或 Postgres Pro：

  1. 安装管理服务器补丁以支持迁移到 PostgreSQL 和 Postgres Pro。联系卡巴斯基技术支持以获取此补丁。

     对于 Kaspersky Security Center 15.1 Windows，您可以更新至版本 15.1.0.22239，而非安装补丁。

  2. 使用 klbackup 实用程序创建备份副本。

     如果从命令行运行 klbackup，请使用 `-migrate postgres` 标志。

     如果使用 klbackup 界面，请启用“**迁移到 Postgres 格式**”选项。

创建备份副本后，断开 Kaspersky Security Center Windows 管理服务器与网络的连接。

### 3 准备一台新设备用于安装 Kaspersky Security Center Linux

在方案的该步骤，执行以下操作：

1. 选择要安装管理服务器的新设备。该设备必须满足硬件和软件要求。此外，请检查管理服务器上使用的端口是否可用。
2. 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）。

### 4 安装和配置 DBMS

在方案的该步骤，执行以下操作：

1. 选择提供最佳性能的 DBMS 类型。考虑联网设备的数量、网络拓扑和网络工作负载。您可以选择任何受支持的 DBMS。
2. 根据创建备份时选择的 DBMS 类型安装 DBMS。对于如何安装所选 DBMS 的信息，请参考其文档。

   为 IAM 手动创建数据库。

   > 新的数据库版本不得低于当前数据库版本。

3. 配置与 Kaspersky Security Center Linux 配合使用的 DBMS：

- 配置与 Kaspersky Security Center Linux 配合使用的 MariaDB x64 服务器
- 配置与 Kaspersky Security Center Linux 配合使用的 PostgreSQL 或 Postgres Pro 服务器
- 配置与 Kaspersky Security Center Linux 配合使用的 MySQL x64 服务器

### 5 安装 Kaspersky Security Center Linux

在新设备上安装 Kaspersky Security Center Linux。

安装期间创建的管理员内部用户账户以及从备份恢复管理服务器数据之前创建的其他对象（组、策略、组任务、用户）将在恢复后丢失。这些对象将被备份中包含的容器替换。

### 6 从备份副本恢复管理服务器数据

在方案的该步骤，执行以下操作：

1. 使用klbackup 实用程序在新设备上恢复管理服务器数据。

   由于PostgreSQL 的限制，您需要临时授予管理服务器用于连接 DBMS 的账户 PostgreSQL 超级用户权限。

2. 如果您没有用于登录 Kaspersky Security Center Windows 管理服务器的管理员内部用户账户，并且使用了本地 Windows 账户或域账户，请使用 kladduser 实用程序创建管理员账户，如下所示：

   ```
   /opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <密码>
   ```

   其中<密码>参数满足以下要求：

   - 用户密码不能少于 8 个字符或超过 256 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 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

7. **配置管理服务器和 IAM 服务器的证书验证。**

8. **安装 Kaspersky Security Center Web Console 和配置管理服务器**

   在方案的该步骤，执行以下操作：

   1. 安装 Kaspersky Security Center Web Console。

      如果之前安装了 Kaspersky Security Center Web Console，请使用相同的响应文件重新安装它。

      使用管理员的内部用户账户登录 Kaspersky Security Center Web Console。

      恢复管理服务器数据后，数据初始化过程通常需要 15 分钟，但时间取决于硬件性能和管理服务器数据的大小。在此期间，Kaspersky Security Center Web Console 可能无法连接并显示错误。

   2. 当数据库中的数据初始化完成后，检查主要管理服务器功能是否正常。验证管理服务器是否与受管理设备同步以及管理服务器数据是否已恢复。

   3. 轮询域控制器可恢复有关域中包含的设备的域结构、用户账户、安全组和 DNS 名称的信息。

   4. 查看已迁移的任务。如果其任何参数包含 Windows 文件路径，则将其替换为相应的 Linux 文件路径。

   5. 如有必要，从以前的设备中卸载管理服务器和数据库服务器。

      在同一个网络上，不能存在多个管理服务器共享相同连接地址和管理服务器证书的情况。

管理员有权访问原 Kaspersky Security Center Windows 中的管理服务器数据及受管理设备，同时需确保相关功能在 Kaspersky Security Center Linux 受支持。

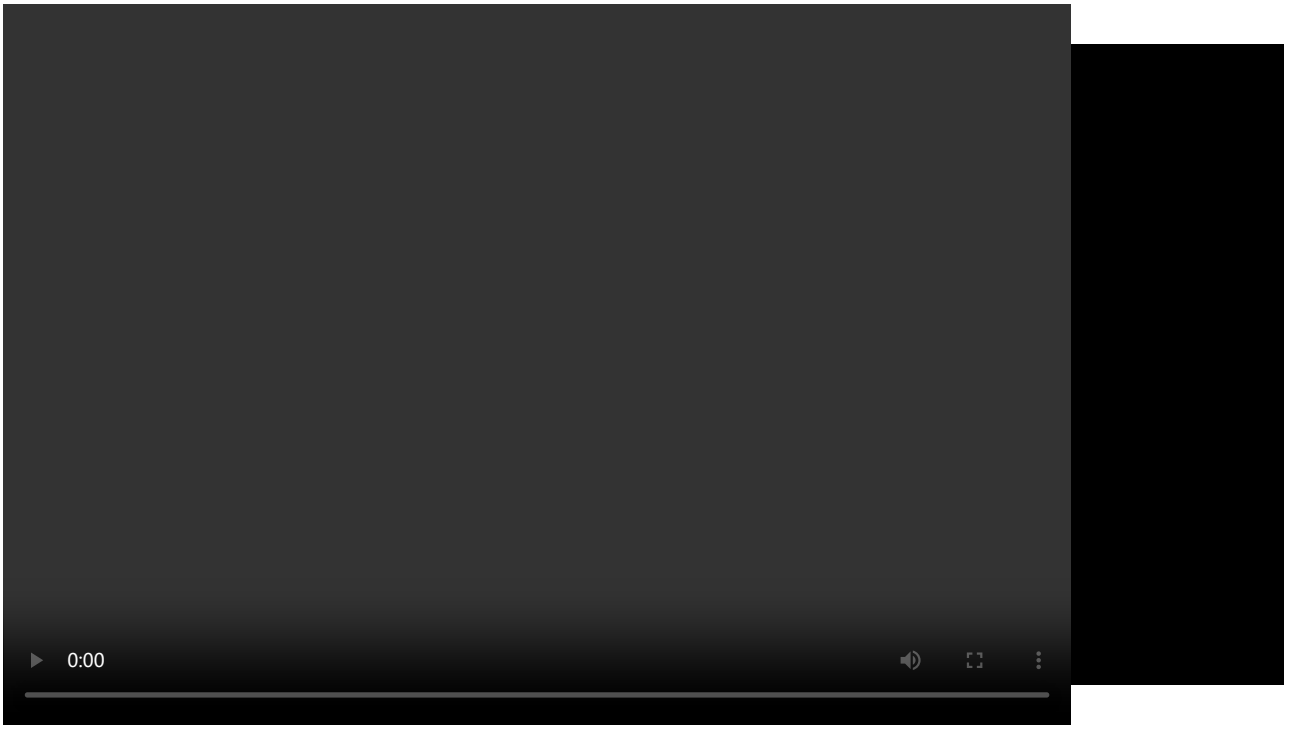
# 教程视频：使用管理服务器数据备份迁移到 Kaspersky Security Center Linux

观看视频，了解如何使用管理服务器数据备份（使用klbackup 实用程序）将 Kaspersky Security Center Windows 管理服务器数据迁移到 Kaspersky Security Center Linux。

为支持迁移到 PostgreSQL 或 Postgres Pro，您必须向卡巴斯基技术支持提出请求并安装以下补丁之一：

- 对于 Kaspersky Security Center 14.2 Windows：14.2.0.26967-pf5
- 对于 Kaspersky Secure Mobility Management（基于 Kaspersky Security Center 14.2 Windows）：14.2.0.48079-pf5
- 对于 Kaspersky Security Center 15.1 Windows：15.1.0.20748-pf2

将 Kaspersky Security Center Windows 更新至版本 15.1.0.22239 后，也可以迁移到 PostgreSQL 或 Postgres Pro。




使用管理服务器数据备份迁移到 Kaspersky Security Center Linux。视频

# 通过迁移向导迁移到 Kaspersky Security Center Linux

通过使用此方案，您可以将管理组结构、包含的管理设备和其他组对象（策略、任务、全局任务、标签和设备分类）从 Kaspersky Security Center Windows 转移到 Kaspersky Security Center Linux 的管理下。

限制：

- 只能从 Kaspersky Security Center Windows 版本 14.2 或更高版本迁移到 Kaspersky Security Center Linux 版本 15 或更高版本。
- 您只能使用 Kaspersky Security Center Web Console 来执行此方案。

在开始之前，请详细了解 Kaspersky Security Center Linux 的功能和限制：

- Kaspersky Security Center Windows 和 Kaspersky Security Center Linux 之间的功能差异
- Kaspersky Security Center Linux 支持的 Kaspersky 应用程序列表

## 阶段

迁移方案分阶段进行：

1. **选择迁移方法**

   您可以通过迁移向导迁移到 Kaspersky Security Center Linux。迁移向导步骤取决于 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux 的管理服务器是否排列为层次结构：

   - 使用管理服务器层级进行迁移

     如果 Kaspersky Security Center Windows 管理服务器充当 Kaspersky Security Center Linux 管理服务器的辅助服务器，请选择此选项。您可以在 Kaspersky Security Center Web Console 的单个实例中管理迁移过程并在服务器之间切换。如果您更喜欢此选项，可以将管理服务器排列成层次结构以简化迁移过程。为此，请在开始迁移之前创建层次结构。

   - 使用导出文件（ZIP 存档）进行迁移

     如果 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux 的管理服务器未按层次结构排列，请选择此选项。您使用 Kaspersky Security Center Web Console 的两个实例管理迁移过程：一个实例用于 Kaspersky Security Center Windows，另一个实例用于 Kaspersky Security Center Linux。在这种情况下，您将使用在从 Kaspersky Security Center Windows 导出期间创建和下载的导出文件并将此文件导入到 Kaspersky Security Center Linux。

2. **备份 Kaspersky Security Center Windows 管理服务器的证书和私钥（可选步骤）**

   您可能希望通过从备份副本恢复管理服务器的证书和私钥，将受管理设备置于 Kaspersky Security Center Linux 管理服务器的管理之下。在此情况下，备份 Kaspersky Security Center Windows 管理服务器的证书和私钥。然后在第 6 阶段，您必须恢复证书和私钥。

3. **从 Kaspersky Security Center Windows 导出数据**

   打开 Kaspersky Security Center Windows，然后运行迁移向导。

4. **将数据导入到 Kaspersky Security Center Linux**

   继续运行迁移向导将导出的数据导入到Kaspersky Security Center Linux。如果服务器按层次结构排列，则在同一向导中成功导出后，导入会自动开始。如果服务器未按层次结构排列，您可以在切换到Kaspersky Security Center Linux 后继续运行迁移向导。

5. **执行其他操作以手动将对象和设置从 Kaspersky Security Center Windows 传输到 Kaspersky Security Center Linux（可选步骤）**

您可能还想传输无法通过迁移向导传输的对象和设置。例如，您还可以执行以下操作：

- 传输管理服务器和受管理应用程序使用的授权许可密钥
- 配置管理服务器的全局任务
- 配置网络代理策略设置
- 创建应用程序安装包
- 创建虚拟服务器
- 配置设备移动规则
- 配置自动标记设备规则
- 创建应用程序类别
- 分配和配置分发点

  如果您将充当分发点的设备移动到另一台管理服务器，包括在分发点范围中的设备不会被自动移动。您必须单个移动每个设备。如果分发点充当网关，您必须运行 `# /opt/kaspersky/klnagent64/bin/setup/postinstall.pl` 脚本，以使该分发点不再用作网关。

**6 移动 Kaspersky Security Center Linux 管理的导入的受管理设备**

要完成迁移，请将导入的受管理设备移至 Kaspersky Security Center Linux 的管理下。您可以通过以下方式之一进行操作：

- 通过klmover 实用程序

  使用 klmover 实用程序并指定新管理服务器的连接设置。

- 通过*更改管理服务器*任务

  创建*更改管理服务器*任务，指定导入的受管理设备、新的管理服务器以及其他任务设置。然后运行任务，将受管理设备置于 Kaspersky Security Center Linux 管理服务器的管理之下。

- 通过删除（如果已安装）并在受管理设备上进一步安装网络代理

  创建新的网络代理安装包，并在安装包属性中指定新管理服务器的连接设置。删除导入的受管理设备上的网络代理，然后使用安装包通过远程安装任务在导入的受管理设备上安装网络代理。您还可以创建并使用独立的安装包在本地安装网络代理。有关详细信息，请参阅切换受 Kaspersky Security Center Linux 管理的受管理设备。

- 通过从备份副本恢复管理服务器的证书和私钥（仅适用于迁移到 Kaspersky Security Center Linux 版本 15.1 或更高版本）

  为安装了 Kaspersky Security Center Linux 管理服务器设备分配与 Kaspersky Security Center Windows 管理服务器相同的网络地址。使用 `-cert_only` 参数运行 klbackup 实用程序，从您在第 2 阶段保存的备份副本中恢复管理服务器证书和私钥。在命令行中，执行以下命令：`/opt/kaspersky/ksc64/sbin/klbackup -path <管理服务器证书备份副本的路径> -restore -cert_only`。有关详细信息，请参阅使用 klbackup 实用程序切换受管理设备至另一台管理服务器的管理下。

**7 将网络代理更新到最新版本**

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

**8 确保受管理设备在新管理服务器上可见**

在 Kaspersky Security Center Linux 管理服务器上，打开受管理设备列表（**资产管理→资产(设备)**），然后检查**可见**、**网络代理已安装**和**上一次连接到管理服务器**列中的值。

### 其他数据迁移方法

除了迁移向导之外，还有其他方法可以传输您当前的对象，但这些方法只允许您传输策略和任务。

- 从 Kaspersky Security Center Windows 导出任务，然后导入任务到 Kaspersky Security Center Linux。
- 从 Kaspersky Security Center Windows 导出特定策略，然后导入政策到 Kaspersky Security Center Linux。相关的策略配置文件与选定的策略一起导出和导入。

## 从 Kaspersky Security Center Windows 导出组对象

从 Kaspersky Security Center Windows 到 Kaspersky Security Center Linux 的迁移管理组结构、包括的受管理设备和其他组对象，需要您首先选择要导出的数据并创建导出文件。导出文件包含有关要迁移的所有组对象的信息。导出文件将用于以后导入到 Kaspersky Security Center Linux 中。

您可以导出以下对象：

- 受管理应用程序的任务和策略
- 全局任务
- 自定义设备分类
- 管理组结构和包含的设备
- 已分配给迁移设备的标签

开始导出前，请阅读有关迁移到 Kaspersky Security Center Linux 的一般信息。选择迁移方法——使用或不使用 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux 管理服务器的层次结构。

*通过迁移向导导出受管理设备和相关组对象：*

1. 根据 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux 的管理服务器是否被排列成层次结构，执行以下操作之一：
   - 如果服务器被排列成层次结构，打开 Kaspersky Security Center Web Console，然后切换到 Kaspersky Security Center Windows 的服务器。
   - 如果服务器未排列成层次结构，请打开连接到 Kaspersky Security Center Windows 的 Kaspersky Security Center Web Console。
2. 在主菜单中，转到“**操作 → 迁移**”。
3. 选择**迁移到 Kaspersky Security Center Linux 或 Open Single Management Platform**启动向导并按照其步骤操作。
4. 选择要导出的管理组或子组。请确保所选的管理组或子组包含的设备不得超过 10,000 台。

5. 选择将导出其任务和策略的受管理应用程序。仅选择 Kaspersky Security Center Linux 支持的应用程序。不受支持的应用程序的对象仍将被导出，但将不可操作。

6. 使用左侧的链接，以选择全局任务、设备分类和要导出的报告。您可通过“**组对象**”链接在导出中排除自定义角色、内部用户和安全组以及自定义应用程序类别。

导出文件（ZIP 存档）已创建。根据您是否使用管理服务器层次结构支持执行迁移，导出文件将保存如下：

- 如果服务器排列成层次结构，导出文件将被保存到Kaspersky Security Center Web Console 服务器上的临时文件夹中。
- 如果服务器未排列成层次结构，则导出文件将被下载到您的设备。

对于具有管理服务器层次结构支持的迁移，导入会在成功导出后自动开始。对于没有管理服务器层次结构支持的迁移，您可以手动将保存的导出文件导入到 Kaspersky Security Center Linux。

# 将导出文件导入到 Kaspersky Security Center Linux

要传输有关从 Kaspersky Security Center Windows 导出的受管理设备、对象及其设置的信息，必须将其导入 Kaspersky Security Center Linux 或 Kaspersky Next XDR Expert。

*通过迁移向导导入受管理设备和相关组对象：*

1. 根据 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux 的管理服务器是否被排列成层次结构，执行以下操作之一：
   - 如果服务器按层次结构排列，则在导出完成后继续执行迁移向导的下一步。在此向导中成功导出后，导入会自动开始（请参阅本说明的步骤 2）。
   - 如果服务器未按层次结构排列：
     a. 打开连接到 Kaspersky Security Center Linux 或 Kaspersky Next XDR Expert 的 Kaspersky Security Center Web Console。
     b. 在主菜单中，转到“**操作 → 迁移**”。
     c. 选择您在从 Kaspersky Security Center Windows 导出过程中创建并下载的导出文件（ZIP 存档）。开始上传导出文件。
2. 导出文件上传成功后，即可继续导入。如果要指定其他导出文件，请单击**更改**链接，然后选择所需的文件。
3. Kaspersky Security Center Linux 管理组的整个层次结构将得以显示。
   选中目标管理组旁边的复选框，导出的管理组的对象（受管理设备、策略、任务和其他组对象）必须还原到该目标管理组。
4. 开始导入组对象。导入期间将无法最小化迁移向导和执行任何并行操作。等待至对象列表中所有项目旁边的刷新图标 (🔄) 均替换为绿色复选标记 (✓)，导入完成。
5. 导入完成后，导出的管理组结构（包括设备详情）将显示在所选目标管理组下。如果还原的对象的名称与现有对象的名称相同，则将为还原的对象添加一个增量后缀。

如果在迁移的任务中指定了运行该任务的账户的详细信息，则导入完成后您必须打开该任务并再次输入密码。

如果导入已完成但出现错误，您可以执行以下操作之一：

- 对于具有管理服务器层次结构支持的迁移，您可以再次开始导入导出文件。
- 对于没有管理服务器层次结构支持的迁移，您可以启动迁移向导选择另一个导出文件，然后再次导入。

您可以检查导范围中包含的组对象是否已成功导入到 Kaspersky Security Center Linux。为此，请转到**资产管理**部分并确保导入的对象是否出现在相应的子部分中。

请注意，导入的受管理设备显示在**受管理设备**子部分中，但它们在网络中不可见，并且网络代理未安装并在其上运行（**可见**、**网络代理已安装**和**网络代理正在运行**列中的*否*值）。

要完成迁移，您需要将受管理设备切换到Kaspersky Security Center Linux 的管理之下。

# 将受管理设备切换为受 Kaspersky Security Center Linux 管理

将受管理设备、对象及其设置的信息成功导入 Kaspersky Security Center Linux 后，您需要将受管理设备切换到 Kaspersky Security Center Linux 的管理下才能完成迁移。

您可以通过以下方法之一将受管理设备移至Kaspersky Security Center Linux 下：

- 使用klmover 实用程序。
- 使用*更改管理服务器*任务。
- 从备份副本恢复管理服务器的证书和私钥（仅适用于迁移到 Kaspersky Security Center Linux 15.1 或更高版本）。

  有关详细信息，请参阅主要迁移场景的第 6 阶段。
- 通过远程安装任务在受管理设备上安装网络代理。

*要通过安装网络代理将受管理设备切换为由 Kaspersky Security Center Linux 管理：*

1. 删除将在 Kaspersky Security Center Linux 管理下切换的导入受管理设备上的网络代理。
2. 切换到 Kaspersky Security Center Windows 的管理服务器。
3. 进入**软件管理** → **安装包**，然后打开网络代理程序现有安装包的属性。

   如果软件包列表中没有网络代理安装包，请下载新的安装包。

   您还可以创建并使用独立的安装包在本地安装网络代理。
4. 在**设置**选项卡上，选择**连接**区域。指定 Kaspersky Security Center Linux 的管理服务器的连接设置。

5. 为导入的受管理设备创建远程安装任务，然后指定重新配置的网络代理安装包。

   您可以通过 Kaspersky Security Center Windows 的管理服务器或通过充当分发点的基于 Windows 的设备安装网络代理。如果您使用管理服务器，请启用**通过管理服务器使用操作系统资源**选项。如果您使用分发点，请启用“**通过分发点使用操作系统资源**”选项。

6. 运行远程安装任务。

远程安装任务成功完成后，请转至 Kaspersky Security Center Linux 的管理服务器并确保受管理设备在网络中可见，并且网络代理已安装并在其上运行（**可见**、**网络代理已安装**和**网络代理正在运行**列中的“*是*”值）。

# 配置管理服务器

本部分介绍 Kaspersky Security Center 管理服务器的配置过程和属性。

# 配置管理服务器连接地址

管理服务器连接地址是用于以下用途的网络地址：

- 作为创建网络代理安装包时的默认地址
  安装网络代理后，受管理设备通过此地址连接到管理服务器。
- 作为 KSN 代理服务器地址
  受管理设备通过此地址连接到 KSN 代理服务器。

*配置管理服务器连接地址：*

1. 在主菜单中，单击管理服务器名称。
   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. 在打开的窗口中，在**管理服务器连接地址** 字段中，指定新的管理服务器连接地址。
   连接地址的最大长度为 255 个字符。
   您可以将管理服务器连接地址指定为 NetBIOS 名称、FQDN 或管理服务器的 IP 地址。
4. 单击“**保存**”按钮。

指定的地址用作管理服务器地址和 KSN 代理服务器地址。

# 配置 Kaspersky Security Center Web Console 到管理服务器的连接

您可以通过管理服务器属性或使用管理服务器策略设置来配置 Kaspersky Security Center Web Console 与管理服务器的连接。

*要通过管理服务器属性设置连接端口：*

1. 在主菜单中，单击管理服务器名称。
   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. 如有必要，请指定**Web Console 的 SSL 端口**设置或指定其他管理服务器连接端口。

所选服务器的主要连接设置已指定。

*要通过管理服务器策略设置来设置连接端口：*

1. 在主菜单中，转到“**资产管理**”→“**策略**”。

2. 单击管理服务器策略的名称，然后转到**应用程序设置**选项卡。

3. 如有必要，请指定**Web Console 的 SSL 端口**设置或指定其他管理服务器连接端口。

> 如果您禁用**打开 Web Console 的端口**选项并且此策略设置将被应用于设备，您将无法使用 Kaspersky Security Center Web Console 连接到管理服务器。在这种情况下，连接将被终止。如果您拥有未应用此策略的管理服务器，您可以通过 Kaspersky Security Center Web Console 重新连接到该管理服务器。

所选服务器的主要连接设置已指定。

# 配置用于连接到 Kaspersky Security Center Linux 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 Linux。例如，您可以在任何满足要求的设备上安装Kaspersky Security Center Web Console 服务器，Kaspersky Security Center Web Console 服务器将与 Kaspersky Security Center Linux 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 Web Console 服务器连接到 Kaspersky Security Center Linux，他或她将无法登录Kaspersky Security Center Linux。

当用户登录 Kaspersky Security Center Linux 或运行通过 Kaspersky Security Center Linux OpenAPI 与管理服务器交互的应用程序时，将验证 IP 地址。此时，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 Web Console 服务器

  如果您通过 Kaspersky Security Center Web Console 登录 Kaspersky Security Center Linux，您可以使用操作系统的标准方式在安装了 Kaspersky Security Center Web Console 服务器 的设备上配置防火墙。然后，如果有人尝试在一台设备上登录 Kaspersky Security Center Linux 并且 Kaspersky Security Center Web Console 服务器安装在另一台设备上，防火墙将有助于防止入侵者干扰。

- 通过 klakaut 自动化对象与管理服务器交互的应用程序
- 通过 OpenAPI 与管理服务器交互的应用程序，例如 Kaspersky Anti Targeted Attack Platform 或 Kaspersky Security for Virtualization

因此，请指定安装了上述应用程序的设备的地址。

您可以设置 IPv4 和 IPv6 地址。您不能指定 IP 地址范围。

## 如何建立 IP 地址允许列表

如果您之前未设置允许列表，请按照下面的说明操作。

*要建立用于登录 Kaspersky Security Center Linux 的 IP 地址允许列表：*

1. 在管理服务器设备上，在具有管理员权限的账户下运行命令提示符。
2. 将当前目录更改为 Kaspersky Security Center Linux 安装文件夹（通常为 /opt/kaspersky/ksc64/sbin）。
3. 在根账户下输入以下命令：
   ```
   klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP 地址>" -t s
   ```
   指定满足上述要求的 IP 地址。多个 IP 地址必须用分号隔开。
   如何只允许一台设备连接到管理服务器的示例：
   ```
   klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0" -t s
   ```
   如何允许多台设备连接到管理服务器的示例：
   ```
   klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 198.51.100.0; 203.0.113.0" -t s
   ```
4. 重启管理服务器服务。

您可以在管理服务器上的 Syslog 事件日志中查看您是否已成功配置 IP 地址允许列表。

## 如何更改 IP 地址允许列表

您可以像第一次建立允许列表那样进行更改。为此，请运行相同的命令并指定一个新的允许列表：

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP 地址>" -t s
```

如果要从允许列表中删除某些 IP 地址，请将其重写。例如，您的允许列表包括以下 IP 地址：192.0.2.0; 198.51.100.0; 203.0.113.0。您要删除 198.51.100.0 IP 地址。为此，在命令提示符处输入以下命令：

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 203.0.113.0" -t s
```

不要忘记重新启动管理服务器服务。

如何重置已配置的 IP 地址允许列表

*要重置已配置的 IP 地址允许列表：*

1. 在根账户下的命令提示符处输入以下命令：
   ```
   klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "" -t s
   ```
2. 重启管理服务器服务。

之后，不再验证 IP 地址。

# 指定管理服务器的互联网连接设置

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

*要指定管理服务器的互联网访问设置：*

1. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**配置互联网访问**”区域。
3. 如果您要在连接到互联网时使用代理服务器，请启用“**使用代理服务器**”选项。如果启用此选项，字段可用于输入设置。为代理服务器连接指定以下设置：

   - **地址**

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

   - **端口号**

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

   - **对本地地址不使用代理服务器**

     将不会使用代理服务器连接本地网络的设备。

   - **代理服务器身份验证**

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

   - **用户名**

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

   - **密码**

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

您还可以使用快速启动向导配置互联网访问。

# 管理服务器层级

一些客户公司，例如 MSP，可能运行多个管理服务器。可能不方便管理几个不同的管理服务器，因此可以应用层次结构。在层次结构中，基于 Linux 的管理服务器既可以作为主服务器也可以作为辅助服务器。基于 Linux 的主服务器可以管理基于 Linux 和基于 Windows 的从属服务器。基于 Windows 的主服务器可以管理基于 Linux 的辅助服务器。

两个管理服务器的"主/从"配置提供了以下选项：

- 一个从属管理服务器从主管理服务器继承策略、任务、用户角色和安装包，从而防止了重复设置。
- 主管理服务器上的设备分类可以包含从属管理服务器的设备。
- 主管理服务器的报告可以包含从属管理服务器的数据（包括详细信息）。
- 主管理服务器可以用作从属管理服务器的更新源。

主管理服务器仅接收来自上面列出的选项范围内的非虚拟从属管理服务器的数据。此限制不适用于虚拟管理服务器，虚拟管理服务器与其主管理服务器共享数据库。

管理服务器的层次结构为多租户模式提供支持。此模式允许主管理员独立地集中管理多个客户端。每个客户端组织或办公室都与其他组织或办公室隔离，被称为租户。您可以将多个受管理设备及其相关数据、设置、策略和任务分配给一个租户，并按租户配置用户权限。

安装在主要组织基础设施中的主管理服务器充当主要租户。主管理服务器使从属或虚拟管理服务器（其隔离的租户）能够独立接收和处理自己的事件并使用自己的资源、服务和配置。

拥有多个客户端组织的服务提供商可以向每个客户端组织独立提供 Kaspersky Security Center Linux 功能，包括警报聚合和响应操作。为了实现这点，服务提供商将从属或虚拟管理服务器作为每个客户端组织的租户进行连接。服务提供商使用自己的人员和资源提供服务。

# 创建管理服务器层级：添加从属管理服务器

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

## 添加从属管理服务器（在未来的主管理服务器上执行）

您可以添加管理服务器作为从属管理服务器，从而建立"主/从属"层级。

*要添加可以通过 Kaspersky Security Center Web Console 连接的从属管理服务器：*

1. 请确保未来主管理服务器的 13000 端口可用。

   构建层次结构后，此端口将用于主管理服务器和从属管理服务器之间的交互。

2. 转到未来主管理服务器的属性：

   a. 在主菜单中，选择一个区域（“**市场**”、“**控制台导航**”和“**设置**”除外），然后在页面顶部单击“**显示层级**”按钮。

   b. 在打开的导航窗格中，将鼠标光标悬停在所需管理服务器的名称上，然后单击设置图标 (⚙)。

   或者，您可以单击管理服务器名称，然后在主菜单中显示该名称后，在主菜单中单击该名称以打开服务器属性窗口。

3. 在打开的属性窗口中，单击“**管理服务器**”选项卡。

4. 选择您要向其添加管理服务器的管理组名称旁边的复选框。

5. 在菜单行中，单击“**连接从属管理服务器**”。

   “添加从属管理服务器向导”启动。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**

     指定构建层级结构后用于主管理服务器和从属管理服务器之间交互的 SSL 端口号。默认端口号是 13000。

   - **管理服务器 API 端口**

     Web Console 将用于通过 OpenAPI 接收来自从属管理服务器的连接的端口号。默认端口号是 13299。

     构建层级结构时，Web Console 会连接到未来的从属服务器，请求凭证，检索公共证书并执行初始设置。

     管理服务器层级结构构建完成后，将不再使用端口 13299。管理服务器将通过端口 13000 进行交互。

   - **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：

     - **代理服务器地址**
     - **用户名**
     - **密码**

7. 指定连接设置：

   - 输入将来的主管理服务器的地址。
   - 如果将来的从属管理服务器使用代理服务器，请输入代理服务器地址和用户凭证以连接到代理服务器。

8. 输入对将来的从属管理服务器具有访问权限的用户的凭证。

向导已完成，与将来的从属服务器的连接已建立，并且已建立“主/从属”层级。

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。

连接在以下情况下失败：

- 连接设置不正确。

  您必须检查设置或手动指定将来的从属服务器的证书。

- 将来的从属服务器是使用 Kaspersky Security Center Linux 自动生成的自签名证书进行身份验证的。因此，浏览器可能会阻止下载自签名证书。

  您可以执行以下操作之一：

  - 对于将来的从属服务器，创建在您的基础架构中受信任且满足自定义证书要求的证书。
  - 将将来的从属服务器的自签名证书添加到受信任浏览器证书列表中。我们建议您仅在无法创建自定义证书时才使用此选项。有关将证书添加到受信任证书列表中的信息，请参阅所用浏览器的文档。

### 添加从属管理服务器（在未来的从属管理服务器上执行）

如果您无法连接到未来从属管理服务器（例如，它临时被断开或无法连接或从属管理服务器的证书文件为自签名），您仍可以添加从属管理服务器。

*要添加不可以通过 Kaspersky Security Center Web Console 连接的管理服务器作为从属：*

1. 将未来主管理服务器的证书文件发送给未来从属管理服务器所在办公室的系统管理员。（例如，您可以将文件写入闪存驱动器等外部设备，或通过电子邮件发送它。）

   证书文件位于未来的主管理服务器上的 /var/opt/kaspersky/klnagent_srv/1093/cert/ 中。

2. 提示未来从属管理服务器的责任系统管理员做以下事情：

   a. 单击管理服务器名称。

   b. 在打开的属性页面上，转到“**常规**”选项卡的“**管理服务器层级**”区域。

   c. 选择**该管理服务器是服务器层级中的从属**选项。

   d. 在“**主管理服务器地址**”字段中，输入将来的主管理服务器的网络名称。

   e. 通过单击“**浏览**”选择先前保存的带有未来主管理服务器证书的文件。

   f. 如有必要，选中“**连接主管理服务器到 DMZ 中的从属管理服务器**”复选框。

g. 如果通过代理服务器连接到将来的主管理服务器，则选中“**使用代理服务器**”选项并指定连接设置。

h. 点击“**保存**”。

“主/从属”层级被创建。主管理服务器开始使用端口 13000 从从属管理服务器接收连接。主管理服务器的任务和策略被接收和应用。从属管理服务器显示在主管理服务器上，在添加其的管理组中。

# 查看从属管理服务器列表

*要查看从属（包括虚拟）管理服务器列表：*

1. 在主菜单中，选择一个区域（“**市场**”、“**控制台导航**”和“**设置**”除外）。
2. 在页面顶部，单击“**显示层级**”按钮。

在打开的导航窗格中，显示辅助（包括虚拟）管理服务器的列表。您可以通过单击名称转到任一管理服务器。

如果您从“**IP 范围**”和“**已删除对象**”区域打开了导航窗格，则无法转到虚拟管理服务器。
管理组也会显示。如果您从以下区域打开导航窗格，则可以管理这些组：“**资产(设备)**”、“**策略**”、“**任务**”和“**分发点**”。否则，这些组将显示为灰色。

如果您在 Kaspersky Security Center Web Console 中连接到主管理服务器，但无法连接到由从属管理服务器管理的虚拟管理服务器，您可以使用以下方法之一：

- **修改现有的 Kaspersky Security Center Web Console 安装，以将从属服务器添加到受信任的管理服务器列表中**。然后您将能够在 Kaspersky Security Center Web Console 中连接到该虚拟管理服务器。

  1. 在安装了 Kaspersky Security Center Web Console 的设备上，使用具有管理权限的账户运行与您设备上安装的 Linux 发行版相对应的 Kaspersky Security Center Web Console 安装文件。

     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 Web Console 直接连接到在其中创建了虚拟服务器的从属管理服务器。然后您将能够在 Kaspersky Security Center Web Console 中切换到该虚拟管理服务器。

# 管理虚拟管理服务器

本部分介绍管理虚拟管理服务器的以下操作：

- 创建虚拟管理服务器
- 启用和禁用虚拟管理服务器
- 为虚拟管理服务器分配管理员
- 更改客户端设备的管理服务器
- 删除虚拟管理服务器

# 创建虚拟管理服务器

您可以创建虚拟管理服务器并添加它们到管理组。

当您创建虚拟管理服务器时，它会继承主管理服务器的用户列表和所有用户权限。如果用户有权访问主服务器，则该用户也有权访问虚拟服务器。创建后，您可以单独配置对服务器的访问权限。

*要创建和添加虚拟管理服务器：*

1. 在主菜单中，单击管理服务器名称。
2. 在打开的页面上，转到“**管理服务器**”选项卡。
3. 选择您要添加虚拟管理服务器到的管理组。
   虚拟管理服务器将管理选定组（包括子组）中的设备。
4. 在菜单行中，单击“**新虚拟管理服务器**”。
5. 在打开的页面上，定义新虚拟管理服务器的属性：
   - **虚拟管理服务器名称**。
   - **管理服务器连接地址**
     您可以指定管理服务器的名称或 IP 地址。
6. 从用户列表中，选择虚拟管理服务器管理员。如果您想，您可以编辑现有账户之一，然后分配其管理员角色，或创建一个新用户账户。
   如有必要，您可以使用 kladduser 实用程序创建一个将充当虚拟管理服务器管理员的新账户。为此，请使用以下命令：
   ```
   kladduser -n <user_name> -p <password> -vs <virtual_server_name>
   ```
   其中 `virtual_server_name` 是虚拟管理服务器的名称。
7. 点击“**保存**”。

新的虚拟管理服务器将创建，添加到管理组并显示在“**管理服务器**”选项卡上。

如果您在 Kaspersky Security Center Web Console 中连接到主管理服务器，但无法连接到由从属管理服务器管理的虚拟管理服务器，您可以使用以下方法之一：

- **修改现有的 Kaspersky Security Center Web Console 安装，以将从属服务器添加到受信任的管理服务器列表中**。然后您将能够在 Kaspersky Security Center Web Console 中连接到该虚拟管理服务器。

  1. 在安装了 Kaspersky Security Center Web Console 的设备上，使用具有管理权限的账户运行与您设备上安装的 Linux 发行版相对应的 Kaspersky Security Center Web Console 安装文件。

     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 Web Console 直接连接到在其中创建了虚拟服务器的从属管理服务器。然后您将能够在 Kaspersky Security Center Web Console 中切换到该虚拟管理服务器。

# 启用或禁用虚拟管理服务器

当您创建新的虚拟管理服务器时，默认情况下会启用它。您可以随时禁用或再次启用它。禁用或启用虚拟管理服务器等同于关闭或打开物理管理服务器。

*要启用或禁用虚拟管理服务器：*

1. 在主菜单中，单击管理服务器名称。

2. 在打开的页面上，转到“**管理服务器**”选项卡。

3. 选择要启用或禁用的虚拟管理服务器。

4. 在菜单行上，单击“**启用/禁用虚拟管理服务器**”按钮。

   虚拟管理服务器状态被更改为已启用或禁用，具体取决于其先前的状态。更新的状态将显示在管理服务器名称旁边。

# 为虚拟管理服务器分配管理员

当您在组织中使用虚拟管理服务器时，可能希望为每个虚拟管理服务器分配一名专门的管理员。例如，当您创建虚拟管理服务器来管理组织的独立办公室或部门时，或者如果您是 MSP 提供商并通过虚拟管理服务器来管理您的租户时，这可能很有用。

当您创建虚拟管理服务器时，它会继承主管理服务器的用户列表和所有用户权限。如果用户有权访问主服务器，则该用户也有权访问虚拟服务器。创建后，您可以单独配置对服务器的访问权限。如果您想要仅为虚拟管理服务器分配管理员，请确保该管理员没有主管理服务器的访问权限。

您可以通过向管理员授予虚拟管理服务器的访问权限来为虚拟管理服务器分配管理员。您可以通过以下方式之一授予所需的访问权限：

- 手动配置管理员的访问权限
- 为管理员分配一个或多个用户角色

要登录 Kaspersky Security Center Web Console，虚拟管理服务器的管理员要指定虚拟管理服务器名称、用户名和密码。Kaspersky Security Center Web Console 会对管理员进行身份验证并打开管理员有权访问的虚拟管理服务器。管理员不能在管理服务器之间切换。

## 先决条件

在开始之前，请确保满足以下条件：

- 虚拟管理服务器已创建。
- 在主管理服务器上，您已为希望为其分配虚拟管理服务器的管理员创建一个账户。
- 您在“**修改对象 ACL** right in the **常规功能** → **用户权限**“修改对象 ACL”权限。

## 手动配置访问权限

*要为虚拟管理服务器分配管理员：*

1. 切换到所需的虚拟管理服务器：
   a. 在主菜单中，选择一个区域（“**市场**”、“**控制台导航**”和“**设置**”除外），然后在页面顶部单击“**显示层级**”按钮。
   b. 在打开的导航窗格中，单击所需虚拟管理服务器的名称。

   > 您无法从“**IP 范围**”和“**已删除对象**”区域切换到虚拟管理服务器。

   在主菜单中，管理服务器将更改为您选择的服务器。
2. 在主菜单中单击管理服务器的名称，移动到其属性。
   或者，在导航窗格中，将鼠标光标悬停在所需虚拟管理服务器的名称上，然后单击设置图标 (⚙)。
   管理服务器属性窗口将打开。
3. 在“**访问权限**”选项卡上，单击“**添加**”按钮。
   系统会打开主管理服务器和当前虚拟管理服务器的用户的统一列表。
4. 从用户列表中，选择要为虚拟管理服务器分配的管理员帐户，然后单击**确定**按钮。
   应用程序将选定的用户添加到**访问权限**选项卡上的用户列表中。
5. 选中已添加帐户旁边的复选框，然后点按**访问权限**按钮。

6. 配置管理员将拥有的虚拟管理服务器的权限。
   要成功进行身份验证，管理员至少必须具有以下权限：
   - 在**常规功能→基本功能**区域中**读取**权限
   - 在**常规功能→虚拟管理服务器**功能区域中**读取**权限

   应用程序将修改后的用户权限保存到管理员账户中。

*要为多个虚拟管理服务器分配管理员：*

1. 在主菜单中，单击主管理服务器名称。
2. 在打开的页面上，转到**访问权限**选项卡，然后单击**分配**。
   在打开的**添加用户或组**窗口中，选中要指定为管理员的用户旁边的复选框。
3. 您可以切换到**组**选项卡来选择用户群组。
4. 单击“**下一步**”。
5. 选择要为其分配管理员的服务器，然后单击**下一步**。
6. 如有必要，选择要为用户设置的管理员角色。
   如果要为用户设置当前管理服务器的自定义角色，请转到所需管理服务器的属性，单击**设置角色**，然后选择自定义角色。
7. 单击**完成**以应用更改。

   具有所选角色的管理员随即分配给多个虚拟管理服务器。

*要撤销管理员访问权限：*

1. 切换到所需的管理服务器。
2. 在主菜单中，单击管理服务器名称。
3. 在打开的页面上，前往**访问权限**选项卡。
4. 选中要撤销其访问权限的用户旁边的复选框。
5. 单击**撤销**并确认您的操作。

   所选用户的访问权限已被撤销。

通过分配用户角色配置访问权限

或者，您可以通过用户角色向虚拟管理服务器管理员授予访问权限。例如，如果您想在同一个虚拟管理服务器上分配多个管理员，这可能很有用。如果是这种情况，您可以为管理员账户分配相同的一个或多个用户角色，而不是为多个管理员配置相同的用户权限。

*通过分配用户角色为虚拟管理服务器分配管理员：*

1. 在主管理服务器上，创建一个新的用户角色，然后指定管理员在虚拟管理服务器上必须拥有的所有所需访问权限。您可以创建多个角色，例如，如果您想要单独访问不同的功能区域。
2. 切换到所需的虚拟管理服务器：
   a. 在主菜单中，选择一个区域（“**市场**”、“**控制台导航**”和“**设置**”除外），然后在页面顶部单击“**显示层级**”按钮。
   b. 在打开的导航窗格中，单击所需虚拟管理服务器的名称。

   > 您无法从“**IP 范围**”和“**已删除对象**”区域切换到虚拟管理服务器。

   在主菜单中，管理服务器将更改为您选择的服务器。
3. 向管理员账户分配新角色或多个角色。

应用程序向管理员账户分配角色。

配置对象级别的访问权限

除了分配功能区域级别的访问权限，您还可以在虚拟管理服务器上配置对特定对象的访问，例如对特定管理组或任务的访问。为此，请切换到虚拟管理服务器，然后在对象的属性中配置访问权限。

# 更改客户端设备的管理服务器

您可以使用“*更改管理服务器*”任务来更改管理客户端设备的管理服务器。任务执行完毕后，选定的客户端设备将由指定的管理服务器管理。

> 您不能对通过连接网关连接到管理服务器的客户端设备使用*更改管理服务器*任务。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。

*要更改管理客户端设备的管理服务器：*

1. 在主菜单中，转到“**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. 在向导的“**新任务设置**”步骤中，指定以下设置：
   a. 在“**应用程序**”下拉列表中，选择**Kaspersky Security Center**。
   b. 在**任务类型**字段中，选择**更改管理服务器**。
   c. 在**任务名称**字段中，指定您正在创建的任务的名称。
      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（*<>-_?:\"|）。

d. 选择要将任务分配到的设备：

- **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。

4. 在向导的**任务范围**步骤，指定管理组、具有特定地址的设备或设备分类。

5. 在向导的该步骤，确认您同意更改客户端设备的管理服务器的条款。

6. 在向导的该步骤，选择要用于管理选定设备的管理服务器：

- **更改到另一个主管理服务器**

  要将客户端设备移动至另一台主管理服务器，请指定以下管理服务器连接设置：

  1. 在**管理服务器地址**字段中，指定新的主管理服务器的地址。

  2. 在**端口号**字段中，指定要连接到管理服务器的端口号。

     默认端口号是 14000。

  3. 在**SSL 端口**字段中，指定主管理服务器上的 SSL 端口号。

     默认端口号是 13000。

  4. 如有必要，请启用**使用代理服务器**选项。

     如果此选项被禁用，则使用直接连接将设备连接到管理服务器。

     如果此选项被启用，请指定代理服务器参数：

     - **代理服务器地址**

     - **代理服务器端口**

     如果您的代理服务器需要身份验证，请在 **用户名** 和 **密码**字段中指定与代理服务器建立连接的账户的凭据。我们建议您指定仅具有代理服务器身份验证所需的最低权限的账户的凭据。

  5. 如有必要，请上传新的管理服务器证书。

- **在该主服务器上更改到另一个虚拟服务器**

  选择此选项可以将客户端设备移动到当前主管理服务器上的虚拟管理服务器。为此，在**虚拟管理服务器名称**下拉列表中，选择必要的虚拟管理服务器。

7. 在向导的**选择账户以运行任务**步骤中，指定账户设置：

   - **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。

8. 如果要更改默认任务设置，请在向导的**完成任务创建**步骤中启用**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。您可以稍后随时更改默认设置。

9. 单击“**完成**”按钮。
   任务被创建并显示在任务列表。

10. 单击创建的任务的名称以打开任务属性窗口。

11. 如果要更改默认任务设置，请在任务属性窗口中根据需要指定常规任务设置。

12. 单击“**保存**”按钮。
    任务被创建和配置。

13. 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。

# 删除虚拟管理服务器

如果删除虚拟管理服务器，在管理服务器上创建的所有对象（包括策略和任务）也将被删除。由虚拟管理服务器管理的管理组中的受管理设备将被从管理组中删除。要返回 Kaspersky Security Center Linux 管理的设备，请运行网络轮询，然后将找到的设备从未分配的设备组移动到管理组。

*要删除虚拟管理服务器：*

1. 切换到要删除的虚拟管理服务器所属的主物理管理服务器：
   a. 在主菜单中，选择一个区域（**市场**、**控制台导航**和**设置**除外），然后在页面顶部单击**显示层级**按钮。
   b. 在打开的导航面板中，点击主物理管理服务器的名称。
      在主菜单中，管理服务器将更改为您选择的服务器。
2. 通过以下方式之一移动到主物理管理服务器的属性：
   - 在导航面板中，将鼠标光标悬停在所需管理服务器的名称上，然后点击设置图标（⚙）。
   - 在主菜单中，单击管理服务器名称。
3. 在打开的属性窗口上，转到“**管理服务器**”选项卡。
4. 选择要删除的虚拟管理服务器。
5. 在菜单项目上，单击“**删除**”按钮。

虚拟管理服务器被删除。

# 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设施中的连接，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. 在主菜单中，单击管理服务器名称。
   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。

后续所有入站连接到管理服务器的事件、身份验证结果和 SSL 错误将被保存至 /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**”部分，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. 在主菜单中，单击管理服务器名称。

   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。

此外，您可以执行以下操作：

- 更改任何任务的设置以保存与任务进度相关的事件，或者仅保存任务执行结果。
- 减少或禁用安装在受管理设备上的管理服务器、网络代理和卡巴斯基应用程序的事件的存储期限。

为此，您将降低数据库中的事件数量，提高与数据库中事件表分析相关的场景的执行速度，并降低严重事件被大数量事件覆盖的风险。

# 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 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 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 Linux 指令的“h”项）。如果需要将数据库服务器保留在以前的设备上，请在安装 Kaspersky Security Center Linux 指令的“h”项中输入以前的设备的 IP 地址。

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 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。

# 更改管理服务器名称

更改服务器名称的步骤可能因您的环境而异。您可以选择以下场景之一来更改服务器名称：

- 通过添加新的 DNS 记录来保持连接。
- 通过切换到基于 IP 地址的连接来保持连接。
- 更改服务器名称后恢复中断的连接。

如果您在更改服务器名称时遇到困难，请联系技术支持。

## 通过添加新的 DNS 记录来保持连接

在此场景中，重命名管理服务器后，受管理设备和 Kaspersky Security Center Web Console 会继续连接到旧的管理服务器地址。要进行此配置，请添加以下 DNS 记录类型之一：

- A 记录，用于将旧管理服务器地址指向新的管理服务器 IP 地址。
- CNAME 记录，用于将旧管理服务器名称映射到新的管理服务器名称。

  有关配置所需记录的更多信息，请参阅您的 DNS 服务器文档。

*要通过添加新的 DNS 记录来保留连接：*

1. **更改服务器名称**。

   由于安装期间组件的配置方式，如果不重新安装管理服务器，则无法更改管理服务器名称。

   *要更改服务器名称：*

   1. 使用 klbackup 实用程序创建管理服务器的新备份。
   2. 在所有管理员工作站上卸载 Kaspersky Security Center Linux 和 Kaspersky Security Center Web Console。
   3. 手动删除管理服务器数据库和 IAM 数据库。管理服务器在卸载期间不会自动删除它们。
   4. 根据您的操作系统文档，在管理服务器的操作系统中重命名该设备。

5. 使用管理服务器的新 FQDN 安装 Kaspersky Security Center Linux 管理服务器。

6. 安装后，恢复之前准备的管理服务器备份。

7. 检查 IAM 服务器配置，并且在必要时将管理服务器地址添加到 IAM 服务器配置文件。

8. 通过在响应文件中指定管理服务器的新 FQDN，在所有管理员工作站上安装 Web Console。

2. 为旧管理服务器地址添加新的 DNS 记录。

3. 在 Kaspersky Security Center Web Console 的管理服务器设置中指定新地址。

4. 在可直接访问管理服务器的设备上运行 **更改管理服务器** 任务。之后，受管理设备将能够使用新名称连接到管理服务器。

   请勿在无法直接访问服务器的设备上运行此任务，否则这些设备将失去与管理服务器和连接网关的连接。

   通过连接网关连接的受管理设备不会检查管理服务器名称。因此，无需对这些设备执行任何其他操作。管理服务器地址的信息不会在 klnagchk 诊断命令的输出中更新。

服务器名称更改后，将保留与管理服务器的连接。

更改服务器名称后，证书信息将过期。由于这不会影响组件的运行，因此不建议计划外更换自签名证书。这些证书是在 Kaspersky Security Center 安装过程中生成的，并由服务器自动续订。在下次自动更换证书期间，它们将使用新的管理服务器名称重新颁发。

在重新安装期间，将为 IAM 服务器和 Web Console 服务器颁发新证书。如有必要，请将它们替换为证书颁发机构针对新的管理服务器名称颁发的自定义证书。有关详细信息，请参阅以下文章：关于 Kaspersky Security Center Linux 证书。

# 通过切换到基于 IP 地址的连接来保持连接

在此场景中，受管理设备连接到管理服务器的方式会发生变化。设备使用管理服务器 IP 地址而不是管理服务器名称进行连接。切换所有受管理设备可能需要一些时间，具体取决于设备数量以及它们出现在管理服务器所在网络中的频率。

*要通过切换到基于 IP 地址的连接来保持连接：*

1. **在更改管理服务器名称之前准备 Kaspersky Security Center 基础架构。**

   1. 使用 IP 地址将受管理设备连接到管理服务器。更改管理服务器名称后，使用其名称进行连接的设备将与管理服务器断开连接。要通过 IP 地址连接，请在可直接访问管理服务器的设备上运行“更改管理服务器”任务，包括充当连接网关的设备。

      请勿在无法直接访问服务器的设备上运行此任务，否则这些设备将失去与管理服务器和连接网关的连接。

      通过连接网关连接的受管理设备不会检查管理服务器名称。因此，无需对这些设备执行任何其他操作。在 klnagchk 诊断命令的输出中，不会更新有关管理服务器地址的信息。

2. 确保所有受管理设备都通过 IP 地址连接到管理服务器。为此，请检查以下内容：

   - 可直接访问管理服务器的受管理设备上，“管理服务器地址”行中的 klnagchk 诊断命令结果。
   - 在设备上安装时网络代理安装包的属性信息。
     必须先将网络代理配置为使用 IP 地址连接到管理服务器。

     > 如果您在未先卸载现有安装的情况下将网络代理安装到现有安装之上，则网络代理配置中指定的管理服务器连接地址和证书将不会更新。

3. 在现有的管理服务器连接配置文件中指定新名称。
4. 如果您使用移动设备管理角色（管理 Android 和 iOS 设备），请按照如何更改使用 MDM 或 KSMM 角色的 Kaspersky Endpoint Security for Android 的移动设备上的管理服务器地址 中的说明操作。

2. **更改服务器名称**。

   由于安装期间组件的配置方式，如果不重新安装管理服务器，则无法更改管理服务器名称。

   *要更改服务器名称：*

   1. 使用 klbackup 实用程序创建管理服务器的新备份。
   2. 在所有管理员工作站上卸载 Kaspersky Security Center Linux 和 Kaspersky Security Center Web Console。
   3. 手动删除管理服务器数据库和 IAM 数据库。管理服务器在卸载期间不会自动删除它们。
   4. 根据您的操作系统文档，在管理服务器的操作系统中重命名该设备。
   5. 使用管理服务器的新 FQDN 安装 Kaspersky Security Center Linux 管理服务器。
   6. 安装后，恢复之前准备的管理服务器备份。
   7. 检查 IAM 服务器配置，并且在必要时将管理服务器地址添加到 IAM 服务器配置文件。
   8. 在所有管理员工作站上安装 Web Console，方法是在响应文件中指定管理服务器的新 FQDN。

3. **在管理服务器设置中更新管理服务器地址**。

   更改管理服务器名称后，在 Kaspersky Security Center Web Console 的管理服务器设置中指定新的 FQDN 地址。为此，请检查并更新以下各项设置中的 FQDN 地址：

   - 卡巴斯基安全网络代理服务器地址
   - Web 服务器
   - 网络代理安装包属性
   - 安全代码颁发者名称 (2FA)

此外，请执行以下操作：

- 在其他卡巴斯基应用程序的策略和设置中指定新的服务器名称。
- 重新发布每个已发布的独立包和移动设备包。
- 如果您使用管理服务器层级结构，并且服务器是通过名称而不是 IP 地址连接的，请重新连接从属管理服务器。

4. 在可直接访问管理服务器的设备上运行 **更改管理服务器** 任务，以将受管理设备上的连接地址更改为新的管理服务器名称。

更改服务器名称后，与管理服务器的连接将保留。

更改服务器名称后，证书信息将过期。由于这不会影响组件的运行，因此不建议计划外更换自签名证书。这些证书是在 Kaspersky Security Center 安装过程中生成的，并由服务器自动续订。在下次自动更换证书期间，它们将使用新的管理服务器名称重新颁发。

在重新安装期间，将为 IAM 服务器和 Web Console 服务器颁发新证书。如有必要，请将它们替换为证书颁发机构针对新的管理服务器名称颁发的自定义证书。有关详细信息，请参阅以下文章：关于 Kaspersky Security Center Linux 证书。

# 更改服务器名称后恢复中断的连接

此场景适用于以下情况：

- 如果您已失去管理服务器设备域名的所有权，但仍然可以访问管理服务器。
- 如果管理服务器不再管理受管理设备。
- 如果由于其他原因，无法为旧的 Kaspersky Security Center Linux 地址添加 DNS 记录。

*要在更改服务器名称后恢复中断的连接：*

1. **更改服务器名称**。

   由于安装期间组件的配置方式，如果不重新安装管理服务器，则无法更改管理服务器名称。

   *要更改服务器名称：*

   1. 使用 klbackup 实用程序创建管理服务器的新备份。
   2. 在所有管理员工作站上卸载 Kaspersky Security Center Linux 和 Kaspersky Security Center Web Console。
   3. 手动删除管理服务器数据库和 IAM 数据库。管理服务器在卸载期间不会自动删除它们。
   4. 根据您的操作系统文档，在管理服务器的操作系统中重命名该设备。
   5. 使用管理服务器的新 FQDN 安装 Kaspersky Security Center Linux 管理服务器。
   6. 安装后，恢复之前准备的管理服务器备份。

7. 检查 IAM 服务器配置，并且在必要时将管理服务器地址添加到 IAM 服务器配置文件。

8. 在所有管理员工作站上安装 Web Console，方法是在响应文件中指定管理服务器的新 FQDN。

2. **在管理服务器设置中更新管理服务器地址**。

更改管理服务器名称后，在 Kaspersky Security Center Web Console 的管理服务器设置中指定新的 FQDN 地址。为此，请检查并更新以下各项设置中的 FQDN 地址：

- 卡巴斯基安全网络代理服务器地址
- Web 服务器
- 网络代理安装包属性
- 安全代码颁发者名称 (2FA)

此外，请执行以下操作：

- 在其他卡巴斯基应用程序的策略和设置中指定新的服务器名称。
- 重新发布每个已发布的独立包和移动设备包。
- 如果您使用管理服务器层级结构，并且服务器是通过名称而不是 IP 地址连接的，请重新连接从属管理服务器。

3. 在之前受管理的设备上恢复与管理服务器的连接：

- 在可直接访问管理服务器的设备上，使用 klmover 实用程序指定包含新管理服务器名称的连接地址。有关详细信息，请参阅以下文章：使用 klmover 实用程序将网络代理连接到管理服务器。
- 在充当连接网关的设备上，重新安装网络代理并重新配置连接网关角色。有关详细信息，请参阅以下文章：在 DMZ 中添加连接网关作为分发点。
- 通过连接网关连接的设备将在连接网关恢复后自动重新连接。网络代理连接到连接网关时不使用管理服务器名称。

  请勿在通过连接网关连接的设备上使用 klmover 实用程序。有关详细信息，请参阅以下文章：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。

服务器名称更改后，将恢复与管理服务器的连接。

更改服务器名称后，证书信息将变为过时。由于这不会影响组件的运行，因此不建议计划外更换自签名证书。这些证书是在 Kaspersky Security Center 安装过程中生成的，并由服务器自动续订。在下次自动更换证书期间，它们将使用新的管理服务器名称重新颁发。

在重新安装期间，将为 IAM 服务器和 Web Console 服务器颁发新证书。如有必要，请将它们替换为证书颁发机构针对新的管理服务器名称颁发的自定义证书。有关详细信息，请参阅以下文章：关于 Kaspersky Security Center Linux 证书。

# 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。

### 更改管理服务器数据库凭证

*要在Linux环境中使用klsrvconfig实用程序更改管理服务器数据库凭证：*

1. 运行klsrvconfig实用程序。

   ```
   sudo /opt/kaspersky/ksc64/sbin/klsrvconfig -set_dbms_cred
   ```

2. 指定一个新的账户名。您应该指定 DBMS 中存在的账户的凭据。
3. 输入新密码。
4. 指定新密码以确认。

管理服务器数据库凭证已更改。

### 更改IAM数据库凭证

*要在Linux环境中通过修改配置文件来更改IAM数据库凭证：*

1. IAM配置文件位于：/var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
2. 在 `dbms_iam` 部分，在用户和密码字段中指定新帐户凭据。您应该指定 DBMS 中存在的账户的凭据。
3. 运行以下命令：

   ```
   systemctl restart kliam_srv.service
   ```

IAM数据库凭证已更改。

# 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，您可以将管理服务器从一台设备上转移至其他设备或者将其升级为新版本 Kaspersky Security Center。此外，您还可以使用数据备份将管理服务器数据从 Kaspersky Security Center Windows 移至 Kaspersky Security Center Linux 的管理下（不支持将数据从 Kaspersky Security Center Linux 移至 Kaspersky Security Center Windows ）。

> 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。

在备份管理服务器数据之前，请执行以下操作：

- **遵循在管理服务器16或更早版本上创建备份并将其还原到16.1或更高版本的要求**
  - 如果您在管理服务器16或更早版本上创建数据备份并将其还原到管理服务器16.1或更高版本，则会启用双重身份验证。更多信息，请参阅关于帐户的双重身份验证。

为确保用户能够使用已配置的双重身份验证密钥通过现有帐户登录云控制台，并确保OpenAPI自动化脚本在恢复后继续运行，您必须执行以下步骤：

- 为所有用户启用双重身份验证
- 管理员必须为其自己的帐户配置双重身份验证
- 从双重身份验证中排除所需的账户

  如有需要，请将用于通过OpenAPI运行脚本的集成帐户添加到排除项列表中。

如果在创建备份之前无法配置双重身份验证，则用户账户将被添加到双重身份验证允许列表中，并在登录云控制台时配置双重身份验证。有关将帐户添加到允许列表的更详细条件，请参阅允许用户配置双重身份验证话题。

- 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。
- 要备份或恢复Kaspersky Security Center Linux故障转移集群，您必须在备份或恢复完成后停止整个集群进行维护，然后重新启动它。

您可以使用以下方式之一创建管理服务器数据的备份副本：

- 通过 Kaspersky Security Center Web Console 创建并运行数据备份任务。
- 通过在已安装管理服务器的设备上运行 klbackup 实用程序。该实用程序包含在 Kaspersky Security Center 分发包。管理服务器安装完毕后，该实用程序位于在安装应用程序时指定的目标文件夹的根目录中（通常为 /opt/kaspersky/ksc64/sbin/klbackup）。

以下数据保存在管理服务器的备份副本中：

- 管理服务器数据库（策略、任务、应用程序设置、管理服务器上保存的事件）。
- 有关管理组和客户端设备的结构的配置详情。
- 远程安装的应用程序分发包的存储库。
- 管理服务器证书。
- 为用户帐户配置的双重身份验证密钥。
- 排除在双重身份验证之外的用户帐户列表。

您可以通过创建和运行数据备份任务或使用klbackup实用程序来创建管理服务器数据的备份副本。只有使用klbackup实用程序才能恢复管理服务器数据。您必须在刚刚安装的、与备份副本具有相同或更新版本的管理服务器的可运行实例上执行恢复。请勿使用任何第三方工具进行备份或恢复，并且如果可能，请在配置和数据传输完全完成之前不要删除之前的Kaspersky Security Center Linux安装程序。

# 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. 在主菜单中，转到"**任务**"。
2. 单击**添加**。
   "新任务向导"启动。使用**下一步**按钮进行向导。
3. 在"**应用程序**"列表中，选择"**Kaspersky Security Center 16.3**"，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。

对于要执行还原的管理服务器的实例，必须使用相同类型的 DBMS。管理服务器版本可以相同（带有相同或更新补丁）或更新。

如果您在使用早期版本的 MariaDB DBMS 时备份了 Kaspersky Security Center Linux 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 <备份路径> [-linux_path <DBMS 备份路径>-node_cert <证书路径>] [-logfile <日志文件> [-use_ts]|[-restore] [-password <密码>] [-cert_only]
```

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 <备份路径>` — 将信息保存在备份文件夹中，或使用备份文件夹中的数据进行恢复（必填参数）。
- `-linux_path <DBMS 备份路径>` — 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 实用程序需要获得对 DBMS 备份文件夹中的数据进行更改的权限。
- `-node_cert <证书路径>` — 用于在恢复后配置非活动故障转移集群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 <日志文件>` — 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 实用程序需要获得对备份文件夹中的数据进行更改的权限。
- `-use_ts` — 保存数据时，将信息复制到备份文件夹中以 `klbackup YYYY-MM-DD # HH-MM-SS` 格式命名的子文件夹中，其中包括当前日期及 UTC 时间的操作时间。如果未指定密钥，信息将保存在备份文件夹的根目录中。

  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。系统将基于备份文件夹内包含的信息执行数据恢复。如果没有可用密钥，数据将备份至备份文件夹中。
- `-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。

- `-cert_only` — 仅保存或恢复管理服务器的证书和私钥。

  当您执行从 Kaspersky Security Center Windows 的管理服务器迁移到 Kaspersky Security Center Linux 的管理服务器时，此标志可能有用。此外，您还可以在 Kaspersky Security Center Linux 管理服务器之间以及 Kaspersky Security Center Windows 管理服务器之间迁移受管理设备。

您可以使用数据备份将 Kaspersky Security Center Windows 管理服务器数据移至 Kaspersky Security Center Linux 的管理之下。
如果您使用 MySQL 或 MariaDB 作为 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux 的 DBMS，则 `lower_case_table_names` 参数在当前 DBMS 和新 DBMS 中必须一致。
在创建数据备份之前，请检查`lower_case_table_names`参数。然后，在为 Kaspersky Security Center Linux 安装 MySQL 或 MariaDB 时，必须将 `lower_case_table_names` 参数的值设置为与 Windows 版一致。

如果在恢复过程中，管理服务器通用证书被备份中的另一个证书替换，请执行以下步骤以确保正常运行：
1.请重新安装 Web Console以避免以下错误：
*管理服务器使用不受信任的证书。请通过指定有效证书重新配置应用程序，或联系主管理员。*
2.检查 IAM 服务器配置，并且在必要时将管理服务器地址添加到 IAM 服务器配置文件。

# 使用 klbackup 实用程序切换受管理设备至另一台管理服务器的管理下

klbackup 实用程序可让您切换受管理设备至另一台管理服务器的管理下。您可以在执行迁移时使用 klbackup 实用程序将 Kaspersky Security Center Windows 管理服务器更改为 Kaspersky Security Center Linux 管理服务器。此外，您还可以在 Kaspersky Security Center Linux 管理服务器之间以及 Kaspersky Security Center Windows 管理服务器之间迁移受管理设备。

开始之前， **查看自自定义证书的要求**。

如果您使用的是自定义证书而不是自签名证书，则在将 Kaspersky Security Center Linux 升级到更高版本之前，必须确保证书包含主题备用名称 (SAN)。如果没有，在升级 Kaspersky Security Center Linux 之前替换证书至关重要。否则，升级后您将无法登录 Web Console。

*要确保证书包含 SAN：*

1. 在安装了管理服务器的设备上，执行命令：

   - 对于 Linux 设备：

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout
     -ext subjectAltName
     ```

   - 对于 Windows 设备：

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. 请确保命令输出中包含“使用者备用名称”，并且名称包含管理服务器设备的地址。

3. 如果缺少“使用者备用名称”，请使用 klsetsrvcert 实用程序将自定义证书替换为符合要求的证书。

*要使用 klbackup 实用程序切换受管设备至另一台管理服务器的管理下：*

1. 在之前的设备上，创建管理服务器证书和私钥的备份副本。

您可以使用下列可用方法之一指定一个备份副本：

- 通过使用 klbackup 实用程序界面（仅适用于 Kaspersky Security Center Windows 管理服务器）

  运行位于 Kaspersky Security Center 安装文件夹中的 klbackup 实用程序，然后使用**仅恢复或备份管理服务器证书**选项创建备份。

- 使用命令提示符（适用于 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux 管理服务器 15.1 或更高版本）

  从命令行运行带有 `-cert_only` 键的 klbackup 实用程序，以创建管理服务器证书和私钥的备份副本：

  ```
  klbackup -path <管理服务器证书备份副本的路径> -cert_only
  ```

2. 在之前的设备上，断开管理服务器与网络的连接。

3. 使用另一台管理服务器为设备分配相同域名。

   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）。

   如果无法将设备的相同地址分配给另一台管理服务器，则必须生成新的管理服务器证书，并在 IAM 配置文件中指定该证书。安装管理服务器后，您需要手动将网络代理切换到新的管理服务器。

4. 在具有另一台管理服务器的设备上，从备份副本恢复管理服务器证书和私钥。

   您可以使用下列可用方法之一恢复备份副本：

   - 通过使用 klbackup 实用程序界面（仅适用于 Kaspersky Security Center Windows 管理服务器）

     运行 klbackup 实用程序，然后使用**仅恢复或备份管理服务器证书**选项恢复备份。

   - 使用命令提示符（适用于 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux 管理服务器 15.1 或更高版本）

     从命令行运行带有 `-cert_only` 键的 klbackup 实用程序，以恢复管理服务器证书和私钥的备份副本：

     ```
     klbackup -path <管理服务器证书备份副本的路径> -restore -cert_only
     ```

5. 配置管理服务器和 IAM 服务器的证书验证。

受管理设备受到另一台管理服务器的管理。您可以转至管理服务器并确保受管理设备在网络中可见，并且网络代理已安装并在其上运行（***可见***、**可见**和**网络代理已安装**列中的网络代理正在运行值）。

# 使用 MySQL 或 MariaDB 时备份和恢复管理服务器数据

您可以使用数据备份将管理服务器数据从 Kaspersky Security Center Windows 迁移到 Kaspersky Security Center Linux 的管理下。仅支持使用管理服务器数据备份进行迁移，以便从任何受支持的 Kaspersky Security Center Windows 版本迁移到 Kaspersky Security Center Linux 15.2 或更高版本。

如果您使用 MySQL 或 MariaDB 作为 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux 的 DBMS，则 `lower_case_table_names` 参数必须与当前和新的 DBMS 匹配。否则，管理服务器数据将被错误迁移。

在 Kaspersky Security Center Windows 上备份管理服务器数据之前，请检查 `lower_case_table_names` 参数值。如果您之前在 DBMS 安装期间没有指定此参数，则使用默认参数值。Windows 的 `lower_case_table_names` 参数的默认值为 `1`。

在为 Kaspersky Security Center Linux 安装 MySQL 或 MariaDB 时，请使用MySQL 网站的说明将 `lower_case_table_names` 参数设置为与 Windows 中此参数指定的值相同的值。如果不指定此参数，则使用默认参数值。对于基于 Linux 的操作系统，`lower_case_table_names` 参数的默认值与 Windows 的默认值不同。

如果要安装 MySQL 8.0，可能无法按照此说明指定 `lower_case_table_names` 参数。在这种情况下，您必须首先安装 MySQL 5.7，使用操作说明指定 `lower_case_table_names` 参数，然后将 MySQL 5.7 升级到 MySQL 8.0。如果当前和新的 DBMS 的 `lower_case_table_names` 参数不匹配，则管理服务器数据将被错误恢复。

# 管理服务器维护

通过管理服务器维护，您可以腾出管理服务器文件夹中的空间，并通过删除不再需要的对象来减少数据库存储量。这有助于您提高应用程序的性能和运行可靠性。我们建议您至少每周维护一次管理服务器。

管理服务器通过专用任务进行维护。在维护管理服务器时，应用程序执行以下操作：

- 从存储文件夹中删除不必要的文件夹和文件。
- 从表中删除不必要的记录（也称为“悬垂指针”）。
- 清除缓存。
- 维护数据库（如果您使用 PostgreSQL 作为 DBMS）：
  - 重组数据库索引。
  - 更新数据库统计信息。
  - 收缩数据库（如果必要）。

管理服务器维护任务支持 MariaDB 版本 10.3 及更高版本。如果您使用 MariaDB 10.2 或更早版本，管理员必须自行维护此 DBMS。

安装 Kaspersky Security Center Linux 时，会自动创建“管理服务器维护”任务。如果“管理服务器维护”任务被删除，您可以手动创建它。

*要创建管理服务器维护任务，请执行以下操作：*

1. 在主菜单中，转到“**任务**”。
2. 单击“**添加**”按钮。
   “新任务向导”启动。
3. 在向导的“**新任务设置**”窗口中，选择“**管理服务器维护**”为任务类型并单击“**Next**下一步”按钮。
4. 遵照剩余的向导说明。

新创建的任务显示在任务列表中。一台管理服务器仅可以运行一个“管理服务器维护”任务。如果已经为管理服务器创建了“管理服务器维护”任务，则无法创建新的“管理服务器维护”任务。

# 删除管理服务器层级

如果不再想拥有管理服务器层级结构，您可以从该层级将其断开连接。

*要删除管理服务器层级：*

1. 在主菜单中，单击管理服务器名称。
2. 在打开的页面上，转到“**管理服务器**选项卡。
3. 在要从其中删除从属管理服务器的管理组中，选择从属管理服务器。
4. 在菜单项目上，单击“**删除**”按钮。
5. 在打开的窗口中，单击“**确定**”以确认您要删除该从属管理服务器。

先前的主管理服务器和从属管理服务器现在彼此独立。层级不再存在。

# 访问公共 DNS 服务器

如果无法使用系统 DNS 访问卡巴斯基服务器，Kaspersky Security Center Linux 可以按以下顺序使用这些公共 DNS 服务器：

1. Google Public DNS (8.8.8.8)
2. Cloudflare DNS (1.1.1.1)
3. Alibaba Cloud DNS (223.6.6.6)
4. Quad9 DNS (9.9.9.9)
5. CleanBrowsing (185.228.168.168)

对这些 DNS 服务器的请求可能包含域地址和管理服务器的公共 IP 地址，因为应用程序建立了到 DNS 服务器的 TCP/UDP 连接。如果 Kaspersky Security Center Linux 使用公共 DNS 服务器，则数据处理受相关服务的隐私政策约束。

*要通过使用 klscflag 实用程序配置公共 DNS 的使用：*

1. 运行命令行，然后将当前目录更改为包含 klscflag 实用程序的目录。klscflag 实用程序位于安装管理服务器的目录中。默认安装路径为/opt/kaspersky/ksc64/sbin。
2. 要禁用公共 DNS 的使用，请在根账户下运行以下命令：

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 1
   ```

3. 要启用公共 DNS 的使用，请在根账户下运行以下命令：

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 0
   ```

# 配置界面

您可以将 Kaspersky Security Center 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 Web Console 界面：*

1. 在主菜单中，转到“**设置**” → “**界面选项**”。
2. 启用或禁用所需的选项：
   - **显示数据加密和保护**
   - **显示 EDR 警告**
3. 单击“**保存**”。

启用所需选项后，控制台会在主菜单中显示相应的部分。例如，如果您启用“**显示 EDR 警告**”，则“**监控**”→“**警报**”区域会出现在主菜单中。

# 到管理服务器的加密连接

客户端设备和管理服务器之间的数据交换可以使用 TLS（传输层安全）协议进行。TLS 协议能够识别交互方、将传输数据加密并防止数据在传输过程中被篡改。TLS 协议使用公钥对交互方和加密数据进行身份验证。

在客户端设备首次连接到管理服务器时，设备上的网络代理会下载管理服务器证书的副本并将其存储在本地。

如果您在设备本地安装网络代理，您可以手动选择管理服务器证书。

下载的证书将用于在以后的连接中验证管理服务器权限。

在以后的会话中，网络代理将在每次设备与管理服务器连接时请求管理服务器证书，并将其与本地副本进行比较。如果副本不一致，设备将不允许访问管理服务器。

# 使用 TLS 的加密通信

要修复您组织企业网络中的漏洞，您可以使用 TLS 协议启用流量加密。您可以在管理服务器上启用 TLS 加密协议和支持的密码套件。Kaspersky Security Center Linux 支持 TLS 协议版本 1.0、1.1、1.2 和 1.3。您可以选择所需的加密协议和加密套件。

Kaspersky Security Center Linux 使用自签发证书。您也可以使用您自己的证书。Kaspersky 专家建议使用由受信任证书机构发布的证书。

*要在管理服务器上配置允许的加密协议和加密套件：*

1. 运行命令行，然后将当前目录更改为包含 klscflag 实用程序的目录。klscflag 实用程序位于安装管理服务器的目录中。默认安装路径为/opt/kaspersky/ksc64/sbin。

2. 使用 SrvUseStrictSslSettings 标志在管理服务器上配置允许的加密协议和加密套件。在根账户下的命令行处执行以下命令：

   ```
   ./klscflag -fset -pv ".core/.independent" -s Transport -n SrvUseStrictSslSettings -v <value> -t d
   ```

   指定 SrvUseStrictSslSettings 标志的<value>参数：

   - 4—仅启用 TLS 1.2 和 TLS 1.3 协议。此外，还启用了具有 TLS_RSA_WITH_AES_256_GCM_SHA384 的加密套件（向后兼容 Kaspersky Security Center Linux 先前版本需要这些加密套件）。这是默认值。

     TLS 1.2 协议支持的密码套件：

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - AES256-GCM-SHA384（具有 TLS_RSA_WITH_AES_256_GCM_SHA384 的密码套件）
     - ECDHE-RSA-AES128-GCM-SHA256
     - ECDHE-RSA-AES128-SHA256

     TLS 1.3 协议支持的密码套件：

     - TLS_AES_256_GCM_SHA384
     - TLS_CHACHA20_POLY1305_SHA256
     - TLS_AES_128_GCM_SHA256
     - TLS_AES_128_CCM_SHA256

   - 5—仅启用 TLS 1.2 和 TLS 1.3 协议。对于 TLS 1.2 和 TLS 1.3 协议，支持下面列出的特定密码套件。

     TLS 1.2 协议支持的密码套件：

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - ECDHE-RSA-AES128-GCM-SHA256
     - ECDHE-RSA-AES128-SHA256

TLS 1.3 协议支持的密码套件：

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256

我们不建议使用 0、1、2 或 3 作为 SrvUseStrictSslSettings 标志的参数值。这些参数值对应于不安全的 TLS 协议版本（TLS 1.0 和 TLS 1.1）和不安全的密码套件，仅用于向后兼容早期 Kaspersky Security Center 版本。

3. 重新启动以下 Kaspersky Security Center Linux 服务：
   - 管理服务器
   - Web 服务器
   - 激活代理

这样就启用了使用 TLS 协议的流量加密。

您可以使用 KLTR_TLS12_ENABLED 和 KLTR_TLS13_ENABLED 标志分别启用对 TLS 1.2 和 TLS 1.3 协议的支持。这些标志默认启用。

*要启用或禁用对 TLS 1.2 和 TLS 1.3 协议的支持：*

1. 运行 klscflag 实用程序。

   运行命令行，然后将当前目录更改为包含 klscflag 实用程序的目录。klscflag 实用程序位于安装管理服务器的目录中。默认安装路径为/opt/kaspersky/ksc64/sbin。

2. 在根账户下的命令行处执行以下命令之一：
   - 使用此命令启用或禁用对 TLS 1.2 协议的支持：

     ```
     ./klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS12_ENABLED -v <值> -t d
     ```

   - 使用此命令启用或禁用对 TLS 1.3 协议的支持：

     ```
     ./klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS13_ENABLED -v <值> -t d
     ```

   指定标志的 < 值 > 参数：

   - `1` – 启用对 TLS 协议支持。
   - `0`–禁用对 TLS 协议的支持。

# 用于与外部服务交互的网络设置

Kaspersky Security Center Linux 使用以下网络设置与外部服务交互。

网络设置

| 网络设置 | 地址 | 描述 |
| --- | --- | --- |
| 端口：<br>443<br>协议：<br>HTTPS | https://activation-v2.kaspersky.com | 应用程序激活。 |
| 端口：<br>443<br>协议：<br>HTTPS | https://s00.upd.kaspersky.com<br>https://s01.upd.kaspersky.com<br>https://s02.upd.kaspersky.com<br>https://s03.upd.kaspersky.com<br>https://s04.upd.kaspersky.com<br>https://s05.upd.kaspersky.com<br>https://s06.upd.kaspersky.com<br>https://s07.upd.kaspersky.com<br>https://s08.upd.kaspersky.com<br>https://s09.upd.kaspersky.com<br>https://s10.upd.kaspersky.com<br>https://s11.upd.kaspersky.com<br>https://s12.upd.kaspersky.com<br>https://s13.upd.kaspersky.com<br>https://s14.upd.kaspersky.com<br>https://s15.upd.kaspersky.com<br>https://s16.upd.kaspersky.com<br>https://s17.upd.kaspersky.com<br>https://s18.upd.kaspersky.com<br>https://s19.upd.kaspersky.com<br>https://cm.k.kaspersky-labs.com | 更新卡巴斯基数据库、软件模块和应用程序。 |
| 端口：<br>443<br>协议：<br>HTTPS | https://downloads.upd.kaspersky.com | • 更新卡巴斯基数据库、软件模块和应用程序。<br>• 检查卡巴斯基服务器是否可访问。<br>在下载卡巴斯基数据库和软件模块之前，Kaspersky Security Center Linux 会检查卡巴斯基服务器是否可访问。如果无法使用系统 DNS 访问服务器，应用程序将使用公共 DNS 服务器。 |

| 网络设置 | 地址 | 描述 |
| --- | --- | --- |
| 端口：80<br>协议：HTTP | http://p00.upd.kaspersky.com<br>http://p01.upd.kaspersky.com<br>http://p02.upd.kaspersky.com<br>http://p03.upd.kaspersky.com<br>http://p04.upd.kaspersky.com<br>http://p05.upd.kaspersky.com<br>http://p06.upd.kaspersky.com<br>http://p07.upd.kaspersky.com<br>http://p08.upd.kaspersky.com<br>http://p09.upd.kaspersky.com<br>http://p10.upd.kaspersky.com<br>http://p11.upd.kaspersky.com<br>http://p12.upd.kaspersky.com<br>http://p13.upd.kaspersky.com<br>http://p14.upd.kaspersky.com<br>http://p15.upd.kaspersky.com<br>http://p16.upd.kaspersky.com<br>http://p17.upd.kaspersky.com<br>http://p18.upd.kaspersky.com<br>http://p19.upd.kaspersky.com<br>http://downloads0.kaspersky-labs.com<br>http://downloads1.kaspersky-labs.com<br>http://downloads2.kaspersky-labs.com<br>http://downloads3.kaspersky-labs.com<br>http://downloads4.kaspersky-labs.com<br>http://downloads5.kaspersky-labs.com<br>http://downloads6.kaspersky-labs.com<br>http://downloads7.kaspersky-labs.com<br>http://downloads8.kaspersky-labs.com<br>http://downloads9.kaspersky-labs.com<br>http://downloads.kaspersky-labs.com<br>http://cm.k.kaspersky-labs.com | 更新卡巴斯基数据库、软件模块和应用程序。 |
| 端口：443<br>协议：HTTPS | https://ds.kaspersky.com<br>https://dc1.ksn.kaspersky-labs.com<br>https://dc1-file.ksn.kaspersky-labs.com<br>https://dc1-pp.ksn.kaspersky-labs.com<br>https://dc1-st.ksn.kaspersky-labs.com/<br>https://dc1-cert.ksn.kaspersky-labs.com<br>https://dc1-cf.ksn.kaspersky-labs.com<br>https://dc1-file.ksn.kaspersky-labs.com<br>https://dc1-kas.ksn.kaspersky-labs.com<br>https://dc1-ml.ksn.kaspersky-labs.com<br>https://dc1-pp.ksn.kaspersky-labs.com<br>https://dc1-st.ksn.kaspersky-labs.com<br>https://dc1.ksn.kaspersky-labs.com | 使用卡巴斯基安全网络。 |

| 网络设置 | 地址 | 描述 |
| --- | --- | --- |
| 端口：443、1443<br>协议：HTTPS | https://ksn-file-geo.kaspersky-labs.com<br>https://ksn-verdict-geo.kaspersky-labs.com<br>https://ksn-url-geo.kaspersky-labs.com<br>https://ksn-a-p2p-geo.kaspersky-labs.com<br>https://ksn-info-geo.kaspersky-labs.com<br>https://ksn-cinfo-geo.kaspersky-labs.com | 使用卡巴斯基安全网络。 |
| 端口：443、1443<br>协议：KSN | ksn://ksn-a-p2p-geo.kaspersky-labs.com<br>ksn://ksn-a-stat-geo.kaspersky-labs.com<br>ksn://ksn-ca-geo.kaspersky-labs.com<br>ksn://ksn-cinfo-geo.kaspersky-labs.com<br>ksn://ksn-crypto-catm-geo.kaspersky-labs.com<br>ksn://ksn-crypto-dnscheck-geo.kaspersky-labs.com<br>ksn://ksn-crypto-hash-geo.kaspersky-labs.com<br>ksn://ksn-crypto-ipm-geo.kaspersky-labs.com<br>ksn://ksn-crypto-whocalls-geo.kaspersky-labs.com<br>ksn://ksn-crypto-wifiplus-geo.kaspersky-labs.com<br>ksn://ksn-eu-stat-kmp.kaspersky-labs.com<br>ksn://ksn-file-geo.kaspersky-labs.com<br>ksn://ksn-his-geo.kaspersky-labs.com<br>ksn://ksn-info-geo.kaspersky-labs.com<br>ksn://ksn-kas-geo.kaspersky-labs.com<br>ksn://ksn-kddi.kaspersky-labs.com<br>ksn://ksn-ml-geo.kaspersky-labs.com<br>ksn://ksn-oui-geo.kaspersky-labs.com<br>ksn://ksn-pp.kaspersky-labs.com<br>ksn://ksn-src.kaspersky-labs.com<br>ksn://ksn-stat-geo.kaspersky-labs.com<br>ksn://ksn-tcert-geo.kaspersky-labs.com<br>ksn://ksn-url-geo.kaspersky-labs.com<br>ksn://ksn-verdict-geo.kaspersky-labs.com<br>ksn://mdr.ksn.kaspersky-labs.com<br>ksn://stat-eu.ksn.kaspersky-labs.com<br>ksn://stat-hq.ksn.kaspersky-labs.com<br>ksn://stat-ru.ksn.kaspersky-labs.com<br>ksn://stat-sa.ksn.kaspersky-labs.com<br>ksn://stat-sbr.ksn.kaspersky-labs.com | 使用卡巴斯基安全网络。 |
| 端口：443<br>协议：HTTPS | https://click.kaspersky.com<br>https://redirect.kaspersky.com | 打开界面中的链接。 |

| 网络设置 | 地址 | 描述 |
| --- | --- | --- |
| 端口：80<br>协议：HTTP | `http://crl.kaspersky.com`<br>`http://ocsp.kaspersky.com` | 这些服务器是公钥基础设施 (PKI) 的一部分，验证卡巴斯基数字签名证书的有效性状态所必需。CRL 是已撤销证书的列表。OCSP 允许您实时请求特定证书的状态。这些服务器有助于确保与数字证书交互的安全性并防止可能的攻击。 |
| 端口：443<br>协议：HTTPS | `https://ipm-klca.kaspersky.com` | 营销公告。 |
| 端口：443<br>协议：HTTPS | `https://tip.kaspersky.com` | 通过卡巴斯基威胁情报门户应对威胁（使用Kaspersky Next XDR Optimum 功能时）。 |
| 端口：443<br>协议：HTTPS | 有关完整地址列表，请参阅地址和域名结构文章 | 通过 Kaspersky Automated Security Awareness Platform 应对威胁（使用 Kaspersky Next XDR Optimum 功能时）。 |

为确保 Kaspersky Security Center Linux 与外部服务正常交互，请考虑以下建议：
- 必须允许未加密的网络流量通过组织的网络设备和代理服务器上的端口 443 和 1443。
- 当管理服务器与卡巴斯基更新服务器和卡巴斯基安全网络服务器交互时，必须避免通过证书替换劫持网络流量（MITM 攻击）。

*要使用 klscflag 实用程序通过 HTTP 或 HTTPS 协议下载更新：*

1. 运行命令行，然后将当前目录更改为包含 klscflag 实用程序的目录。klscflag 实用程序位于安装管理服务器的目录中。默认安装路径为/opt/kaspersky/ksc64/sbin。
2. 如果您想通过 HTTP 协议下载更新，请在根账户下运行以下命令之一：

   - 在安装了管理服务器的设备上：

     ```
     klscflag -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 1
     ```

   - 在分发点上：

     ```
     klscflag -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 1
     ```

   如果您想通过 HTTPS 协议下载更新，请在根账户下运行以下命令之一：

   - 在安装了管理服务器的设备上：

     ```
     klscflag -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 0
     ```

   - 在分发点上：

     ```
     klscflag -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 0
     ```

# 子网全局列表

对于使用的每个管理服务器，您可以设置一个全局子网列表来存储有关网络子网的信息。该列表帮助您匹配对（IP 地址、掩码）和物理单元，例如分支办公室。您可以在网络规则和设置中使用该列表中的子网。

*要添加子网到子网全局列表：*

1. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**全局子网**”部分。
3. 单击“**添加**”按钮。
   “**新子网**”窗口将开启。
4. 填充以下字段：
   - **名称**
   - **子网地址**
   - **子网掩码**
   - **描述**
5. 单击“**保存**”按钮。

窗口关闭，子网出现在子网列表中。

如有必要，您可以在全局子网列表中执行以下操作：

- 通过选择所需子网并单击**删除**按钮，从列表中删除子网。
- 单击所需子网名称的链接，然后执行步骤 4-5 中描述的操作，修改子网的属性。

# 使用 klscmodchk 和 integrity_checker 实用程序检查模块的完整性

Kaspersky Security Center Linux 包含动态链接库、可执行文件、配置文件和接口文件形式的多个二进制模块。入侵者可以用包含恶意代码的其他文件替换一个或多个可执行模块或应用程序文件。为了防止模块和文件替换，Kaspersky Security Center Linux 使用 klscmodchk 和 integrity_checker 实用程序提供组件完整性检查。这些实用程序可检查模块和文件是否有未经授权的更改或损坏。如果模块或应用程序文件的校验和不正确，则被视为已损坏。

klscmodchk 实用程序对以下 Kaspersky Security Center Linux 组件执行完整性检查：

- 管理服务器
- 网络代理

integrity_checker 实用程序可对以下 Kaspersky Security Center Linux 组件执行完整性检查：

- 管理服务器
- 网络代理
- Kaspersky Security Center Web Console

这两个实用程序都可根据 kl_file_integrity_manifest.xml 清单文件检查模块完整性，该文件是 Kaspersky Security Center Linux 内部版本的一部分，位于安装程序文件夹中。组件清单文件包含的文件的完整性对于 Kaspersky Security Center Linux 组件的正确运行非常重要。清单文件本身的完整性也会得到检查。

强烈建议不要修改 kl_file_integrity_manifest.xml 清单文件，因为这将使数字签名无效并导致完整性检查失败。

要检查 Kaspersky Security Center Linux 组件的完整性，请运行以下命令之一：

- `$ klscmodchk [ 参数 ]`

  klscmodchk 实用程序使用 `--verbose` 参数启动 integrity_checker 实用程序并检查模块的完整性。

  klscmodchk 实用程序的参数：

  - `-logfile < log_file_path >` — 指定磁盘上用于记录的文件的路径。默认情况下，信息被输出到控制台。
  - `-verbose` — 在完整性检查期间输出扩展信息。

- `$ integrity_checker [ 参数 ] < manifest_file_path >`

  integrity_checker 实用程序的参数：

  - `--help` — 显示 integrity_checker 实用程序帮助。
  - `--version` — 显示 integrity_checker 实用程序版本。
  - `--verbose` — 显示有关实用程序操作的信息。执行完整性检查时，在命令中使用此参数就足够了。

每个清单文件的检查结果以以下格式显示在清单文件名旁边：

- SUCCEEDED — 文件完整性得到确认（返回代码 0）。
- FAILED — 文件完整性未确认（非零返回代码）。

您还可以将完整性检查配置为在启动应用程序时自动运行。默认情况下，自动完整性检查处于禁用状态。

*要启用自动完整性检查：*

1. 在安装了管理服务器的设备上，在命令提示符中输入以下命令：

   ```
   ./klscflag -fset -pv klserver -n KLMODCHK_ENABLE_CHECKING -t d -v 1
   ```

2. 重启设备(&R)

自动完整性检查已启用。

下次运行 Kaspersky Security Center 时，klscmodchk 实用程序将与管理服务器一起运行，并启动模块完整性检查。完整性检查的结果将被写入卡巴斯基事件日志。

# 发现网络设备

该部分描述网络设备的搜索和发现。

Kaspersky Security Center Linux 允许您按照指定规则查找设备。您可以保存搜索结果到文本文件。

搜索和发现功能允许您查找以下设备：

- Kaspersky Security Center 管理服务器及其从属管理服务器的管理组中的受管理设备。
- 由 Kaspersky Security Center 管理服务器及其从属管理服务器管理的未分配设备。

# 情景：发现网络设备

您必须在安装安全应用程序之前执行设备发现。当所有网络设备被发现时，您可以接收它们的信息并通过策略管理。常规网络轮询用于发现是否有新设备以及先前发现的设备是否仍在网络中。

网络设备发现分步骤进行：

1. **初始设备发现**

   完成快速启动向导后，手动执行设备发现。

2. **配置未来轮询**

   确保 IP 范围轮询已启用且轮询计划满足您组织的需要。当配置轮询计划时，使用建议的网络轮询频率。

   如果您的网络包括 IPv6 设备，还可以启用 Zeroconf 轮询。

   如果域中包含联网设备，建议使用域控制器轮询。

   使用基于 Windows 的分发点来轮询 Windows 网络。

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）。

# Windows 网络轮询

## 关于 Windows 网络轮询

Kaspersky Security Center Linux 管理服务器不支持 Windows 网络轮询。使用基于 Windows 的分发点来轮询 Windows 网络。

在快速轮询过程中，分发点只从所有网络域和工作组中设备的 NetBIOS 名称列表检索信息。在完整轮询中，以下信息被从每个客户端设备请求：

- 操作系统名称
- IP 地址
- DNS 名称
- NetBIOS 名称

快速轮询和完整轮询都需要以下：

- 端口 UDP 137/138、TCP 139、UDP 445、TCP 445、必须在网络中可用。
- SMB 协议已启用。
- 必须使用 Microsoft Computer Browser 服务，且主浏览器计算机必须在管理服务器上启用。
- 必须使用 Microsoft Computer Browser 服务，且主浏览器计算机必须在客户端设备上启用：
  - 至少一台设备上，如果网络设备数量不超过 32。
  - 对每 32 台网络设备至少一台设备上。

完整轮询仅在快速轮询至少运行了一次时可以运行。

# IP 范围轮询

Kaspersky Security Center Linux 尝试使用标准 DNS 请求为指定范围的每个 IPv4 地址执行反向名称解析到 DNS 名称。如果该操作成功，服务器发送 `ICMP ECHO REQUEST`（和 ping 命令相同）到所接收名称。如果设备响应，其信息被添加到 Kaspersky Security Center Linux 数据库。反向名称解析对于排除具有 IP 地址但不是计算机的网络设备是必要的，例如网络打印机或路由器。

该轮询方法依赖正确配置的本地 DNS 服务。它必须具有反向查询域。如果该域未被配置，IP 子网轮询将没有结果。

开始，Kaspersky Security Center Linux 从其所在设备的网络设置获取 IP 轮询范围。如果设备地址是 192.168.0.1 且子网掩码是 255.255.255.0，Kaspersky Security Center Linux 自动包含网络 192.168.0.0/24 到轮询地址。Kaspersky Security Center Linux 从 192.168.0.1 到 192.168.0.254 之间轮询所有地址。

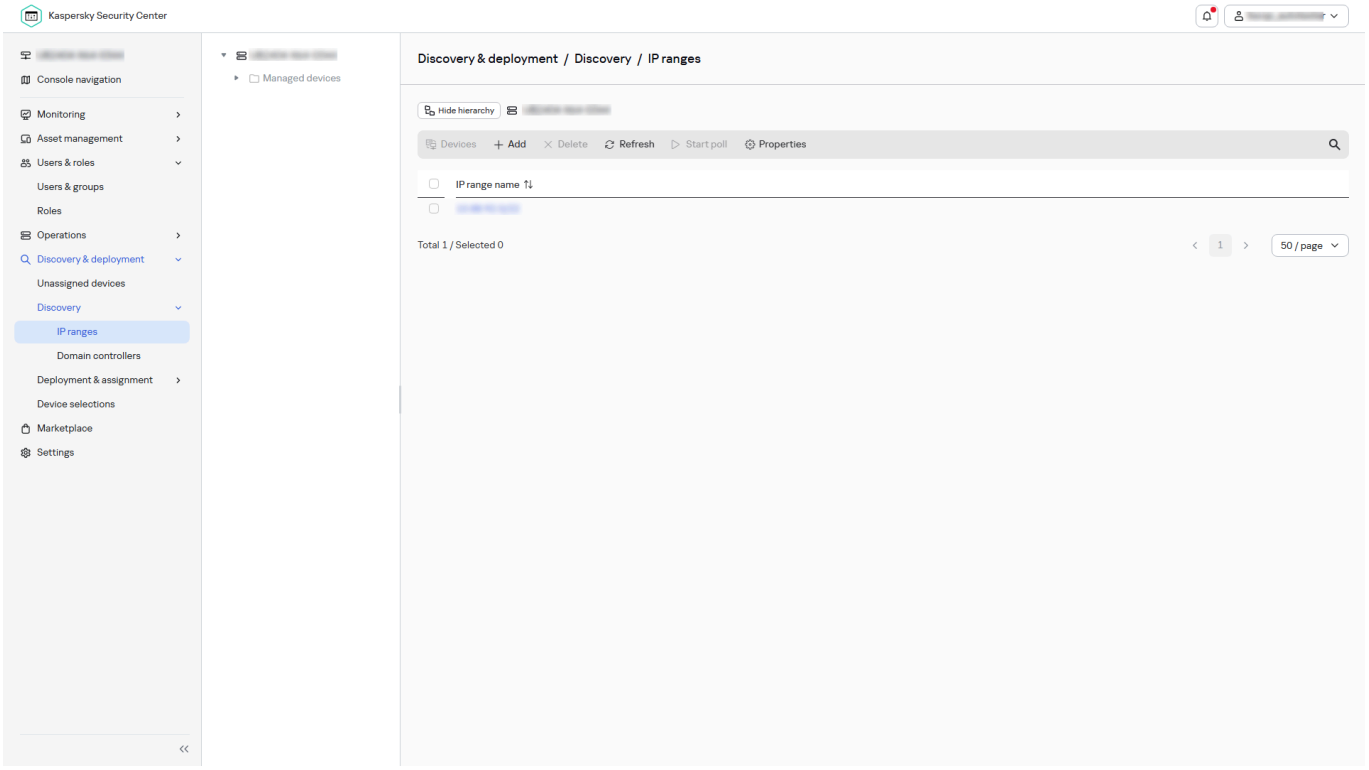
如果仅启用 IP 范围轮询，Kaspersky Security Center Linux 只会发现具有 IPv4 地址的设备。如果您的网络包括 IPv6 设备，请开启设备的 Zeroconf 轮询。

对于 Microsoft Active Directory、Samba、FreeIPA 或 ALD Pro 域控制器内的所有基于 Linux 的主机，在`/etc/samba/smb.conf`文件中指定`netbios name`和`workgroup`参数。否则，轮询结果可能包含重复的主机。

## 浏览和修改 IP 范围轮询设置

*要浏览和修改 IP 范围轮询设置：*

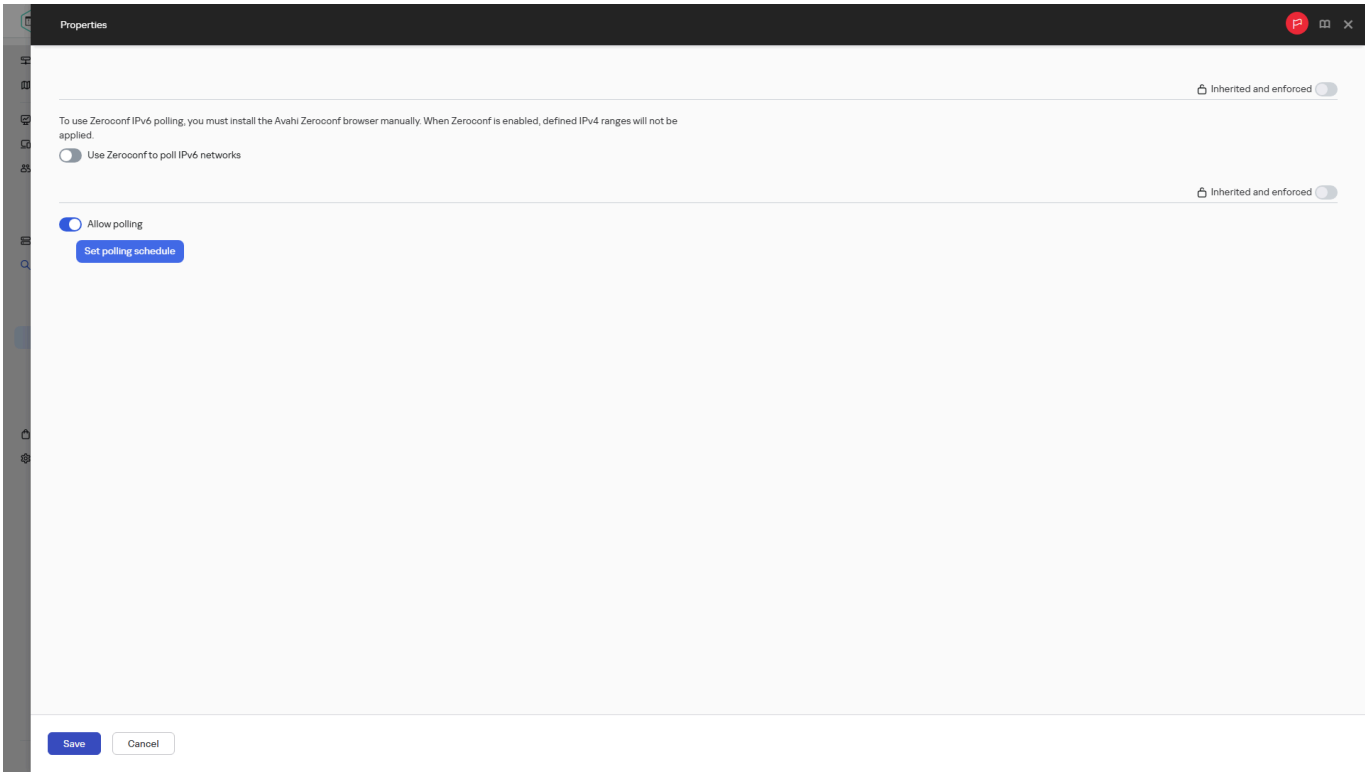
1. 在主菜单中，转到“**发现和部署**” → “**发现**” → “**IP 范围**”。




IP 范围列表

2. 单击“**属性**”按钮。

IP 轮询属性窗口将开启。




IP 轮询属性

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。

   - **每月在所选工作日**

     轮询定期运行，在指定月日的指定时间。

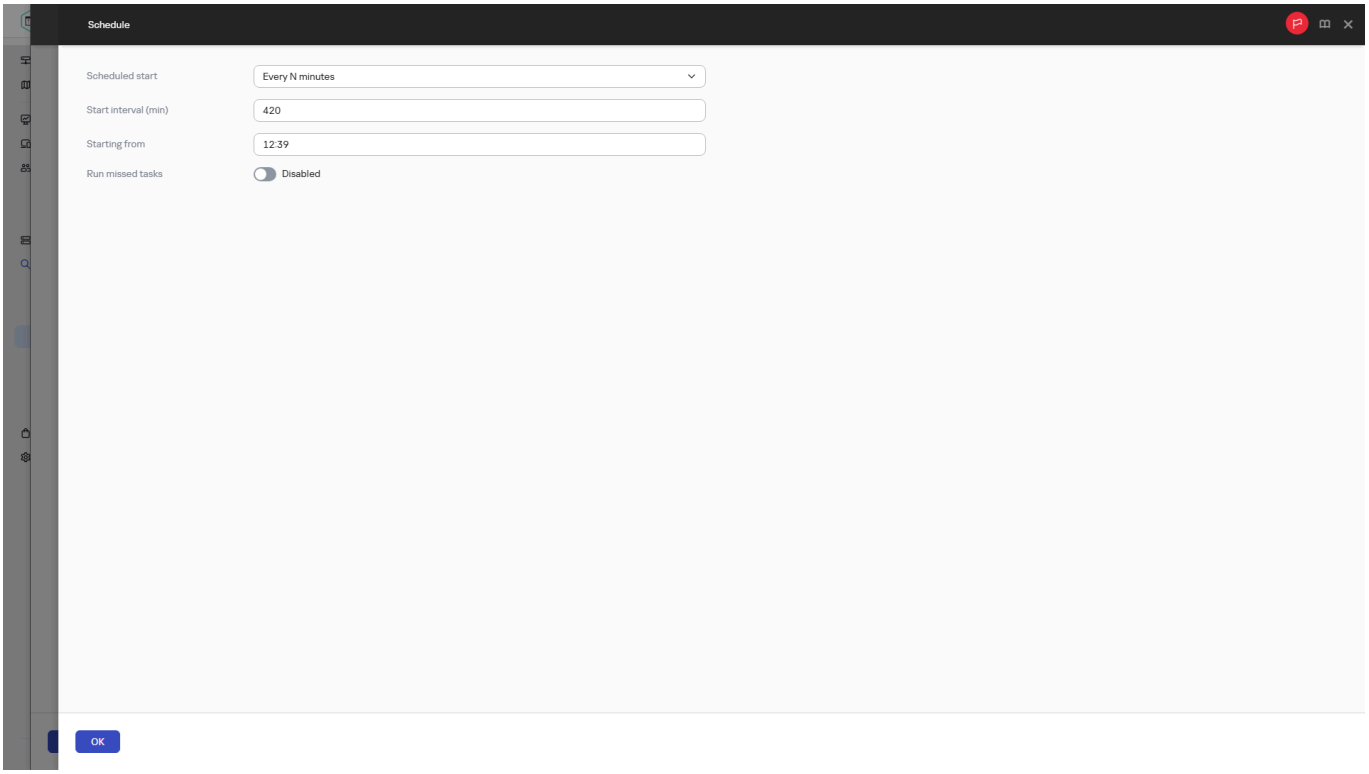
   - **运行错过的任务**

     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。




配置轮询计划

5. 单击“**保存**”按钮。

属性包保存并应用到所有 IP 范围。

手动运行轮询

*要立即运行轮询，*

单击**开始轮询**。

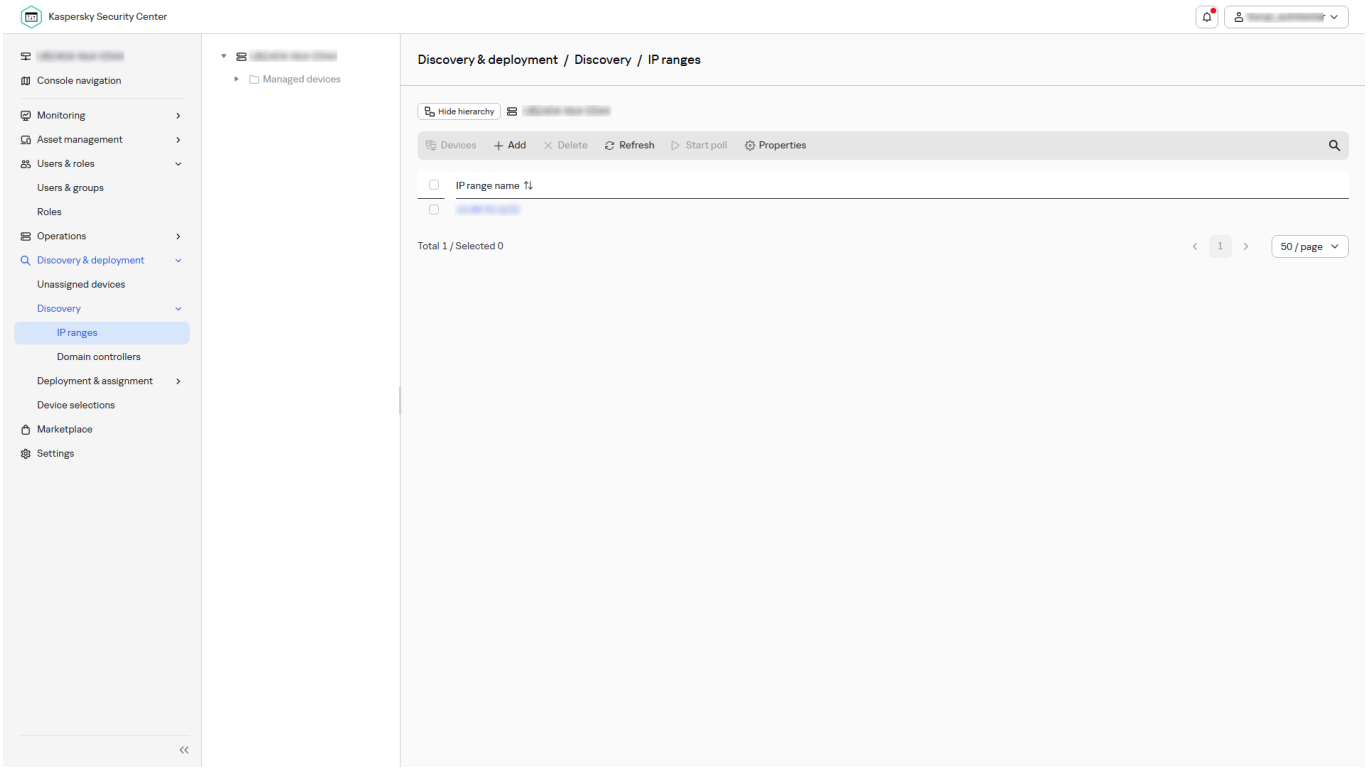
# 添加和修改 IP 范围

开始，Kaspersky Security Center Linux 从其所在设备的网络设置获取 IP 轮询范围。如果设备地址是 192.168.0.1 且子网掩码是 255.255.255.0，Kaspersky Security Center Linux 自动包含网络 192.168.0.0/24 到轮询地址。Kaspersky Security Center Linux 从 192.168.0.1 到 192.168.0.254 之间轮询所有地址。您可以修改自动定义的 IP 范围或添加自定义 IP 范围。

您只能创建 IPv4 地址范围。如果启用 Zeroconf 轮询，Kaspersky Security Center Linux 将轮询整个网络。

*要添加新 IP 范围：*

1. 在主菜单中，转到“**发现和部署**” → “**发现**” → “**IP 范围**”。




IP 范围列表

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"。

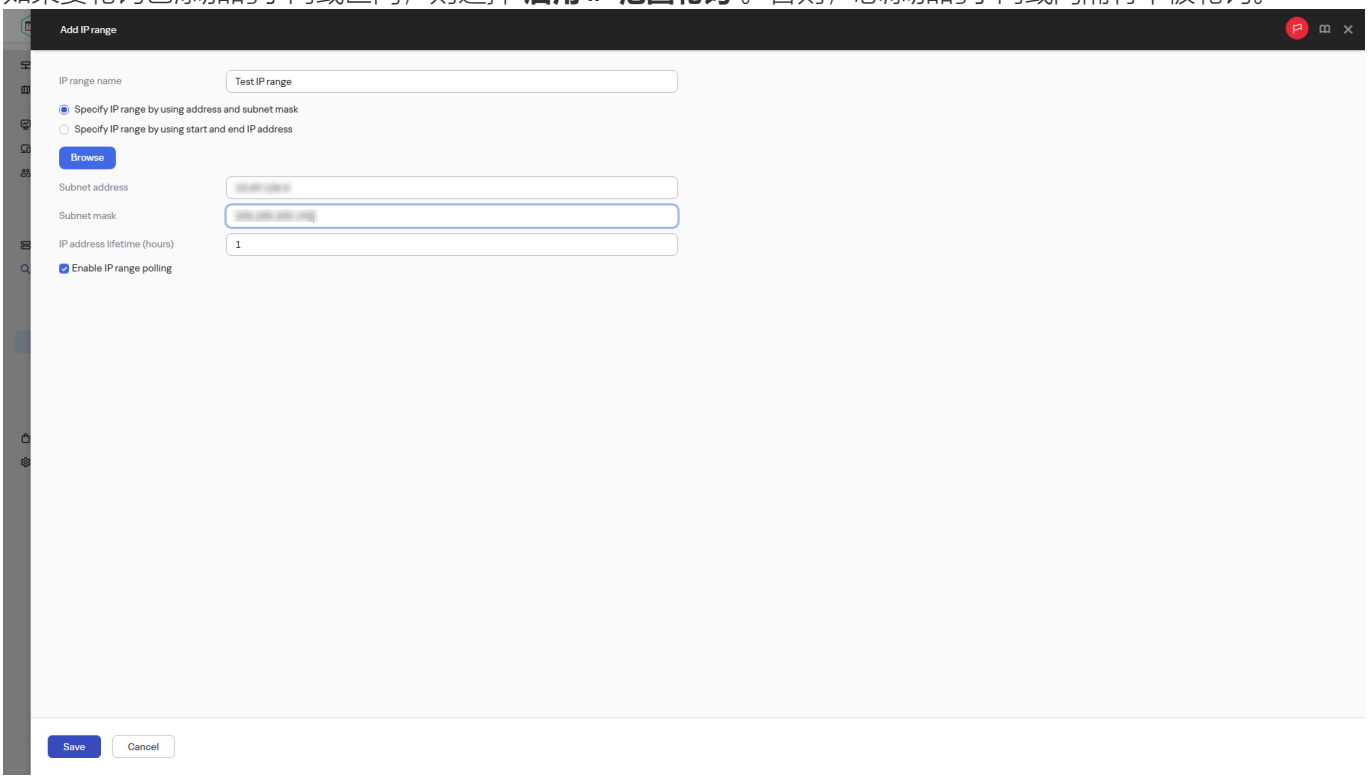
   - **IP 间隔或子网地址和掩码**

     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。




指定 IP 范围设置

5. 单击“**保存**”按钮。

新 IP 范围被添加到 IP 范围列表。

您可以使用“**开始轮询**”按钮分别对每个 IP 范围运行轮询。默认下，轮询结果的寿命是 24 小时，且等于 IP 地址生命周期设置。

*要添加子网到现有 IP 范围：*

1. 在主菜单中，转到“**发现和部署**”→“**发现**”→“**IP 范围**”。
2. 点击您要添加到子网的 IP 范围名称。
3. 在打开的窗口中，单击“**添加**”按钮。
4. 通过使用地址或者掩码指定子网，或者通过使用 IP 范围中的第一个和最后一个 IP 地址。或者，单击“**浏览**”按钮来添加一个现有子网。
5. 单击“**保存**”按钮。

   新子网被添加到 IP 范围。
6. 单击“**保存**”按钮。

IP 范围的新设置被保存。

您可以添加无限多的子网。命名 IP 范围不被允许重叠，IP 范围中的非命名子网没有此限制。您可以对每个 IP 范围独立启用和禁用轮询。

# Zeroconf 轮询

只有基于 Linux 的分发点支持此轮询类型。

Kaspersky Security Center Linux 可以轮询具有 IPv6 地址的设备的网络。在这种情况下，不指定 IP 范围，并且 Kaspersky Security Center Linux 使用零配置网络（也称为 *Zeroconf*）轮询整个网络。要开始使用 Zeroconf，您必须在轮询网络的 Linux 设备（管理服务器或分发点）上安装 avahi-browse 实用程序。

*要启用 Zeroconf 轮询：*

1. 在主菜单中，转到“**发现和部署**”→“**发现**”→“**IP 范围**”。
2. 单击“**属性**”按钮。
3. 在打开的窗口中，开启“**使用 Zeroconf 轮询 IPv6 网络**”切换按钮。

之后，Kaspersky Security Center Linux 将开始轮询您的网络。在这种情况下，指定的 IP 范围将被忽略。

# 域控制器轮询

Kaspersky Security Center Linux 支持轮询以下域控制器类型：

- Microsoft Active Directory
- Samba
- FreeIPA
- ALD Pro

对于 Samba 域控制器，Samba 4 用作 Active Directory 域控制器。

当您轮询域控制器时，管理服务器或分发点会检索有关域中包含的设备的域结构、用户账户、安全组和 DNS 名称的信息。

如果所有联网设备都是域的成员，我们建议使用域控制器轮询。如果某些联网设备未包含在域中，则域控制器轮询无法发现这些设备。

先决条件

轮询域控制器之前，请确保允许通过防火墙或代理服务器连接到域控制器。还要确保域控制器上启用了以下协议：

- 轻量级目录访问协议 (LDAP)
- 简单身份验证和安全层 (SASL)

  如果使用 SASL 身份验证建立与域控制器的连接，则使用此协议。管理服务器和分发点仅支持 DIGEST-MD5 机制。
- 安全套接字层上的轻量级目录访问协议 (LDAPS)

  如果您需要通过加密连接来连接到域控制器，则使用此协议。

确保域控制器设备上的以下端口可用：

- 389 表示 LDAP 协议和简单身份验证（包括 SASL）
- 636 表示 LDAPS 协议

对于 FreeIPA 和 ALD Pro， LDAP 和 LDAPS 协议仅用于域轮询。Kaspersky Security Center Linux 不支持通过 LDAP (S) 对 FreeIPA 账户进行身份验证。要允许 FreeIPA 和 ALD Pro 用户登录 Web Console，您必须通过 IAM 服务配置 Kerberos 身份验证。

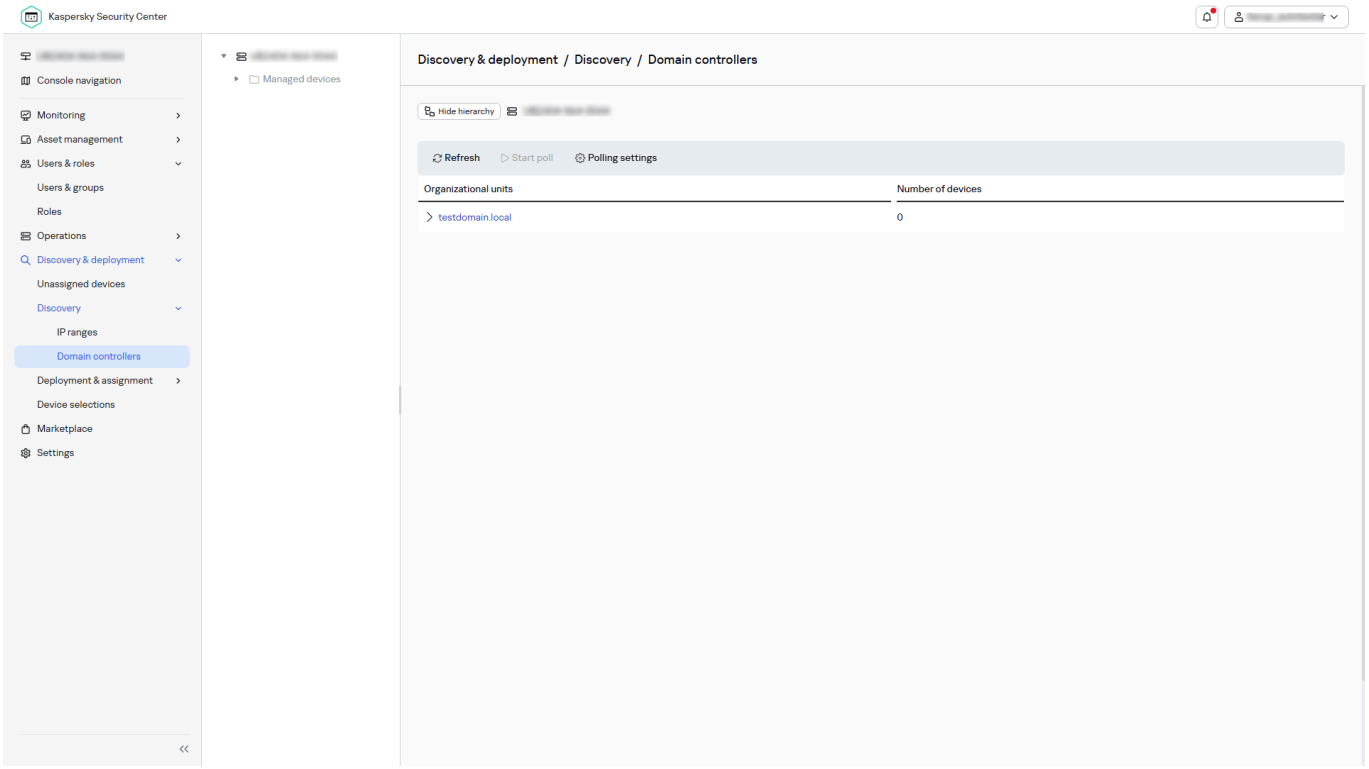
对于 Microsoft Active Directory、Samba、FreeIPA 或 ALD Pro 域控制器内的所有基于 Linux 的主机，您需要在 `/etc/samba/smb.conf` 文件中指定 `netbios name` 和 `workgroup` 参数。否则，轮询结果可能包含重复的主机。

如果 Microsoft Active Directory 域包含多个域控制器，则不支持在域轮询期间选择特定控制器。将与检测到的第一个域控制器建立连接。为确保与 Microsoft Active Directory 域进行正确的身份验证，证书的“使用者备用名称 (SAN)”字段必须包含此域中包含的所有域控制器的地址，以及 Microsoft Active Directory 域的 NetBIOS 名称。

## 使用管理服务器进行域控制器轮询

*要使用管理服务器轮询域控制器：*

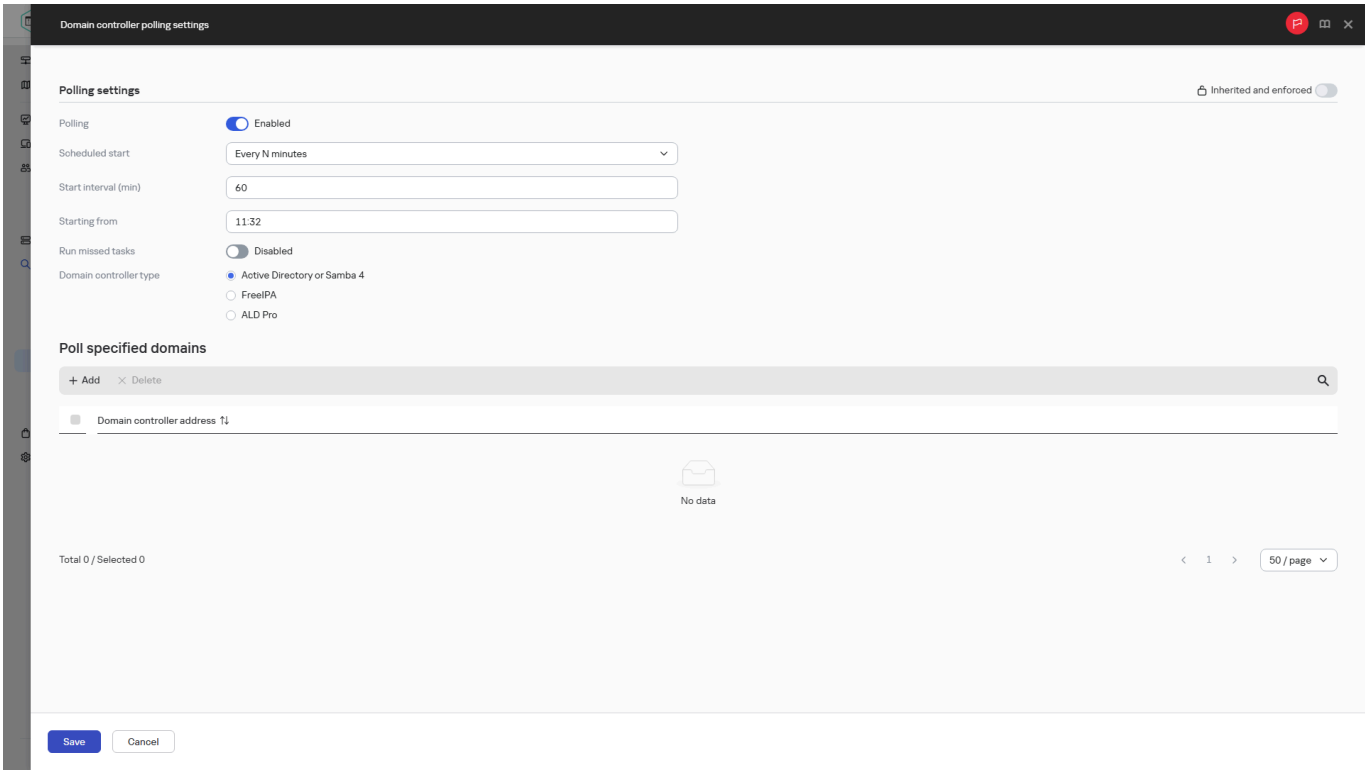
1. 在主菜单中，转到**发现和部署 → 发现 → 域控制器**。




域控制器轮询窗口

2. 单击**配置轮询设置**。

   **域控制器轮询设置**窗口将打开。




域控制器轮询设置

3. 在**轮询**字段中，将切换按钮切换到**已启用**位置。

4. 在**轮询指定域**中，单击**添加**，然后指定域控制器的地址和用户凭据。

5. 在**域控制器轮询设置**窗口中，执行以下操作：

- 选择要轮询的域控制器的类型：**Active Directory 或 Samba 4**、**FreeIPA**、**ALD Pro**。
- 如果必要，指定轮询计划：默认间隔是一小时。下次轮询接收的数据会完全替换旧数据。
  有以下轮询计划选项可用：
  - **每 N 天**

    轮询定期运行，按照指定天数间隔，从指定的日期和时间开始。
    默认下，轮询每天运行一次，从当前系统日期和时间开始。
  - **每 N 分钟**

    轮询定期运行，按照指定分钟间隔，从指定的时间开始。
  - **按星期中的天数**

    轮询定期运行，在指定星期的指定时间。
  - **每月在所选工作日**

    轮询定期运行，在指定月日的指定时间。
  - **运行错过的任务**

    如果在计划轮询期间管理服务器被切换掉或不可用，管理服务器可以在切换回来后立即启动轮询，或者等待下次计划轮询。
    如果启用该选项，管理服务器在它切换回来后立即启动轮询。
    如果禁用该选项，管理服务器等待下一次计划轮询。
    默认情况下已禁用该选项。

如果您更改域安全组中的用户账户，这些更改将在您轮询域控制器一小时后显示在 Kaspersky Security Center Linux 中。

6. 单击**保存**以应用更改。

7. 如果您要立即执行轮询，请单击“**开始轮询**”按钮。

## 使用分发点进行域控制器轮询

您还可以使用分发点轮询域控制器。基于 Windows 或 Linux 的受管理设备可以充当分发点。

对于 Linux 分发点，支持轮询所有类型的域控制器。
对于 Windows 分发点，仅支持轮询 Microsoft Active Directory 域控制器。
不支持使用 Mac 分发点进行轮询。

*要使用分发点配置域控制器轮询：*

1. 打开分发点属性。
2. 选择**域控制器轮询**部分。
3. 在**轮询**字段中，将切换按钮切换到**已启用**位置。
4. 如果使用 Linux 分发点，请选择要轮询的域控制器的类型：**Active Directory 或 Samba 4**、**FreeIPA**、**ALD Pro**。
   使用分发点和使用管理服务器配置轮询时，不必指定相同的域控制器类型。
5. 选择要轮询的域控制器。
   如果您使用 Linux 分发点，请在“**轮询指定域**”部分中单击“**添加**”，然后指定域控制器的地址和用户凭据。
   如果您使用 Windows 分发点，则可以选择以下选项之一：
   - **轮询当前域**
   - **轮询整个域森林**
   - **轮询指定域**
6. 如果需要，单击“**设置轮询计划**”按钮以指定轮询计划选项。
   轮询仅根据指定的时间表开始。无法手动启动轮询。

轮询完成后，域结构将显示在**域控制器**部分。

如果设置并启用了设备移动规则，则新发现的设备将自动包含在“**受管理设备**”组中。如果未启用移动规则，新发现的设备将自动包含在“**未分配的设备**”组。

发现的用户账户可用于Kaspersky Security Center Web Console 中的域身份验证。

# 身份验证和连接到域控制器

## 轮询域时进行身份验证并连接到域控制器

当轮询域控制器时，管理服务器或分发点识别连接协议以建立与域控制器的初始连接。该协议用于将来与域控制器的所有连接。在建立与域控制器的初始连接时，您可以使用网络代理标志（KLNAG_LDAP_TLS_REQCERT 和 KLNAG_LDAP_SSL_CACERT）来更改连接选项。您可以按照本文所述使用 klscflag 配置网络代理标志。

与域控制器的初始连接过程如下：

1. 管理服务器或分发点尝试通过 LDAPS 连接到域控制器。

   默认情况下不需要证书验证。将 KLNAG_LDAP_TLS_REQCERT 标记设置为 1 以强制执行证书验证。

   KLNAG_LDAP_TLS_REQCERT 标记的可能值：

   - 0—已请求证书，但如果未提供证书或证书验证失败，则 TLS 连接仍被视为成功创建（默认值）。
   - 1—需要严格验证 LDAP 服务器证书。

   默认情况下，如果未指定 KLNAG_LDAP_SSL_CACERT 标志，则使用与操作系统相关的证书颁发机构 (CA) 的路径来访问证书链。使用 KLNAG_LDAP_SSL_CACERT 标志指定自定义路径。

2. 如果 LDAPS 连接失败，管理服务器或分发点将尝试使用 SASL (DIGEST-MD5) 通过非加密的 TCP 连接来连接到域控制器。

## 在向管理服务器验证域用户身份时，需要进行身份验证并连接到域控制器

当域用户在管理服务器上进行身份验证时，管理服务器会识别协议来与域控制器建立连接。

对于 FreeIPA 和 ALD Pro， LDAP 和 LDAPS 协议仅用于域轮询。Kaspersky Security Center Linux 不支持通过 LDAP (S) 对 FreeIPA 账户进行身份验证。要允许 FreeIPA 和 ALD Pro 用户登录 Web Console，您必须通过 IAM 服务配置 Kerberos 身份验证。

与域控制器建立连接的过程如下：

1. 管理服务器尝试通过 LDAPS 连接到域控制器。

   需要严格验证 LDAP 服务器证书。

   默认情况下，如果未指定 KLNAG_LDAP_SSL_CACERT 标志，则使用与操作系统相关的证书颁发机构 (CA) 的路径来访问证书链。使用 KLNAG_LDAP_SSL_CACERT 标志指定自定义路径。

2. 如果 LDAPS 连接失败，则会出现连接域控制器的错误，并且不会使用其他连接协议。

配置标记

您可以使用 klscflag 实用程序来配置标志。

运行命令行，然后将当前目录更改为包含 klscflag 实用程序的目录。在管理服务器设备上，klscflag 实用程序位于安装目录中。默认安装路径为/opt/kaspersky/ksc64/sbin。

例如，以下命令强制执行证书验证：

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_TLS_REQCERT -t d -v 1
```

# 配置 Samba 域控制器

Kaspersky Security Center Linux 支持仅在 Samba 4 上运行的 Linux 域控制器。

Samba 域控制器支持与 Microsoft Active Directory 域控制器相同的架构扩展。您可以使用 Samba 4 架构扩展启用 Samba 域控制器与 Microsoft Active Directory 域控制器完全兼容。这是一个可选操作。

我们建议启用 Samba 域控制器与 Microsoft Active Directory 域控制器完全兼容。这将确保 Kaspersky Security Center Linux 和 Samba 域控制器之间的正确交互。

*要启用 Samba 域控制器与 Microsoft Active Directory 域控制器完全兼容：*

1. 执行以下命令以使用 RFC2307 架构扩展：

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. 在 Samba 域控制器中启用架构更新。为此，请将以下行添加到 `/etc/samba/smb.conf` 文件：

   ```
   dsdb:schema update allowed = true
   ```

   如果架构更新完成时出现错误，则需要对充当架构主机的域控制器执行完整还原。

对于 Samba 域控制器中的所有基于 Linux 的主机，请在 `/etc/samba/smb.conf` 文件中指定 `netbios name` 和 `workgroup` 参数。否则，轮询结果可能包含重复的主机。

# 设备清单

用于清查设备的硬件清单（**资产管理 → 硬件**）以两种方式填充：自动和手动。每次网络轮询后，所有检测到的设备都会自动添加到列表中；但是，如果您不希望轮询网络，也可以手动添加设备。您可以手动将其他设备添加到列表中，例如路由器、打印机或设备硬件。

您可以在设备的属性中查看并编辑有关该设备的详细信息。

硬件列表可能包含以下类型的设备：

- 计算机
- 移动设备
- 网络设备
- 虚拟设备
- OEM 组件
- 计算机周边设备
- 已连接设备
- VoIP 电话
- 网络存储库

管理员可以将“*企业设备*”属性分配给所检测到的设备。管理员可以在设备的属性中手动分配该属性，或者指定自动分配该属性的条件。在这种情况下，系统将按设备类型分配“*企业设备*”属性。

Kaspersky Security Center Linux 允许注销设备。为此，请在设备属性中选择“**写入**”选项。此类设备不会显示在设备列表中。

管理员可以在“**硬件**”文件夹管理可编程逻辑控制器 (PLC) 的列表。管理 PLC 列表的详细信息提供在 *Kaspersky Industrial CyberSecurity for Nodes 用户指南*。

# 添加有关新设备的信息

*若要添加网络中新设备的信息，请执行以下操作：*

1. 在主菜单中，转到**资产管理→ 硬件**。
2. 单击**添加**按钮打开**新设备**窗口。
3. 在“**新设备**”窗口中，从“**设备类型**”下拉列表中选择您要添加的设备类型。
4. 单击“**确定**”。
   此时将打开设备属性窗口，显示“**常规**”区域。
5. 在“**常规**”区域中使用设备数据填写输入字段。“**常规**”区域将显示以下设置：
   - **企业设备**。如果您希望将“*企业*”属性分配给该设备，请选择该选框。您可以使用该属性搜索“**硬件**”文件夹中的设备。
   - **写入**。如果您不希望该设备显示在“**硬件**”文件夹中的设备列表中，请选中该复选框。
6. 单击“**应用**”。

新设备将显示在“**硬件**”页面的工作区中。

# 配置用于定义企业设备的标准

*若要配置企业设备的检测标准，请执行以下操作：*

1. 在主菜单中，转到**资产管理→ 硬件**。
2. 在**硬件**页面顶部，单击**设置企业设备规则**链接。
   **设置企业设备规则**面板被调用。
3. 在**设置企业设备规则**面板中，启用**为设备自动设置 "企业" 属性**。指定为其自动分配*企业*属性的设备类型。

   此选项仅影响通过网络轮询添加的设备。对于手动添加的设备，请手动设置"*企业*"属性。

4. 单击"**确定**"。

企业设备的检测标准得到配置。

# 在客户端设备上使用 VDI 动态模式

虚拟基础架构可以使用临时虚拟机部署企业网络。Kaspersky Security Center Linux 检测到临时虚拟机和他们在管理服务器数据库的附加信息。用户使用完临时虚拟机后，这些虚拟机将从虚拟架构中移除。然而，以后虚拟机的记录可以保存在管理服务器数据库中。此外，不存在的虚拟机可能会显示在 Kaspersky Security Center Web Console 中。

为了防止不存在的虚拟机被保存，Kaspersky Security Center Linux 支持动态模式的虚拟桌面基础架构 (VDI)。管理员可以在被安装到临时虚拟机的网络代理安装包的属性中启用支持动态 VDI。

当临时虚拟机被禁用，网络代理通知管理服务器该虚拟机已被禁用。如果虚拟机被成功禁用，它将从连接到管理服务器的设备列表中被移除。如果虚拟机被禁用错误，网络代理没有发送禁用虚拟机的通知到管理服务器，使用备份方案。使用这个方案，和管理服务器尝试同步三次未成功后，虚拟机从连接管理服务器的设备列表移除。

# 在网络代理安装包属性中启用 VDI 动态模式

*要启用 VDI 动态模式，请执行以下操作：*

1. 在主菜单中，前往**软件管理→安装包**。
2. 在网络代理安装包的上下文菜单中，选择"**属性**"。
   **属性**窗口将打开。
3. 在**属性**窗口中，选择"**高级**"部分。
4. 在"**高级**"部分中，选择"**启用 VDI 动态模式**"选项。

要安装网络代理的设备成为 VDI 的一部分。

# 将组成 VDI 的设备移至管理组

*要将组成 VDI 的设备移至管理组，请执行以下操作：*

1. 转到 **资产管理** → **移动规则**。
2. 单击**添加**。
3. 在“**规则条件**”选项卡上，选择“**虚拟机**”选项卡。
4. 将“**这是一台虚拟机**”规则设置为“**是**”，将“**虚拟桌面基础架构的一部分**”设置为“**是**”。
5. 单击“**保存**”。

# 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。**规则条件**设备可根据 Rule conditions 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. 在主菜单中，转到“**资产管理**” → “**资产(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。

- **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。

- **设备所有者**

  设备所有者的名称。您可以作为设备所有者，通过单击**管理设备所有者**链接分配或删除用户。

- **完整组名称**

  包括了客户端设备的管理组。

- **反病毒数据库上次更新**

  设备上病毒数据库或应用程序最后更新日期。

- **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。

- **上一次可见**

  设备在网络中最后可见的日期和时间。

- **网络代理版本**

  安装的网络代理的版本。

- **创建日期**

  Kaspersky Security Center Linux 内的设备创建日期。

- **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。

- **会话**

  本部分包含一个表格，其中含有有关当前登录到设备的用户的信息。该表在相应的列中显示以下数据：

  - 用户名
  - SAM 账户名
  - 用户主体名称
  - 邮件地址

  要正确显示有关域用户会话的信息，必须使用域控制器轮询。

- “**网络**”区域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。
  - **IPv6 地址**
- “**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。
  - **操作系统**
  - **CPU 架构**
  - **设备名称**
  - **虚拟机类型**

    虚拟机制造商。
  - **作为 VDI 一部分的动态虚拟机**

    此行显示客户端设备是否是作为 VDI 一部分的动态虚拟机。
- “**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：
  - **可见**

    客户端设备的可见状态。
  - **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。
  - **状态描述**

    客户端设备保护和与管理服务器连接的状态。
  - **保护状态**

    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。
  - **上一次全盘扫描**

    客户端设备上次执行恶意软件扫描的日期和时间。

- **检测到的病毒**

  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。

- **清除失败的对象**

  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。

- **磁盘加密状态**

  设备本地驱动器上的当前文件加密状态。有关状态的说明，请参阅 Kaspersky Endpoint Security for Windows 帮助。

  只能在安装了 Kaspersky Endpoint Security for Windows 的受管理设备上加密文件。

- "**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。如果推送服务器无法触达受管理设备，但启用了与管理服务器的持续连接模式（启用了**常规**部分中的**不断开与管理服务器的连接**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。

  您可以导出、复制和删除设备事件。

- **安全问题**

  在**安全问题**选项卡上，可以为客户端设备查看、编辑和创建安全问题。安全问题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。例如，如果用户定期将恶意软件从其可移动驱动器移至设备，则管理员可以创建安全问题。管理员可以在安全问题文本中提供情况的简要说明和建议的操作（例如对于一个用户的纪律性操作），还可以添加链接到用户。

  对其采用了所有必要操作的安全问题被称为*已处理安全问题*。存在的未处理安全问题可被选为将设备的状态更改为*严重*或*警告*的条件。

此部分包含已为设备创建的安全问题的列表。安全问题按严重级别和类型分类。安全问题类型由创建安全问题的卡巴斯基应用程序定义。选中**已处理**列中的复选框即可突出显示列表上的已处理安全问题。

- **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**

      单击“**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**

      单击“**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。

    如果网络代理安装在运行 Windows 的设备上，它会向管理服务器发送有关设备硬件的以下信息：

    - RAM
    - 大容量存储设备
    - 主板
    - CPU
    - 网络适配器
    - 监控器
    - 视频适配器
    - 声卡

    如果网络代理安装在运行 Linux 或 macOS 的设备上，它会向管理服务器发送有关设备硬件的以下信息（如果该信息由操作系统提供）：

    - 总 RAM 容量
    - 大容量存储设备总容量

- 主板
- CPU
- 网络适配器

- **可用更新**。该区域显示在该设备上发现的未安装的软件更新列表。
- **软件漏洞**。此区域提供有关客户端设备上安装的第三方应用程序中的漏洞信息。

  要将漏洞保存到文件中，请选择要保存的漏洞旁边的复选框，然后单击“**导出到 CSV**”按钮或“**导出到 TXT**”按钮。

  此部分包含以下设置：

  - **仅显示可以被修复的漏洞**

    如果启用此选项，该区域会显示可通过使用补丁修复的漏洞。

    如果禁用此选项，该区域会同时显示可通过使用补丁修复的漏洞，以及未发布补丁的漏洞。

    默认情况下已启用该选项。

  - **漏洞属性**

    单击列表中的软件漏洞名称，以在单独的窗口中查看所选软件漏洞的属性。在窗口中，您可以执行以下操作：

    - 忽略此受管理设备上的软件漏洞（在 Kaspersky Security Center Web Console 中）。
    - 查看该漏洞的建议修复程序列表。
    - 手动指定软件更新以修复漏洞（在 Kaspersky Security Center Web Console 中）。
    - 查看漏洞实例。
    - 查看现有任务列表以修复漏洞，并创建新任务以修复漏洞。

- **远程诊断**。在此区域，您可以执行远程诊断客户端设备。

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。

# 手动检查客户端设备与管理服务器之间的连接。Klnagchk 工具

您可以通过使用 klnagchk 实用程序手动检查连接和获取客户端设备与管理服务器之间的连接设置信息。klnagchk 实用程序位于网络代理安装文件夹。

从命令行启动时，klnagchk 实用程序能够执行以下操作（根据使用的键值）：

- 显示或记录用以连接设备上网络代理到管理服务器的设置值。
- 将网络代理统计数据（自上次启动以来）和实用程序运行结果记录在事件日志文件中或者显示在屏幕上。
- 尝试在网络代理和管理服务器之间建立连接。
  如果连接尝试失败，实用程序将发送一个 ICMP 包检查装有管理服务器的设备状态。

*要使用 klnagchk 实用程序检查客户端设备和管理服务器之间的连接，请执行以下操作：*

在安装了网络代理的设备上，以本地管理员账户从命令行启动 klnagchk 实用程序。

实用程序命令行语法：

```
klnagchk [-logfile <文件名>] [-sp] [-savecert <证书文件路径>] [-restart][-sendhb]
```

参数描述：

- `-logfile <文件名>` — 将网络代理和管理服务器之间连接设置的值和实用程序操作结果记录到日志文件中。
  默认情况下，信息保存在标准输出流（stdout）中。如果未使用该键值，设置、运行结果和错误信息将显示在屏幕上。
- `-sp` — 在代理服务器显示用于用户验证的密码。
  如果是通过代理服务器与管理服务器建立的连接，则使用本密钥。
- `-savecert <文件名>` – 在指定文件中保存用于访问管理服务器的证书。
- `-restart` — 实用程序操作完成后启动网络代理。
- `-sendhb` — 启动网络代理与管理服务器的同步。

启动后，klnagchk 实用程序将访问网络代理的配置文件并显示连接参数。这些参数在网络代理安装期间和网络代理策略设置中指定：

- `Current device` — 客户端设备的 Windows 网络名。
- `Network Agent version` — 设备上安装的网络代理版本（带补丁）的完整编号。
- `Administration Server address` — 管理服务器的地址。
- `Use SSL` — 该参数指示连接到管理服务器时是否使用安全连接。
  可能值：
  - 0—不使用安全连接。
  - 1—使用安全连接。
- `Compress traffic` — 该参数指示客户端设备和管理服务器之间的流量是否被压缩。
- `Numbers of the Administration Server SSL ports` — 使用安全连接与管理服务器通信的有效端口数。
- `Numbers of the Administration Server ports` — 使用普通连接与管理服务器通信的有效端口数。

- `Use proxy server` — 指示是否使用代理服务器的参数。

  可能值：

  - 0—不使用代理服务器。
  - 1—使用代理服务器。

- `Address` — 代理服务器的地址和端口，以冒号分隔。仅当使用代理服务器时才会显示此参数。
- `User name` — 用于访问代理服务器的用户名。仅当使用代理服务器时才会显示此参数。
- `Password` — 用于访问代理服务器的密码。仅当使用代理服务器时才会显示此参数。要显示代理服务器密码，需要在命令中使用`sp`密钥。
- `Administration Server certificate` — 指示客户端设备是否具有管理服务器证书的参数。例如，如果网络代理从未成功连接到管理服务器，则证书可能不存在。

  可能值：

  - `not installed` — 客户端设备没有管理服务器证书。
  - `available` — 客户端设备具有管理服务器证书。

- `Open UDP port` — 该参数指示网络代理是否使用 UDP 端口接收来自管理服务器的同步请求。

  可能值：

  - 0—UDP 端口已关闭，无法接收来自管理服务器的同步请求。
  - 1—UDP 端口已打开，可用于接收来自管理服务器的同步请求。

- `Numbers of UDP ports` — 网络代理可以使用的 UDP 端口数。
- `Location name` — 设备的网络位置。
- `State of network location` — 指示客户端设备是否可以从一个管理服务器连接配置文件切换到另一个管理服务器连接配置文件的参数。

  可能值：

  - `Enabled` — 可以为客户端设备切换管理服务器连接配置文件。
  - `Disabled` — 无法为客户端设备切换管理服务器连接配置文件。

- `Profile to use` — 管理服务器的连接配置文件。
- `Condition` — 客户端设备所连接的网络的 IP 地址和子网掩码。
- `Synchronization interval (min)` — 同步之间的标准间隔。
- `Connection timeout (in seconds)` — 连接超时。
- `Send / receive timeout (in seconds)` — 读写操作的连接超时。
- `Device ID` — 网络中的设备标识符。`Device ID`在特定管理服务器管理的客户端设备中是唯一的。

- `Locations of connection gateways` — 通过连接网关将客户端设备连接到管理服务器的参数。
- `Location of distribution points` — 通过分发点将客户端设备连接到管理服务器的参数。
- `Connection with server` — 该参数指示连接网关是否与管理服务器具有持续的连接。仅当客户端设备充当连接网关时才显示该参数。

  可能值：

  - `active` — 连接网关与管理服务器保持持续连接。
  - `inactive` — 连接网关与管理服务器没有持续连接。
- `Connection with server through connection gateway` — 该参数指示是否正确建立了通过连接网关与管理服务器的连接。仅当客户端设备充当连接网关时才显示该参数。

  可能值：

  - `active` — 通过连接网关与管理服务器的连接已正确建立。
  - `inactive` — 通过连接网关与管理服务器的连接建立不正确。

此外，klnagchk 实用程序输出可能包含以下行之一：

- `Administration Server is installed on this device` — klnagchk 实用程序在管理服务器设备上运行。
- `This device has been assigned a connection gateway but is not yet registered on Administration Server` — klnagchk 实用程序在安装了网络代理的设备上以连接网关模式运行。配置的连接网关正在等待来自管理服务器的连接，但管理服务器未将该设备列在管理设备中。您需要确保管理服务器发起与连接网关的连接。
- `This device is a connection gateway` — klnagchk 实用程序在充当连接网关的设备上运行。
- `Acts as a distribution point` — klnagchk 实用程序在充当分发点的设备上运行。

klnagchk 实用程序可检查网络代理服务的状态。如果该服务未运行，实用程序将停止。如果服务正在运行，实用程序将显示以下连接统计信息：

- `Total number of synchronization requests` — 尝试连接客户端设备到管理服务器的次数。
- `The number of successful synchronization request` — 尝试将客户端设备连接到管理服务器的成功次数。
- `Total number of synchronizations` — 尝试将客户端设备设置与管理服务器设置同步的次数。
- `The number of successful synchronizations` — 尝试将客户端设备设置与管理服务器同步的成功次数。
- `Date/time of the last request for synchronization` — 上次连接的日期和时间。

在分析管理服务器和网络代理之间的连接时，需要使用`Total number of synchronization requests`和`The number of successful synchronization request`。仅当管理服务器设置发生更改时（例如，添加了新任务或修改了策略设置），客户端设备设置才会与管理服务器设置同步。否则，`Total number of synchronizations`和`The number of successful synchronizations`参数值保持不变。

有关如何解决网络代理连接到管理服务器的问题的更多信息，请参阅Kaspersky Security Center Linux 常见问题解答。

# 设备移动规则

建议通过*设备移动规则*自动分配设备到管理组。设备移动规则由三个主要部分组成：名称、执行条件（带设备属性的逻辑表达式）和目标管理组。如果设备属性满足规则执行条件，则规则移动设备到目标管理组。

所有设备移动规则都有优先级。管理服务器检查设备属性以查看它们是否满足每条规则的执行条件（升序优先级）。如果设备属性满足某条规则的执行条件，设备被移动到目标组，至此规则处理在该设备上完成。如果设备属性满足多个规则的条件，设备被移动到具有高优先级的规则的目标组。

设备移动规则可以被间接创建。例如，在安装包或远程安装任务的属性中，您可以指定安装网络代理后设备必须被移动到的管理组。而且，设备移动规则可以被 Kaspersky Security Center Linux 管理员明确创建，在“**资产管理**”→“**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）。

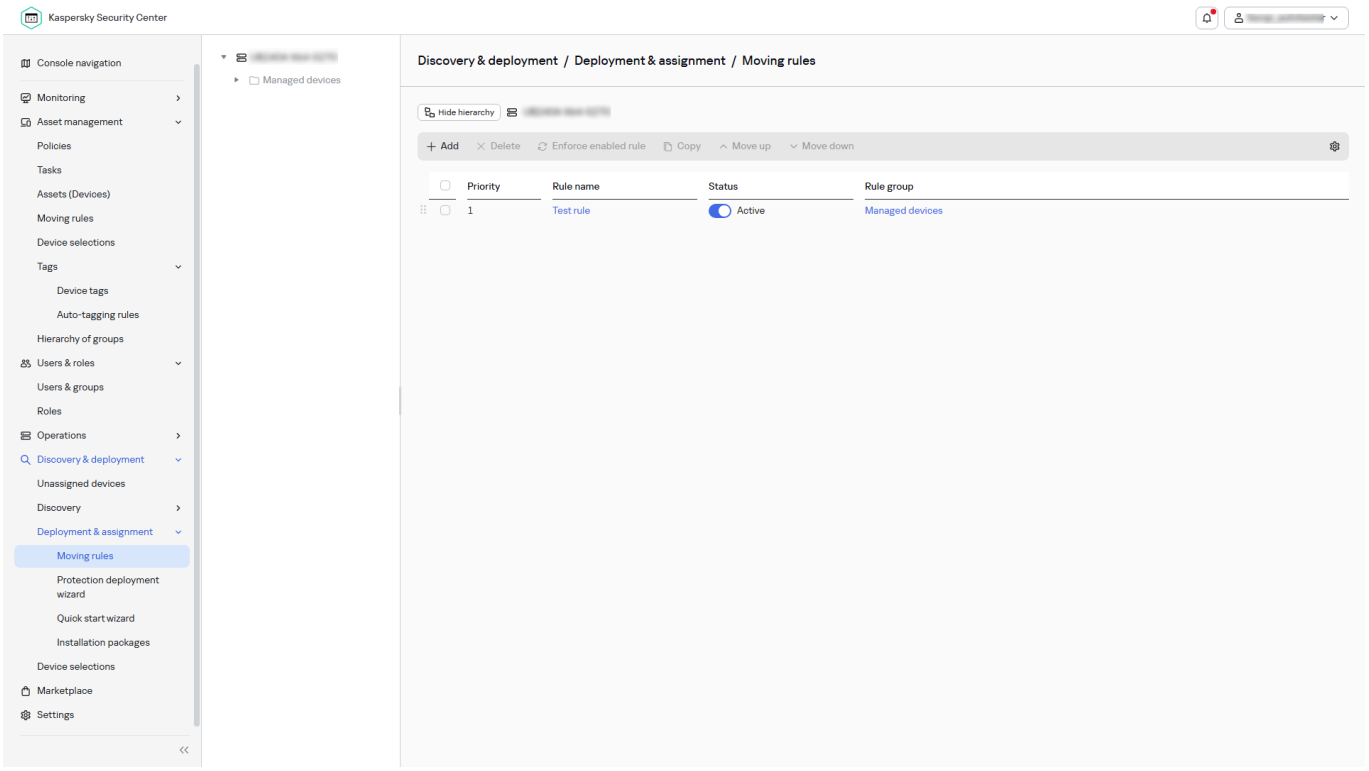
此类方案不被支持，因为它们显著增加了管理服务器负载和网络流量。这些方案也与 Kaspersky Security Center Linux 的操作原则冲突（尤其在访问权限、事件和报告方面）。必须找到其他解决方案，例如，通过使用策略配置文件、设备分类的任务、根据标准方案分配网络代理。

# 创建设备移动规则

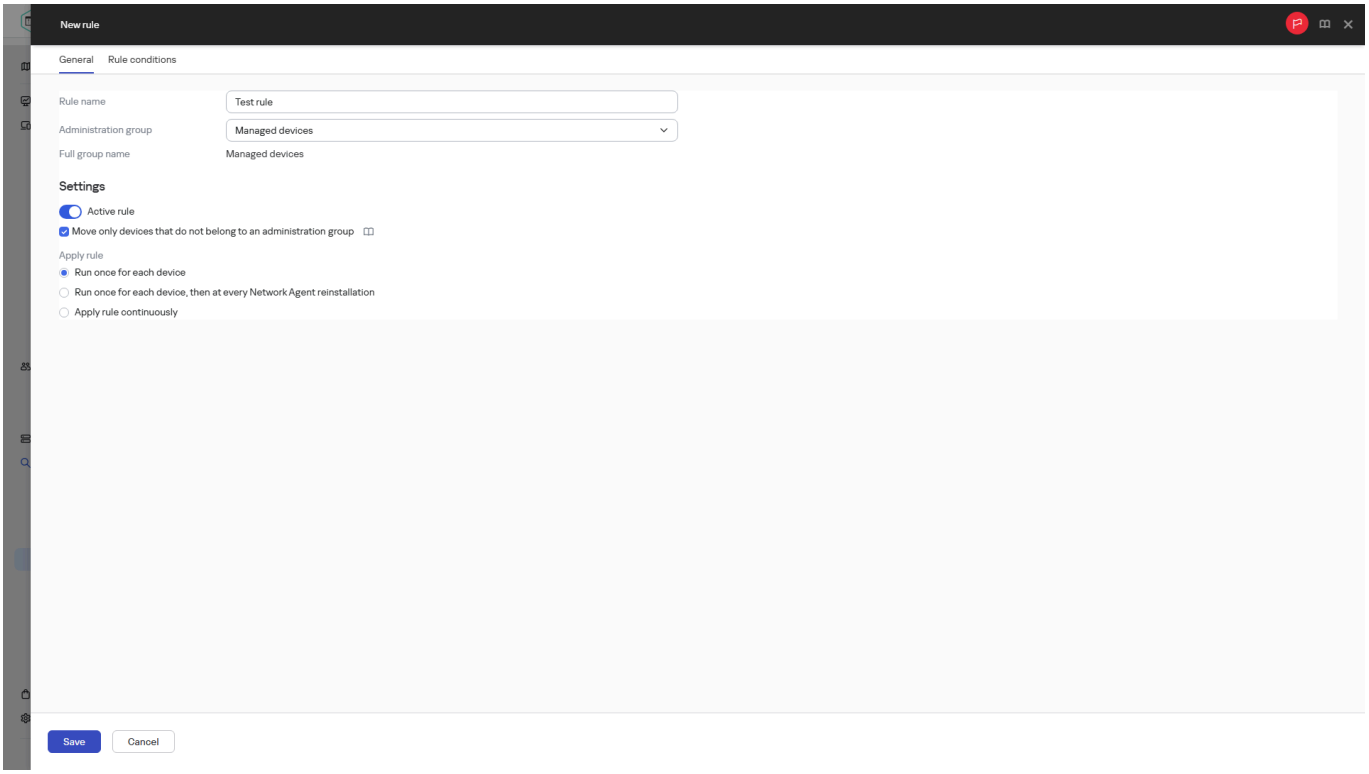
您可以设置设备移动规则，即自动分配设备到管理组的规则。

*要创建移动规则：*

1. 在主菜单中，转到“**资产管理**”→“**移动规则**”。




2. 单击**添加**。“**新规则**”窗口将开启。




3. 在打开的窗口中，在“**常规**”选项卡上指定以下信息：

- **规则名称**

  输入新规则名称。

  如果您正复制规则，新规则与源规则名称相同，但是索引格式 () 被添加到名称，例如：(1)。

- **管理组**

  选择要自动移动设备的管理组。

- **激活的规则**

  如果启用该选项，规则被启用并在被保存后开始工作。

  如果禁用该选项，规则被创建，但不被启用。直到您启用该选项它才工作。

- **优先级**

  您可以指定移动规则的优先等级。最高优先级为1。**优先级**值越大，规则的优先等级越低，在列表中的位置也越靠后。

  如果未指定优先等级，则规则的优先等级为最低。

  复制规则时，副本的优先等级与原规则相同。原规则的优先等级则加1。

- **仅移动不属于任何管理组的设备**

  如果启用该选项，仅未分配的设备将被移动到所选组。

  如果禁用该选项，已经属于其他管理组的设备以及未分配的设备将被移动到所选组。

- **应用规则**

  您可以选择以下选项之一：

  - **对每台设备运行一次**

    规则对匹配标准的每台设备应用一次。

  - **对每台设备运行一次，然后在每次网络代理重新安装时**

    规则对匹配标准的每台设备应用一次，然后仅在网络代理被重新安装到这些设备时。

  - **持续应用规则**

    规则根据管理服务器自动设置的计划被应用（通常每几个小时）。

4. 在“**规则条件**”选项卡上，指定至少一个标准，设备将依据该标准移至管理组。
5. 单击“**保存**”。

移动规则被创建。它显示在移动规则列表。

列表上的位置越高，规则的优先级越高。

*要更改优先级：*

1. 选中移动规则的复选框。
2. 执行以下操作之一：

   - 单击**更改优先级**按钮，然后指定新的优先级。
   - 单击**上移**或**下移**按钮，即可分别在列表中向上或向下移动规则。

3. 单击“**保存**”按钮。

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

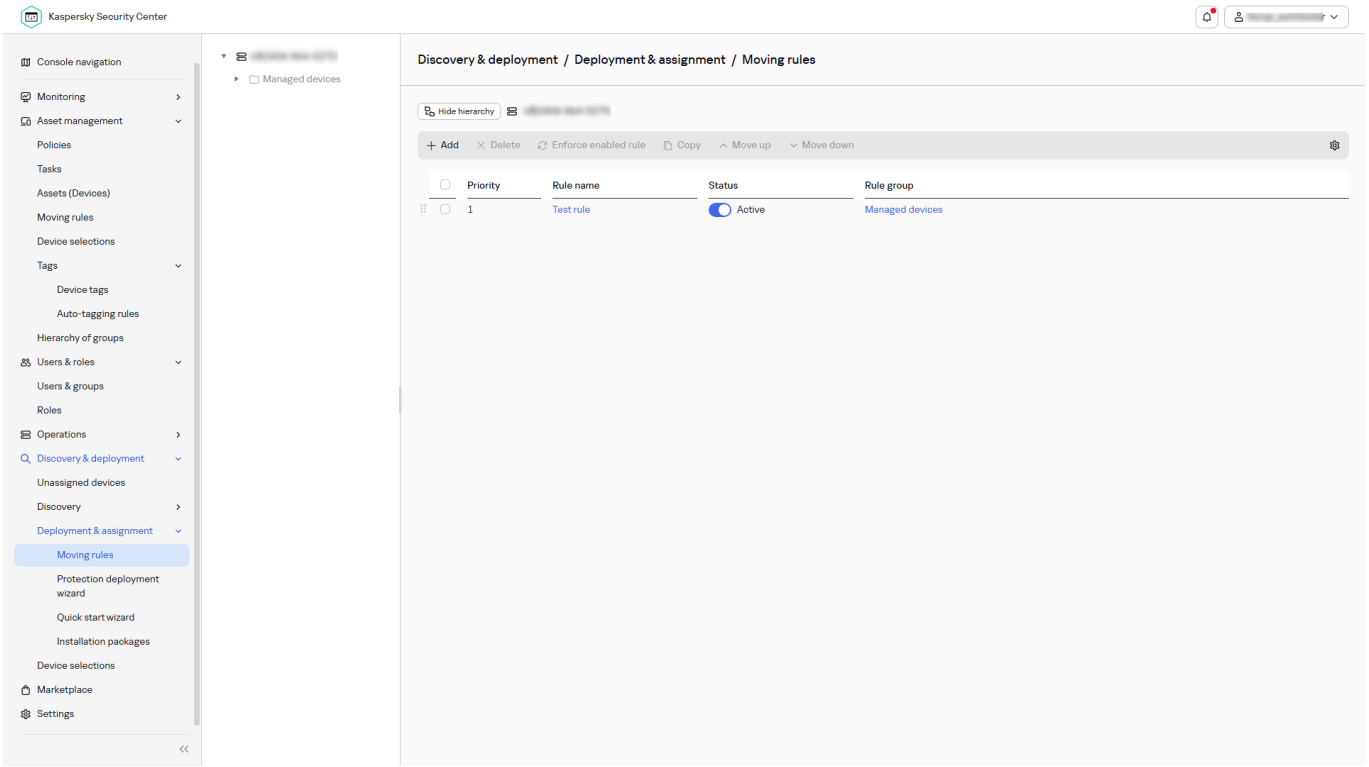
您可以复制移动规则，例如，如果您要对不同目标管理组拥有几个相同规则。

要复制现有移动规则：

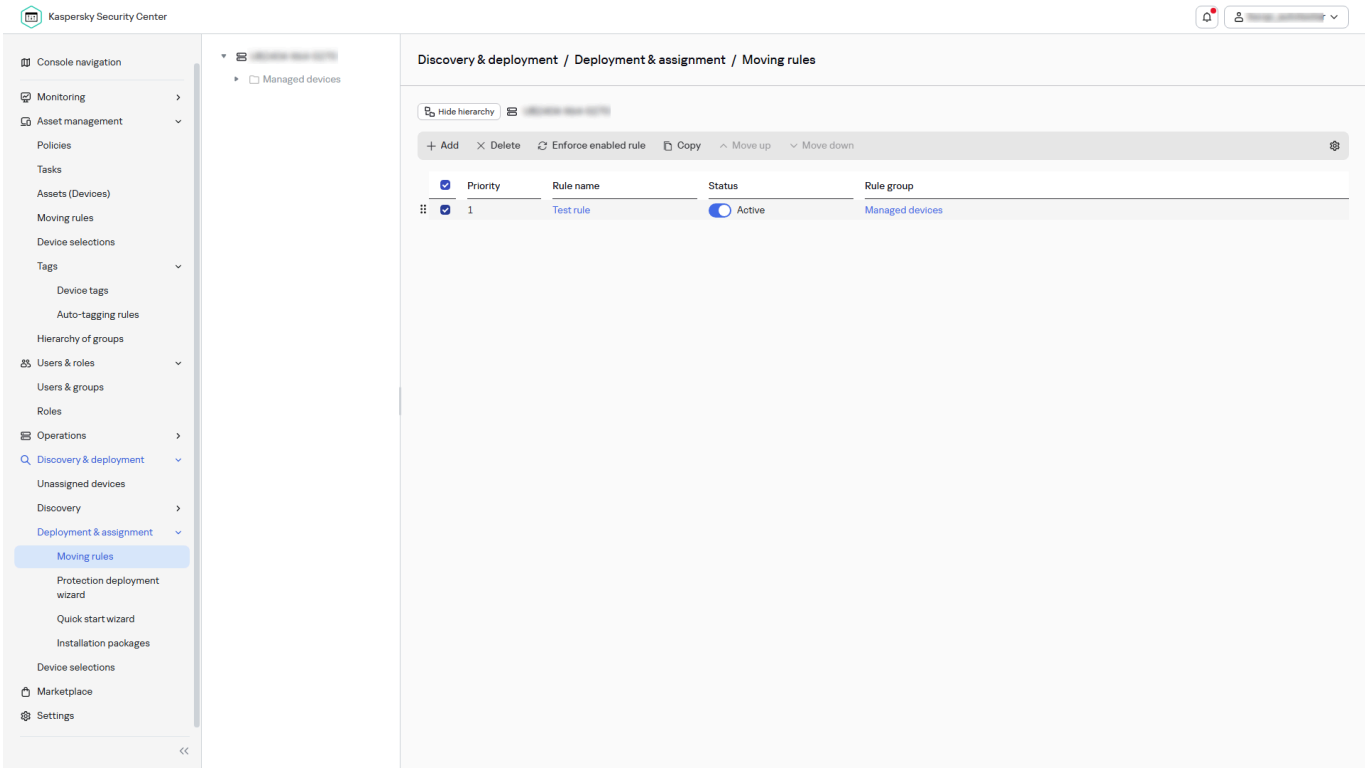
1. 执行以下操作之一：

   - 在主菜单中，转到“**资产管理**”→“**移动规则**”。
   - 在主菜单中，转到“**发现和部署**”→“**部署和分配**”→“**移动规则**”。

   移动规则列表被显示。



2. 选择您要复制的规则旁边的复选框。




3. 单击**复制**。

4. 在打开的窗口中的"**常规**"选项卡上更改以下信息或不进行任何更改（如果您仅想复制规则而不更改其设置）：

- **规则名称**

  输入新规则名称。

  如果您正复制规则，新规则与源规则名称相同，但是索引格式 () 被添加到名称，例如：(1)。

- **管理组**

  选择要自动移动设备的管理组。

- **激活的规则**

  如果启用该选项，规则被启用并在被保存后开始工作。

  如果禁用该选项，规则被创建，但不被启用。直到您启用该选项它才工作。

- **优先级**

  您可以指定移动规则的优先等级。最高优先级为1。**优先级**值越大，规则的优先等级越低，在列表中的位置也越靠后。

  如果未指定优先等级，则规则的优先等级为最低。

  复制规则时，副本的优先等级与原规则相同。原规则的优先等级则加1。

- **仅移动不属于任何管理组的设备**

  如果启用该选项，仅未分配的设备将被移动到所选组。

  如果禁用该选项，已经属于其他管理组的设备以及未分配的设备将被移动到所选组。

- **应用规则**

  您可以选择以下选项之一：

  - **对每台设备运行一次**

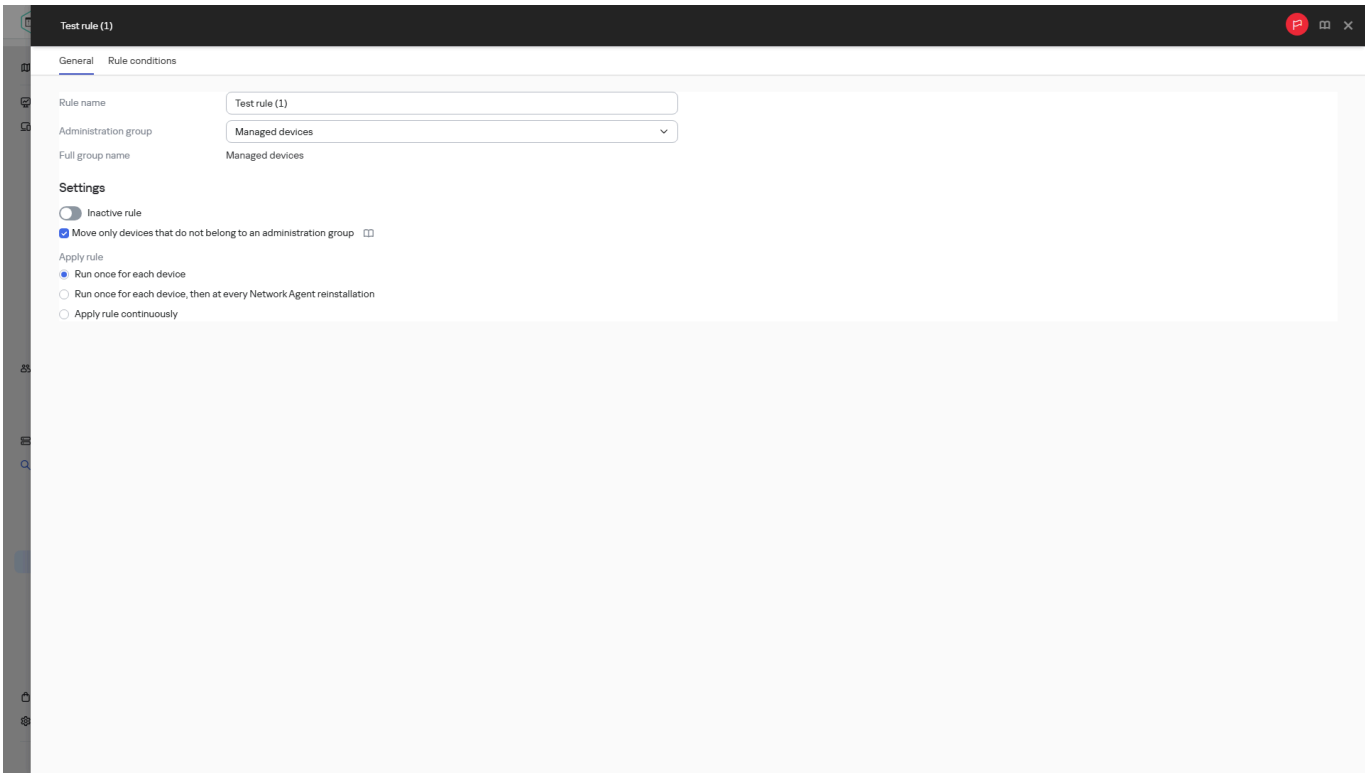
    规则对匹配标准的每台设备应用一次。

  - **对每台设备运行一次，然后在每次网络代理重新安装时**

    规则对匹配标准的每台设备应用一次，然后仅在网络代理被重新安装到这些设备时。

  - **持续应用规则**

    规则根据管理服务器自动设置的计划被应用（通常每几个小时）。




5. 在“**规则条件**”选项卡上，为您希望自动移动的设备指定至少一个标准。

6. 单击“**保存**”。

新移动规则被创建。它显示在移动规则列表。

# 设备移动规则的条件

当创建或复制将客户端设备移动到管理组的规则时，在“**规则条件**”选项卡上设置移动设备的条件。要确定移动哪些设备，可以使用以下标准：

- 分配给客户端设备的标签。
- 网络参数。例如，您可以移动具有指定范围内 IP 地址的设备。
- 安装在客户端设备上的受管理应用程序，例如网络代理或管理服务器。
- 虚拟机，即客户端设备。

您可以在下面找到有关如何在设备移动规则中指定此信息的说明。

如果在规则中指定多个条件，AND 逻辑运算符将生效并且所有条件同时适用。如果不选择任何选项或将某些字段留空，则此类条件不适用。

### 标签选项卡

在该选项卡上，可以基于先前添加到客户端设备描述的设备标签配置设备移动规则。为此，请选择所需标签。此外，还可以启用以下选项：

- **应用到没有指定标签的设备**

  如果启用此选项，则具有指定标签的所有设备都将从设备移动规则中排除。如果禁用此选项，则设备移动规则应用于具有所有选定标签的设备。

  默认情况下已禁用该选项。

- **如果至少一个指定的标签匹配则应用**

  如果启用此选项，则设备移动规则将应用于具有至少一个选定标签的客户端设备。如果禁用此选项，则设备移动规则应用于具有所有选定标签的设备。

  默认情况下已禁用该选项。

### 网络选项卡

在此选项卡上，可以指定设备移动规则考虑的设备的网络数据：

- **Windows 网络中的设备名**

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

- **设备的 DNS 名称**

  要移动的客户端设备的 DNS 域名。如果网络包含 DNS 服务器，请填写此字段。

  > 如果为您用于 Kaspersky Security Center Linux 的数据库设置了区分大小写的排序规则，请在指定设备 DNS 名称时保持大小写。否则，设备移动规则将不起作用。

- **DNS 域**

  设备移动规则应用于指定主 DNS 后缀中包含的所有设备。如果网络包含 DNS 服务器，请填写此字段。

- **IP 范围**

  如果启用此选项，您可以输入应该包括相关设备的 IP 范围的初始和最终 IP 地址。

  默认情况下已禁用该选项。

- **用于连接管理服务器的 IP 地址**

  如果启用此选项，则可以设置客户端设备用于连接到管理服务器的 IP 地址。为此，请指定包含所有必要 IP 地址的 IP 范围。

默认情况下已禁用该选项。

- **设备在 IP 范围中**

  如果启用此选项，您可以选择之前在**IP 范围**部分添加的 IP 范围。相关设备必须包含在所选的 IP 范围内。
  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。

“设备所有者”选项卡

在此选项卡上，您可以根据设备所有者、安全组成员身份和角色配置设备移动规则：

- **设备所有者**

  从内部安全组中选择设备所有者的用户名。在本部分中了解有关用户和用户角色的更多信息。

  > 最多只能有一名用户注册为设备所有者。

- **在活动目录安全组中的设备所有者成员关系**

  选择设备所有者所属的外部活动目录安全组。

  > 用户可以是活动目录安全组的一部分，也可以是此活动目录安全组中包含的组的一部分。

- **设备所有者角色**

  选择设备所有者的指定角色。在本文中了解有关用户角色的更多信息。

- **设备所有者在内部安全组中的成员身份**

  选择设备所有者所属的内部安全组。

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 16.3 网络代理** 或 **Kaspersky Security Center 16.3 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。

- **OS 架构**

  您可以按操作系统位数来剔除客户端设备。在“**操作系统架构**”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架构：*

  1. 在主菜单中，转到**资产管理** → **资产(设备)**区域。
  2. 单击右侧的“**列设置**”按钮 ( )。
  3. 选择**OS 架构**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架构。

- **OS 包管理器**

  您可以按操作系统包管理器来筛选客户端设备。在“**OS 包管理器**”字段中，您可以选择以下值之一：

  - rpm — 适用于运行 Red Hat Enterprise Linux、CentOS、Fedora、SUSE、Oracle Linux 操作系统的设备
  - apt (dpkg) — 适用于运行 Debian、Ubuntu、Kali 操作系统的设备
  - pkg — 适用于运行 FreeBSD、OpenBSD 操作系统的设备

*要检查客户端设备的操作系统包管理器：*

1. 在主菜单中，转到**资产管理** → **资产(设备)**区域。
2. 单击右侧的“**列设置**”按钮（ ）。
3. 选择“**OS 包管理器**”选项，然后单击“**保存**”按钮。

每个受管理设备都会显示操作系统软件包管理器。

- **OS 服务包版本**

  在该字段中，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。

- **OS 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。

- **OS 发布号**

  > 该设置仅应用到 Windows 操作系统。

  您可以指定所选操作系统必须具有相同、更早还是更晚的版本号。您也可以为除指定版本号外的所有版本号配置设备移动规则。

虚拟机选项卡

在该选项卡上，可以根据客户端设备是否是虚拟机或虚拟桌面基础架构 (VDI) 的一部分来配置设备移动规则：

- **这是一台虚拟机**

  在该下拉列表中，可以选择以下选项之一：
  - **N/A**。条件不适用。
  - **否**。移动非虚拟机设备。
  - **是**。移动虚拟机设备。

- **虚拟机类型**
- **虚拟桌面基础架构的一部分**

  在该下拉列表中，可以选择以下选项之一：
  - **N/A**。条件不适用。
  - **否**。移动不属于 VDI 的设备。
  - **是**。移动属于 VDI 的设备。

域控制器选项卡

在此选项卡上，您可以指定需要移动域组织单元中包含的设备。您还可以从指定域组织单元的所有子组织单元移动设备：

- **设备包含在以下组织单元中**

  如果启用此选项，则设备移动规则将应用于该选项下的列表中指定的域控制器组织单元中的设备。
  默认情况下已禁用该选项。
- **包括子组织单元**

  如果启用此选项，选择范围将包括指定域控制器组织单元的所有子组织单元中的设备。
  默认情况下已禁用该选项。
- **将设备从子单元移动到对应子组**
- **创建对应于新检测到设备的容器的子组**
- **删除域中不存在的子组**
- **设备包含在以下域安全组中**

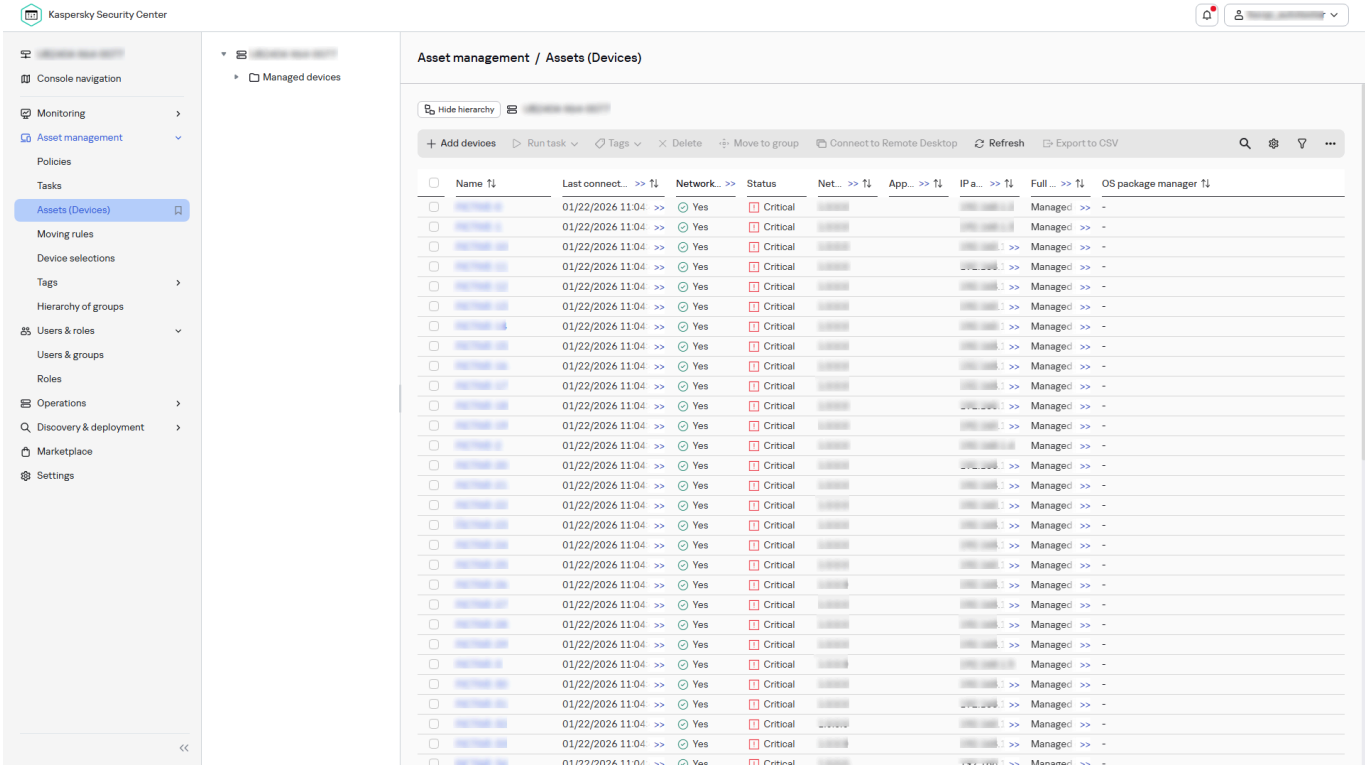
  如果启用此选项，设备移动规则将应用于该选项下的列表中指定的域安全组中的设备。
  默认情况下已禁用该选项。

# 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。本部分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. 在主菜单中，转到**资产管理 → 资产(设备)**。




受管理设备列表

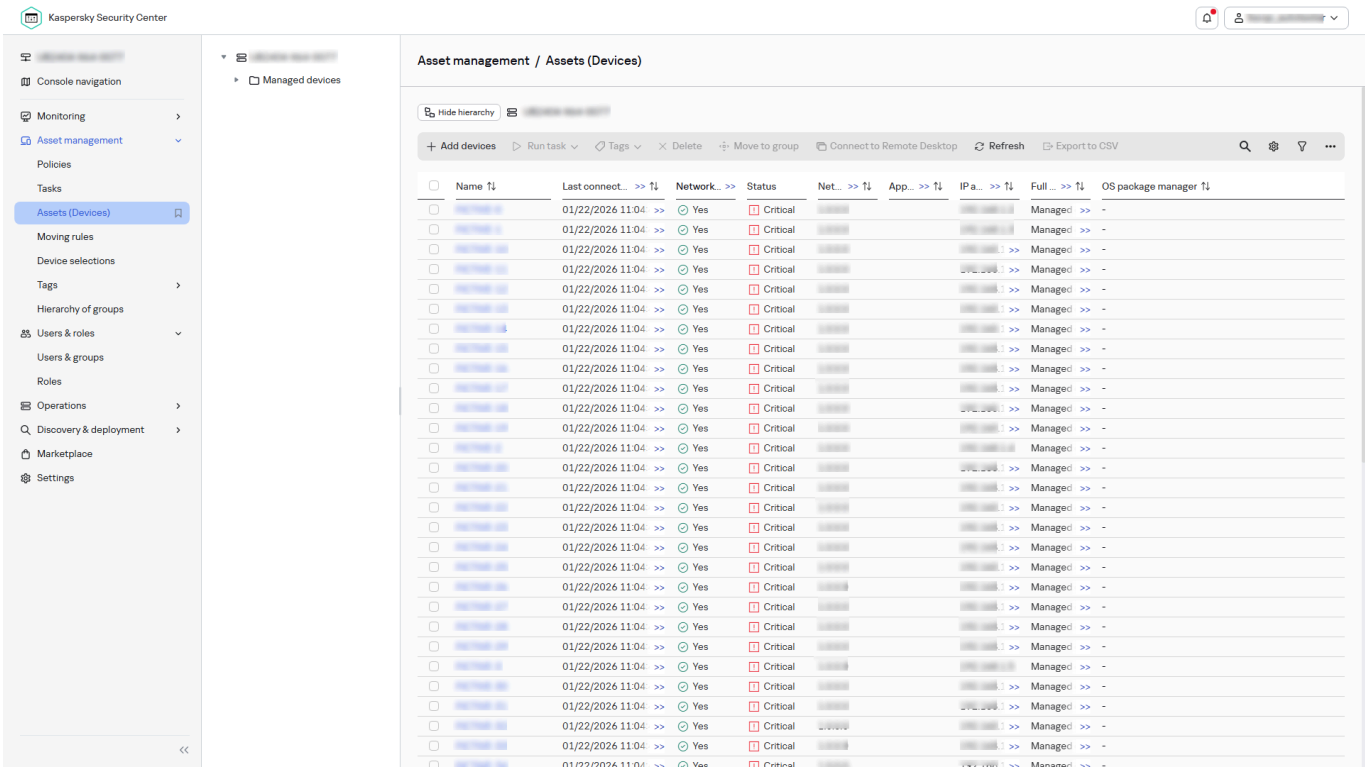
2. 选择您要向其添加设备的管理组：

- 对于根组：
  在这种情况下，您可以继续下一步。
- 对于子组：

  a. 单击页面顶部的“**显示层级**”按钮。
  按钮名称将更改为“**隐藏层级**”。

  b. 在打开的窗口中，单击子组的名称。

所选组的路径显示在页面顶部。如果需要，您可以单击带有管理组名称的链接前往该组。默认情况下，路径中的最后一个链接不活动。您也可以单击“**隐藏层级**”按钮关闭层次结构窗口。




选择管理组

3. 单击“**添加设备**”按钮。

   移动设备向导启动。

4. 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。

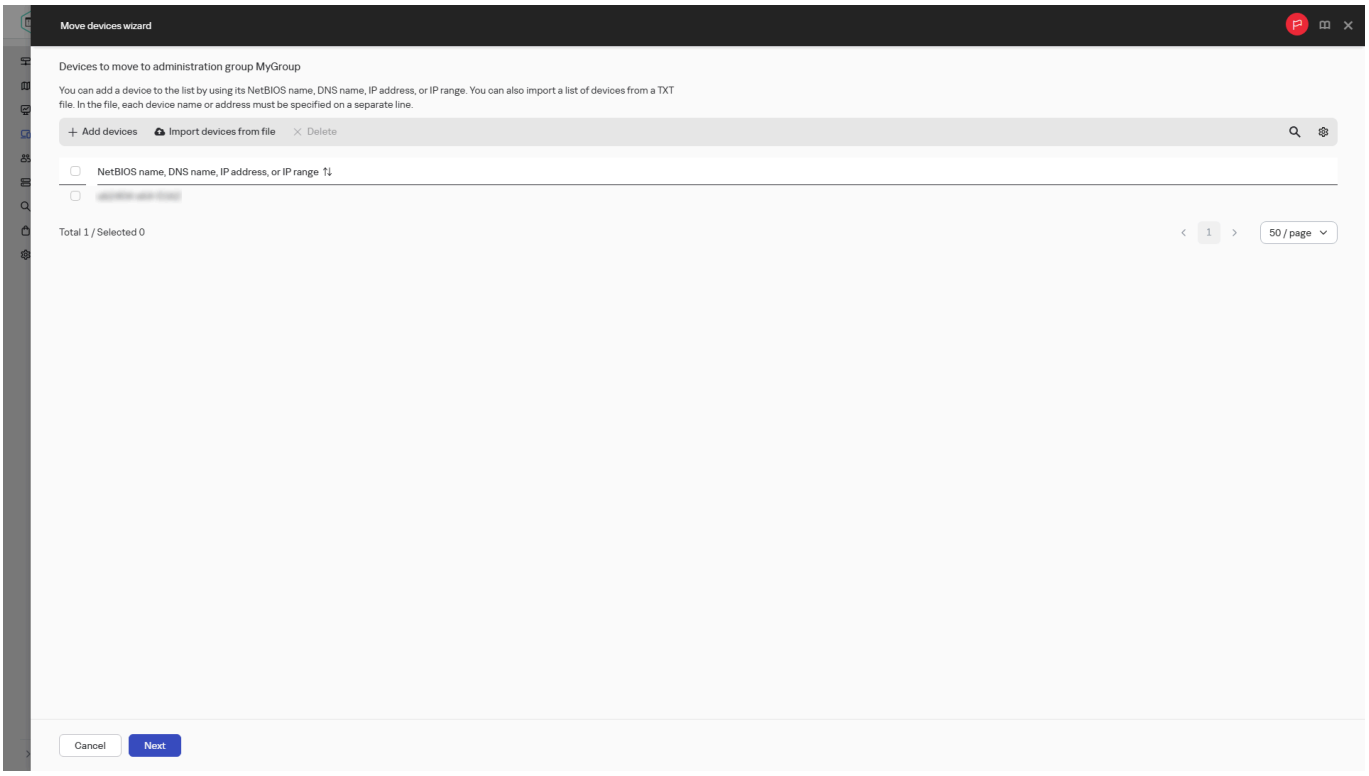
    > IP地址范围不得包含超过1,048,576个地址。

  - 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：,\/*‘“;:&`~!@#$^()=+[]{}|<>%




选择要移动到管理组的设备

5. 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。

6. 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。

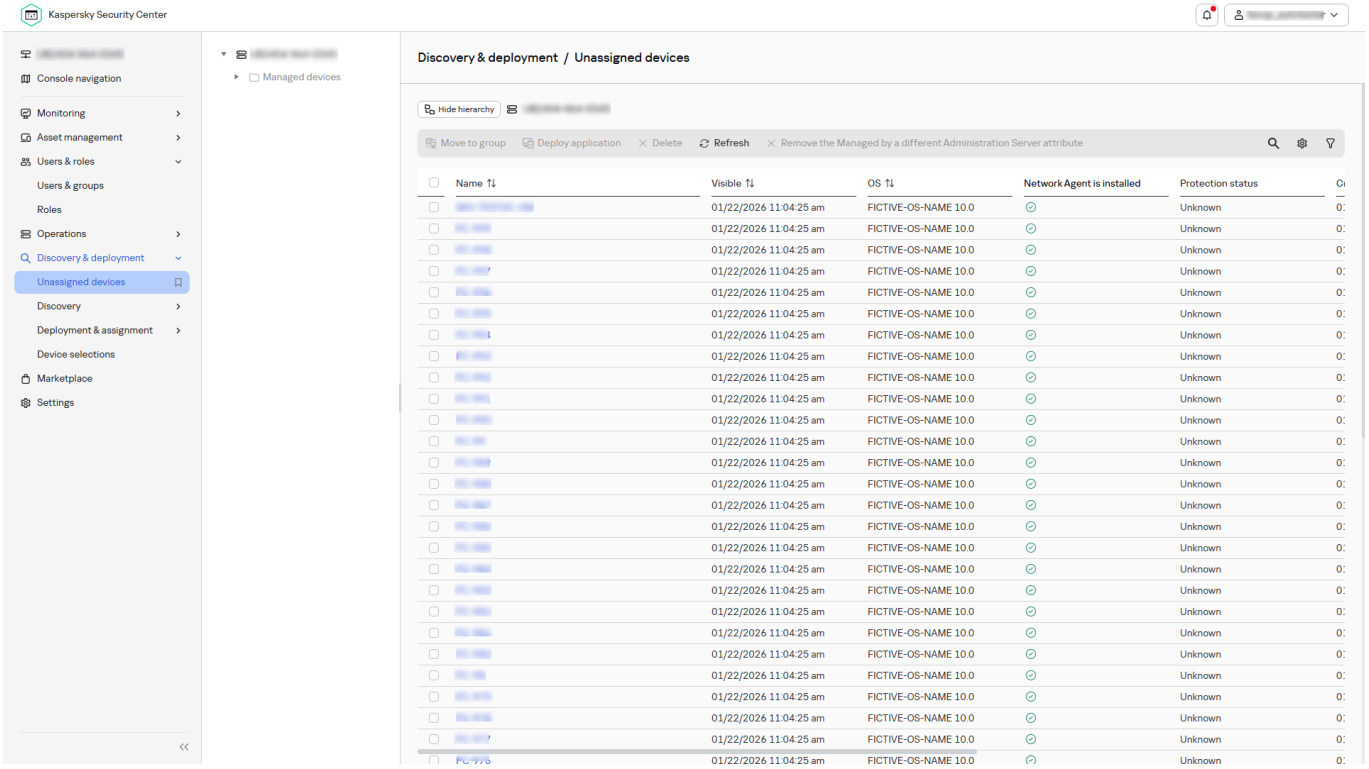
# 手动将设备或者集群移动至管理组

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**资产管理→资产(设备)**，然后选择所需的管理组。
     - 对于根组，您可以继续进行下一步。
     - 对于子组，单击页面顶部的“**显示层级**”按钮，然后在打开的窗口中选择所需的管理组。
   - 要打开**未分配的设备**群组，请在主菜单中，前往**资产管理→未分配的设备**。




未分配的设备列表

2. 如果管理组包含集群或服务器阵列，则**资产(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。

# 关于集群和服务器阵列

Kaspersky Security Center Linux 支持集群技术。如果网络代理向管理服务器发送信息确认组成服务器阵列的客户端设备上已安装该应用程序，则该客户端设备就成为一个集群节点。

如果管理组包含集群或服务器阵列，则“**资产(设备)**”页面将显示两个选项卡：一个用于单个设备，另一个用于集群和服务器阵列。受管理设备被检测为集群节点后，集群将被作为单独对象添加到“**集群和服务器阵列**”选项卡。

集群或服务器阵列节点与其他受管理设备一起列在**设备**选项卡上。您可以将节点作为单个设备查看属性并执行其他操作，但不能删除集群节点或将其从集群中单独移动到另一个管理组。您只能删除或移动整个集群。

您可以对集群或服务器阵列执行以下操作：

- 查看属性
- 将集群或服务器阵列移至另一个管理组

  当您将集群或服务器阵列移动到另一个组时，其所有节点都会随之移动，因为集群及其任何节点始终属于同一管理组。
- 删除

  仅当集群或服务器阵列不在组织网络中存在时，删除该集群或服务器阵列才合理。如果集群在您的网络上仍然可见，并且网络代理和卡巴斯基安全应用程序仍然安装在集群节点上， Kaspersky Security Center Linux 会自动将已删除的集群及其节点返回到受管理设备列表。

# 集群或服务器阵列的属性

*要查看集群或服务器阵列的设置：*

1. 在主菜单中，转到“**资产管理**”→“**资产(设备)**”→“**集群和服务器阵列**”。

   集群和服务器阵列的列表将显示。
2. 单击所需集群或服务器阵列的名称。

所选集群或服务器阵列的属性窗口将显示。

## 常规

**常规**部分显示有关集群或服务器阵列的常规信息。信息基于上一次集群节点与管理服务器之间的同步接收的数据来提供：

- **名称**
- **描述**
- **Windows 域**

  Windows 域或工作组，包含集群或服务器阵列。
- **NetBIOS 名称**

  集群或服务器阵列的 Windows 网络名称。
- **DNS 名称**

  集群或服务器阵列的 DNS 域名称。

### 任务

在“**任务**”选项卡中，您可以管理分配给集群或者服务器阵列的任务：查看现有任务列表；创建新任务；删除、启动和停止任务；修改任务设置；查看执行结果。列出的任务与安装在集群节点上的卡巴斯基安全应用程序相关。Kaspersky Security Center Linux 从集群节点接收任务列表和任务状态详细信息。如果未建立连接，则不显示状态。

### 节点

此选项卡显示集群或服务器阵列中包含的节点列表。您可以单击节点名称来查看设备属性窗口。

### 卡巴斯基应用程序

属性窗口还可能包含其他选项卡，其中包含与集群节点上安装的卡巴斯基安全应用程序相关的信息和设置。

# 分发点和连接网关的调整

Kaspersky Security Center Linux 中的管理组结构执行以下功能：

- 设置策略范围
  将相关设置应用到设备还有一种方式：使用*策略配置文件*。
- 设置组任务范围
  还有一个不基于管理组层级定义组任务范围的方法：使用设备分类的任务和特定设备的任务。
- 设置设备、虚拟管理服务器和从属管理服务器的访问权限。
- 分配分发点

当建立管理组结构时，您必须考虑到组织网络的拓扑以便最优分配分发点。分发点的最优分发允许您在企业网络中保存流量。

根据组织图表和网络拓扑，以下标准配置可以被应用到管理组结构：

- 单一办公室
- 多个小远程分办公室

作为分发点的设备必须被保护，包括物理保护，以防范非授权的访问。

# 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。

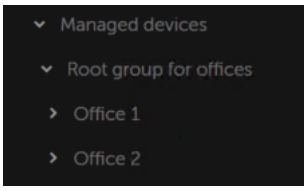
有以下构建管理组结构的方法：

- 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/5000 + 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。

运行基于Arm架构的Microsoft Windows的设备不能充当分发点。

*要自动分配分发点：*

1. 在主菜单中，单击管理服务器名称。
   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。但是，如果您出于任何原因必须选择不自动分配分发点（例如，如果您想使用专门分配的服务器），您可以在计算分发点的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。

运行基于 Arm 架构的 Microsoft Windows 的设备不能充当分发点。

*要手动指派设备做为分发点：*

1. 在主菜单中，单击管理服务器名称。
   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。
     - **已启用**

       如果启用此选项，将使用 IP 多点传送自动向组内的客户端设备上分发安装包。
       IP 多点传送减少了将应用程序从安装包安装到一组客户端设备所需的时间，但是增加了在将应用程序安装到单个客户端设备时的安装时间。

- **IP 多点传送地址**

  用于多点传送的 IP 地址。您可以定义范围是 224.0.0.0 – 239.255.255.255 的 IP 地址

  默认情况下，Kaspersky Security Center Linux 自动分配一个在给定范围内的唯一 IP 多播地址。

- **IP 多点传送端口号**

  IP 多点传送的端口号。

  默认情况下，端口号指定为 15001。如果运行管理服务器的设备指定为分发点，端口 13001 默认用于 SSL 连接。

- **远程设备的分发点地址**

  远程设备连接到分法点的网络地址。

- **已启用**

  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。

- **已启用**

  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。

- **已启用**

  在 Kaspersky Security Center Linux 中，分发点可以用作通过移动协议管理的设备和由网络代理管理的设备的推送服务器。例如，如果您希望能强制 KasperskyOS 设备与管理服务器同步，则必须启用推送服务器。推送服务器与启用该推送服务器的分发点具有相同的受管理设备范围。如果为同一个管理组分配了多个分发点，则可以在每个分发点上都启用推送服务器。在这种情况下，管理服务器会平衡分发点之间的负载。

- **推送服务器端口**

  推送服务器的端口号。您可以指定任何未占用的端口号。

- 在“**范围**”区域中，指定分发点将向其分发更新的管理组。

- 在“**更新源**”区域中，可以选择分发点的更新源：

  - **更新源**

    选择分发点的更新源：

    - 要允许分发点从管理服务器接收更新，请选择“**从管理服务器检索**”。
    - 要允许分发点使用任务接收更新，请选择“**使用更新下载任务**”，然后指定“*将更新下载至分发点存储库*”任务：
      - 如果设备上已存在此类任务，请在列表中选择该任务。
      - 如果设备上尚不存在此类任务，请单击“**创建任务**”链接创建任务。“新任务向导”启动。遵照向导的说明操作。

  - **下载差异文件**

    该选项启用下载 diff 文件功能。

    默认情况下已启用该选项。

- 如果您的分发点在连接到互联网时使用代理服务器，则可以在**互联网连接设置**子部分中指定以下设置：

  - **使用代理服务器**

    如果选中此复选框，则使用互联网代理服务器将分发点连接到卡巴斯基更新服务器。您可以在输入字段中配置代理服务器连接。

    默认情况下已清除该选框。

  - **代理服务器地址**

    代理服务器地址。

  - **端口号**

    用于连接的端口号。

  - **对本地地址不使用代理服务器**

    如果启用此选项，将不使用代理服务器连接本地网络的设备。

    默认情况下已禁用该选项。

  - **代理服务器身份验证**

    如果选择该选框，您可以在输入字段中为代理服务器身份验证指定凭证。

    默认情况下已清除该选框。

  - **用户名**

    建立连接代理服务器的用户账户。

  - **密码**

    任务运行时使用的账户的密码。

- 在“**KSN 代理**”区域，您可以配置应用程序使用分发点从受管理设备转发 KSN 请求：

  - **在分发点端启用 KSN 代理**

    KSN 代理服务运行在用作分发点的设备上。使用该功能重新分发和优化网络流量。

    分发点发送列在Kaspersky Security Network声明中的KSN统计信息到卡巴斯基。

    默认情况下已禁用该选项。启用该选项仅在**使用管理服务器作为代理服务器** 和 **我同意使用卡巴斯基安全网络**选项在管理服务器属性窗口中被启用时起作用。

    您可以分配活动被动集群节点到分发点并在该节点上启用 KSN 代理服务器。

  - **转发 KSN 请求到管理服务器**

    分发点从受管理设备转发 KSN 请求到管理服务器。

    默认情况下已启用该选项。

  - **通过互联网直接访问 KSN 云/KPSN**

    分发点从受管理设备转发 KSN 请求到 KSN 云或 KPSN。分发点本身上生成的 KSN 请求也直接发送到 KSN 云或 KPSN。

  - **当连接到 KPSN 时忽略代理服务器设置**

    如果您在分发点属性或网络代理策略中配置了代理服务器设置，但您的网络架构要求您直接使用 KPSN，则启用此选项。否则，从受管理应用程序的请求无法到达 KPSN。

    如果您选择“**通过互联网直接访问 KSN 云/KPSN**”选项，则此选项可用。

  - **端口**

    受管理设备将用于连接到 KSN 代理服务器的 TCP 端口号。默认端口号是 13111。

  - **使用 UDP 端口**

    如果需要受管理设备通过 UDP 端口连接到 KSN 代理，则启用“**使用 UDP 端口**”选项并指定 UDP 端口号。默认情况下已启用该选项。

  - **UDP 端口**

    受管理设备将用于连接到 KSN 代理服务器的 UDP 端口号。连接到 KSN 代理的默认 UDP 端口是 15111。

  - **使用 HTTPS**

    如果需要受管理设备通过 HTTPS 端口连接到 KSN 代理服务器，启用“**使用 HTTPS 端口**”选项，并指定 **HTTPS 端口**号。连接到 KSN 代理服务器的默认 HTTPS 端口是 17111。

  - **HTTPS 端口**

    受管理设备用于连接到 KSN 代理服务器的 HTTPS 端口号。连接到 KSN 代理服务器的默认 HTTPS 端口是 17111。

- 在“**连接网关**”区域中，可以配置分发点，充当网络代理实例和管理服务器之间连接的网关：

  - **连接网关**

    如果由于您的网络组织而无法在管理服务器和网络代理之间建立直接连接，您可以使用分发点作为管理服务器和网络代理之间的连接网关。

    如果您需要分发点充当网络代理和管理服务器之间的连接网关，请启用此选项。默认情况下已禁用该选项。

- **从管理服务器建立连接到网关(如果网关位于 DMZ 中)**

  如果管理服务器位于隔离区域 (DMZ) 之外，在局域网中，安装在远程设备上的网络代理无法连接到管理服务器。您可以使用分发点作为具有反向连接的连接网关（管理服务器建立到分发点的连接）。

  如果您需要将管理服务器连接到 DMZ 中的连接网关，请启用此选项。

- **为 Kaspersky Security Center Web Console 打开本地端口**

  如果您需要 DMZ 中的连接网关为位于 DMZ 中或互联网上的 Web Console 打开一个端口，请启用此选项。指定将用于从 Web Console 连接到分发点的端口号。默认端口号是 13299。

  如果启用“**从管理服务器建立连接到网关(如果网关位于 DMZ 中)**”选项，则此选项可用。

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 身份验证的端口，则分发移动设备证书的唯一方式是通过安装包。

- 通过基于 Windows 的分发点配置 Windows 网络轮询。

  - **Windows 域**

    您可以启用 Windows 域设备发现并为发现设置计划。

- 配置分发点的域控制器轮询。

  - **域控制器轮询**

    您可以对域控制器启用设备发现。

    在**轮询**字段中，将切换按钮切换到**已启用**位置后，您可以选择要轮询的域控制器，还可以为它们指定轮询计划。

    如果使用 Linux 分发点，请在“**轮询指定域**”区域中单击“**添加**”，然后指定域控制器的地址和用户凭据。另外，您可以指定要轮询的域的类型：Active Directory 或 Samba、FreeIPA、ALD Pro。

如果您使用 Windows 分发点，则可以选择以下选项之一：

- **轮询当前域**
- **轮询整个域森林**
- **轮询指定域**

- 按分发点配置 IP 范围轮询。
  - **IP 范围轮询**

    您可以针对 IPv4 范围和 IPv6 网络启用设备发现。

    如果启用“**启用范围轮询**”选项，则可以添加扫描范围并为其设置计划。您可以添加 IP 范围到已扫描范围列表。

    如果启用“**使用 Zeroconf 轮询 IPv6 网络**”选项，分发点将使用零配置网络（也称为 *Zeroconf*）自动轮询 IPv6 网络。在这种情况下，指定的 IP 范围将被忽略，因为分发点会轮询整个网络。如果分发点运行 Linux，则**使用 Zeroconf 轮询 IPv6 网络**选项可用。要使用 Zeroconf IPv6 轮询，您必须在分发点上安装 avahi-browse 实用程序。

- 在**高级**区域，指定分发点必须使用以存储发布数据的文件夹。
  - **使用默认的文件夹**

    如果您选择此选项，应用程序使用分发点上的网络代理安装文件夹。

  - **使用指定的文件夹**

    如果您选择该选项，则可以在下面的字段中指定该文件夹的路径。它可以是分发点上的本地文件夹，也可以是企业网络中任何设备上的目录。

    分发点上用于运行网络代理的用户账户必须具有对指定文件夹的访问权限以进行读写操作。

10. 单击“**确定**”按钮。

所选设备作为分发点运行。

# 在 DMZ 中添加连接网关作为分发点

如果管理服务器在隔离区 （DMZ） 以外，则安装在外部设备上的网络代理无法连接管理服务器。在这种情况下，您可以使用分发点作为 DMZ 中的连接网关。分发点会打开一个端口，供管理服务器创建连接。当管理服务器启动时，它连接到一个分发点并在整个会话期间维持该连接。

如果您需要在网络代理和管理服务器同步期间之外建立管理服务器和受管理设备之间的连接，则必须在分发点侧启用推送服务器并打开端口 13295。

我们建议您使用专门指定的设备作为连接网关。有关客户端设备（包括移动设备）的最大数量信息，请参阅筛分向导。

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。这意味着在连接网关安装到 DMZ 中的某个设备上之后，管理服务器不会在受管理设备中列出该设备。因此，您需要一个特殊程序来确保管理服务器发起与连接网关的连接。

*要添加具有连接网关的设备作为分发点：*

1. 在主菜单中，单击管理服务器名称。

   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. 在工具栏上，单击**分配**按钮。

5. 在打开的右侧窗格中，执行以下操作：

   a. 选择**按地址使用 DMZ 连接网关**选项。

   b. 在**连接网关地址**字段中，指定设备 IP 地址或 DNS 名称。

   c. 单击**分配**按钮。

   d. 窗格关闭，并显示名称为**连接网关的临时入口**的分发点。

6. 单击“**保存**”按钮。

   管理服务器会尝试连接到您指定了地址的连接网关。如果成功，该条目的名称将更改为连接网关设备的名称。此过程最多需要 5 分钟。

如果单击**连接网关的临时入口**名称来打开分发点属性，所有选项将灰显。您只能查看显示分发点名称的“常规”选项卡。默认情况下使用端口 (13000)。只有在管理服务器连接到分发点后，才能配置分发点。在连接网关的临时条目转换为命名条目的同时，连接网关也会出现在“未分配的设备”组中。

*要将连接网关添加到先前配置的网络：*

1. 以连接网关模式安装网络代理。

2. 在要连接到新添加的连接网关的设备上重新安装网络代理。

# 修改管理组的分发点列表

您可以查看为特定管理组分配的分发点列表并通过添加或删除分发点来修改列表。

*要查看和修改分配给管理组的分发点列表：*

1. 在主菜单中，转到“**资产管理**” → “**资产(设备)**”。

2. 通过单击页面顶部的“**显示层级**”按钮，选择要查看所分配的分发点的管理组，然后在打开的窗口中单击所需组的名称。

   这将启用**分发点**菜单项。

   所选组的路径显示在页面顶部。如果需要，您可以在此路径中单击带有管理组名称的链接转到该组。默认情况下，路径中的最后一个链接不活动。

3. 在主菜单中，转到“**资产管理**”→“**分发点**”。

4. 要为管理组添加新的分发点，请单击**分配**按钮。

5. 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 Linux 中，分发点可以用作通过移动协议管理的设备和由网络代理管理的设备的推送服务器。例如，如果您希望能强制 KasperskyOS 设备与管理服务器同步，则必须启用推送服务器。推送服务器与启用该推送服务器的分发点具有相同的受管理设备范围。如果为同一个管理组分配了多个分发点，则可以在每个分发点上都启用推送服务器。在这种情况下，管理服务器会平衡分发点之间的负载。

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. 在主菜单中，单击管理服务器名称。
   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“**已启用**”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. 在用作分发点的 Linux 设备上，执行以下命令：

```
systemctl edit klnagent64.service
```

2. 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=< 软资源限制 >:< 硬资源限制 >

   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。

3. 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。

4. 运行以下命令重新加载 systemd 进程：

   systemctl daemon-reload

5. 运行以下命令重新启动网络代理服务：

   systemctl restart klnagent

6. 运行以下命令以确保正确应用指定的参数：

   less /proc/< nagent 进程 ID >/limits

   其中< nagent 进程 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。

# 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）。例如，如果某个受管理设备因满足“*数据库已过期*”条件而被分配“*严重*”状态，之后又为设备设置了可见性标志，则该设备被分配“*正常*”状态。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。

| 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，恶意软件扫描任务，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。 |
| 恶意软件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。 |
| 需要重启后的时间 | 设备在网络上可见，但应用程序要求重启的时间已超过指定时间间隔。 | 超过 0 分钟。 |
| 重启原因 | 设备在网络上可见，但由于所选原因之一，应用程序需要重新启动设备。 | • 未知原因<br>• 应用程序在重启前不会运行<br>• 需要重启以完成更新；应用程序正在运行<br>• 需要重启以启动更新<br>• 需要重启以完成扫描或清除<br>• 需要重启以完成远程安装/卸载<br>• 即将完成磁盘的数据加密 |
| 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。 |
| 检测到软件漏洞 | 设备在网络中可见且网络代理已安装到设备，但“*查找漏洞和所需更新*”任务在设备应用程序中检测到指定严重级别的漏洞。 | • 严重。<br>• 高。<br>• 中。<br>• 如果漏洞无法被修复则忽略。<br>• 如果为安装分配了更新则忽略。 |
| 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。 |

| 条件 | 条件描述 | 可用值 |
| --- | --- | --- |
| Windows Update 更新检查已长时间未执行 | 设备在网络中可见，但"*寻找漏洞和所需更新*"任务在指定时间段内未运行。 | 超过 1 天。 |
| 无效的加密状态 | 网络代理已安装到设备，但设备加密结果等于指定值。 | • 由于用户拒绝未遵从策略(仅对外部设备)。<br>• 由于错误未遵从策略。<br>• 应用策略时需要重启。<br>• 未指定加密策略。<br>• 不支持。<br>• 当应用策略时。 |
| 移动设备设置不遵从策略 | 移动设备设置不同于 Kaspersky Endpoint Security for Android 策略中指定的设置。 | • 开关按钮被关闭。<br>• 开关按钮被开启。 |
| 检测到未处理的安全问题 | 设备上发现了一些未处理的安全问题。安全问题可以通过安装在客户端设备上的受管卡巴斯基应用程序自动创建，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。<br>无论 Kaspersky Security Center Linux 设置如何，受管理设备的状态都可能由受管理应用程序定义。当此状态返回一个由 Kaspersky Security Center Linux 定义的状态后，管理服务器将为受管理设备分配一个最终状态。该状态选自以下两者中最为严重的一项：受管理应用程序返回的状态和管理服务器分配的状态。受管理应用程序定义的状态会附带由受管理应用程序传输的描述。您可以在受管理设备列表的"**状态描述**"列中查看这些描述。 | • 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。<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**"，则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。

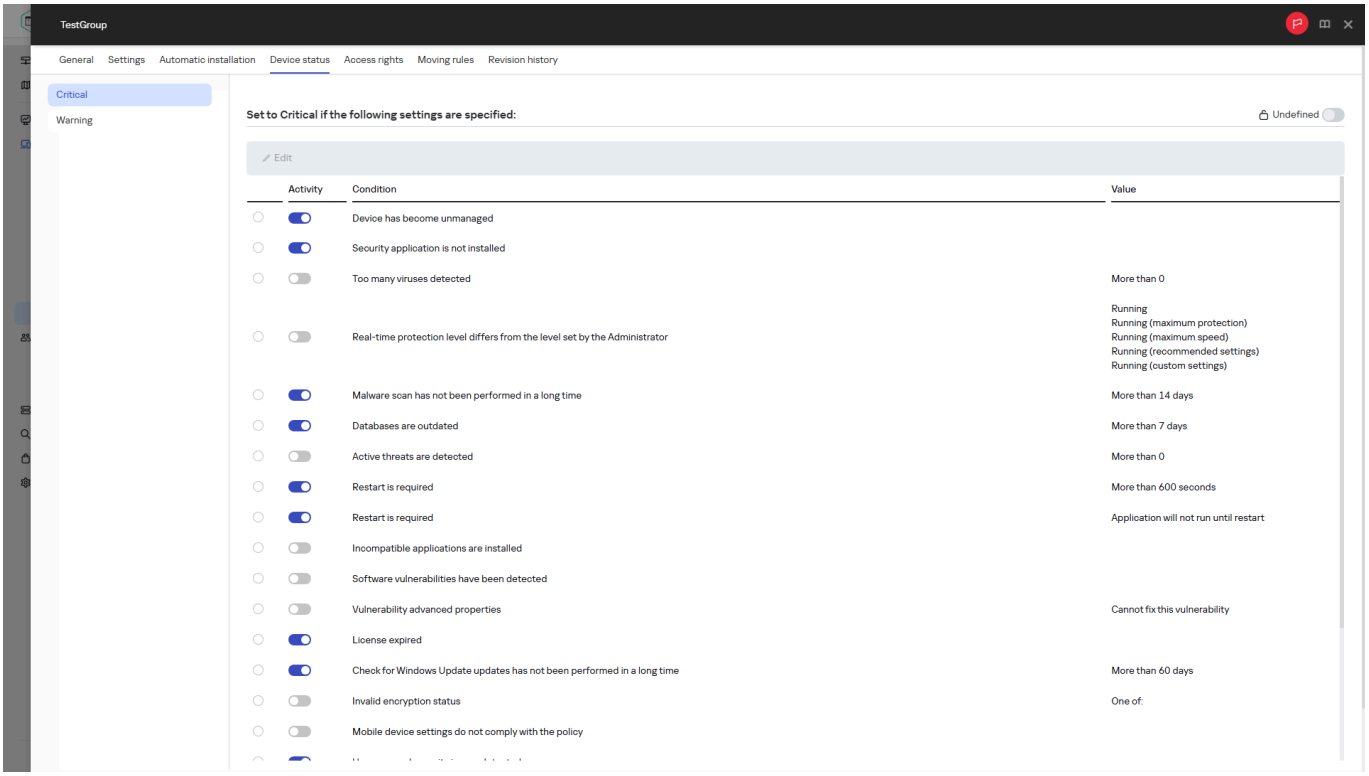
# 配置设备状态切换

您可以更改条件以将*严重*或*警告*状态分配给设备。

*要启用更改设备状态到严重：*

1. 在主菜单中，转到“**资产管理**”→“**组层级**”。
2. 通过以下方式之一，转到要更改设备状态的管理组的属性：
   - 单击管理组的名称。
   - 单击页面顶部的“**显示层级**”按钮。在打开的导航窗格中，将鼠标光标悬停在所需组的名称上，然后单击设置图标（⚙）。

   管理组属性窗口将开启。
3. 在属性窗口中，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“**如果指定了以下设置，则设置为“严重”**”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“**资产管理**” → “**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“**如果指定了以下设置，则设置为“警告”**”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。

# 设备分类

*设备分类*是根据特定条件筛选设备的工具。您可以使用设备分类管理几个设备：例如，查看仅查看这些设备的报告或移动所有这些设备到其他组。

Kaspersky Security Center Linux 提供大量的*预定义分类*（例如，**处于“严重”状态的设备**，**保护已禁用**，**检测到活动威胁**）。预定义分类无法被删除。您也可以创建和配置附加*用户定义分类*。

在用户定义分类中，您可以设置搜索范围并选择所有设备、受管理设备、或者未分配的设备。搜索参数在条件中指定。在设备分类中，您可以创建带有不同搜索参数的多个条件。例如，您可以创建两个条件并指定不同的 IP 范围。如果多个条件被指定，分类显示满足任意条件的设备。相比之下，条件中的搜索参数是附加的。如果 IP 范围和已安装应用程序名称都被指定在一个条件，仅安装了应用程序且 IP 地址处于指定范围的设备被显示。

# 从设备分类中查看设备列表

Kaspersky Security Center Linux 允许您从设备分类中查看设备列表。

*若要从设备分类中查看设备列表：*

1. 在主菜单中，转到“**资产管理** → **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“**资产管理**”→“**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“**资产管理**” → “**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**

默认情况下已禁用该选项。

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。

以下示例展示了反转工作的逻辑：

- **条件**：您的设备上存在操作系统类型为 Linux 且内部版本号为 00.0.000 的设备。
- **反转条件**：您的设备上存在操作系统类型为非 Linux 且内部版本号为非 00.0.000 的设备，这等价于：
  存在操作系统类型为非 Linux 或内部版本号为非 00.0.000 的设备。

因此，选择范围将包括操作系统类型为 Windows 且内部版本号为 00.0.000 的设备，或者 Linux 且内部版本号不为 00.0.000 的设备。

### 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。

- **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“**域控制器**”子区域，您可以配置基于域成员包含设备到分类的标准:

- **设备在域组织单元中**

  如果启用此选项，选择范围将包括输入字段中指定的域组织单元中的设备。

  默认情况下已禁用该选项。

- **该设备是域安全组成员**

  如果启用此选项，选择范围将包括输入字段中指定的域安全组中的设备。

  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：“*确定*”、“*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：*确定*、*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（*未知*、*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（*未知*、*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（*未知*、*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（*未知*、*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。

- **OS 服务包版本**

  在该字段中，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。

- **OS 架构**

  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。

- **OS 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。

- **OS 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。

在“**漏洞和更新**”子区域，您可以指定根据 Windows 更新源包含设备到分类的标准：

#### WUA 已切换到管理服务器

您可以在下拉列表中选择以下搜索选项之一：

- **是**。如果选中该选项，搜索结果会包含从管理服务器收到 Windows Update 更新的设备。
- **否**。如果选中该选项，搜索结果将包含从其它源收到 Windows Update 更新的设备。

### 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，可设置按卡巴斯基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，可设置按卡巴斯基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。

- **选择模块上次更新的时间段**

  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。

- **设备通过管理服务器管理**

  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，您可以按上次恶意软件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恶意软件扫描的时段。

  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。

在“**加密**”子区域中，您可以配置基于所选的加密算法包含设备到分类的标准：

**加密算法**

高级加密标准(AES)对称分组密码算法。在下拉列表中，您可以选择加密密钥大小(56 位、128 位、192 位或 256 位)。

可用值：*AES56*、*AES128*、*AES192* 和 *AES256*。

**应用程序组件**子区域包含在 Kaspersky Security Center 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。您也可以配置对除指定版本外的所有版本进行搜索。

### 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。

- **所有带有此标签的设备**

  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。

- **所有没有此标签的设备**

  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。

### 设备所有者

在“**设备所有者**”部分，您可以根据设备的注册所有者、他们的角色以及他们在安全组中的成员资格来设置将设备纳入选择范围的条件：

- **设备所有者**

  从内部安全组中选择设备所有者的用户名。在本部分中了解有关用户和用户角色的更多信息。

  > 最多只能有一名用户注册为设备所有者。

- **在活动目录安全组中的设备所有者成员关系**

  选择设备所有者所属的外部活动目录安全组。

  > 用户可以是活动目录安全组的一部分，也可以是此活动目录安全组中包含的组的一部分。

- **设备所有者角色**

  选择设备所有者的指定角色。在本文中了解有关用户角色的更多信息。

- **设备所有者在内部安全组中的成员身份**

  选择设备所有者所属的内部安全组。

# 从设备分类中导出设备列表

Kaspersky Security Center Linux 允许您将设备分类中的设备信息保存并导出为 CSV 或 TXT 文件。

*若要从设备分类中导出设备列表：*

1. 从设备分类中打开包含设备的表格。
2. 使用以下方法之一选择要导出的设备：
   - 要选择特定设备，请选中它们旁边的复选框。
   - 要从当前表格页面选择所有设备，请选中设备表格表头中的复选框，然后选中**全选当前页面**复选框。
   - 要从表中选择所有设备，请选中设备表格表头中的复选框，然后选择**全选**复选框。
3. 单击**导出到 CSV**或**导出到 TXT**按钮。表中包含的有关所选设备的所有信息都将被导出。

> 请注意，如果您将筛选条件应用于设备表，则只有来自显示列的筛选数据将被导出。

# 在分类中从管理组中删除设备

在使用设备分类时，你可以直接从管理组中删除设备，而不是切换到包含这些设备的管理组。

*要从管理组删除设备，请执行以下操作：*

1. 在主菜单中，转到“**资产管理**” → “**设备分类**”或者“**发现和部署**” → “**设备分类**”。
2. 在分类列表中，单击设备分类的名称。
   该页面会显示一个表格，其中包含有关设备分类中包含的设备的信息。
3. 选择要删除的设备，然后单击“**删除**”。
   所选设备即从相应管理组中删除。

# 设备标签

Kaspersky Security Center Linux 允许您*标记*设备。标签是字符串值，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。如果您想标记单个设备，则可以使用手动标记。Kaspersky Security Center Linux 通过以下方式之一执行自动标记：

- 按照指定的标记规则。
- 通过应用程序。

我们不建议您使用不同的标记方式来分配相同的标签。例如，如果标签是由规则分配的，则不建议手动将此标签分配给设备。

如果标签是通过规则分配的，则当满足指定的规则时，设备会自动被标记。每个标签对应一条单独的规则。规则会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此标签；这将帮助您整理所有 CentOS 设备，并向其分配任务。

每个标签只能添加一条自动标记规则。如果为同一标签创建新规则，则之前的规则将被替换。

在以下情况下标签从设备上被自动删除：

- 当设备停止满足分配标签的规则的条件时。
- 当分配标签的规则被禁用或删除时。

每个管理服务器的标签列表和规则列表是独立的，包括主管理服务器和从属虚拟管理服务器。规则仅被应用到来自创建规则的相同管理服务器的设备。

# 创建设备标签

*要创建设备标签：*

1. 在主菜单中，转到“**资产管理**”→“**标签**”→“**设备标签**”。
2. 单击**添加**。
   新标签窗口打开。
3. 在“**标签**”字段中，输入标签名称。
4. 单击“**保存**”保存设置。

新标签出现在设备标签列表。

# 重命名设备标签

*要重命名设备标签：*

1. 在主菜单中，转到“**资产管理**”→“**标签**”→“**设备标签**”。
2. 单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

您只能删除手动分配的标签。

*要删除手动分配的设备标签：*

1. 在主菜单中，转到“**资产管理 → 标签 → 设备标签**“。
   显示标签列表。
2. 选择要删除的设备标签。

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。

当您删除通过自动标记规则分配给设备的标签时，不会删除该规则，而且当新设备首次满足规则条件时，该标签将被分配给该设备。如果删除自动标记规则，规则条件中指定的标签将从分配了该标签的所有设备中删除，但不会从标签列表中删除。如有必要，您可以手动从列表中删除该标签。

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。若要管理这些标签，请使用 klscflag 实用程序。

# 查看分配了标签的设备

*要查看分配了标签的设备：*

1. 在主菜单中，转到“**资产管理 → 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。

   您将被重定向到主菜单的“**资产(设备)**”部分，其中的设备将按您单击“**查看设备**”链接的标签进行过滤。

3. 如果您想返回设备标签列表，单击您浏览器的“**后退**”按钮。

查看已分配标签的设备后，您可以创建并分配新标签，也可以将现有标签分配给其他设备。在这种情况下，您必须按标签删除过滤器，选择设备，然后分配标签。

# 查看分配到设备的标签

*要查看分配到设备的标签：*

1. 在主菜单中，转到 “**资产管理**” → “**资产(设备)**”。

2. 单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。

在工具栏中，您可以进行以下操作：

- 为设备分配另一个标签。
- 移除已分配的标签。
- 查看管理服务器上存在的所有设备标签。

> 您无法在设备上本地查看分配的标签。

# 手动标记设备

*要手动分配标签到设备：*

1. 查看分配到您要分配其他标签的设备的标签。
2. 单击**添加**。
3. 在打开的窗口中，执行以下操作之一：
   - 要创建和分配新标签，请选择“**创建新标签**”，然后指定新标签的名称。
   - 要选择现有标签，请选择“**分配现有标签**”，然后在下拉列表中选择所需标签。
4. 单击“**确定**”应用更改。
5. 单击“**保存**”保存设置。

所选的标签被分配到设备。

# 从设备上删除分配的标签

*要从设备上删除标签：*

1. 在主菜单中，转到 “**资产管理**” → “**资产(设备)**”。
2. 单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。若要管理这些标签，请使用 klscflag 实用程序。

# 查看自动标记设备规则

*要查看自动标记设备规则，*

做以下任意：

- 在主菜单中，转到“**资产管理**”→“**标签**”→“**自动标记规则**”。
- 在主菜单中，转到“**资产管理**”→“**标签**”→“**设备标签**”，然后单击“**设置自动标记规则**”链接。
- 查看分配给设备的标签，然后单击“**设置**”按钮。

自动标记设备规则列表出现。

# 编辑自动标记设备规则

*要编辑自动标记设备规则：*

1. 查看自动标记设备规则。
2. 单击您要编辑的规则名称。
   规则设置窗口打开。
3. 编辑规则的常规属性：
   a. 在“**规则名称**”字段中，更改规则名称。
      名称不能包括 256 个以上字符。
   b. 做以下任意：
      - 通过将切换按钮切换到“**规则已启用**”来启用规则。
      - 通过将切换按钮切换到“**规则已禁用**”来禁用规则。

4. 做以下任意：

   - 如果要添加新条件，请单击“**添加**”按钮，然后在打开的窗口中指定新条件的设置。
   - 如果要编辑现有条件，请单击要编辑的条件名称，然后编辑条件设置。
   - 如果要删除条件，请选中要删除的条件名称旁边的复选框，然后单击“**删除**”。

5. 在条件设置窗口中单击“**确定**”。

6. 单击“**保存**”保存设置。

编辑的规则显示在列表。

# 创建自动标记设备规则

*要创建自动标记设备规则：*

1. 查看自动标记设备规则。

2. 单击**添加**。
   新规则设置窗口打开。

3. 配置规则的常规属性：

   a. 在“**规则名称**”字段中，输入规则名称。
   名称不能包括 256 个以上字符。

   b. 执行以下操作之一：

   - 通过将切换按钮切换到“**规则已启用**”来启用规则。
   - 通过将切换按钮切换到“**规则已禁用**”来禁用规则。

   c. 在“**标签**”字段中，输入新设备标签名称或从列表中选择现有设备标签之一。
   名称不能包括 256 个以上字符。

4. 在条件区域中，单击“**添加**”按钮以添加新条件。
   新条件设置窗口打开。

5. 输入条件名称。
   名称不能包括 256 个以上字符。名称必须在规则内唯一。

6. 设置根据以下条件的规则触发。您可以选择多个条件。

   - **网络**—设备的网络属性，例如设备的 DNS 名称，或设备是否属于某个 IP 子网。

     如果为您用于 Kaspersky Security Center Linux 的数据库设置了区分大小写的排序规则，请在指定设备 DNS 名称时保持大小写。否则，自动标记规则将不起作用。

- **应用程序** – 设备上是否存在网络代理，操作系统类型、版本、架构和包管理器。
- **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。

4. 如果您想要确保 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。

# 数据加密和保护

如果您的笔记本电脑或硬盘驱动器被盗或丢失，数据加密可降低敏感数据和公司数据意外泄露的风险。此外，数据加密还可让您防止未经授权的用户和应用程序进行访问。

如果您的网络包括安装了 Kaspersky Endpoint Security for Windows 的基于 Windows 的受管理设备，您可以使用数据加密功能。在这种情况下，在运行 Windows 操作系统的设备上，您可以管理以下类型的加密：

- BitLocker 驱动器加密
- 卡巴斯基磁盘加密

我们不建议在 VDI 中启用加密。

通过使用 Kaspersky Endpoint Security for Windows 的这些组件，您可以（例如）启用或禁用加密、查看加密驱动器列表或生成和查看有关加密的报告等活动。

若要配置加密，请在 Kaspersky Security Center Linux 中定义 Kaspersky Endpoint Security for Windows 策略。Kaspersky Endpoint Security for Windows 会根据活动策略执行加密和解密。有关如何配置加密功能的规则和描述的详细说明，请参阅 Kaspersky Endpoint Security for Windows 帮助。

目前，Web Console 中不提供管理服务器层次结构的加密管理。使用主管理服务器来管理加密的设备。

您可以使用用户界面设置来显示或隐藏与加密管理功能相关的某些界面元素。

# 查看加密驱动器列表

在 Kaspersky Security Center Linux 中，您可以查看有关加密驱动器和在驱动器级别加密的设备的详细信息。驱动器上的信息解密后，该驱动器将自动从列表中移除。

*要查看加密驱动器列表，*

在主菜单中，转到“**操作**”→“**数据加密和保护**”→“**加密驱动器**”。

如果该区域不在菜单上，则表示它已隐藏。在“用户界面设置”中启用“**显示数据加密和保护**”选项来显示该区域。

您可以将加密驱动器列表导出到 CSV 文件或 TXT 文件。为此，请单击**导出到 CSV**或**导出到 TXT**按钮。

# 查看加密事件列表

在设备上运行数据加密或解密任务时，Kaspersky Endpoint Security for Windows 会将以下类型的事件信息发送给 Kaspersky Security Center Linux：

- 无法加密或解密文件，或者由于磁盘空间不足无法创建加密的压缩包。
- 无法加密或解密文件，或者由于授权许可问题无法创建加密的压缩包。
- 无法加密或解密文件，或者由于缺少访问权限无法创建加密的压缩包。
- 应用程序被禁止访问加密文件。
- 未知错误。

*要查看在设备上加密数据时发生的事件的列表：*

在主菜单中，转到“**操作**”→“**数据加密和保护**”→“**加密事件**”。

如果该区域不在菜单上，则表示它已隐藏。在“用户界面设置”中启用“**显示数据加密和保护**”选项来显示该区域。

您可以将加密驱动器列表导出到 CSV 文件或 TXT 文件。为此，请单击**导出到 CSV**或**导出到 TXT**按钮。

或者，您可以检查每个受管理设备的加密事件列表。

*要查看受管理设备的加密事件：*

1. 在主菜单中，转到“**资产管理 → 资产(设备)**”。
2. 单击受管理设备的名称。
3. 在**常规**选项卡上，转到**保护**部分。
4. 单击**查看数据加密错误**链接。

# 创建和查看加密报告

您可以生成以下报告：

- “受管理设备加密状态报告”。此报告提供有关各种受管理设备的数据加密的详细信息。例如，该报告显示应用已配置加密规则的策略的设备数量。此外，您还可以了解需要重启的设备数量。该报告还包含有关每个设备的加密技术和算法的信息。
- 大容量存储设备加密状态报告。此报告包含与受管理设备加密状态报告类似的信息，但它仅提供大容量存储设备和可移动驱动器的数据。
- 加密驱动器访问权限报告。此报告显示哪些用户账户可以访问加密驱动器。

- “文件加密错误报告”。该报告包含在设备上运行数据加密或解密任务时相关的错误信息。
- “加密文件访问被阻止报告”。该报告包含了阻止应用程序访问加密文件的信息。如果未经授权的用户或应用程序试图访问加密文件或驱动器，此报告会很有帮助。

您可以在“**监控 → 报告**”区域中生成任何报告。或者，在**操作→数据加密和保护**区域中，您可以生成以下加密报告：

- 大容量存储设备加密状态报告
- 加密驱动器访问权限报告
- 文件加密错误报告

*要在**数据加密和保护**区域中生成加密报告：*

1. 确保您启用了界面选项中的“**显示数据加密和保护**”选项。
2. 在策略属性中，打开“**事件配置**”选项卡。
3. 在**严重**部分，单击**添加事件**，然后选中*应用文件加密/解密规则时出错*事件旁边的复选框。
4. 单击“**确定**”。
5. 在主菜单中，转到**操作→数据加密和保护**。
6. 打开以下区域之一：
   - **加密驱动器**可生成大容量存储设备加密状态报告或加密驱动器访问权限报告。
   - **加密事件**可生成文件加密错误报告。
7. 单击您要生成的报告的名称。

报告生成将开始。

# 授予对处于离线模式的加密驱动器的访问权限

用户可能请求访问加密设备，例如，当受管理设备上未安装 Kaspersky Endpoint Security时。在您收到请求后，您可以创建访问密钥文件并将其发送给用户。Kaspersky Endpoint Security帮助文档中提供了所有使用案例和详细说明。

*若要在Kaspersky Endpoint Security for Windows中以离线模式访问加密驱动器：*

1. 从用户那里获取请求访问文件（具有 FDERTC 扩展名的文件）。按照 Kaspersky Endpoint Security for Windows 帮助 中的说明在 Kaspersky Endpoint Security for Windows 中生成文件。
2. 在主菜单中，转到“**操作**”→“**数据加密和保护**”→“**加密驱动器**”。
   将显示加密驱动器列表。
3. 选择用户请求访问权限的驱动器。
4. 单击**授予移动模式设备访问权限**按钮。

5. 在打开的窗口中，选择 Kaspersky Endpoint Security for Windows 插件。

6. 按照 Kaspersky Endpoint Security for Windows 帮助 中提供的说明进行操作（请参阅本节末尾的 Kaspersky Security Center Web Console 操作说明）。

之后用户可以使用收到的文件来访问加密驱动器和读取驱动器上存储的数据。

# 在管理服务器之间传输加密密钥

如果在受管理设备上启用数据加密功能，加密密钥存储在管理服务器上。加密密钥用于访问加密数据和管理加密策略。

在以下情况下，必须将加密密钥传输到其他管理服务器：

- 重新配置受管理设备上的网络代理，以将该设备分配给其他管理服务器。如果此设备包含加密数据，则必须将加密密钥传输到目标管理服务器。否则，数据将无法解密。
- 对连接到由管理服务器 S1 管理的设备 D1 的可移动驱动器进行加密，然后将该可移动驱动器连接到由管理服务器 S2 管理的设备 D2。要访问该可移动驱动器上的数据，必须将加密密钥从管理服务器 S1 传输到管理服务器 S2。
- 对由管理服务器 S1 管理的设备 D1 上的文件进行加密，然后在由管理服务器 S2 管理的设备 D2 上尝试访问该文件。要访问该文件，必须将加密密钥从管理服务器 S1 传输到管理服务器 S2。

您可以通过以下方式传输加密密钥：

- 自动传输，通过在必须互相传输加密密钥的两个管理服务器的属性中启用“**使用管理服务器层级获取加密密钥**”选项。如果对其中一个管理服务器禁用此选项，则无法自动传输加密密钥。

  在管理服务器属性中启用“**使用管理服务器层级获取加密密钥**”选项后，管理服务器会将其存储库中存储的所有加密密钥发送到层级中上一级的主管理服务器（如果有）。

  当您尝试访问加密数据时，管理服务器首先在其自己的存储库中搜索加密密钥。如果启用了“**使用管理服务器层级获取加密密钥**”选项，并且在存储库中找不到所需的加密密钥，则管理服务器还会向主管理服务器（如果有）发送请求，以提供所需的加密密钥。该请求将发送到所有主管理服务器，直到最高层级的服务器。

- 通过导出和导入包含加密密钥的文件，手动将密钥从一个管理服务器传递到另一个。

  加密密钥的导出和导入是加密密钥管理功能中包含的操作。要执行这些操作，需要通过以下方式之一为 Kaspersky Security Center Linux 用户配置对功能的访问权限：

  - 向自从属管理服务器导出加密密钥的用户授予对加密密钥管理功能的“**读取**”访问权限。
  - 向对目标管理服务器导入加密密钥的用户授予对加密密钥管理功能的“**写入**”访问权限。

*要启用在层级内的管理服务器之间自动传输加密密钥：*

1. 转到所需管理服务器的属性：

   a. 在主菜单中，选择一个区域（“**市场**”、“**控制台导航**”和“**设置**”除外），然后在页面顶部单击“**显示层级**”按钮。

   b. 在打开的导航窗格中，将鼠标光标悬停在所需管理服务器的名称上，然后单击设置图标 (⚙)。

   或者，您可以单击管理服务器名称，然后在主菜单中显示该名称后，在主菜单中单击该名称以打开服务器属性窗口。

2. 在打开的属性窗口中，选择“**加密算法**”区域。

3. 启用**使用管理服务器层级获取加密密钥**选项。

4. 单击“**确定**”应用更改。

下次同步（心跳）时，加密密钥将传输到主管理服务器（如果有）。该管理服务器还将根据请求将其存储库中的加密密钥提供给从属管理服务器。

*要在管理服务器之间手动传输加密密钥：*

1. 转到要从中导出加密密钥的管理服务器的属性：

   a. 在主菜单中，选择一个区域（“**市场**”、“**控制台导航**”和“**设置**”除外），然后在页面顶部单击“**显示层级**”按钮。

   b. 在打开的导航窗格中，将鼠标光标悬停在所需管理服务器的名称上，然后单击设置图标 (⚙)。

   或者，您可以单击管理服务器名称，然后在主菜单中显示该名称后，在主菜单中单击该名称以打开服务器属性窗口。

2. 在打开的属性窗口中，选择“**加密算法**”区域。

3. 单击“**从管理服务器导出加密密钥**”。

   确保向从服务器导出加密密钥的用户授予对加密密钥管理功能的“**读取**”访问权限。

4. 在“**导出加密密钥**”窗口中：

   - 单击“**浏览**”按钮，然后指定文件保存位置。
   - 指定密码以防止文件被未经授权访问。

   > 记住密码。丢失的密码无法恢复。如果密码丢失，则必须重复导出程序。因此，请记下密码并使其随时可用。

5. 例如，通过共享文件夹或可移动驱动器将文件传输到另一个管理服务器。

6. 转到要向其导入加密密钥的管理服务器的属性。

7. 在属性窗口中，选择“**加密算法**”区域。

8. 单击**导入加密密钥到管理服务器**。

   确保向对服务器导入加密密钥的用户授予对加密密钥管理功能的“**写入**”访问权限。

9. 在“**导入加密密钥**”窗口中：

   - 单击“**浏览**”按钮，然后选择包含加密密钥的文件。
   - 指定密码。

10. 单击“**确定**”。

加密密钥将传输到目标管理服务器。

# 更改客户端设备的管理服务器

对于特定客户端设备，您可以将管理服务器更改为不同的管理服务器。为此，请使用“*更改管理服务器*”任务。

*要更改管理客户端设备的管理服务器：*

1. 连接至管理设备的管理服务器。
2. 创建管理服务器更改任务。

   “新任务向导”启动。遵照向导的说明操作。在新任务向导的“**新任务**”窗口中，选择“**Kaspersky Security Center 16.3**”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。

如果管理服务器支持加密和数据保护，并且您正在创建*更改管理服务器*任务，将显示警告。警告声明如果有加密数据存储在设备，在新服务器开始管理设备之后，用户将仅可以访问他之前使用过的加密数据。除此之外，将不会提供对加密数据的访问权限。有关不提供加密数据访问权限的情况的详细说明，请参见 Kaspersky Endpoint Security for Windows 帮助。

# 避免多个管理服务器之间的冲突

如果您的网络中有多于一个管理服务器，它们可以看到相同的客户端设备。例如，这可能会导致管理服务器安装已被另一个管理服务器安装的应用程序，以及其他冲突。为了防止应用程序被安装在由另一台管理服务器管理的设备上，您必须在**仅安装到通过该管理服务器管理的设备远程安装应用程序**任务属性中启用远程安装应用程序仅在通过此管理服务器管理的设备上安装选项。

如果启用**仅安装到通过该管理服务器管理的设备**选项，然后运行*远程安装应用程序*任务，则会执行检查以确定设备是否由另一台管理服务器管理。对于由另一台管理服务器管理的设备，**由不同管理服务器管理**属性值将被设置为[[true。*远程安装应用程序*任务将不会被应用于这些设备。

**由不同管理服务器管理**属性值显示在**受管理设备由不同管理服务器管理未分配的设备**列表中的由不同管理服务器管理列中。

您也可以使用"**由不同管理服务器管理**"属性作为以下目的的标准：

- 显示受管理设备
- 设备分类
- 设备移动规则
- 自动标记规则

*若要重设由不同管理服务器管理属性：*

1. 在卡巴斯基安全管理中心云控制台的主菜单中，转至**资产管理** → **未分配的设备**。
2. 选择所需的设备，然后单击**删除"由不同管理服务器管理"属性**按钮。

   **由不同管理服务器管理**属性被重设。

# 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 "<网关 IP 或者名称>" -svt STRING_T -ss "|ss_type = \"SS_SETTINGS\";"`

     在此，`<网关 IP 或者名称>`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。

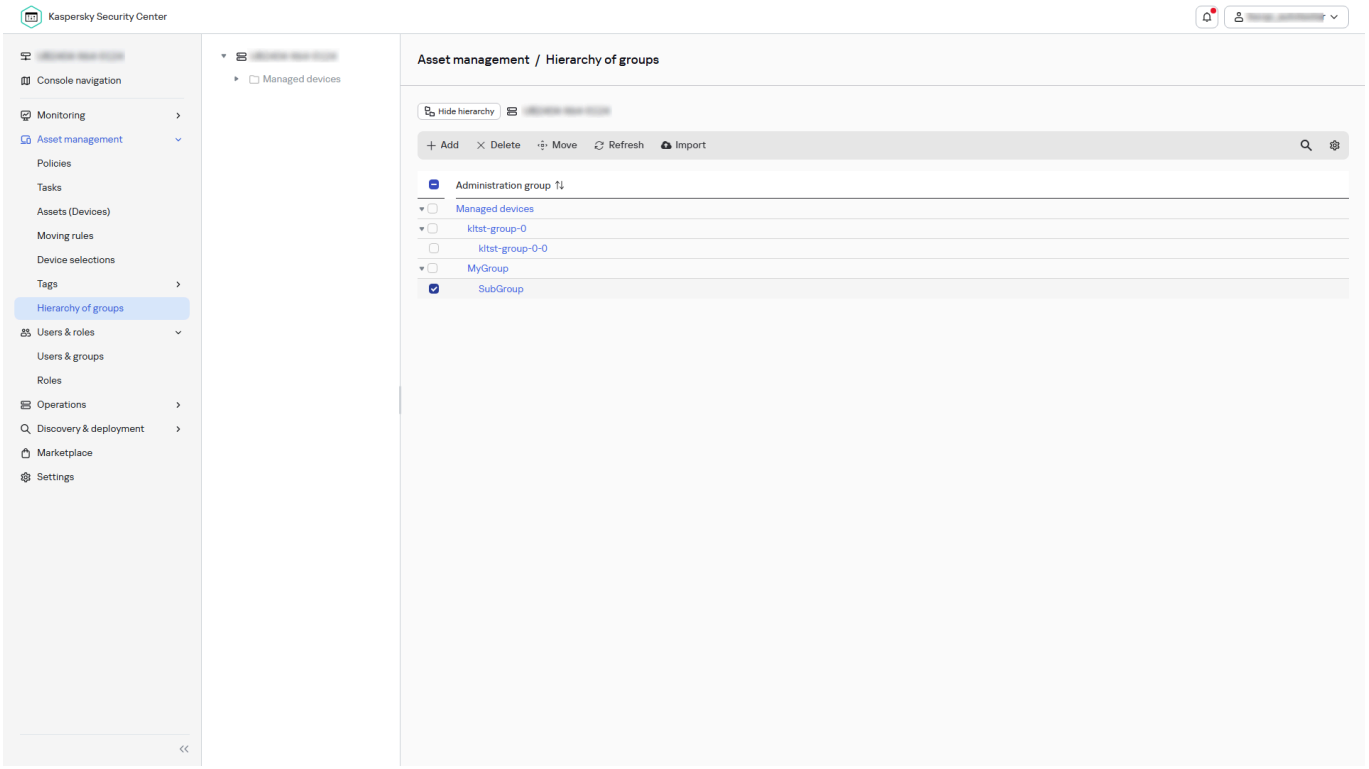
该设备将被移动到新的管理服务器并通过新的连接网关进行连接。

# 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“**资产管理**”→“**组层级**”。
2. 通过以下方式之一转到所需管理组的属性：
   - 单击管理组的名称。
   - 单击页面顶部的“**显示层级**”按钮。在打开的导航窗格中，将鼠标光标悬停在所需组的名称上，然后单击设置图标 ( ⚙ )。




管理组的层次结构

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。

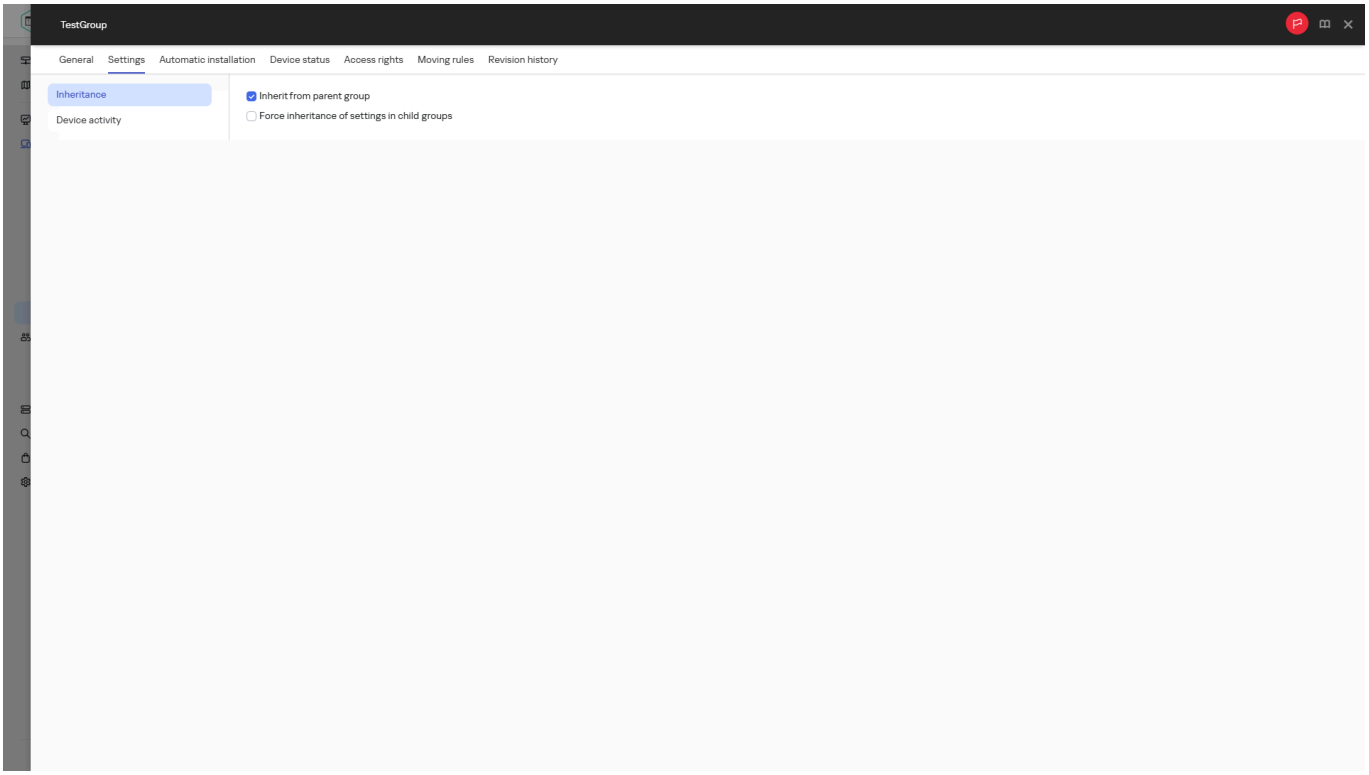
  该选项仅在管理组拥有父组时可用。

  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。




管理组属性

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**

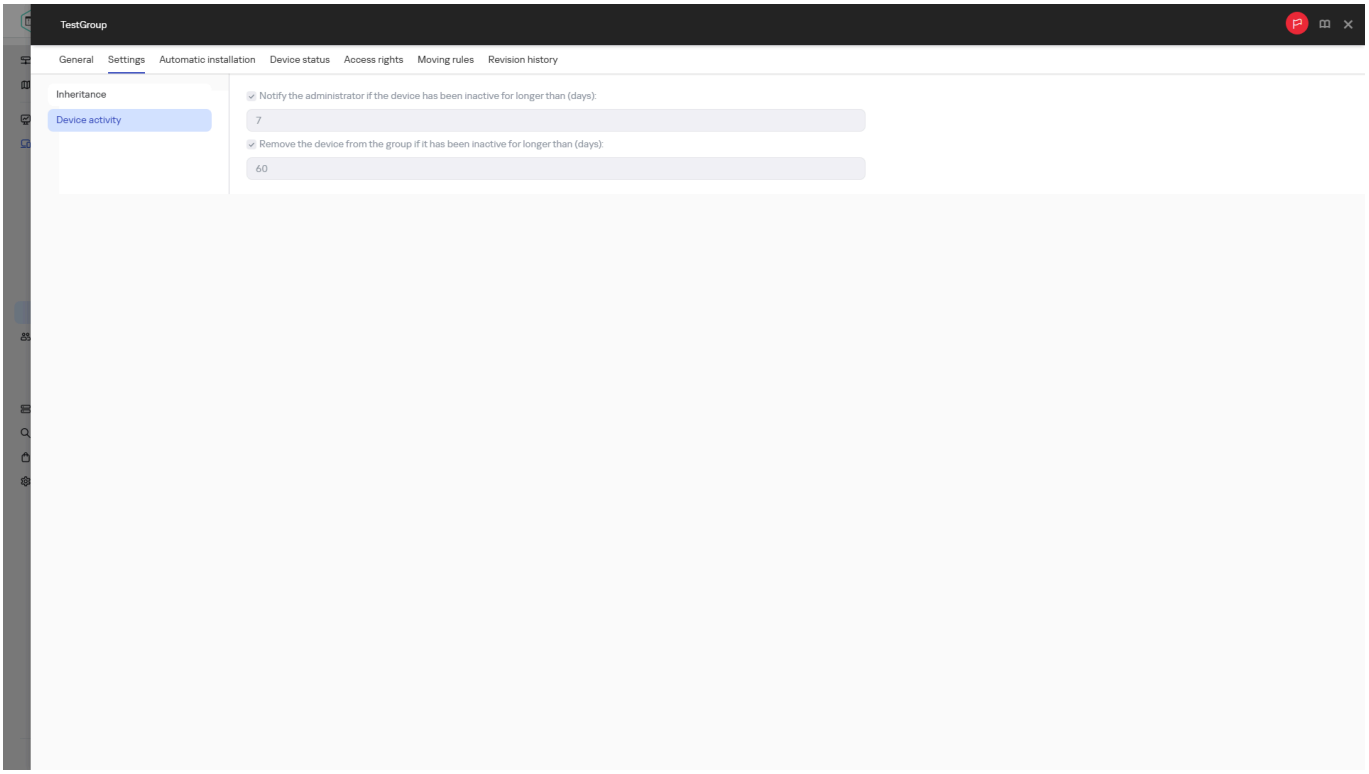
  如果启用该选项，管理员接收不活动设备的通知。您可以指定**设备在网络上已长时间没有活动**事件被创建的时间间隔。默认时间间隔是 7 天。

  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。




管理组属性

6. 点击“**保存**”。

您的更改已保存并应用。

# 发送消息到设备用户

*要发送消息到设备用户：*

1. 在主菜单中，转到“**任务**”。
2. 单击**添加**。
“新任务向导”启动。
3. 在**任务类型**下拉列表中，选择**将消息发送至用户**。
4. 选择一个选项以指定管理组、设备分类或应用程序任务的设备。
5. 运行创建的任务。

任务完成后，创建的消息将被发送给选定设备用户。**将消息发送至用户**任务仅对 Windows 设备可用。

# 远程开启、关闭和重启客户端设备

Kaspersky Security Center Linux 允许您远程管理客户端设备：开机、关机和重启。

*要远程管理客户端设备：*

1. 在主菜单中，转到“**任务**”。
2. 单击**添加**。
   “新任务向导”启动。
3. 在“**任务类型**”下拉列表中，选择“**管理设备**”。
4. 选择一个选项以指定管理组、设备分类或应用程序任务的设备。
5. 选择命令（打开、关闭或重新启动）。
6. 如果有必要，请为关闭和重启命令配置以下设置：
   - 打开**提示用户确认**切换按钮以指定用户提示消息以及重复提示和重新启动或关闭设备的时间间隔。
   - 选中**在该时间后强制关闭阻止会话中的应用程序(分钟)**复选框并指定时间。

   这些设置仅适用于 Windows 客户端设备。任务完成后 Linux 设备将立即重启或关闭。
7. 运行创建的任务。

任务完成后，选定设备将执行所选命令（开启、关闭或重启）。

# 远程访问受管理设备

Kaspersky Security Center Linux 允许您建立与受管理设备的远程连接。管理员可以通过设备上安装的网络代理获取对受管理设备的远程访问权限。即使客户端设备的 TCP 和 UDP 端口关闭，也可以通过网络代理远程连接至设备。在与设备建立连接后，管理员会获取对此设备上存储的信息的完全访问权限，以便他或她可以管理其上安装的应用程序。

建立远程连接的方法取决于安装有 Kaspersky Security Center Web Console 的设备上使用的平台。Kaspersky Security Center Web Console 可以安装在管理服务器设备以外的设备上，即基于 Windows 或 Linux 的设备上。

从安装在 Linux 设备上的 Kaspersky Security Center Web Console，您可以建立以下连接：

- 使用以下方式到基于 Linux 的受管理设备：
  - 远程桌面连接 (RDP)
  - 虚拟网络计算 (VNC)
- 通过使用以下方式到基于 Windows 的受管理设备：
  - 远程桌面连接 (RDP)
  - 虚拟网络计算 (VNC)

从安装在 Windows 设备上的 Kaspersky Security Center Web Console，您可以建立以下连接：

- 使用以下方式到基于 Linux 的受管理设备：
  - 远程桌面连接 (RDP)
  - 虚拟网络计算 (VNC)
- 通过使用以下方式到基于 Windows 的受管理设备：
  - 远程桌面连接 (RDP)
  - Windows 桌面共享 (WDS)

从运行 Microsoft Windows on Arm 的设备访问 Kaspersky Security Center Web Console 时，不支持远程连接到受管理设备。

要建立与设备的远程连接，您必须有：

- klsctunnel 实用程序

  卡巴斯基实用程序用于在受管理设备和管理服务器之间建立隧道连接。

  Kaspersky Security Center Linux 允许通过管理服务器的从 Kaspersky Security Center Web Console 的 TCP 连接通道，然后通过网络代理到受管理设备上的指定端口。通道设计用于连接安装了 Kaspersky Security Center Web Console 的设备上的客户端应用程序到受管理设备上的 TCP 端口—如果 Kaspersky Security Center Web Console 和目标设备之间没有直接连接可用。

  如果用于连接到管理服务器的端口在设备上不可用，则需要客户端设备和管理服务器之间的连接隧道。在以下情况下设备端口可能不可用：

  - 远程设备连接到使用 NAT 装置的本地网络。
  - 远程设备是本地网络管理服务器的一部分，但是它的端口被防火墙关闭。

  通过Kaspersky Security Center云控制台或从卡巴斯基网站手动建立远程连接时，可以下载该实用程序。

  klsctunnel实用程序安装在管理服务器设备上，用于所有类型的远程连接（RDP、VNC、WDS）。

- RDP 或 VNC 客户端

  RDP 或 VNC 客户端安装在管理服务器设备上。此客户端允许您使用 klsctunnel 实用程序提供的本地连接的地址和端口来获取对受管理设备的远程访问。

  RDP 到用户的当前远程桌面会话的连接是在用户不知道的情况下建立的。一旦管理员连接会话，设备用户将在没有通知的情况下从会话断开连接。

- Windows 桌面共享（仅适用于基于 Windows 的受管理设备）

  此功能可让您连接至客户端设备上的现有会话而不会断开此会话中的用户。在这种情况下，设备上的管理员和会话用户将共享桌面访问权限。

  当连接到远程桌面的现有会话时，设备上的会话用户会收到来自管理员的连接请求。Kaspersky Security Center Linux 创建的报告中不会保存有关设备上的远程活动及其结果的任何信息。

  管理员可以在远程客户端设备上配置用户活动的审核。审核期间，应用程序会保存有关客户端设备上管理员打开和/或修改过的文件的信息。

# 使用 Kaspersky Security Center Web Console 从基于 Linux 的设备远程访问基于 Linux 的受管理设备

先决条件

在您开始之前，确保您已做了如下：

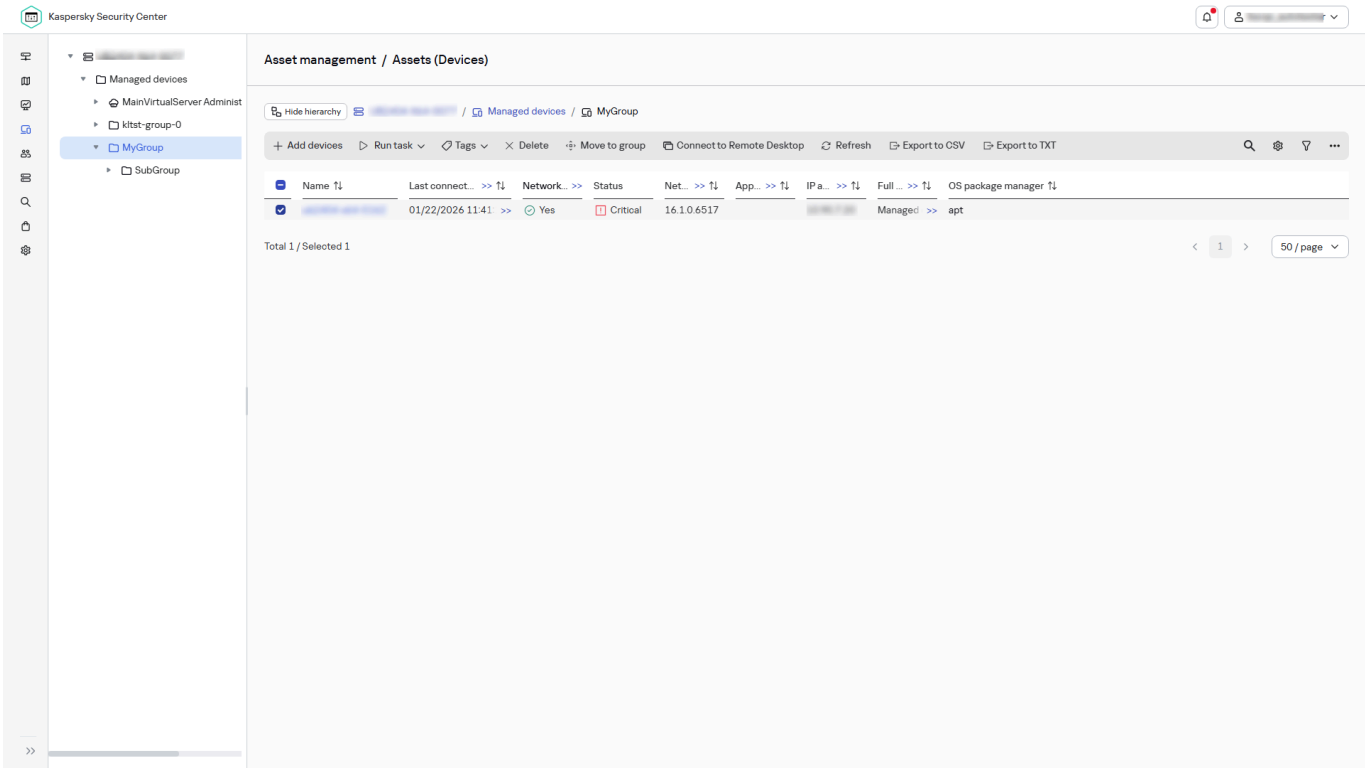
- 在运行 Linux 的受管理设备上，安装了网络代理 15.3 或更高版本的安装程序。
- 在运行 Linux 的受管理设备上，安装了 RDP 服务器（如果您使用远程桌面连接连接到受管理设备）。
- 在运行 Linux 的受管理设备上，安装了 VNC 服务器（如果您使用虚拟网络计算连接到受管理设备）。
- 用于建立 RDP 隧道连接的端口已打开（在管理服务器属性窗口的**打开用于建立 RDP 连接通道的端口**部分中启用了**连接端口**选项）。
- 管理员具有**启动 RDP 会话**权限来建立 RDP 连接（如果您使用远程桌面连接连接到受管理设备）。
- 管理员有**创建通道** 权限来建立 VNC 隧道连接（如果您使用虚拟网络计算连接到受管理设备）。

*要通过在基于 Linux 的受管理设备上打开的Kaspersky Security Center Web Console 使用 RDP 或 VNC 连接到基于 Linux 的受管理设备：*

1. 在主菜单中，转到**资产管理→资产(设备)**部分或打开设备分类。
2. 选中要远程连接的受管理设备旁边的复选框，然后单击**连接到远程桌面**按钮。

   “**连接到远程桌面**窗口将打开。

如果您选择多个设备、一个移动设备或一个运行 macOS 的设备，则“**连接到远程桌面**按钮将被禁用。




受管理设备列表

3. 单击**下载**按钮下载 klsctunnel 实用程序，然后运行它。

   下载该实用程序时，请考虑以下事项：

   - 要获取 klsctunnel 实用程序的最新版本，请确保管理服务器可以访问卡巴斯基更新服务器。

     您可以运行*下载更新到管理服务器存储库*任务并选择卡巴斯基更新服务器作为更新源。如果任务成功完成，管理服务器就可以访问卡巴斯基更新服务器。

   - 如果实用程序文件无法下载，则会显示一条错误消息。在这种情况下，手动下载实用程序，然后将其放在管理服务器设备的 /var/opt/kaspersky/klnagent_srv 目录中。

4. 在**连接到远程桌面**窗口中，指定连接端口。默认情况下使用端口 3389。

5. 单击**生成 Blob**按钮生成具有编码连接参数的文本 blob，然后将文本复制并粘贴到 klsctunnel 实用程序中的相应字段中。

   Blob 包含在管理服务器和受管理设备之间建立连接所需的设置。Blob 有效期为 3 分钟。如果已过期，请生成一个新的 Blob。

6. 在 klsctunnel 实用程序中，如果使用代理服务器，请指定代理服务器连接设置。

   klsctunnel 实用程序显示远程访问客户端的本地连接的地址和端口。

   该实用程序允许管理员关闭隧道连接。如果隧道连接关闭，则当前与远程桌面的连接将终止。

7. 运行远程访问客户端（RDP 或 VNC），并使用 klsctunnel 实用程序提供的地址和端口将其连接到受管理设备。

与受管理设备的连接已建立，桌面在远程访问客户端窗口中可用。

# 使用 Kaspersky Security Center Web Console 从基于 Linux 的设备远程访问基于 Windows 的受管理设备

远程桌面连接 (RDP)

**先决条件**

在您开始之前，确保您已做了如下：

- 受管理设备的操作系统设置中允许远程连接。
- 在运行 Windows 的受管理设备上，安装了网络代理 13.0 或更高版本。
- 管理员具有**启动 RDP 会话**权限来建立 RDP 连接。
- 用于建立 RDP 隧道连接的端口已打开（在管理服务器属性窗口的**打开用于建立 RDP 连接通道的端口**部分中启用了**连接端口**选项）。

*要通过在基于 Linux 的设备上打开的 Kaspersky Security Center Web Console 使用 RDP 连接到基于 Windows 的受管理设备：*

1. 在主菜单中，转到**资产管理→资产(设备)**部分或打开设备分类。
2. 选中要远程连接的受管理设备旁边的复选框，然后单击**连接到远程桌面**按钮。

   “**连接到远程桌面**窗口将打开。

   如果您选择多个设备、一个移动设备或一个运行 macOS 的设备，则“**连接到远程桌面**按钮将被禁用。
3. 在**连接到远程桌面**窗口中，选择**RDP**连接类型。
4. 如果受管理设备的操作系统设置中不允许远程连接，请单击**更改设置**按钮集中允许远程连接。

   如果设置正确，则会显示通知。另外，在受管理设备上，在**设置→系统→远程桌面**部分，**启用远程桌面**选项已启用。

   如果受管理设备的操作系统设置中允许远程连接，则不会显示**更改设置**按钮。
5. 单击**下载**按钮下载 klsctunnel 实用程序，然后运行它。

   下载该实用程序时，请考虑以下事项：

   - 要获取 klsctunnel 实用程序的最新版本，请确保管理服务器可以访问卡巴斯基更新服务器。

     您可以运行*下载更新到管理服务器存储库*任务并选择卡巴斯基更新服务器作为更新源。如果任务成功完成，管理服务器就可以访问卡巴斯基更新服务器。
   - 如果实用程序文件无法下载，则会显示一条错误消息。在这种情况下，手动下载实用程序，然后将其放在管理服务器设备的 /var/opt/kaspersky/klnagent_srv 目录中。

6. 单击**生成 Blob**按钮生成具有编码连接参数的文本 blob，然后将文本复制并粘贴到 klsctunnel 实用程序中的相应字段中。

   Blob 包含在管理服务器和受管理设备之间建立连接所需的设置。Blob 有效期为 3 分钟。如果已过期，请生成一个新的 Blob。

7. 在 klsctunnel 实用程序中，如果使用代理服务器，请指定代理服务器连接设置。

   klsctunnel 实用程序显示与远程设备的连接的地址和端口。

   该实用程序允许管理员关闭隧道连接。如果隧道连接关闭，则当前与远程桌面的连接将终止。

8. 运行 RDP 客户端并使用 klsctunnel 实用程序提供的地址和端口将其连接到受管理设备。

与受管理设备的连接已建立，桌面在 RDP 客户端窗口中可用。

在用户不知道的情况下远程连接到用户的当前桌面会话。一旦管理员连接会话，设备用户将在没有通知的情况下从会话断开连接。

虚拟网络计算系统 (VNC)

**先决条件**

在您开始之前，确保您已做了如下：

- 在运行 Windows 的受管理设备上，安装了网络代理 13.0 或更高版本。
- 在运行 Windows 操作系统的受管理设备上，安装了 VNC 服务器。
- 管理员具有**创建通道**权限，可以为 VNC 建立隧道连接。
- 用于建立 RDP 隧道连接的端口已打开（在管理服务器属性窗口的**打开用于建立 RDP 连接通道的端口**部分中启用了**连接端口**选项）。

*要通过在基于 Linux 的设备上打开的 Kaspersky Security Center Web Console 使用 VNC 连接到基于 Windows 的受管理设备：*

1. 在主菜单中，转到**资产管理→资产(设备)**部分或打开设备分类。
2. 选中要远程连接的受管理设备旁边的复选框，然后单击**连接到远程桌面**按钮。

   “**连接到远程桌面**窗口将打开。

   如果您选择多个设备、一个移动设备或一个运行 macOS 的设备，则“**连接到远程桌面**按钮将被禁用。

3. 在**连接到远程桌面**窗口中，选择连接类型**VNC**。
4. 单击**下载**按钮下载 klsctunnel 实用程序，然后运行它。

   如果实用程序文件无法下载，则会显示一条错误消息。在这种情况下，手动下载实用程序。
5. 在**连接到远程桌面**窗口中，指定 VNC 连接端口。默认情况下使用端口 5900。

6. 单击**生成 Blob**按钮生成具有编码连接参数的文本 blob，然后将文本复制并粘贴到 klsctunnel 实用程序中的相应字段中。

   Blob 包含在管理服务器和受管理设备之间建立连接所需的设置。Blob 有效期为 3 分钟。如果已过期，请生成一个新的 Blob。

7. 在 klsctunnel 实用程序中，如果使用代理服务器，请指定代理服务器连接设置。

   klsctunnel 实用程序显示 VNC 客户端本地连接的地址和端口。

   该实用程序允许远程用户关闭隧道连接。如果隧道连接关闭，则当前与远程桌面的连接将终止。

8. 运行 VNC 客户端并使用 klsctunnel 实用程序提供的地址和端口将其连接到受管理设备。

与受管理设备的连接已建立，桌面在 VNC 客户端窗口中可用。

# 使用 Kaspersky Security Center Web Console从基于 Windows 的设备远程访问基于 Linux 的受管理设备

远程桌面连接 (RDP)

**先决条件**

在您开始之前，确保您已做了如下：

- 在运行 Linux 的受管理设备上，安装了 RDP 服务器。
- 在运行 Linux的受管理设备上，安装了网络代理15.3 或更高版本的安装程序。
- 管理员具有**启动 RDP 会话**权限来建立 RDP 连接。
- 用于建立 RDP 隧道连接的端口已打开（在管理服务器属性窗口的**打开用于建立 RDP 连接通道的端口**部分中启用了**连接端口**选项）。

*要通过在基于 Windows 的设备上打开的Kaspersky Security Center Web Console 使用 RDP 连接到基于 Linux 的受管理设备：*

1. 在主菜单中，转到**资产管理→资产(设备)**部分或打开设备分类。
2. 选中要远程连接的受管理设备旁边的复选框，然后单击**连接到远程桌面**按钮。

   “**连接到远程桌面**窗口将打开。

   如果您选择多个设备、一个移动设备或一个运行 macOS 的设备，则“**连接到远程桌面**按钮将被禁用。

3. 在**连接到远程桌面**窗口中，选择**RDP**连接类型。
4. 单击**下载**按钮下载 klsctunnel 实用程序，然后运行它。

下载该实用程序时，请考虑以下事项：

- 要获取 klsctunnel 实用程序的最新版本，请确保管理服务器可以访问卡巴斯基更新服务器。

  您可以运行*下载更新到管理服务器存储库*任务并选择卡巴斯基更新服务器作为更新源。如果任务成功完成，管理服务器就可以访问卡巴斯基更新服务器。

- 如果实用程序文件无法下载，则会显示一条错误消息。在这种情况下，手动下载实用程序，然后将其放在管理服务器设备的 /var/opt/kaspersky/klnagent_srv 目录中。

5. 单击**生成 Blob**按钮生成具有编码连接参数的文本 blob，然后将文本复制并粘贴到 klsctunnel 实用程序中的相应字段中。

   Blob 包含在管理服务器和受管理设备之间建立连接所需的设置。Blob 有效期为 3 分钟。如果已过期，请生成一个新的 Blob。

6. 在 klsctunnel 实用程序中，如果使用代理服务器，请指定代理服务器连接设置。

   为此，请选中**使用代理服务器**复选框，然后指定连接设置。

7. 单击“**打开端口**”按钮。

   将打开远程桌面连接登录窗口。

8. 指定您当前用来登录 Kaspersky Security Center Web Console 的账户的凭据，然后连接到受管理设备。

   klsctunnel 实用程序显示与远程设备的连接的地址和端口。

   该实用程序允许管理员关闭隧道连接。如果隧道连接关闭，则当前与远程桌面的连接将终止。

在与设备建立连接后，可以在 Microsoft Windows 的远程连接窗口使用桌面。

在用户不知道的情况下远程连接到用户的当前桌面会话。一旦管理员连接会话，设备用户将在没有通知的情况下从会话断开连接。

虚拟网络计算系统 (VNC)

**先决条件**

在您开始之前，确保您已做了如下：

- 在运行 Linux 的受管理设备上，安装了网络代理 15.3 或更高版本的安装程序。
- 在运行 Linux 的受管理设备上，安装了 VNC 服务器。
- 管理员具有**创建通道**权限，可以为 VNC 建立隧道连接。
- 用于建立 RDP 隧道连接的端口已打开（在管理服务器属性窗口的**打开用于建立 RDP 连接通道的端口**部分中启用了**连接端口**选项）。

*要通过在基于 Windows 的设备上打开的Kaspersky Security Center Web Console 使用 VNC 连接到基于 Linux 的受管理设备：*

1. 在主菜单中，转到**资产管理→资产(设备)**部分或打开设备分类。
2. 选中要远程连接的受管理设备旁边的复选框，然后单击**连接到远程桌面**按钮。

"**连接到远程桌面**窗口将打开。

如果您选择多个设备、一个移动设备或一个运行 macOS 的设备，则"**连接到远程桌面**按钮将被禁用。

3. 在**连接到远程桌面**窗口中，选择连接类型**VNC**。
4. 单击**下载**按钮下载 klsctunnel 实用程序，然后运行它。

   如果实用程序文件无法下载，则会显示一条错误消息。在这种情况下，手动下载实用程序。
5. 在**连接到远程桌面**窗口中，指定 VNC 连接端口。默认情况下使用端口 5900。
6. 单击**生成 Blob**按钮生成具有编码连接参数的文本 blob，然后将文本复制并粘贴到 klsctunnel 实用程序中的相应字段中。

   Blob 包含在管理服务器和受管理设备之间建立连接所需的设置。Blob 有效期为 3 分钟。如果已过期，请生成一个新的 Blob。
7. 在 klsctunnel 实用程序中，如果使用代理服务器，请指定代理服务器连接设置。

   为此，请选中**使用代理服务器**复选框，然后指定连接设置。
8. 单击"**打开端口**"按钮。

   klsctunnel 实用程序显示 VNC 客户端本地连接的地址和端口。

   该实用程序允许远程用户关闭隧道连接。如果隧道连接关闭，则当前与远程桌面的连接将终止。
9. 运行 VNC 客户端并使用 klsctunnel 实用程序提供的地址和端口将其连接到受管理设备。

与受管理设备的连接已建立，桌面在 VNC 客户端窗口中可用。

# 使用 Kaspersky Security Center Web Console 从基于 Windows 的设备远程访问基于 Windows 的受管理设备

远程桌面连接 (RDP)

**先决条件**

在您开始之前，确保您已做了如下：

- 在运行 Windows 的受管理设备上，安装了网络代理 13.0 或更高版本。
- 管理员具有**启动 RDP 会话**权限来建立 RDP 连接。
- 用于建立 RDP 隧道连接的端口已打开（在管理服务器属性窗口的**打开用于建立 RDP 连接通道的端口**部分中启用了**连接端口**选项）。
- 受管理设备的操作系统设置中允许远程连接。

*要通过在基于 Windows 的受管理设备上打开的Kaspersky Security Center Web Console 使用 RDP 连接到基于 Windows 的受管理设备：*

1. 在主菜单中，转到**资产管理→资产(设备)**部分或打开设备分类。
2. 选中要远程连接的受管理设备旁边的复选框，然后单击**连接到远程桌面**按钮。

   “**连接到远程桌面**窗口将打开。

   如果您选择多个设备、一个移动设备或一个运行 macOS 的设备，则“**连接到远程桌面**按钮将被禁用。
3. 在**连接到远程桌面**窗口中，选择**远程桌面连接**连接类型。
4. 如果受管理设备的操作系统设置不允许远程连接，请单击**更改设置**按钮集中允许远程连接。

   如果设置正确，则会显示通知。另外，在受管理设备上，在**设置→系统→远程桌面**部分，**启用远程桌面**选项已启用。

   如果受管理设备的操作系统设置中允许远程连接，则不会显示**更改设置**按钮。
5. 单击**下载**按钮下载 klsctunnel 实用程序，然后运行它。

   下载该实用程序时，请考虑以下事项：

   - 要获取 klsctunnel 实用程序的最新版本，请确保管理服务器可以访问卡巴斯基更新服务器。

     您可以运行*下载更新到管理服务器存储库*任务并选择卡巴斯基更新服务器作为更新源。如果任务成功完成，管理服务器就可以访问卡巴斯基更新服务器。
   - 如果实用程序文件无法下载，则会显示一条错误消息。在这种情况下，手动下载实用程序，然后将其放在管理服务器设备的 /var/opt/kaspersky/klnagent_srv 目录中。
6. 单击**生成 Blob**按钮生成具有编码连接参数的文本 blob，然后将文本复制并粘贴到 klsctunnel 实用程序中的相应字段中。

   Blob 包含在管理服务器和受管理设备之间建立连接所需的设置。Blob 有效期为 3 分钟。如果已过期，请生成一个新的 Blob。
7. 在 klsctunnel 实用程序中，如果使用代理服务器，请指定代理服务器连接设置。

   为此，请选中**使用代理服务器**复选框，然后指定连接设置。
8. 单击“**打开端口**”按钮。

   将打开远程桌面连接登录窗口。
9. 指定您当前用来登录 Kaspersky Security Center Web Console 的账户的凭据，然后连接到受管理设备。

   klsctunnel 实用程序显示与远程设备的连接的地址和端口。

   该实用程序允许管理员关闭隧道连接。如果隧道连接关闭，则当前与远程桌面的连接将终止。

在与设备建立连接后，可以在 Microsoft Windows 的远程连接窗口使用桌面。

在用户不知道的情况下远程连接到用户的当前桌面会话。一旦管理员连接会话，设备用户将在没有通知的情况下从会话断开连接。

Windows 桌面共享 (WDS)

**先决条件**

在您开始之前，确保您已做了如下：

- 在运行 Windows 的受管理设备上，安装了网络代理 13.0 或更高版本。
- 管理员具有**连接到现有 RDP 会话**权限来建立 WDS 连接。
- 漏洞和补丁管理的授权许可可用。
- 管理员的工作站上安装了 Microsoft Windows Vista 或更高版本。管理服务器设备操作系统的类型对通过 Windows 桌面共享进行连接没有限制。

  检查您的 Windows 版本是否包含 Windows 桌面共享功能，确保 Windows 注册表中存在 CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} 密钥。
- 客户端设备上安装了 Microsoft Windows Vista 或更高版本。

*要通过在基于 Windows 的受管理设备上打开的Kaspersky Security Center Web Console 使用 VNC 连接到基于 Windows 的受管理设备：*

1. 在主菜单中，转到**资产管理→资产(设备)**部分或打开设备分类。
2. 选中要远程连接的受管理设备旁边的复选框，然后单击**连接到远程桌面**按钮。

   “**连接到远程桌面**窗口将打开。

   如果您选择多个设备、一个移动设备或一个运行 macOS 的设备，则“**连接到远程桌面**按钮将被禁用。
3. 在**连接到远程桌面**窗口中，选择连接类型**Windows 桌面共享**。

   如果漏洞和补丁管理授权许可不可用，则会显示错误消息。
4. 单击**下载**按钮下载 klsctunnel 实用程序，然后运行它。

   如果实用程序文件无法下载，则会显示一条错误消息。在这种情况下，手动下载实用程序。
5. 在选定设备上活动的可用用户会话列表中，选择要连接的会话。

   远程用户必须允许连接。如果远程用户拒绝连接或者远程用户在超时期限内不允许连接，则会显示错误消息。
6. 单击**生成 Blob**按钮生成具有编码连接参数的文本 blob，然后将文本复制并粘贴到 klsctunnel 实用程序中的相应字段中。

   Blob 包含在管理服务器和受管理设备之间建立连接所需的设置。Blob 有效期为 3 分钟。如果已过期，请生成一个新的 Blob。
7. 在 klsctunnel 实用程序中，如果使用代理服务器，请指定代理服务器连接设置。

   为此，请选中**使用代理服务器**复选框，然后指定连接设置。
8. 单击“**打开端口**”按钮。

   klsctunnel 实用程序显示 VNC 客户端本地连接的地址和端口。

   该实用程序允许远程用户关闭隧道连接。如果隧道连接关闭，则当前与远程桌面的连接将终止。

桌面共享在新窗口中启动。如果要与设备互动，请单击窗口左上角的“菜单”图标 ()，然后选择**交互模式**。

# 管理移动设备

通过 Kaspersky Security Center 的移动设备保护管理通过使用移动设备管理功能执行。您必须在每台移动设备上添加授权许可密钥才能激活保护应用程序。如果您打算管理组织员工拥有的移动设备，请启用和配置移动设备管理。

移动设备管理可让您管理员工的 Android 和 iOS 设备。该保护由安装在移动设备上的 Kaspersky Endpoint Security for Android 应用和 iOS 设备管理系统提供。这些移动应用可确保保护移动设备免受 Web 威胁、病毒和其他构成威胁的程序的侵害。要通过 Kaspersky Security Center Web Console 进行集中管理，您必须在安装了 Kaspersky Security Center Web Console 的设备上安装以下 Web 管理插件：

- 卡巴斯基移动设备保护和管理

  卡巴斯基移动设备保护和管理插件允许您在Kaspersky Security Center Web Console 中管理运行 Android 和 iOS 的设备。

- iOS MDM 服务器设置

  iOS MDM 服务器设置插件允许您配置用于将 iOS 设备连接到管理服务器并管理 iOS 设备的 iOS MDM 服务器的设置。

有关移动设备的保护部署和管理的信息，请参阅Kaspersky Security for Mobile 帮助 和 Kaspersky Secure Mobility Management 帮助。

# 使用 Firebase Cloud Messaging

为了确保及时向 Android 设备传递命令，Kaspersky Security Center Linux 使用推送通知机制。安卓设备和管理服务器之间通过 Firebase Cloud Messaging（以下简称 FCM）交换推送通知。在 Kaspersky Security Center Linux云控制台中，您可以指定Firebase Cloud Messaging的设置从而将安卓设备连接到服务。

要检索 Firebase Cloud Messaging 的设置，您必须有 Google 账户。

*要启用对 FCM 的使用：*

1. 在 Kaspersky Security Center Linux云控制台主窗口中，选择**资产管理** →**Mobile**→**Devices**。
2. 打开三点菜单（⋮）并选择**Forced Android device synchronization**。
3. 在**Firebase project number**字段中，指定 FCM 发件人 ID。
4. 在**Private key**字段中，选择私钥文件。

   在下次同步管理服务器时，安卓设备将被连接到 Firebase Cloud Messaging。

当切换到不同的 Firebase 项目时，您需要等待 10 分钟才能恢复 FCM。

FCM 服务在以下地址范围内运行：

- 从安卓设备端，需要对以下地址的端口 443 (HTTPS)、5228 (HTTPS)、5229 (HTTPS) 和 5230 (HTTPS) 的访问：
  - google.com
  - fcm.googleapis.com
  - oauth2.googleapis.com
  - android.apis.google.com
  - Google's ASN 15169 中列出的所有 IP 地址
- 从管理服务器端，需要对以下地址的端口 443 (HTTPS) 的访问：
  - fcm.googleapis.com
  - Google's ASN 15169 中列出的所有 IP 地址

如果代理服务器设置已在 Kaspersky Security Center Web Console 的管理服务器属性中指定，则这些设置将用于与 GFCM 交互中。

配置 FCM：获取发件人 ID 和私钥文件

*要配置 FCM：*

1. 在 Google 门户注册。
2. 转到Firebase 控制台。
3. 执行以下操作之一：
   - 要创建新项目，请单击**创建项目**并按照屏幕上的说明进行操作。
   - 打开现有项目。
4. 单击齿轮图标并选择**项目设置**。
   “**项目设置**”窗口将开启。
5. 选择**Cloud Messaging**选项卡。
6. 从**Firebase Cloud Messaging API (V1)**部分中的**发件人 ID**字段检索相关的发件人 ID。
7. 选择**服务账户**选项卡，然后单击**生成新私钥**。
8. 在打开的窗口中，单击**生成密钥**以生成并下载私钥文件。

Firebase Cloud Messaging 现已配置。

# 与公共密钥基础架构整合

您可以通过公钥基础架构（PKI）将证书颁发与 Microsoft Certification Authority（CA）进行集成。与 PKI 集成旨在简化管理服务器颁发域用户证书的过程。整合后，证书自动发布。

有关配置与 PKI 集成以颁发证书的详细信息，请参阅Kaspersky Secure Mobility Management 帮助。

您可以使用指定设置执行 PKI 集成，并指定 PKI 作为特定类型证书的证书源。PKI 集成设置允许您为所有类型的证书设置单独的默认模板。

使用 PKI 集成颁发证书的具体内容：

- 默认 PKI 集成被禁用。有关启用 PKI 和配置其设置的详细信息，请参阅Kaspersky Secure Mobility Management 帮助。
- 证书颁发使用网络代理 Windows 进行，这使得管理服务器和 Microsoft CA 能够集成。由于可以有多个安装了网络代理的设备，因此您可以在**Issuance rules**中指定将连接到 Microsoft CA 的设备。此设备必须在执行与 PKI 集成的账户的证书存储库中安装有 Enrollment Agent (EA) 证书。该证书由域的 CA 管理员颁发。
- 进行与 PKI 集成的账户必须是域用户，并具有*作为服务登录*的权限。
- Kaspersky Security Center Linux 一次只能与一个 PKI（Microsoft CA）集成一起工作。

# 对管理组进行管理

本部分提供有关如何对管理组进行管理的信息。

您可以对管理组采取以下操作：

- 向管理组中添加任何层次结构级别的任意数量的嵌套组。
- 添加设备到管理组。
- 通过将单个设备和整个组移至其他组，改变管理组的层次结构。
- 从管理组中删除嵌套组和设备。
- 将从属服务器和虚拟管理服务器添加至管理组。
- 将设备从管理服务器的管理组移至其他服务器的管理组。
- 定义将哪些 Kaspersky 应用程序自动安装到包括在组中的设备。

仅当您在您要管理的管理组（或这些组所属管理服务器）的**管理组的管理**区域拥有**修改**权限时，您可以执行这些操作。

# 创建管理组

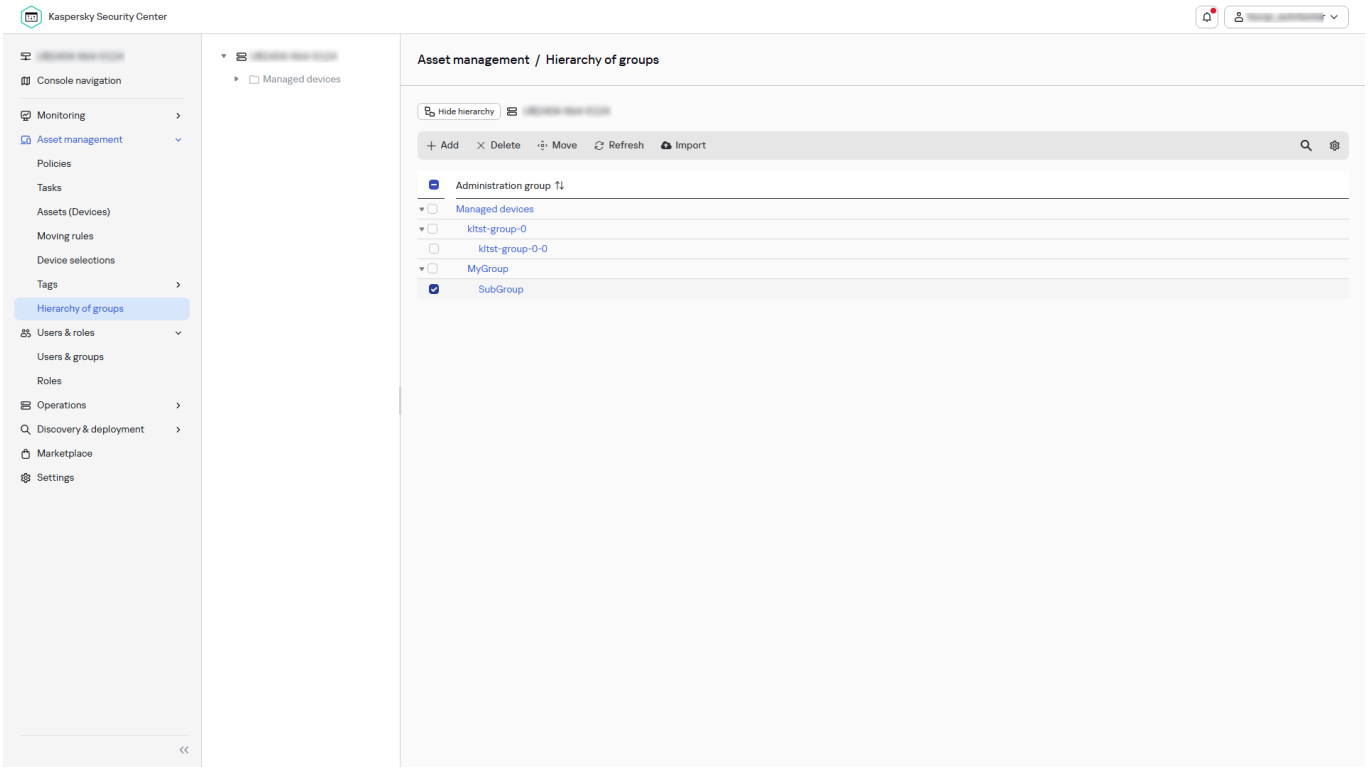
安装 Kaspersky Security Center 后，管理组层次结构仅包含一个名为“**受管理设备**”的管理组。当创建管理组层次结构时，您可以将设备和虚拟机添加到“**受管理设备**”组，并添加嵌套组（请参见下图）。



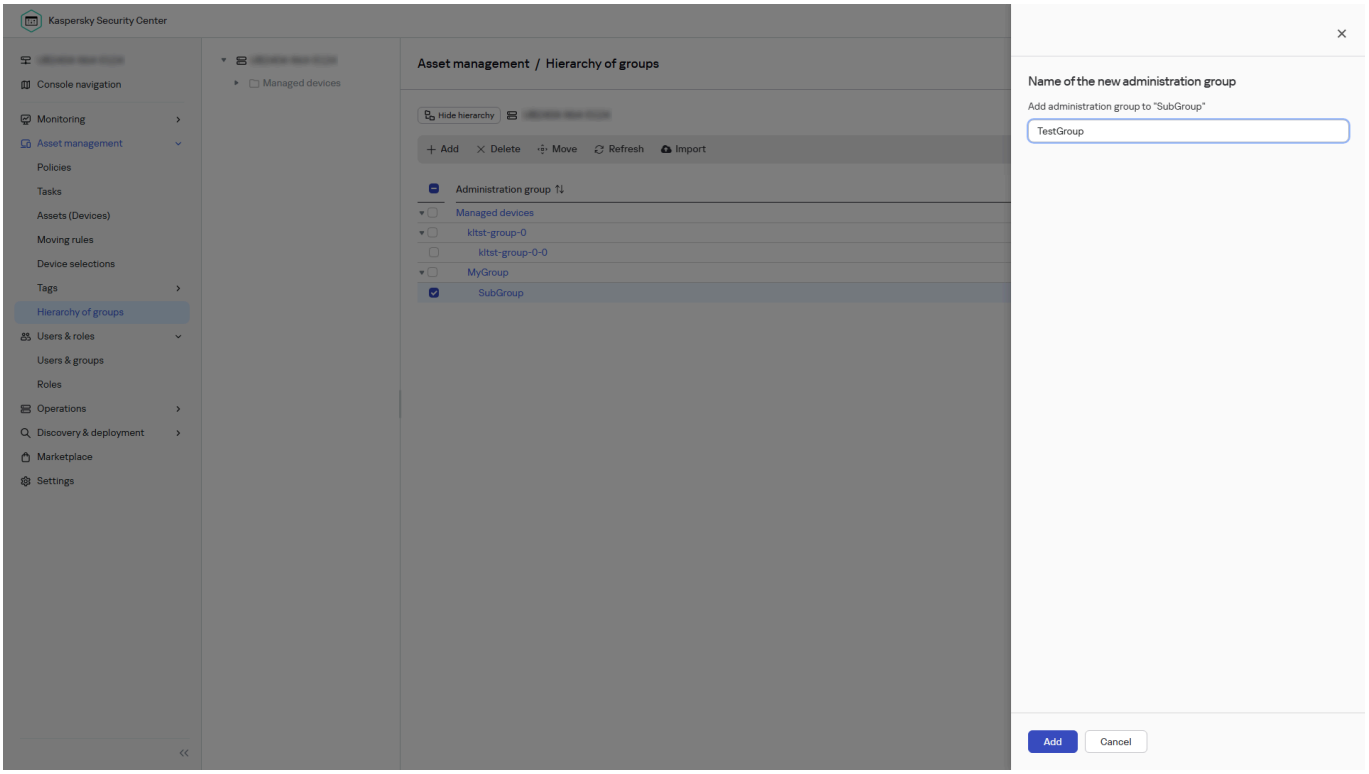

查看管理组层次结构

*要创建管理组，请执行以下操作：*

1. 在主菜单中，转到“**资产管理**” → “**组层级**”。
2. 在管理组结构中，选择要包括新管理组的管理组。




3. 单击“**添加**”按钮。
4. 在打开的“**新管理组名称**”窗口中，输入组的名称，然后单击“**添加**”按钮。




一个具有指定名称的新管理组将出现在管理组层次结构中。

*要创建管理组结构：*

1. 在主菜单中，转到“**资产管理**” → “**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。

# 将应用程序自动安装到管理组中的设备

您可以指定哪些安装包必须用于将 Kaspersky 应用程序自动远程安装到管理组中的客户端设备。

*若要配置将程序自动安装至管理组中的设备上，请执行以下操作：*

1. 在主菜单中，转到“ **资产管理”** → **“组层级**”。
2. 通过以下方式之一转到所需管理组的属性：
   - 单击管理组的名称。
   - 单击页面顶部的“**显示层级**”按钮。在打开的导航窗格中，将鼠标光标悬停在所需组的名称上，然后单击设置图标 ( )。

   管理组属性窗口将开启。
3. 在打开的属性窗口中，转到“**自动安装**”选项卡。
4. 选择需要在设备上安装的应用程序的安装包，然后单击**保存**按钮。
   若您选择了同一个应用程序的多个仅版本不同的安装包，则将保存最新版本的安装包。

选择安装包后，将为每个应用程序创建一个在管理组中的设备上安装应用程序的组任务。这些任务将在新客户端设备加入管理组的时候立即在设备上运行。

# 移动管理组

您可以在组层次结构内移动嵌套的管理组。

管理组与所有嵌套组、从属管理服务器、设备、组策略和任务一起移动。系统将向该组应用与其在管理组层次结构中的新位置相对应的所有设置。

组名称必须在该层次结构的一个级别内唯一。如果在您向其中移动该管理组的文件夹中已有同名的组，则应该更改该管理组的名称。如果尚未更改要移动的组的名称，则在移动该组时，系统将向其名称添加一个 **（<下一个序列号>）** 格式的索引，例如： **（1）** 、 **（2）** 。

> 您不能重命名和移动**受管理设备**组。

*要将管理组移动到管理组层次结构的另一级别：*

1. 在主菜单中，转到 **资产管理** →**组层级**，然后选中要移动的管理组旁边的复选框。
2. 单击工具栏上的**移动**按钮。
3. 在打开的窗口中，选择要移动管理组的位置，然后单击**移动** 按钮。

   窗口关闭，管理组被移至组层次结构的另一级别。

# 删除管理组

如果删除包含从属管理服务器、嵌套组、客户端设备、组任务或为此组创建的策略的管理组，则所有这些也将被删除。

在删除某个管理组之前，您必须从该组中删除所有从属管理服务器、嵌套组和客户端设备。

*要删除管理组，请执行以下操作：*

1. 在主菜单中，转到 **资产管理** →**组层级**，然后选中要删除的管理组旁边的复选框。
2. 单击工具栏上的**删除**按钮。

   管理组被删除。

# 部署 Kaspersky 应用程序

本节介绍通过 Kaspersky Security Center Web Console 在组织中的客户端设备上部署 Kaspersky 应用程序。

# 方案：Kaspersky 应用程序部署

此方案说明如何通过 Kaspersky Security Center Web Console 部署 Kaspersky 应用程序。您可以使用快速启动向导和保护部署向导，或者您可以手动完成所有必要步骤。

以下应用程序可以使用 Kaspersky Security Center Web Console 进行部署：

- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Windows

## 阶段

Kaspersky 应用程序部署分阶段进行：

1. **下载应用程序的管理 Web 插件**

   此阶段由快速启动向导处理。如果您选择不运行向导，请手动下载插件。

2. **下载并创建安装包**

   此阶段由快速启动向导处理。

   通过快速启动向导可以下载带有管理Web 插件的安装包。如果在运行向导时未选择此选项，或者根本没有运行向导，则必须手动下载安装包。

   如果在某些设备（例如远程员工的设备）上无法通过 Kaspersky Security Center Linux 安装卡巴斯基应用程序，则可以为应用程序创建独立安装包。如果您使用独立软件包安装卡巴斯基应用程序，则不必创建和运行远程安装任务，也不必为 Kaspersky Endpoint Security for Windows 创建和配置任务。

   或者，您可以从卡巴斯基网站下载网络代理和安全应用程序的分发包。如果由于某种原因无法远程安装应用程序，您可以使用下载的分发包在本地安装应用程序。

3. **创建、配置和运行远程安装任务**

   此步骤是保护部署向导的一部分。如果您选择不运行保护部署向导，您必须手动创建该任务并手动配置它。

   您也可以为不同管理组或不同设备分类手动创建几个远程安装任务。您可以在这些任务中部署应用程序的不同版本。

   确保您网络中的所有设备均已被发现；然后运行远程安装任务。

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

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。

4. **创建和配置任务**

   必须配置 Kaspersky Endpoint Security 的“*更新*”任务。

   该步骤是快速启动向导的一部分：任务被使用默认设置自动创建和配置。如果您未运行向导，您必须手动创建该任务并手动配置它。如果您使用快速启动向导，请确保任务的计划符合您的要求。（默认情况下，任务的预定开始设置为**手动**，但您可能希望选择其他选项。）

5. **创建策略**

   手动或通过快速启动向导为 Kaspersky Endpoint Security 创建策略。您可以使用策略默认设置；您也可以根据需要随时修改策略默认设置。

6. **验证结果**

   确保部署成功完成：您的每个应用程序都拥有策略和任务，这些应用程序被安装到受管理设备。

结果

完成方案可以导致如下：

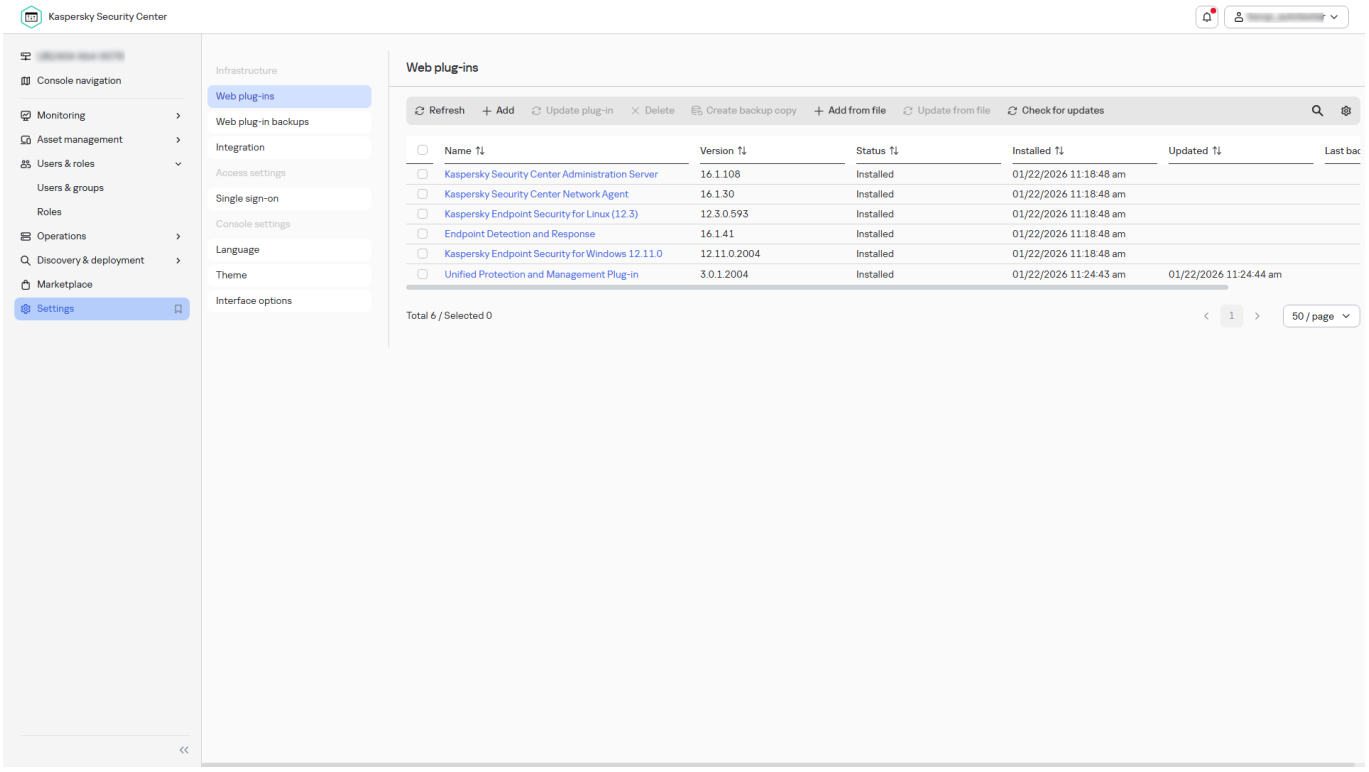
- 所选应用程序的所有所需策略和任务被创建。
- 任务计划根据您的需要被配置。
- 所选应用程序被部署，或者计划在所选客户端设备上部署。

# 添加 Kaspersky 应用程序的管理插件

要部署 Kaspersky 应用程序（例如 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Windows），您必须添加并安装该应用程序的管理 Web 插件。

*要下载 Kaspersky 应用程序的 Web 管理插件：*

1. 在主菜单中，转到“**设置**”→“**Web 插件**”。




已安装的 Web 插件列表

2. 在打开的窗口中，单击“**添加**”按钮。
   可用插件列表被显示。
3. 在可用插件列表中，通过点击其名称选择您要下载的插件（例如，Kaspersky Endpoint Security for Linux）。
   插件描述页面被显示。
4. 在插件描述页面，点击“**安装插件**”。
5. 当安装完成时，点击“**确定**”。

管理 Web 插件使用默认配置进行下载并显示在管理 Web 插件列表中。

您可以从文件添加插件以及更新下载的插件。您可以从卡巴斯基网站下载管理 Web 插件。

*要从文件下载或更新管理 Web 插件：*

1. 在主菜单中，转到**设置** → **Web 插件**。
2. 指定插件文件和文件签名：
   - 单击**从文件添加**以从文件下载插件。
   - 单击**从文件更新**以从文件下载插件更新。

3. 指定文件和文件签名。

4. 下载指定的文件。

管理 Web 插件被从文件下载并显示在管理 Web 插件列表。

# 安装包

*安装包*是为远程安装卡巴斯基应用程序而创建的一组文件。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。

使用以下方法生成安装包：

- 根据包含的*描述符*（扩展名为 kud 的文件，其中包含安装和结果分析规则及其他信息），从指定的分发包中自动生成。
- 来自 ZIP、CAB、TAR 或 TAR.GZ 压缩文件，适用于标准或受支持的应用程序。

生成的安装包以包含子文件夹和文件的文件夹形式分层级组织。除了原始分发包，安装包包含可编辑设置(包含安装程序设置和是否在安装结束时重启操作系统等处理规则)以及小的辅助模块。

单独支持的应用程序的安装设置值可以在创建安装包时在 Kaspersky Security Center Web Console 的用户界面定义。当通过 Kaspersky Security Center Linux 工具执行远程应用程序安装时，安装包被传送到设备，因此运行应用程序安装程序使得所有管理员定义的设置对该应用程序可用。当使用第三方工具安装 Kaspersky 应用程序时，您仅需要确保设备上整个安装包的可用性，即是分发包和其设置的可用性。安装包被 Kaspersky Security Center Linux 创建并存储在共享文件夹下的专用子文件夹。

不在安装包参数中显示授权账户的任何细节。

不支持使用 Microsoft Windows 的组策略进行部署。

在 Kaspersky Security Center Linux 安装之后，一些安装包被自动生成；它们可用于安装并包含网络代理和 Microsoft Windows 安全应用程序包。

尽管应用程序授权许可密钥可以在安装包属性中设置，但是建议您避免使用此授权许可分发方法，因为这样容易获取对安装包的读访问权限。您应该使用自动分发的授权许可密钥，或使用授权许可密钥安装任务。

# 下载和创建卡巴斯基应用程序的安装包

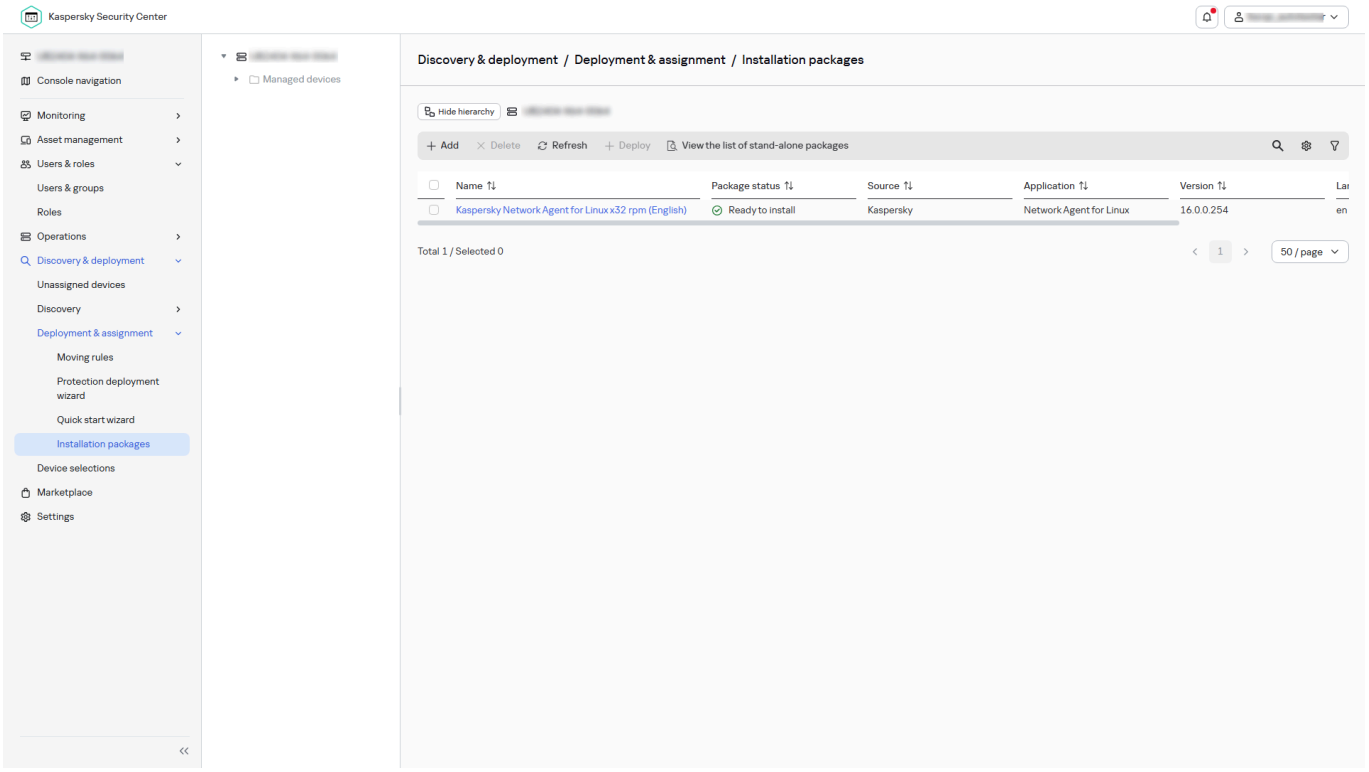
如果管理服务器可以访问 Internet，则可以从 Kaspersky Web 服务器创建卡巴斯基应用程序的安装包。

*要下载并创建卡巴斯基应用程序的安装包：*

1. 在主菜单中，转到“**软件管理**” → “**安装包**”。

   您可以在屏幕通知列表中查看关于卡巴斯基应用程序的新安装包的通知。如果有关于新安装包的通知，您可以单击通知旁边的链接并转到可用安装包列表。

此时会显示管理服务器上可用的安装包的列表。

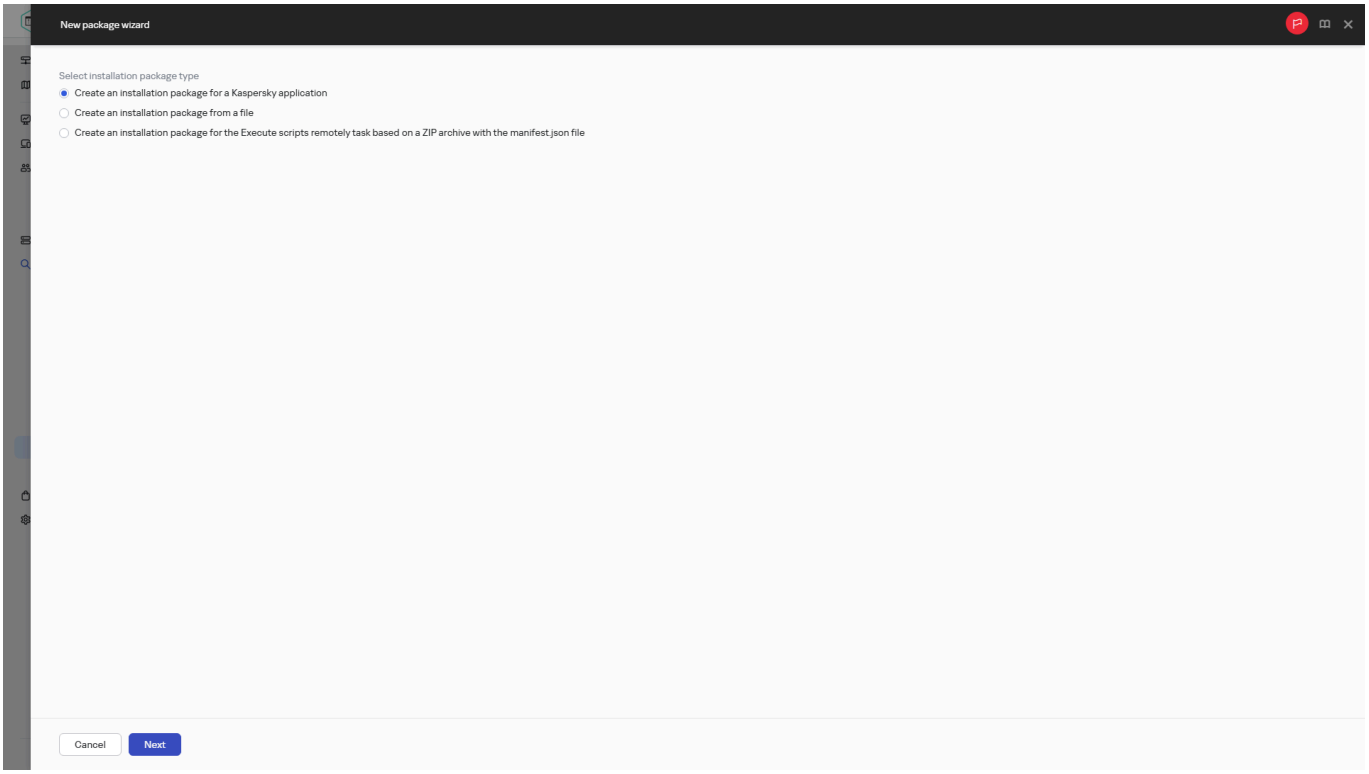



安装包列表

2. 单击**添加**。

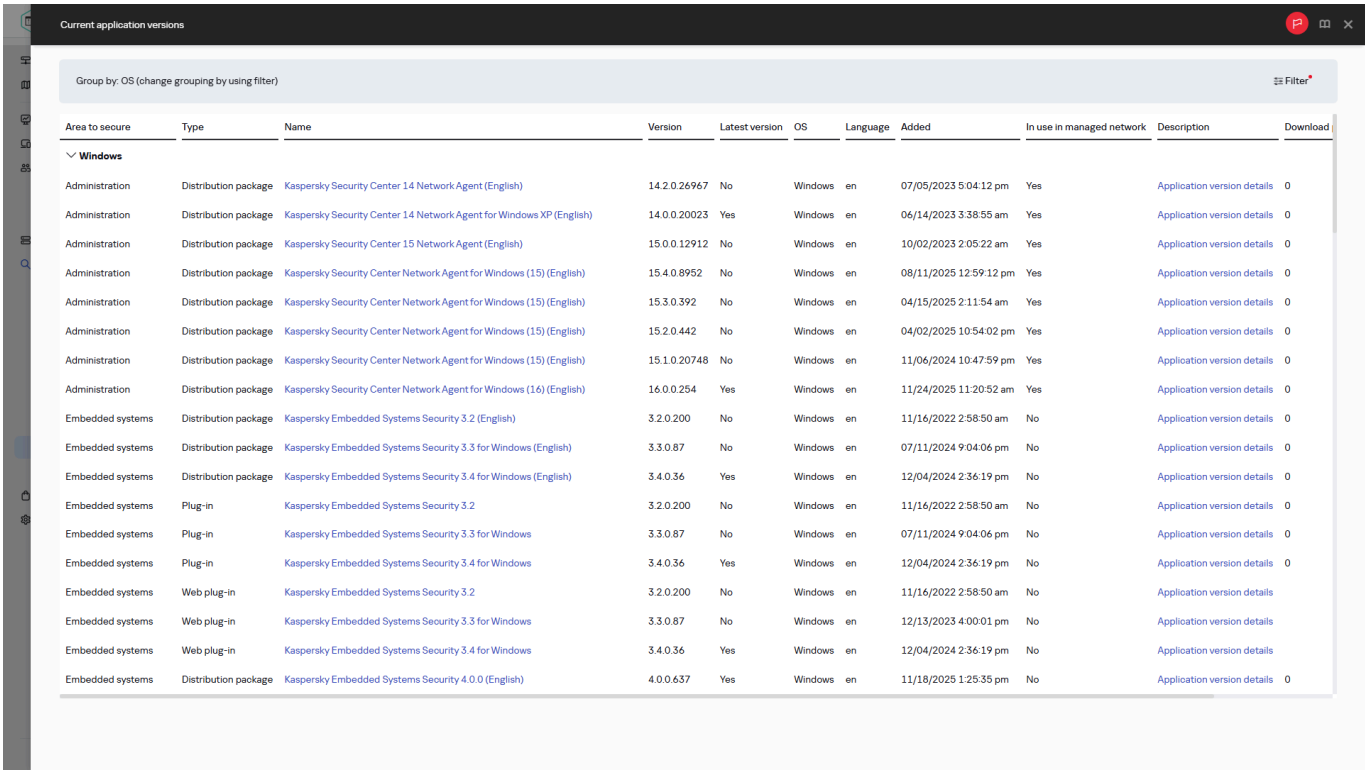
   新安装包向导启动。使用“**下一步**”按钮进行向导。

3. 选择“**为卡巴斯基应用程序创建安装包**”。




选择安装包类型

将显示 Kaspersky Web 服务器上的可用安装包列表。该列表仅包含与当前版本的 Kaspersky Security Center Linux 兼容的应用程序的安装包。默认情况下，列表显示应用程序时仅使用英语以及与界面语言匹配的语言。要显示其他语言，请单击**筛选**并配置筛选设置。



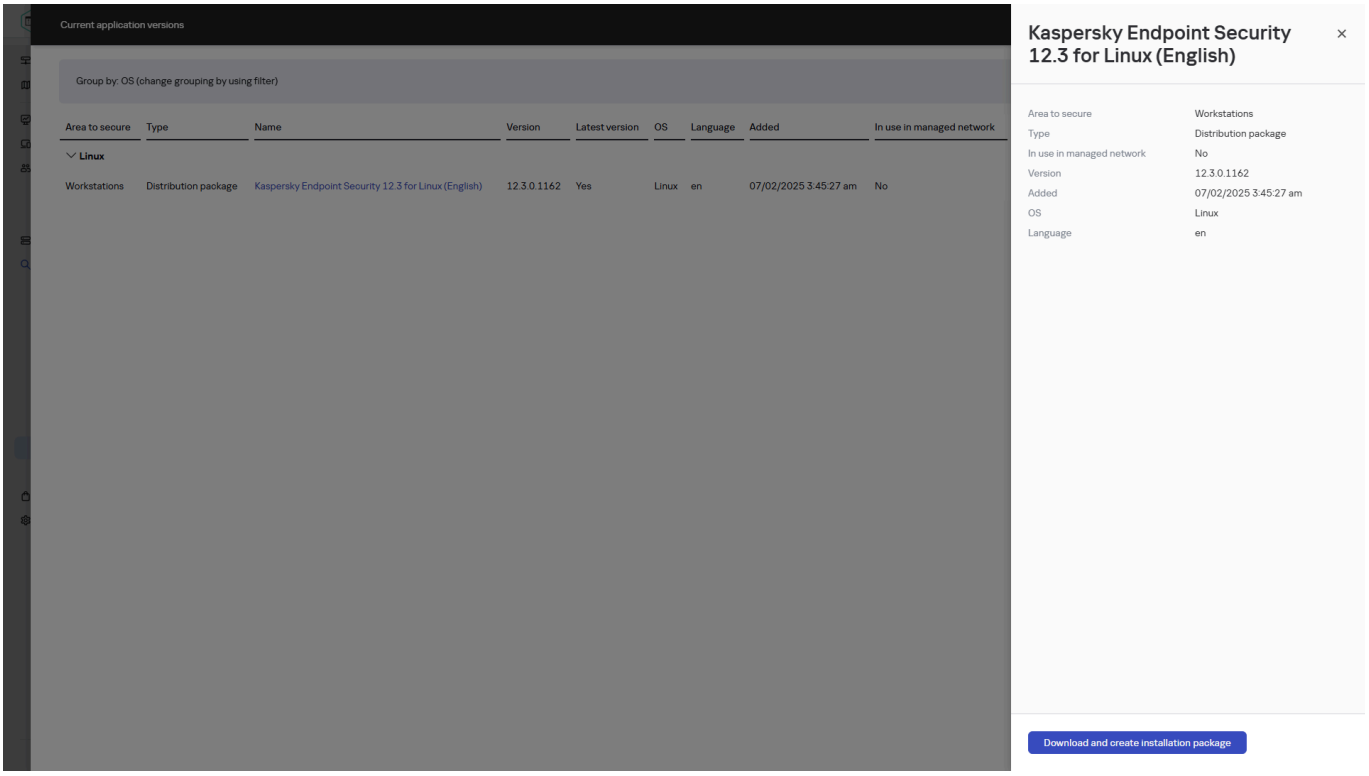

| Area to secure | Type | Name | Version | Latest version | OS | Language | Added | In use in managed network | Description | Download |
|---|---|---|---|---|---|---|---|---|---|---|
| Windows | | | | | | | | | | |
| Administration | Distribution package | Kaspersky Security Center 14 Network Agent (English) | 14.2.0.26967 | No | Windows | en | 07/05/2023 5:04:12 pm | Yes | Application version details | 0 |
| Administration | Distribution package | Kaspersky Security Center 14 Network Agent for Windows XP (English) | 14.0.0.20023 | Yes | Windows | en | 06/14/2023 3:38:55 am | Yes | Application version details | 0 |
| Administration | Distribution package | Kaspersky Security Center 15 Network Agent (English) | 15.0.0.12912 | No | Windows | en | 10/02/2023 2:05:22 am | Yes | Application version details | 0 |
| Administration | Distribution package | Kaspersky Security Center Network Agent for Windows (15) (English) | 15.4.0.8952 | No | Windows | en | 08/11/2025 12:59:12 pm | Yes | Application version details | 0 |
| Administration | Distribution package | Kaspersky Security Center Network Agent for Windows (15) (English) | 15.3.0.392 | No | Windows | en | 04/15/2025 2:11:54 am | Yes | Application version details | 0 |
| Administration | Distribution package | Kaspersky Security Center Network Agent for Windows (15) (English) | 15.2.0.442 | No | Windows | en | 04/02/2025 10:54:02 pm | Yes | Application version details | 0 |
| Administration | Distribution package | Kaspersky Security Center Network Agent for Windows (15) (English) | 15.1.0.20748 | No | Windows | en | 11/06/2024 10:47:59 pm | Yes | Application version details | 0 |
| Administration | Distribution package | Kaspersky Security Center Network Agent for Windows (16) (English) | 16.0.0.254 | Yes | Windows | en | 11/24/2025 11:20:52 am | Yes | Application version details | 0 |
| Embedded systems | Distribution package | Kaspersky Embedded Systems Security 3.2 (English) | 3.2.0.200 | No | Windows | en | 11/16/2022 2:58:50 am | No | Application version details | 0 |
| Embedded systems | Distribution package | Kaspersky Embedded Systems Security 3.3 for Windows (English) | 3.3.0.87 | No | Windows | en | 07/11/2024 9:04:06 pm | No | Application version details | 0 |
| Embedded systems | Distribution package | Kaspersky Embedded Systems Security 3.4 for Windows (English) | 3.4.0.36 | Yes | Windows | en | 12/04/2024 2:36:19 pm | No | Application version details | 0 |
| Embedded systems | Plug-in | Kaspersky Embedded Systems Security 3.2 | 3.2.0.200 | No | Windows | en | 11/16/2022 2:58:50 am | No | Application version details | 0 |
| Embedded systems | Plug-in | Kaspersky Embedded Systems Security 3.3 for Windows | 3.3.0.87 | No | Windows | en | 07/11/2024 9:04:06 pm | No | Application version details | 0 |
| Embedded systems | Plug-in | Kaspersky Embedded Systems Security 3.4 for Windows | 3.4.0.36 | Yes | Windows | en | 12/04/2024 2:36:19 pm | No | Application version details | 0 |
| Embedded systems | Web plug-in | Kaspersky Embedded Systems Security 3.2 | 3.2.0.200 | No | Windows | en | 11/16/2022 2:58:50 am | No | Application version details | |
| Embedded systems | Web plug-in | Kaspersky Embedded Systems Security 3.3 for Windows | 3.3.0.87 | No | Windows | en | 12/13/2023 4:00:01 pm | No | Application version details | |
| Embedded systems | Web plug-in | Kaspersky Embedded Systems Security 3.4 for Windows | 3.4.0.36 | Yes | Windows | en | 12/04/2024 2:36:19 pm | No | Application version details | |
| Embedded systems | Distribution package | Kaspersky Embedded Systems Security 4.0.0 (English) | 4.0.0.637 | Yes | Windows | en | 11/18/2025 1:25:35 pm | No | Application version details | 0 |

可用安装包列表

4. 单击安装包名称。例如，Kaspersky Endpoint Security for Linux。

   带有安装包信息的窗口打开。

如果符合适用的法律法规，您可以下载并使用包含实施强加密的加密工具的安装包。要下载可满足组织需求的有效 Kaspersky Endpoint Security for Windows 安装包，请参考组织的客户端设备所在国家/地区的法律。




下载安装包

5. 阅读信息，然后单击“**下载并创建安装包**”按钮。

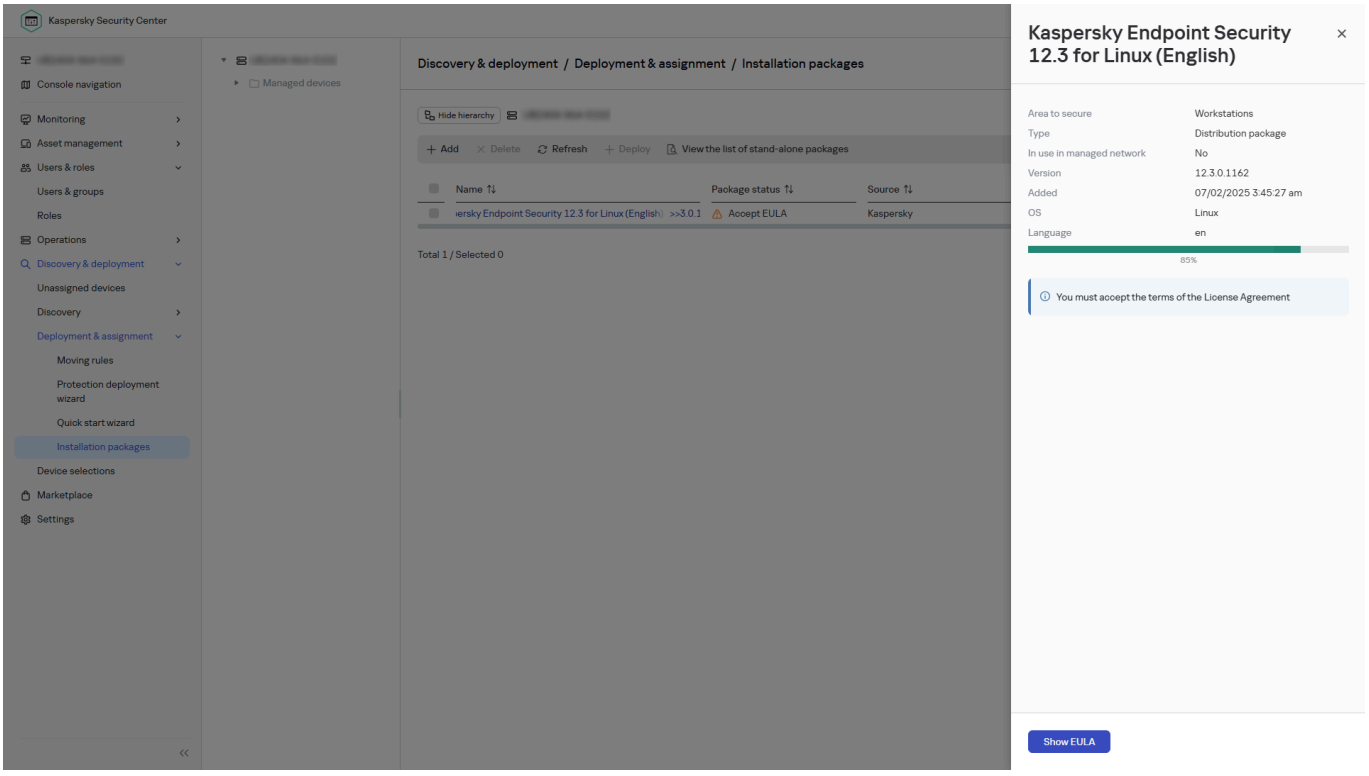
   如果分发包无法转换为安装包，将显示“**下载分发包**”按钮而不是“**下载并创建安装包**”。

对于一些卡巴斯基应用程序，下载之前或者下载过程中将显示“**显示 EULA**”按钮。如果按钮显示，执行以下操作：

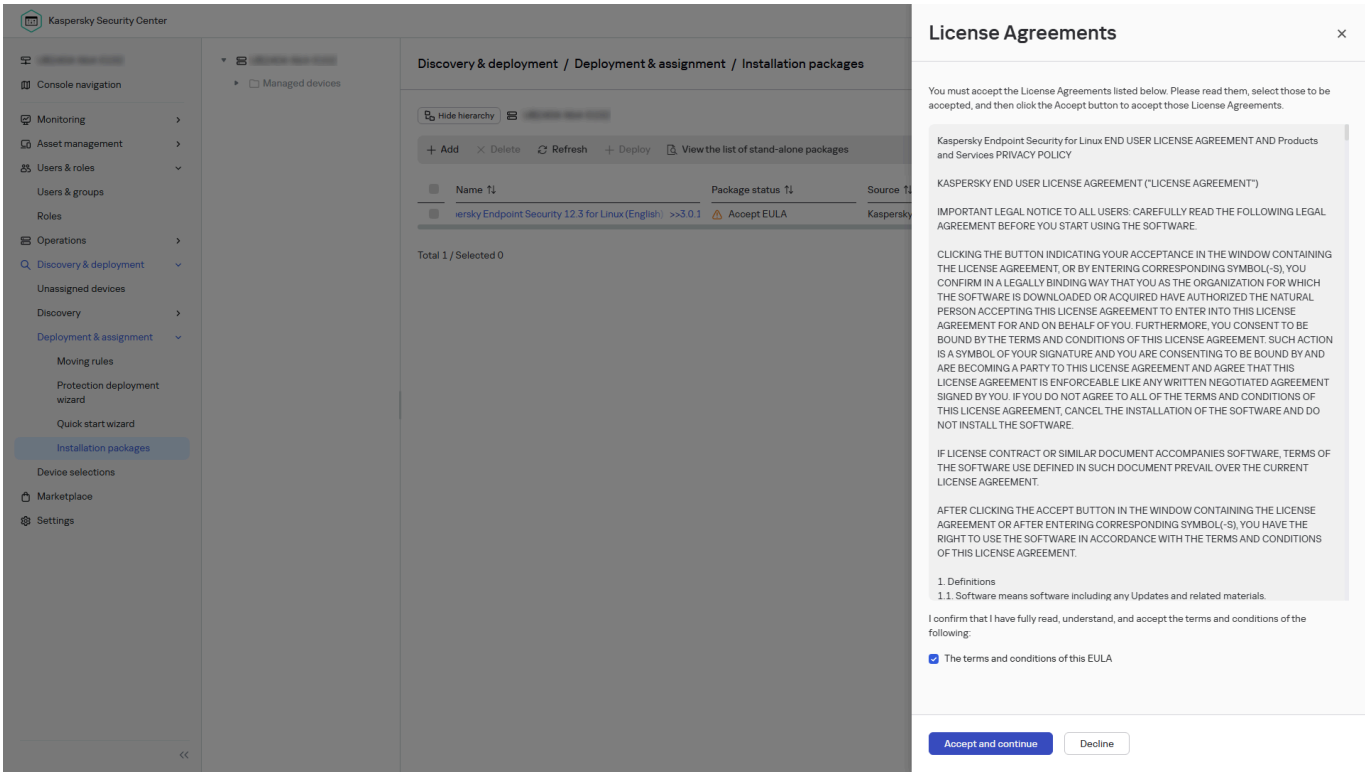
a. 点击“**显示 EULA**”以阅读最终用户授权许可协议（EULA）。

b. 阅读屏幕上显示的 EULA，然后单击“**接受**”。

在您接受 EULA 后，下载继续。如果您单击“**拒绝**”，下载将停止。




下载安装包




接受 EULA

您可以关闭向导窗口。在这种情况下，下载过程将在后台模式下继续。您可以跟踪安装包的下载状态以及在**包状态**列中过滤和排序状态。

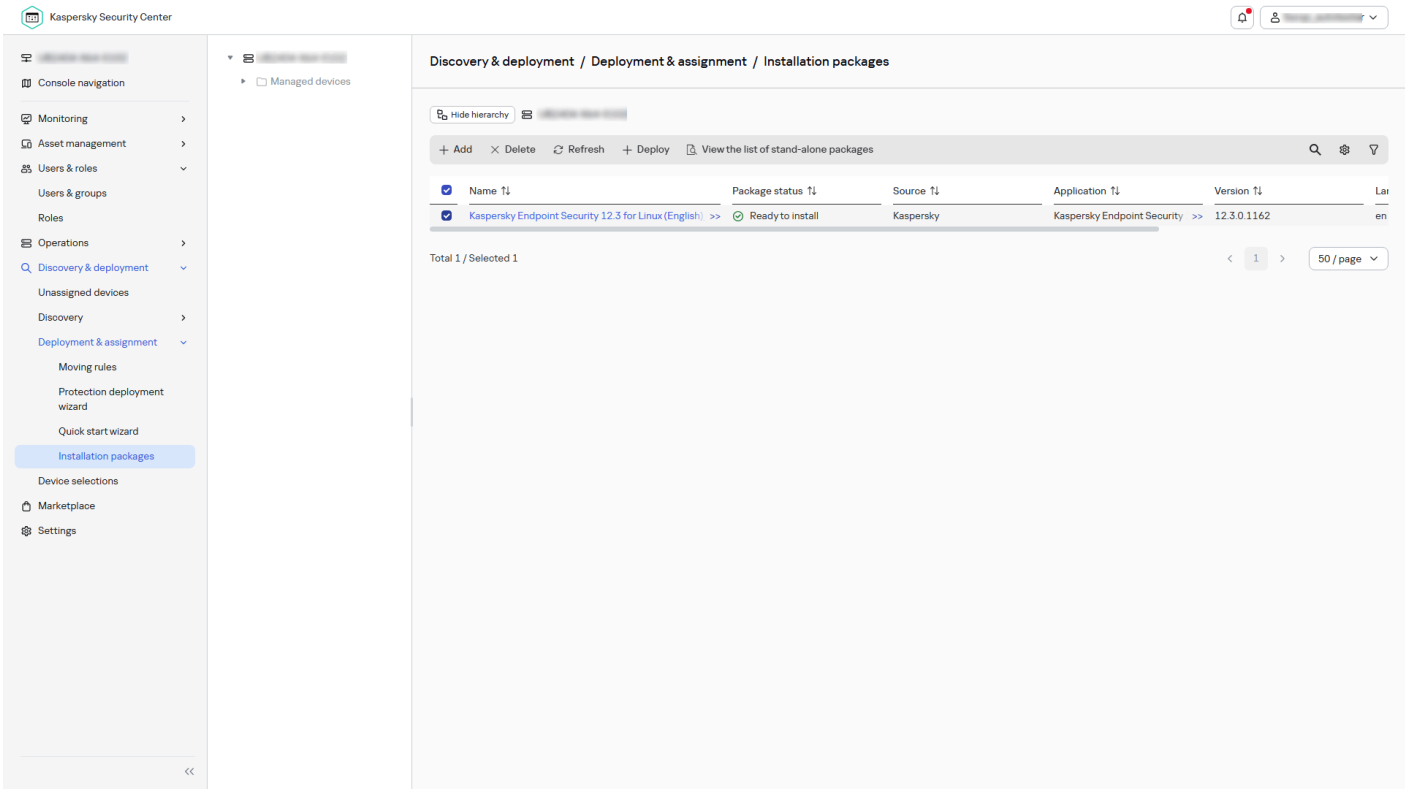
如果下载过程停止并且下载状态切换为“**接受 EULA**”，则单击安装包名称，然后执行步骤 5.a 和 5.b。

默认情况下，状态为**进行中**和**接受 EULA**的安装包会放在列表的开头。

> 如果所选分发包中包含的数据大小超过当前限制，将显示错误消息。您可以更改限制值，然后继续创建安装包。

6. 下载完成后，单击“**关闭**”按钮。

所选安装包将下载到管理服务器共享文件夹及 Packages 子文件夹。下载后，安装包出现在安装包列表。




安装包列表

# 从文件创建安装包

您可以使用自定义安装包执行以下操作：

- 在客户端设备上安装任何应用程序（例如文本编辑器），例如通过任务。
- 创建独立安装包。

自定义安装包是一个包含一组文件的文件夹。创建自定义安装包的源是*存档文件*。存档文件包含一个或多个必须包含在自定义安装包中的文件。

创建自定义安装包时，您可以指定命令行参数，例如以静默模式安装应用程序。

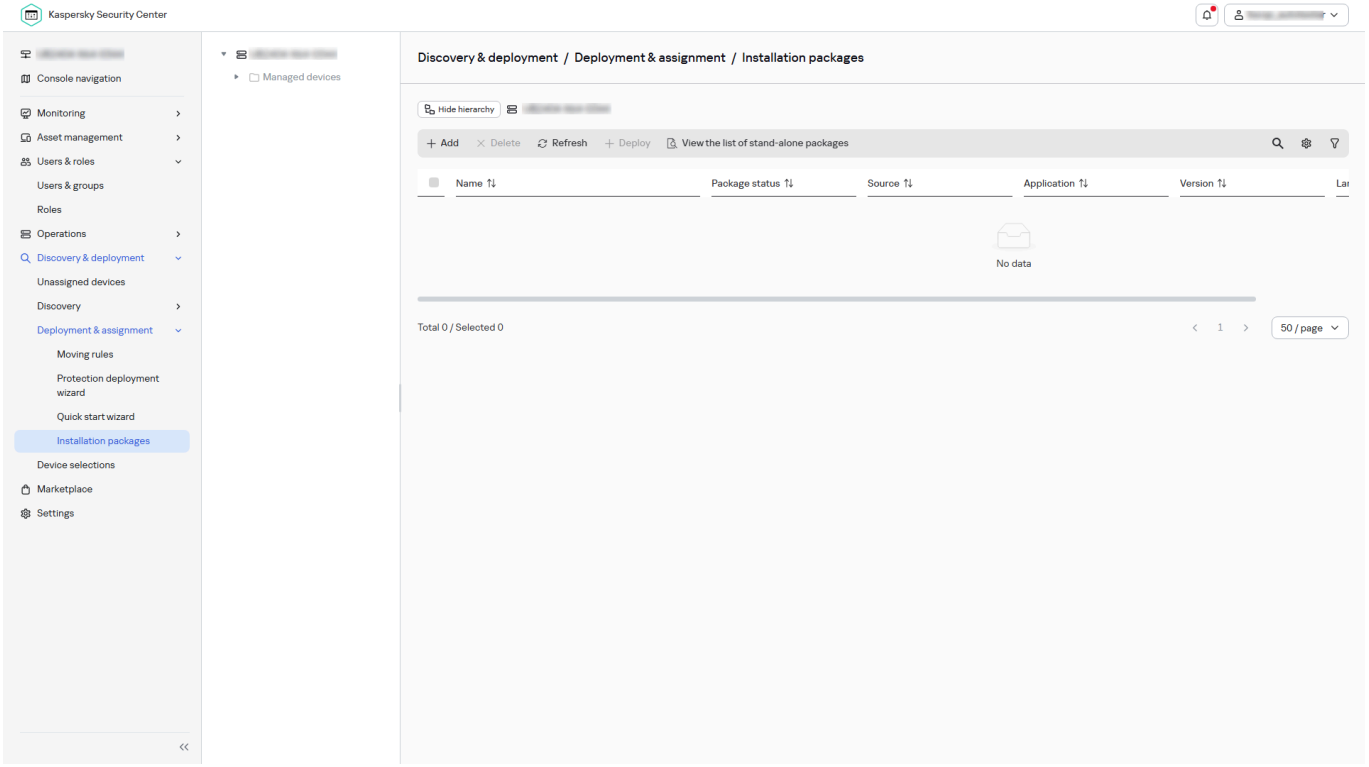
观看视频，了解如何创建和部署适用于 Windows 的自定义安装包。本教程的文字版（适用于 Windows 和 Linux 设备）如下所示。




本教程将介绍如何从文件创建和部署适用于 Windows 的自定义安装包。视频

*要创建自定义安装包：*

1. 在主菜单中，转到“**软件管理**” → “**安装包**”。
   此时会显示管理服务器上可用的安装包的列表。

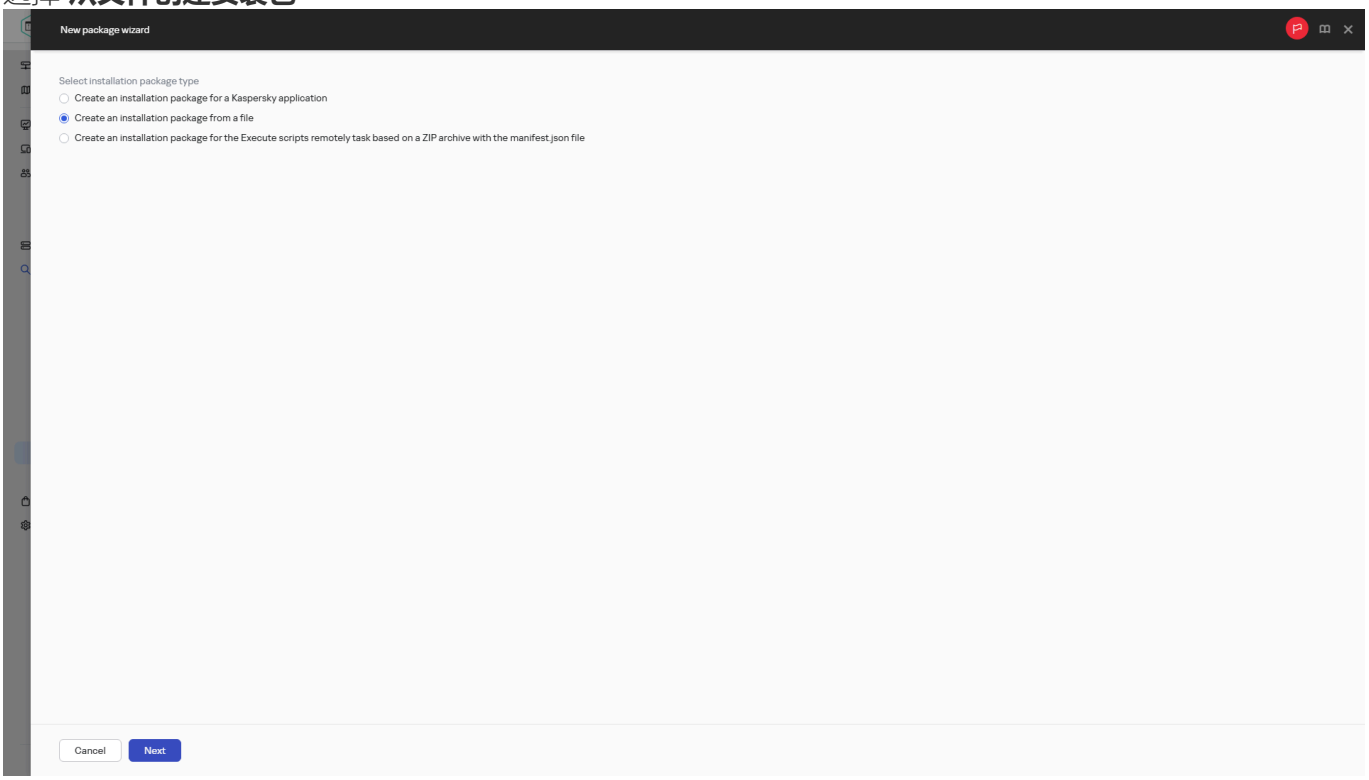



安装包列表

2. 单击**添加**。

   新安装包向导启动。使用**下一步**按钮进行向导。

3. 选择“**从文件创建安装包**”



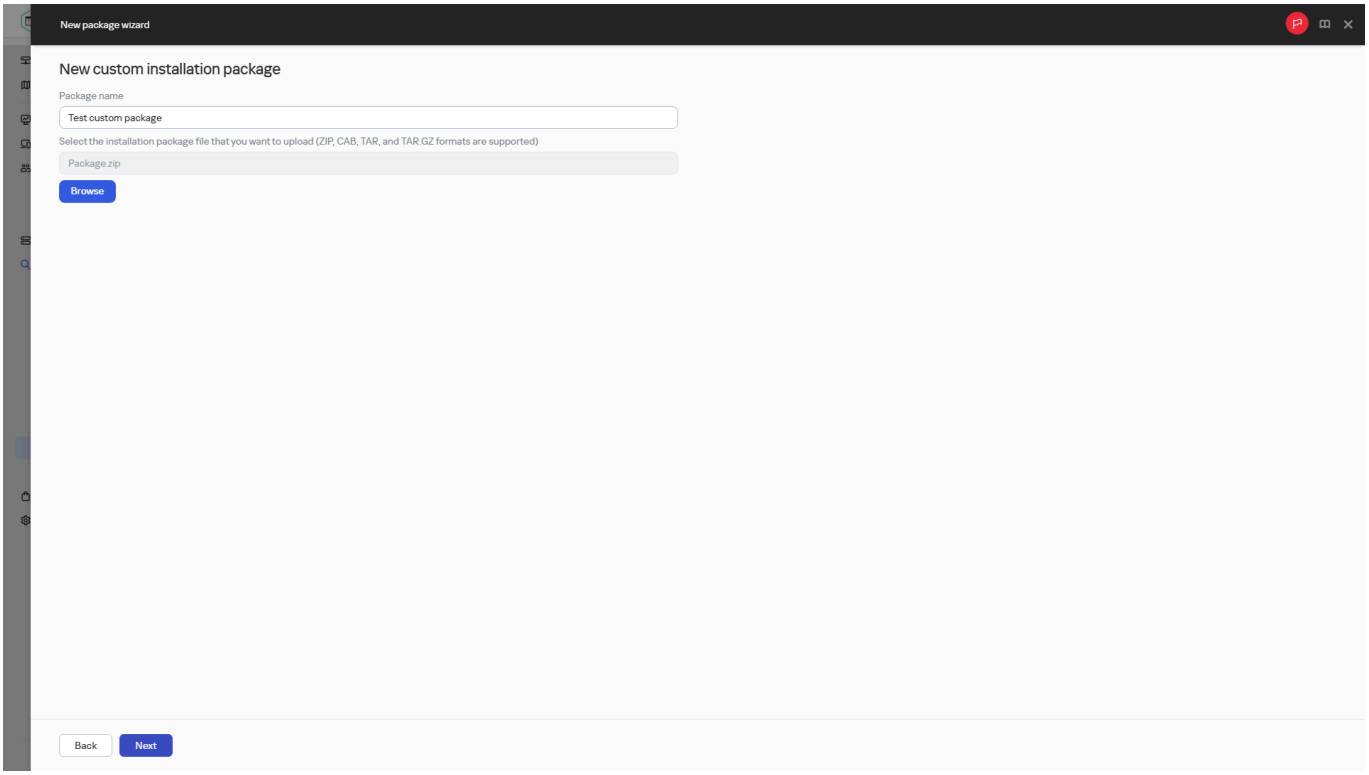

选择安装包类型

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。




指定安装包文件

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。

   **如何创建 deb 或 rpm 格式的安装包**

   1. 使用以下命令创建 `.sh` 脚本：

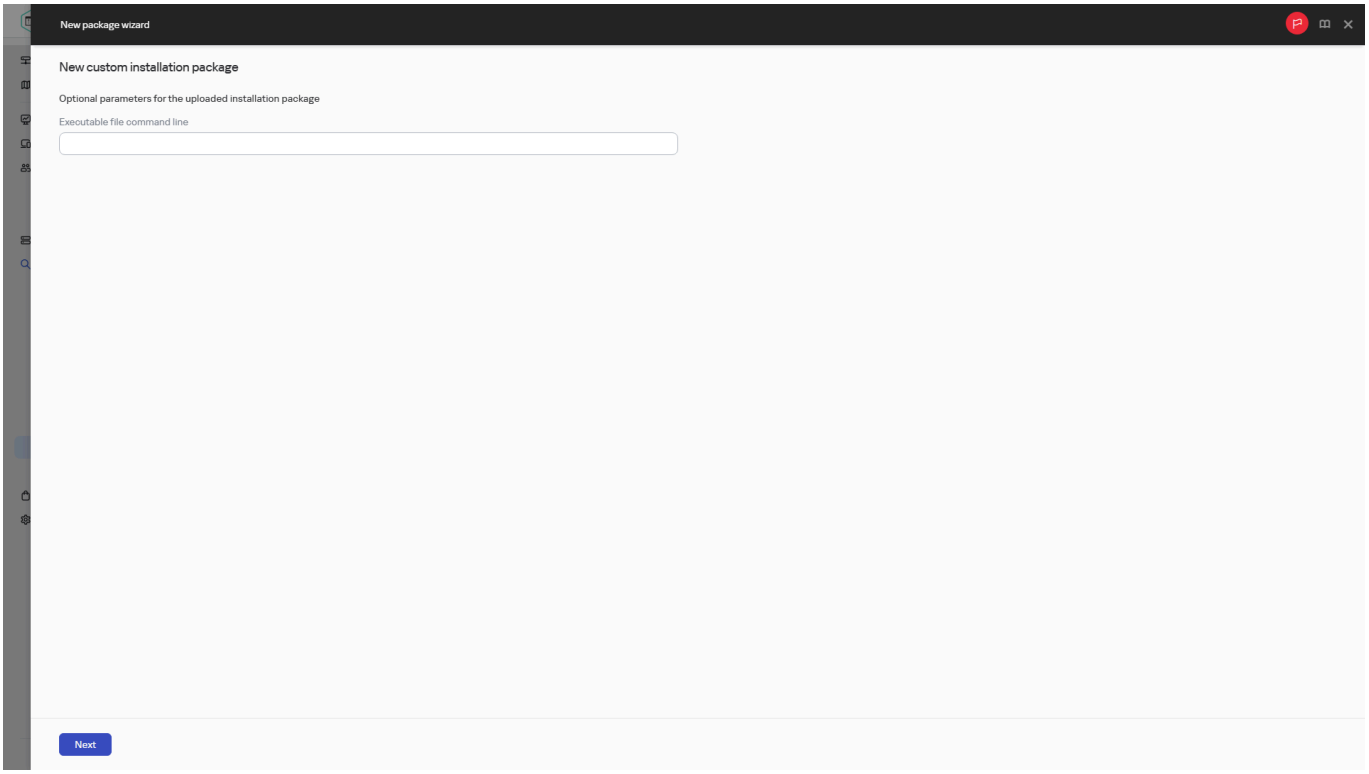
      ```
      #!/bin/sh
      script_dir="$(dirname "$0")"
      apt-get install --yes "$script_dir/<package_name>.deb" </dev/null
      ```

      脚本内容和命令可能因软件包格式和其他细节而异。您可以修改脚本以适应您的特定配置。

   2. 将创建的脚本连同以下文件一起放入压缩包中： `.deb` 或者 `.rpm`。

   3. 创建安装包时，请选择创建的脚本作为可执行文件。

   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。




指定可选的命令行参数

   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。
  - **包状态**。安装包下载状态。
  - **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。
  - **已修改**。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。

如果管理服务器可以访问互联网，则使用**将更新下载至管理服务器存储库**任务来下载创建网络代理程序独立安装包所需的依赖项。如果管理服务器无法访问互联网，请执行以下步骤：

1. 执行以下命令创建 RIUtilsArchiveDirUsed 标志：

   ```
   /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n RIUtilsArchiveDirUsed -t d -v 1
   ```

2. 运行以下命令重新启动管理服务器服务：

   ```
   systemctl restart kladminserver_srv.service
   ```

3. 从卡巴斯基网站下载以压缩文件，并将压缩文件放置在 /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives 文件夹中：
   - ri_utils_win32.zip
   - ri_utils_arm64.zip

请勿重命名存档文件。

管理服务器现在已具备所需的依赖项。

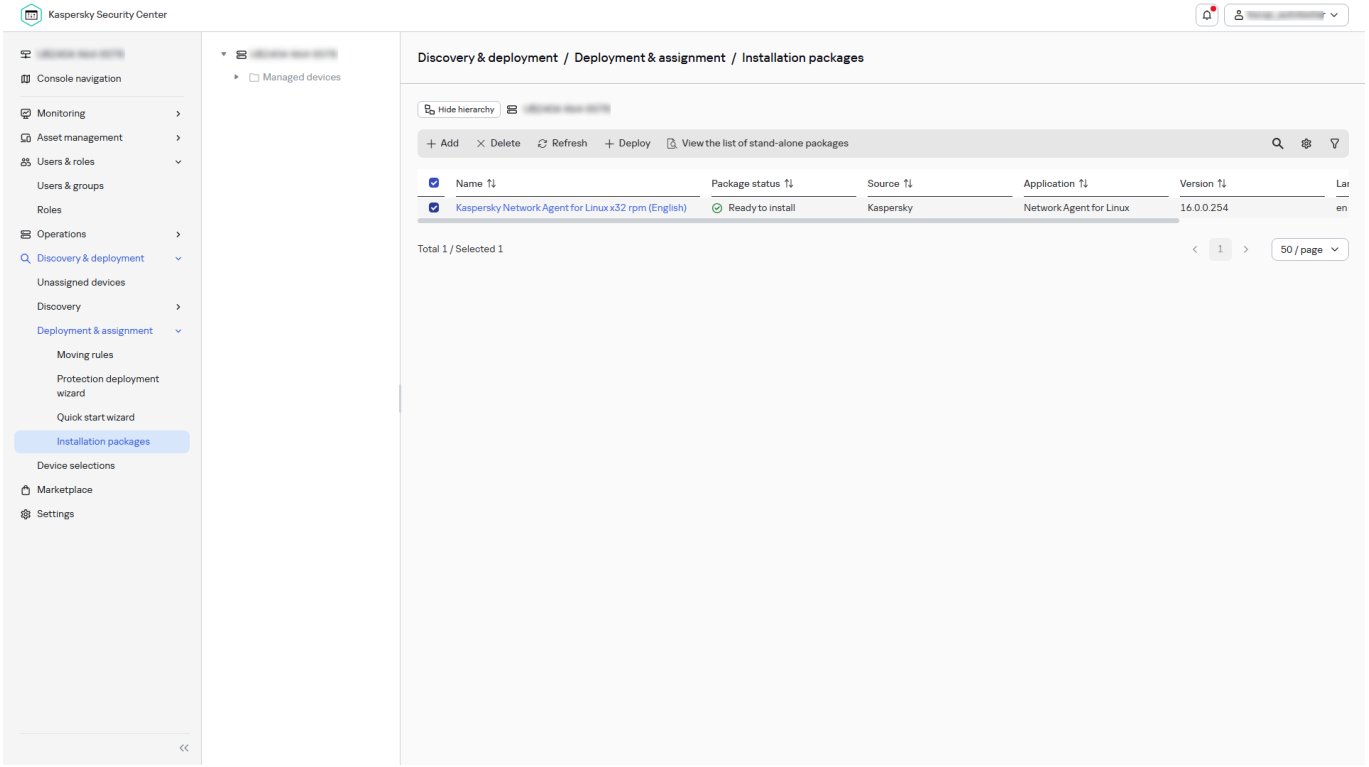
确保独立安装包不适用于第三方。

*要创建独立安装包：*

1. 在主菜单中，转到“**软件管理**” → “**安装包**”。
   此时会显示管理服务器上可用的安装包的列表。

   网络代理独立包或在虚拟管理服务器上创建的任何包的安装包列表中没有关于大小、文件哈希和路径的信息。这些独立包在下载时生成。

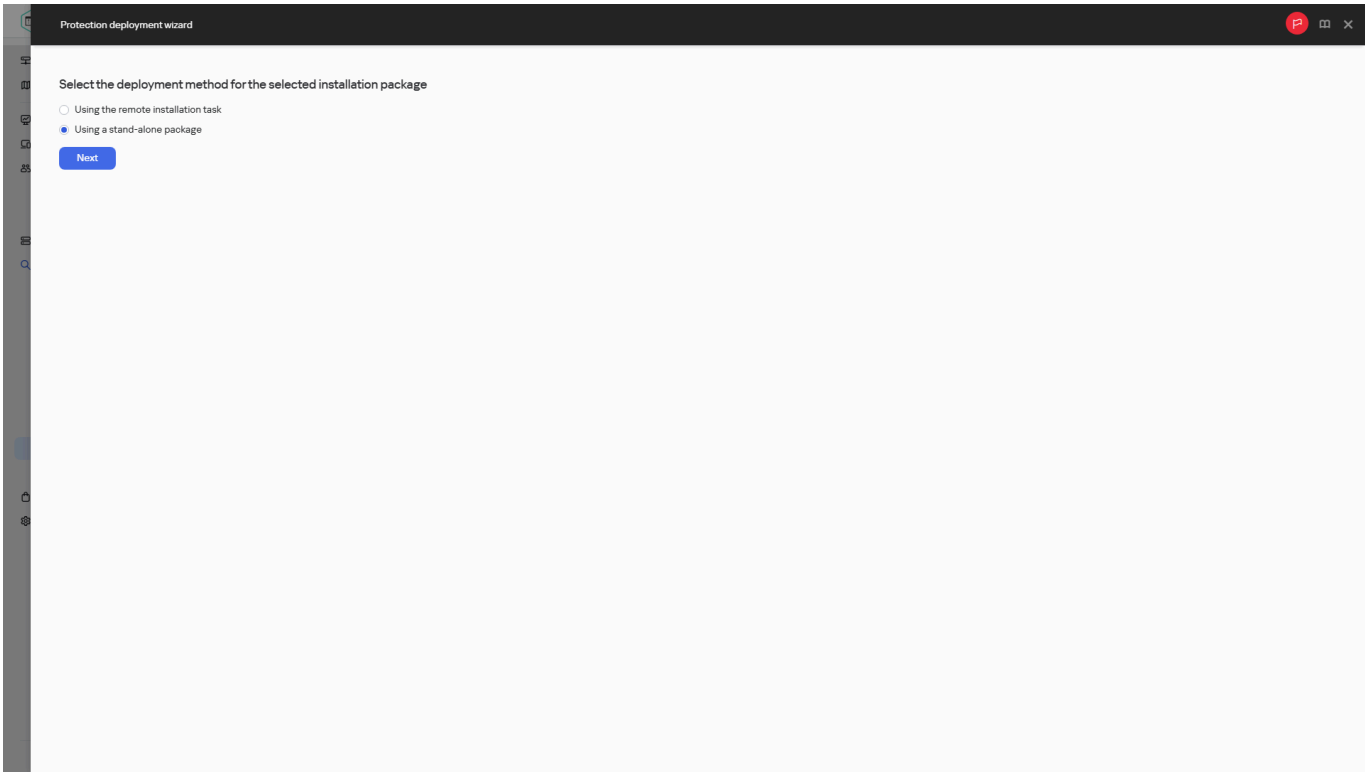
2. 在安装包列表中选择安装包，然后在列表上方单击“**部署**”按钮。




安装包列表

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。




选择安装包的部署方法

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。

> 显示的选项取决于您为其创建独立安装包的应用程序。

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，请将此选项保持选中状态。

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。




选择管理组来移动客户端设备

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。

# 网络代理安装包设置

*要配置网络代理安装包：*

1. 在主菜单中，转到“**软件管理**” → “**安装包**”。

   此时会显示管理服务器上可用的安装包的列表。

2. 单击网络代理安装包的名称。

“网络代理安装包属性”窗口将开启。

网络代理安装包的设置在以下选项卡上分组：

- “**常规**”选项卡

  此选项卡显示有关安装包的以下信息：

  - 安装包名称
  - 为其创建该安装包的应用程序的名称和版本
  - 安装包大小

- 安装包创建日期
- 安装包文件夹的路径

- **设置** 选项卡

  此选项卡显示为确保网络代理在安装后就能正确工作所需的设置。

  - **设置**区域

    - **安装到默认文件夹**

      如果选择该选项，网络代理将安装在 <驱动器>:\Program Files\Kaspersky Lab\NetworkAgent 文件夹中。如果该文件夹不存在，系统会自动创建。

      默认情况下已选定该选项。

    - **安装到指定文件夹**

      如果选择该选项，则网络代理将安装到输入字段中指定的文件夹中。

    - **使用卸载密码**

      如果启用此选项，则可以输入卸载密码（仅适用于运行 Windows 操作系统的设备上的网络代理）。

      默认情况下已禁用该选项。

    - **保护网络代理服务免遭非授权的卸载或终止，并防止设置更改**

      当启用该选项时，网络代理被安装到受管理设备之后，没有所需权限组件无法被卸载或重新配置。网络代理服务无法被停止。此选项对域控制器没有影响。

      启用此选项可保护以本地管理员权限操作的工作站上的网络代理。

      默认情况下已禁用该选项。

    - **对未定义状态的组件自动安装可应用更新和补丁**

      如果启用此选项，将自动安装为管理服务器、网络代理、Kaspersky Security Center Web Console 和 iOS MDM 服务器下载的所有更新和补丁。

      如果禁用此选项，所有已下载的更新和补丁只有在状态更改为“*已批准*”后才会更新。带有*未定义*状态的更新和补丁将不被安装。

      默认情况下已启用该选项。

  - **连接**部分

    在该区域中，您可以配置网络代理至管理服务器的连接：要建立连接，您可以使用 SSL 或 UDP 协议。要配置连接，请指定以下设置：

    - **管理服务器地址**

      安装了管理服务器的设备地址。

    - **端口号**

      用于连接的端口号。

    - **SSL 端口**

      用于通过 SSL 协议的连接的端口号。

- **使用服务器证书**

  如果启用此选项，网络代理访问管理服务器时的身份验证将使用证书文件，您可以通过单击**选择证书文件**按钮来指定该证书文件。

  如果禁用此选项，将在网络代理第一次连接到“**管理服务器地址**”字段指定的地址时从管理服务器接收证书文件。

  我们建议不禁用此选项，因为网络代理在连接到管理服务器时自动接收管理服务器证书被认为是不安全的。

  默认情况下已禁用该选项。

- **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。

  默认情况下已禁用该选项。我们建议您不要禁用此选项，以便您的连接保持安全。

- **使用 UDP 端口**

  如果启用此选项，网络代理将通过 UDP 端口连接至管理服务器。这允许管理客户端设备并接收有关它们的信息。

  UDP 端口必须在安装网络代理的受管理设备上开放。因此，我们建议您不要禁用此选项。

  默认情况下已启用该选项。

- **UDP 端口**

  在该字段中，可以指定使用 UDP 协议连接管理服务器到网络代理的端口。

  默认 UDP 端口 15000。

- **不使用代理服务器**

  如果启用此选项，则使用直接连接将设备连接到管理服务器。

- **使用代理服务器**

  如果此选项被启用，请指定代理服务器参数：

  - **代理服务器地址**
  - **代理服务器端口**

  如果您的代理服务器需要身份验证，请启用**代理服务器身份验证**选项并指定与代理服务器建立连接的账户的**用户名**和**密码**。我们建议您指定仅具有代理服务器身份验证所需的最低权限的账户的凭据。

- **在 Microsoft Windows 防火墙中打开网络代理端口**

  如果启用此选项，网络代理使用的端口将被添加到 Microsoft Windows 防火墙排除列表中。

  默认情况下已启用该选项。

  > 该选项仅适用于运行 Windows 的设备的网络代理安装包。

- **高级**部分

  在该区域中，您可以配置如何使用连接网关。

在**连接网关**设置组中，您可以配置设备和管理服务器之间的连接方法：

- **使用网络代理作为 DMZ 连接网关**

  如果启用此选项，网络代理将被作为非管制区域 (DMZ) 中的连接网关以连接到管理服务器，与之通信，以及在数据传输过程中保持网络代理上的数据安全。

- **通过使用连接网关连接到管理服务器**

  如果启用此选项，则使用连接网关连接到管理服务器以减少与管理服务器的连接数。在这种情况下，请在“**连接网关地址**”字段中输入将充当连接网关的设备的地址。

在**虚拟机**设置组中，如果您的网络包含虚拟机，则可以配置虚拟桌面基础架构 (VDI) 的连接：

- **启用 VDI 动态模式**

  如果启用此选项，将针对虚拟机上安装的网络代理启用虚拟桌面基础架构 (VDI) 的动态模式。

  默认情况下已禁用该选项。

- **优化 VM 设置**

  如果启用此选项，网络代理设置中将禁用以下功能：

  - 获取已安装软件的信息
  - 获取硬件信息
  - 获取检测到的漏洞信息
  - 获取需要更新的信息

  默认情况下已禁用该选项。

如果您想在 Linux 设备上安装网络代理后自动提示用户注册为设备所有者，请启用**允许在安装网络代理后运行用户注册实用工具**选项。

如果启用此选项，用户注册为设备所有者实用程序将在网络代理安装后运行。默认情况下已禁用该选项。

- **标签**部分

  “**标签**”区域显示网络代理安装后可以被添加到客户端设备的关键字列表。您可以在列表中添加和删除标签以及重命名它们。

  如果标签旁的复选框被选中，该标签在网络代理安装过程中被自动添加到受管理设备。

  如果标签旁的复选框被清空，该标签在网络代理安装过程中不被自动添加到受管理设备。您可以手动添加该标签到设备。

  当从列表中删除标签时，它被自动从所有添加了该标签的设备上删除。

  > 自动标记规则不适用于运行 Linux 和 macOS 的设备的网络代理安装包。

- **独立包**选项卡

  在此选项卡上，您可以执行以下操作：

  - 查看可用的独立安装包列表。
  - 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。

- **修订历史**选项卡

  在此选项卡上，您可以查看安装包修订历史。您可以比较修订、查看修订、保存修订到文件和添加/编辑修订描述。

# 运行 Kaspersky Security Center Linux 创建的独立包

以上描述的网络代理和其他应用程序的初始化部署方法无法总被实现，因为不可能满足所有可应用条件。此种情况下，您可以通过 Kaspersky Security Center Linux 创建通用可执行文件，叫做*独立安装包*，使用管理员准备的带有相关安装设置的安装包。独立安装包可以发布在包含在 Kaspersky Security Center Linux 中的内部 Web 服务器（如果这是合理的，到该 Web 服务器的外部访问已为目标设备用户配置），或发布在包含在 Kaspersky Security Center Web Console 中的单独部署 Web 服务器。您也可以复制独立包到其他 Web 服务器。

您可以使用 Kaspersky Security Center Linux 来给所选用户发送电子邮件，其中包含当前使用的 Web 服务器中的独立包文件链接，提示他们运行该文件（在交互模式或带有“-s”参数的静默模式）。您可以附加独立安装包到电子邮件，然后发送它到对 Web 服务器没有访问权限的设备用户。管理员也可以复制独立包到可移动驱动器，将其传送到相关设备然后稍后运行。

您可以从网络代理包或其他应用程序包创建独立包(例如，安全应用程序)。如果独立包从网络代理和其他应用程序创建，安装和网络代理一起启动。

当创建带有网络代理的独立包时，您可以指定当网络代理安装完成时，新设备(未分配到任何管理组的设备)将被自动移动到的管理组。

独立包可以在交互模式下运行(默认)，显示应用程序安装结果，或者可以运行在静默模式(以参数 "-s" 运行)。静默模式可以用在从脚本安装，例如操作系统镜像部署后要运行的脚本。静默模式安装的结果决定与进程返回代码。

# 使用独立包安装应用程序

Kaspersky Security Center 允许您为应用程序创建独立安装包。独立安装包是一个位于 Web 服务器上的可执行文件。它可由电子邮件发送，也可以其他方式传送到客户端设备。收到的文件可以在本地客户端设备上运行，并且安装程序不涉及 Kaspersky Security Center。

*要使用独立安装包安装应用程序：*

1. 在主菜单中，转到“**软件管理**” → “**安装包**”。
2. 选中所需应用程序的安装包旁边的复选框，然后单击**部署**按钮。
3. 在打开的窗口中，选择**使用独立包**，然后单击**下一步**按钮。

   独立安装包创建向导启动。使用“**下一步**”按钮继续向导操作。

4. 选择**创建独立安装包**选项。

5. 指定设备是否在安装网络代理后必须被移动到管理组。

6. 在向导的最后一步，选择将独立安装包传输到客户端设备的方法，然后单击**完成** 按钮结束向导。

7. 将独立安装包传输至客户端设备。

8. 在客户端设备上运行独立安装包。

这样，应用程序将以独立包所指定的设置，安装在客户端设备上。

当您创建独立安装包时，它会自动发布在 Web 服务器上。已创建的独立安装包列表中会显示用于下载独立包的链接。您可以取消发布选中的独立包，也可以重新在 Web 服务器上发布。默认情况下，使用端口 8060 下载独立安装包。

# 安全应用程序安装包上的数据库更新

开始保护部署之前，您必须注意要随安全应用程序的分发包一起更新反病毒数据库(包块模块和自动补丁)。最好在开始部署之前更新应用程序安装包中的数据库(例如， 通过使用所选安装包上下文菜单中的相关命令)。这将减少目标设备在完成保护部署后所需的重启次数。

# 更改自定义安装包数据大小的限制

创建自定义安装包期间解压缩的数据总大小受到限制。默认限制为 1 GB。

如果尝试上传的压缩文件所包含的数据超出当前限制，将显示一条错误消息。从大型分发包创建安装包时，可能必须增加此限制值。

*要更改自定义安装包大小的限制值：*

1. 在管理服务器设备上，在用于安装管理服务器的账户下运行命令提示符。

2. 将当前目录更改为 Kaspersky Security Center Linux 安装文件夹（通常为 /opt/kaspersky/ksc64/sbin）。

3. 根据管理服务器安装的类型，在根账户下输入以下命令之一：

   - 普通本地安装：

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <字节数>
     ```

   - 在 Kaspersky Security Center Linux 故障转移集群上安装：

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <number of bytes> --stp klfoc
     ```

   其中 <number of bytes> 是十六进制或十进制格式的字节数。

   例如，如果要求的限制为 2 GB，您可以指定十进制值 2147483648 或十六进制值 0x80000000。在这种情况下，对于管理服务器的本地安装，您可以使用以下命令：

   ```
   klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v 2147483648
   ```

自定义安装包数据大小的限制即被更改。

# 将安装包分发至从属管理服务器

Kaspersky Security Center Linux 允许您创建安装包用于卡巴斯基应用程序和第三方应用程序，以及将安装包分发至客户端设备并从包中安装应用程序。要优化主管理服务器上的负载，您可以将安装包分发至从属管理服务器。之后，从属服务器将安装包传输到客户端设备，然后您可以在客户端设备上远程安装应用程序。

*要将安装包分发至从属管理服务器：*

1. 请确保从属管理服务器连接至主管理服务器。
2. 在主菜单中，转到“**任务**”。

   将显示任务列表。
3. 单击“**添加**”按钮。

   “新任务向导”启动。遵照向导的说明。
4. 在**新任务设置**页面的 **应用程序**下拉列表中，选择 **Kaspersky Security Center**。然后，从**任务类型**下拉列表中选择**分发安装包**，然后指定任务名称。
5. 在“**任务范围**”页面，通过以下方式之一选择任务分配到的设备：
   - 如果要为特定管理组中的所有从属管理服务器创建任务，选择该组，然后为它创建组任务。
   - 如果要为特定的从属管理服务器创建任务，选择这些服务器，然后为它们创建任务。
6. 在“**分发的安装包**”页面，选择要复制到从属管理服务器的安装包。
7. 指定一个账户，以该账户来运行“*分发安装包*”任务。您可以使用您的账户并保持“**默认账户**”选项为启用状态。或者，您可以指定另一个用于运行该任务并具有必要访问权限的账户。为此，请选择“**指定账户**”选项，然后输入该账户的凭据。
8. 在**完成任务创建**页面上，您可以启用**创建完成时打开任务详情**选项以打开任务属性窗口，然后修改默认任务设置。或者，您可以稍后随时配置任务设置。
9. 单击“**完成**”按钮。

   为了将安装包分发至从属管理服务器而创建的任务显示在任务列表中。
10. 您可以手动运行该任务，或者等待任务按照您在任务设置中指定的时间表启动。

任务完成后，所选的安装包将复制到指定的从属管理服务器。

# 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。
- **已修改**。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。

网络代理独立包或在虚拟管理服务器上创建的任何包的安装包列表中没有关于大小、文件哈希和路径的信息。这些独立包在下载时生成。

*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。

# 安装 Network Agent for Linux

要管理组织设备，您必须在其上安装网络代理。部署分发的 Kaspersky Security Center Linux 到组织设备通常开始于在其上安装网络代理。

在 Linux 受管理设备上初始安装网络代理的方法如下：

- 通过 SSH 连接到受管理设备并运行远程安装任务。
- 通过在受管理设备上运行包安装。

在设备上安装网络代理后，您可以通过该网络代理在该设备上执行卡巴斯基应用程序的远程安装。要安装的应用程序分发包通过网络代理和管理服务器之间的通信渠道，与管理员定义的安装设置一并传输。为了传递分发包，您可以使用中继分发节点，即分发点、组播传递等。

当选择部署应用程序到受管理网络的方法和策略时，您必须考虑很多因素（部分列表）：

- 组织网络的配置。
- 设备总数。
- 在组织网络的设备出席、不是任何域成员、在设备上具有管理员权限的统一账户的出席。
- 管理服务器和设备通道的容量。
- 管理服务器和远程子网之间的通信类型以及那些子网中的网络通道容量。
- 部署开始时在远程设备上应用的安全设置。这些参数允许建立与受管理设备的远程连接并开始安装。

# 准备 Linux 设备以安装网络代理

在 Linux 设备上安装网络代理之前，您必须执行 Linux 设备所需的准备步骤。

*要准备运行 Linux 的设备以远程安装网络代理：*

1. 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。
2. 如果要在 AltOS 上以封闭软件环境模式安装网络代理，请在安装完成前禁用封闭软件环境模式。
3. 使用云控制台界面或从卡巴斯基网站下载网络代理程序安装包。
   如果您需要在运行含glibc 2.5的 Linux操作系统的设备上安装网络代理，则必须使用云控制台界面或从卡巴斯基网站下载 *Kaspersky Network Agent for Linux Legacy*安装包。
4. 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
   - ps实用程序

5. 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. 确保在Linux的未分配设备上，TCP端口22已打开且可访问。

   要成功安装Linux的网络代理程序，必须启用TCP端口22。

   c. 禁用要连接设备的用户账户的 sudo 密码。

   d. 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`

   e. 保存并关闭 sudoers 文件。

   f. 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。

6. 如果要在运行具有 systemd 初始化系统的操作系统的设备上远程安装网络代理，请打开`/etc/systemd/logind.conf`文件，然后执行以下操作之一：

   - 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`。

   **Astra Linux 目标设备**

   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。

   **OSnova 目标设备**

   如果目标设备正在运行 OSnova，请执行以下操作：

   a. 打开 `/usr/lib/systemd/logind.conf/10-enable-kill-user-processes.conf` 文件，然后注释出 `#KillUserProcess=yes` 行。

   b. 打开 `/usr/lib/NESS/pam-user-session` 文件，然后注释出 `#loginctl terminate-session "$XDG_SESSION_ID"` 行。

   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
   ```

7. 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。

8. 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。

9. 如果您想在运行 Ubuntu Server 或 Ubuntu 桌面版本 10.04 的设备上安装网络代理，请执行其他步骤来准备这些设备。

10. 如果要在运行Linux操作系统且安装了glibc 2.5的设备上安装网络代理程序，请执行额外步骤来准备目标设备。

11. 如果您在 AltOS 上以封闭软件环境模式安装网络代理，请重新启用封闭软件环境模式。

12. 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 设备已准备好安装网络代理。您可以远程、在交互模式下或在静默模式下安装网络代理。

# 准备运行 SUSE Linux Enterprise Server 15 的设备以安装网络代理

在运行 SUSE Linux Enterprise Server 15 的设备上安装网络代理之前，您必须执行两个准备过程：下面说明中的一个步骤和适用于任何 Linux 设备的常规准备步骤。

*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，检查该软件包是否已安装。

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` 选项以忽略该警告。

准备好 Linux 设备后，您可以远程、以交互模式或静默模式安装网络代理。

# 准备在封闭软件环境模式下运行 Astra Linux 的设备以安装网络代理

在封闭软件环境模式下运行 Astra Linux 的设备上安装网络代理之前，您必须执行两个准备过程：下面说明中的一个和适用于任何 Linux 设备的常规准备步骤。

以拥有 root 权限的账户运行本说明中提供的命令。

*要准备在封闭软件环境模式下运行 Astra Linux 的设备来安装网络代理：*

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

   ```
   DIGSIG_ELF_MODE=1
   ```

2. 在命令行中，运行以下命令来安装兼容包：

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

3. 为应用程序密钥创建一个目录：

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

4. 将应用程序密钥/opt/kaspersky/klnagent64/share/kaspersky_astra_pub_key.gpg放在上一步创建的目录中：

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

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

5. 更新 RAM 磁盘：

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

   重新启动系统。

Linux 设备已准备好安装网络代理。您可以远程、在交互模式下或在静默模式下安装网络代理。

# 准备在安装了 glibc 2.5（旧版操作系统）的 Linux 操作系统上安装网络代理。

在为运行安装了glibc 2.5（旧版操作系统）的Linux操作系统的设备安装网络代理程序之前，必须执行两个准备步骤：适用于任何Linux设备的通用准备步骤和本文中描述的步骤。

我们建议您使用本地安装方式在安装了 glibc 2.5（旧版操作系统）的 Linux 操作系统上安装网络代理。如果此方案需要使用远程安装任务，则必须执行以下说明中描述的其他步骤。

以拥有 root 权限的账户运行本过程中提供的命令。

我们建议您使用本地安装方式在安装了 glibc 2.5（旧版操作系统）的 Linux 操作系统上安装网络代理。如果此方案需要使用远程安装任务，则必须执行以下说明中描述的其他步骤。

1. 在运行Linux操作系统且安装了glibc 2.5的设备上，执行适用于任何Linux设备的通用准备步骤。
2. 在`/etc/sudoers`文件中，删除`Defaults requiretty`行。
3. 禁用SSH连接的有效加密算法的允许列表，以便能够在运行带有glibc 2.5的Linux操作系统的设备上安装网络代理。

   为此，请在安装了管理服务器的设备上，或在作为分发点且其作用范围包含目标设备的设备上，在命令行中运行以下命令：

   ```
   klscflag -fset -pv ".core/.independent" -s "Transport" -n
   SSH_CLIENT_DISABLE_ALGS_PROTECT -t d -v 1
   ```

Linux 设备已准备好远程安装网络代理。

禁用有效加密算法允许列表可能会影响 SSH 连接的安全性。我们强烈建议您在安装网络代理后立即重新启用有效加密算法的允许列表。要重新启用有效加密算法的允许列表，请运行以下命令：

```
klscflag -fset -pv ".core/.independent" -s "Transport" -n SSH_CLIENT_DISABLE_ALGS_PROTECT
-t d -v 0
```

安装网络代理并重新启用有效加密算法允许列表后，运行带有 glibc 2.5（旧版操作系统）的 Linux 操作系统的设备现在由管理服务器管理。

# 准备在安装了 OpenSSH 6.4（旧版操作系统）的 Linux 操作系统上安装网络代理。

在为使用 OpenSSH 版本 6.4 或更早（旧版操作系统）的设备安装网络代理之前，必须执行两个准备步骤：适用于任何 Linux 设备的一般准备步骤和本文中描述的步骤。

我们建议您使用本地安装方式在安装了 glibc 2.5（旧版操作系统）的 Linux 操作系统上安装网络代理。如果此方案需要使用远程安装任务，则必须执行以下说明中描述的其他步骤。

> 以拥有 root 权限的账户运行本说明中提供的命令。

*要准备使用 OpenSSH 6.4 或更早版本的设备来安装网络代理：*

1. 在使用 OpenSSH 6.4 或更早版本的设备上，执行任何 Linux 设备通用的准备步骤。
2. 禁用SSH连接的有效加密算法的允许列表，以便能够在使用OpenSSH版本6.4或更早版本的设备上安装网络代理。

   为此，请在安装了管理服务器的设备上，或在作为分发点且其作用范围包含目标设备的设备上，在命令行中运行以下命令：

   ```
   klscflag -fset -pv ".core/.independent" -s "Transport" -n
   SSH_CLIENT_DISABLE_ALGS_PROTECT -t d -v 1
   ```

Linux 设备已准备好远程安装网络代理。

禁用有效加密算法允许列表可能会影响 SSH 连接的安全性。我们强烈建议您在安装网络代理后立即重新启用有效加密算法的允许列表。要重新启用有效加密算法的允许列表，请运行以下命令：

```
klscflag -fset -pv ".core/.independent" -s "Transport" -n SSH_CLIENT_DISABLE_ALGS_PROTECT
-t d -v 0
```

安装网络代理并重新启用有效加密算法允许列表后，运行带有 glibc 2.5（旧版操作系统）的 Linux 操作系统的设备现在由管理服务器管理。

# 在 Linux 设备上远程安装网络代理

在基于 Linux 的设备上安装网络代理之前，您必须完成所有基于 Linux 的设备所需的常规准备步骤。

完成常规步骤后，您可以按照您的操作系统特定的附加说明进行操作：

- 准备运行 SUSE Linux Enterprise Server 15 的设备
- 准备在封闭软件环境模式下运行 Astra Linux 的设备
- 准备运行 Ubuntu Server/Desktop 版本 10.04 和 16.04 的设备
- 准备一台运行 Linux 操作系统且安装了 glibc 2.5 的设备

*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. 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`。

# 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。

在基于 Linux 的设备上安装网络代理之前，您必须完成所有基于 Linux 的设备所需的常规准备步骤。

完成常规步骤后，您可以按照您的操作系统特定的附加说明进行操作：

- 准备运行 SUSE Linux Enterprise Server 15 的设备
- 准备在封闭软件环境模式下运行 Astra Linux 的设备
- 准备运行 Ubuntu Server/Desktop 版本 10.04 和 16.04 的设备
- 准备一台运行 Linux 操作系统且安装了 glibc 2.5 的设备

*要以静默模式安装 Linux 网络代理：*

1. 阅读最终用户授权许可协议。只有在您理解并接受最终用户授权许可协议的条款后，才执行下面的步骤。
2. 创建应答文件（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。需要 KLNAGENT_GW_ADDRESS。<br><br>4—网络代理实例用作非管制区域 (DMZ) 中的连接网关。需要服务器证书。 |
| 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。 |
| KLNAGENT_DEVICEOWNER_REGISTRATION_START | 否 | 允许在网络代理安装后作为设备所有者实用程序运行用户注册。如果关闭，则用户无法注册为设备所有者。 | 1— 用户注册为设备所有者实用程序将在网络代理安装后运行。<br><br>其他—已关闭。 |
| PTCH_ALLOW_APPLY_NONAPROVED_PATCHES | 否 | 定义是否为"*未定义*"状态的网络代理自动安装下载的更新。 | true（默认）—自动安装这些更新。<br><br>false—不会自动安装这些更新。 |

3. 运行网络代理安装程序。环境变量 KLAUTOANSWERS 指定应答文件的路径，该变量会被传递给安装命令。运行以下命令之一：

   - 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：
     `sudo KLAUTOANSWERS=<应答文件路径> yum install ./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：
     `sudo KLAUTOANSWERS=<应答文件路径> yum install ./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：
     `sudo KLAUTOANSWERS=<应答文件路径> yum install ./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：
  `sudo KLAUTOANSWERS=<应答文件路径> apt 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：
  `sudo KLAUTOANSWERS=<应答文件路径> apt 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：
  `sudo KLAUTOANSWERS=<应答文件路径> apt install ./klnagent64_<内部版本号>_arm64.deb`

根据操作系统配置，您还可以使用 rpm、dpkg 或 dnf 包管理器来安装网络代理。

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。

# 以交互模式安装 Linux 网络代理

本文介绍了如何通过逐步指定安装参数，以交互模式在 Linux 设备上安装网络代理。或者，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）。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。

在基于 Linux 的设备上安装网络代理之前，您必须完成所有基于 Linux 的设备所需的常规准备步骤。

完成常规步骤后，您可以按照您的操作系统特定的附加说明进行操作：

- 准备运行 SUSE Linux Enterprise Server 15 的设备
- 准备在封闭软件环境模式下运行 Astra Linux 的设备
- 准备运行 Ubuntu Server/Desktop 版本 10.04 和 16.04 的设备
- 准备一台运行 Linux 操作系统且安装了 glibc 2.5 的设备

*在交互模式下安装网络代理：*

1. 运行网络代理安装程序。根据您的 Linux 发行版，运行以下命令之一：

   - 要将网络代理从 RPM 包安装到 32 位操作系统：
     `# yum -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：
     `# yum -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：
     `# yum -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：
     `# apt 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：
     `# apt 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：
     `# apt install ./klnagent64_<内部版本号>_arm64.deb`

2. 运行网络代理配置：

```
# /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
```

3. 阅读最终用户授权许可协议 (EULA)。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：

   - 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”。要使用网络代理，您必须接受 EULA 的条款。
   - 输入 r 以再次显示 EULA。

4. 输入管理服务器的 DNS 名称或 IP 地址。
5. 输入管理服务器端口号。默认情况下使用端口 14000。
6. 输入管理服务器 SSL 端口号。默认情况下使用端口 13000。
7. 如果您想对网络代理和管理服务器之间的流量使用 SSL 加密，请输入 y。否则，输入 n。
8. 选择以下选项之一来配置网络代理：

   - [1]—不配置连接网关。
     您的设备将不会充当连接网关，也不会通过连接网关连接到管理服务器。
   - [2]—不使用连接网关。
     您的设备将不会通过连接网关连接到管理服务器。
   - [3]—使用连接网关连接到服务器。
     您的设备将通过连接网关连接到管理服务器。
   - [4]—用作连接网关。
     您的设备将充当连接网关。

网络代理安装在 Linux 设备上。

# 对网络代理设备文件系统回滚的支持

Kaspersky Security Center Linux 是一个分发的应用程序。在安装了网络代理的设备上回滚文件系统到先前状态将导致数据不同步和 Kaspersky Security Center Linux 功能不正常。

文件系统(或一部分)可以在以下情况下回滚：

- 当复制硬件驱动器镜像时。
- 当通过虚拟架构恢复虚拟机状态时。
- 当从备份副本或恢复点恢复数据时。

安装了网络代理的设备上的第三方软件影响 /var/opt/kaspersky/klnagent 目录的情景仅是 Kaspersky Security Center Linux 的关键情景。因此，如果可能，您必须总是从恢复进程中排除该文件夹。

因此一些组织的工作规则提供了对设备文件系统的回滚，对安装了网络代理的设备的文件系统回滚的支持被添加到了 Kaspersky Security Center Linux，从版本 10 Maintenance Release 1 开始(管理服务器和网络代理必须是版本 10 Maintenance Release 1 或更新)。当检测到时，这些设备被自动连接到管理服务器，带有完整数据清除和完整同步。

默认下，对文件系统回滚检测的支持在 Kaspersky Security Center Linux 中被启用。

在安装了网络代理的设备上，尽量避免回滚 /var/opt/kaspersky/klnagent 目录，因为完整重新同步数据需要大量资源。

系统状态回滚在管理服务器设备上是不允许的。管理服务器使用的数据库的回滚也是不允许的。

您可以仅可以使用标准的 klbackup 实用工具从备份副本恢复管理服务器状态。

# 安装 Network Agent for Windows

您还可以在组织的 Windows 设备上安装网络代理，以便使用管理服务器来管理它们。

在 Microsoft Windows XP 中，网络代理可能错误执行以下操作：直接从卡巴斯基服务器（作为分发点）下载更新并作为 KSN 代理服务器（作为分发点）起作用；检测第三方漏洞（如果漏洞和补丁管理被使用）。

在运行 Microsoft Windows on Arm 的设备上安装网络代理之前，请确保尚未安装 Microsoft Windows x86-64 的网络代理。否则，安装将失败。

在 Windows 受管理设备上初始安装网络代理的方法如下：

- 通过 Windows 分发点运行远程安装任务。

  在对未分配的 Windows 设备执行远程安装之前，基于 Windows 的分发点会自动检查 UDP 端口 137 以确定目标设备的操作系统类型。如果 UDP 端口 137 不可用，分发点会尝试连接到目标设备上的 TCP 端口 445，这是执行安装所必需的。

- 通过使用网络代理的 Windows 安装程序包 (MSI)，借助第三方工具进行应用程序的远程安装。

- 通过在受管理设备上运行应用程序安装程序。

- 通过发送设备用户链接到 Kaspersky Security Center Linux 生成的独立包。独立包是包含所选应用程序分发包的定义了设置的可执行模块集合。

# 以交互模式安装 Windows 网络代理

*要在设备上本地安装网络代理：*

1. 在设备上运行从互联网下载的分发包中的 ksc_<版本号>.<内部版本号>_full_<本地化语言>.exe 文件。

   提示您选择要安装的 Kaspersky 程序的窗口将打开。

2. 在应用程序选择窗口中，单击“**仅安装 Kaspersky Security Center 网络代理**”链接以启动网络代理安装向导。遵照向导的说明操作。

   在安装向导运行期间，您可以指定网络代理高级设置（见下）。

3. 如果您想使用您的设备作为指定管理组的连接网关，在安装向导的“**连接网关**”窗口，选中“**使用网络代理作为 DMZ 连接网关**”。

4. 要在虚拟机上安装时配置网络代理：

   a. 如果您计划从虚拟机镜像创建动态虚拟机，为虚拟桌面基础架构(VDI)启用网络代理动态模式。为此，请在安装向导的“**高级设置**”窗口中选择“**启用 VDI 动态模式**”选项。

      如果您不想从虚拟机镜像创建动态虚拟机，跳过此步。

   b. 优化网络代理的 VDI 操作。为此，请在安装向导的“**高级设置**”窗口中选择“**优化 VM 设置**”选项。

      计算机启动时扫描可执行文件中是否有漏洞将被禁用。另外，会禁用发送关于以下对象的信息至管理服务器：

      - 硬件注册表
      - 设备上安装的应用程序
      - 必须安装在本地客户端设备上的 Microsoft Windows 更新
      - 在本地客户端设备上检测到的软件漏洞

      而且，您将可以在网络代理属性或网络代理策略设置中启用此信息的发送。

安装向导完成后，网络代理被安装在设备。

您可以查看网络代理服务的属性，还可以使用标准的 Microsoft Windows 工具（计算机管理\服务）来启动、停止或监控网络代理活动。

# 以静默模式安装 Windows 网络代理

网络代理可以在静默模式下安装，即，无需交互式输入安装参数。静默安装使用网络代理的 Windows Installer 数据包 (MSI)。MSI 文件位于 Kaspersky Security Center Linux 分发包，在 Packages\NetAgent\exec 文件夹。

仅可在静默模式下从 MSI 包安装网络代理，不支持从 MSI 包进行交互式安装。

*要在静默模式下将网络代理安装至本地设备：*

1. 阅读最终用户授权许可协议。只有在您理解并接受最终用户授权许可协议的条款后，才使用下面的命令。

2. 运行命令

   ```
   msiexec /i "Kaspersky Network Agent.msi" /qn <setup_parameters>
   ```

   其中“`setup_parameters`”是一系列参数，其各自的值用空格隔开 (`PROP1=PROP1VAL PROP2=PROP2VAL`)。

   在参数列表中，您必须包含 `EULA=1`。否则网络代理不会被安装。

如果您正在使用 Kaspersky Security Center 的标准连接设置和远程设备上的网络代理，请运行以下命令：

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

`/l*vx` 是写入日志的键。该日志在网络代理安装期间创建，保存在 C:\windows\temp\nag_inst.log。

除了 nag_inst.log，应用程序还会创建 $klssinstlib.log 文件，其中包含安装日志。此文件存储在 %windir%\temp 或 %temp% 文件夹中。为了进行故障排除，您或 Kaspersky 技术支持专家可能同时需要两个日志文件 - nag_inst.log 和 $klssinstlib.log。

如果您需要另外指定用于连接到管理服务器的端口，请运行以下命令：

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1 SERVERPORT=14000
```

参数 `SERVERPORT` 对应于连接到管理服务器的端口号。

网络代理安装参数区域中列出了在静默模式下安装网络代理时可用到的参数名称和可能的值。

如果要使用 Windows 安装程序升级网络代理，请运行以下命令：

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

# 通过捕获和复制设备镜像来部署

如果您需要安装网络代理到必须安装（或重新安装）操作系统和其他软件的设备，您可以使用捕获和复制设备镜像的机制。

*要通过捕获和复制硬盘驱动器来执行部署：*

1. 创建安装了操作系统和相关软件的"参考"设备，包含网络代理和安全应用程序。
2. 在设备上捕获参考镜像并通过 Kaspersky Security Center Linux 专用任务分发该镜像到新设备。
   要捕获和安装磁盘映像，请使用组织中可用的第三方工具。

使用第三方工具复制磁盘镜像

当应用第三方工具捕获安装了网络代理的设备镜像时，使用以下方法之一：

- 在参考设备上，停止网络代理服务并使用 `-dupfix` 参数运行 klmover 实用工具。实用工具 klmover 包含在网络代理安装包中。在镜像捕获操作完成之前请避免任何网络代理服务的运行。
- 确保在目标设备上首次运行网络代理服务之前，使用 `-dupfix` 密钥运行 klmover 实用工具。这是强制性要求，必须在镜像部署后首次启动操作系统时执行。实用工具 klmover 包含在网络代理安装包中。
- 使用网络代理磁盘克隆模式。

如果硬盘驱动器映像被错误地复制，可以解决此问题。

您还可以捕获未安装网络代理的设备的镜像。为此，在目标设备上执行镜像部署，然后部署网络代理。如果使用此方法，请使用设备中的独立安装包提供对网络文件夹的访问权限。

# 网络代理磁盘克隆模式

克隆参考设备的硬盘驱动器是在新设备上安装软件的流行方法。如果网络代理以标准模式运行在参考设备的硬盘驱动器上，会发生以下问题：

带有网络代理的参考磁盘镜像被部署到新设备后，它们以单一设备显示在 Kaspersky Security Center Web Console 中。该问题发生是因为克隆过程导致新设备保持相同的内部数据，这将允许管理服务器在 Kaspersky Security Center Web Console 中将设备关联到其自己的记录。

一个特别的*网络代理磁盘克隆模式*允许您避免克隆后在 Kaspersky Security Center Web Console 中错误显示新设备的问题。在您通过克隆磁盘部署软件（带有网络代理）到新设备时使用该模式。

在磁盘克隆模式下，网络代理保持运行，但是不连接到管理服务器。当退出克隆模式时，网络代理删除内部数据，这将导致管理服务器关联多个设备到 Kaspersky Security Center Web Console 中的单一记录。在完成参考设备镜像的克隆时，新设备显示在 Kaspersky Security Center Web Console 属性中（在个别记录下）。

## 网络代理磁盘克隆模式使用方案

1. 管理员安装网络代理到参考设备。
2. 管理员使用 klnagchk 实用工具检查网络代理到管理服务器的连接。
3. 管理员启用网络代理磁盘克隆模式。
4. 管理员安装软件和补丁到设备，并重启所需的次数。
5. 管理员克隆参考设备的硬盘驱动器到任意数量的设备。
6. 每个克隆的副本必须满足以下条件：
    a. 设备名称必须更改。
    b. 设备必须重启。
    c. 磁盘克隆模式必须被禁用。

## 使用 klmover 工具启用和禁用磁盘克隆模式

*要启用或禁用网络代理磁盘克隆模式：*

1. 在您必须克隆的安装了网络代理的设备上运行 klmover 工具。
   klmover 工具位于网络代理安装文件夹。
2. 要启用磁盘克隆模式，在 Linux 命令 shell 中输入以下命令：

```
./klmover -cloningmode 1
```

网络代理切换到磁盘克隆模式。

3. 要请求磁盘克隆模式的当前状态，在命令行输入以下命令：

```
./klmover -cloningmode
```

工具显示是否磁盘克隆模式已启用或禁用。

4. 要禁用磁盘克隆模式，在命令行输入以下命令：

```
./klmover -cloningmode 0
```

# 网络代理安装参数

下表描述了安装网络代理时您可以配置的 MSI 属性。所有参数都是可选的，除了 EULA 和服务器地址。

静默模式下安装网络代理的参数

| MSI 属性 | 描述 | 可用值 |
|---|---|---|
| EULA | 是否接受授权许可协议条款 | • 1 – 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>• 0 – 我不接受授权许可协议的条款（将不会执行安装）。<br>• 没有值 – 我不接受授权许可协议的条款（将不会执行安装）。 |
| DONT_USE_ANSWER_FILE | 从响应文件读取安装设置 | • 1–不使用。<br>• 其它值或没有值 – 读取。 |
| INSTALLDIR | 网络代理安装文件夹路径 | 字符串值。 |
| SERVERADDRESS | 管理服务器地址(必需) | 字符串值。 |
| SERVERPORT | 连接管理服务器的端口号 | 数字值。 |
| SERVERSSLPORT | 使用 SSL 协议加密连接到管理服务器的端口号 | 数字值。 |
| USESSL | 是否使用 SSL 连接 | • 1 – 使用。<br>• 其它值或没有值 – 不使用。 |
| OPENUDPPORT | 是否打开 UDP 端口 | • 1 – 打开。<br>• 其它值或没有值 – 不打开。 |
| UDPPORT | UDP 端口号 | 数字值。 |
| USEPROXY | 是否使用代理服务器。 | • 1 – 使用。<br>• 其它值或没有值 – 不使用。 |
| PROXYLOCATION (PROXYADDRESS:PROXYPORT) | 连接到代理服务器的代理地址和端口号 | 字符串值。 |
| PROXYLOGIN | 连接代理服务器的账户 | 字符串值。 |
| PROXYPASSWORD | 用于连接到代理服务器的账户密码（不要在安装包参数中指定授权账户的任何细节。） | 字符串值。 |
| GATEWAYMODE | 连接网关使用模式 | • 0 – 不使用连接网关。<br>• 1 – 使用该网络代理作为连接网关。<br>• 2 – 使用连接网关连接到管理服务器。 |
| GATEWAYADDRESS | 连接网关地址 | 字符串值。 |
| CERTSELECTION | 接收证书的方法 | • GetOnFirstConnection – 从管理服务器接收证书。<br>• GetExistent – 如果选中此选项则选择现有证书，必须指定 CERTFILE 属性。 |

| MSI 属性 | 描述 | 可用值 |
| --- | --- | --- |
| CERTFILE | 证书文件路径 | 字符串值。 |
| VMVDI | 启用虚拟桌面基础架构（VDI）的动态模式 | • 1 – 启用。<br>• 0 – 不启用。<br>• 没有值 – 不启用。 |
| LAUNCHPROGRAM | 安装后是否启动网络代理服务。如果 VMVDI=1，则忽略该参数 | • 1 – 启动。<br>• 其它值或没有值 – 不启动。 |
| NAGENTTAGS | 网络代理标签（优先级高于响应文件中给定的标签） | 字符串值。 |

# 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，您可以在向导窗口中指定设备（最多 1000 部设备），使用以下方法之一：

- **分配任务到管理组**。此种情况下，任务被分配到先前创建的管理组中的设备。
- **手动指定设备地址或从列表导入地址**。您可以指定要为其分配任务的设备的 DNS 名称、IP 地址和 IP 子网。
- **分配任务到设备分类**。此种情况下，任务被分配到先前创建的分类中的设备。您可以指定默认分类或您所创建的自定义分类。您最多只能选择 1000 部设备。

为了避免在未安装网络代理的客户端设备上安装应用程序时可能出现的问题，您必须按照通过 Kaspersky Security Center Linux 的远程安装任务强制部署中所述进行操作。

# 关于 Kaspersky Security Center Linux 中的远程安装任务

Kaspersky Security Center Linux 提供了远程安装应用程序的不同装置，它们作为远程安装任务实现（强制安装、通过复制硬盘驱动器镜像安装）。您可以为指定管理组和特定设备或设备分类创建远程安装任务（此类任务显示在 Kaspersky Security Center Web Console 的**任务**文件夹中）。当创建任务时，您可以选择安装包(网络代理和/或其他应用程序的安装包)以用此任务安装，并指定定义远程安装方法的设置。此外，您可以使用远程安装向导，基于远程安装任务和结果监控。

管理组的任务影响指定组的设备和所有管理组子组的设备。如果任务中启用了相应设置，任务将覆盖组及其任何子组中包括的从属管理服务器的设备。

特定设备的任务在每一次运行时根据分类内容刷新客户端设备列表。如果分类包含连接到从属管理服务器的设备，任务也将在那些设备上运行。对于那些设置的详情和安装方法请参加以下。

要确保远程安装任务在连接到从属管理服务器的设备上成功操作，您必须使用转发任务提前转发您任务使用的安装包到对应的从属管理服务器。

# 远程安装应用程序

本部分包含有关如何在管理组、具有特定地址的设备或选择的设备上远程安装应用程序的信息。

*要在特定设备上安装应用程序：*

1. 在主菜单中，转到“**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。

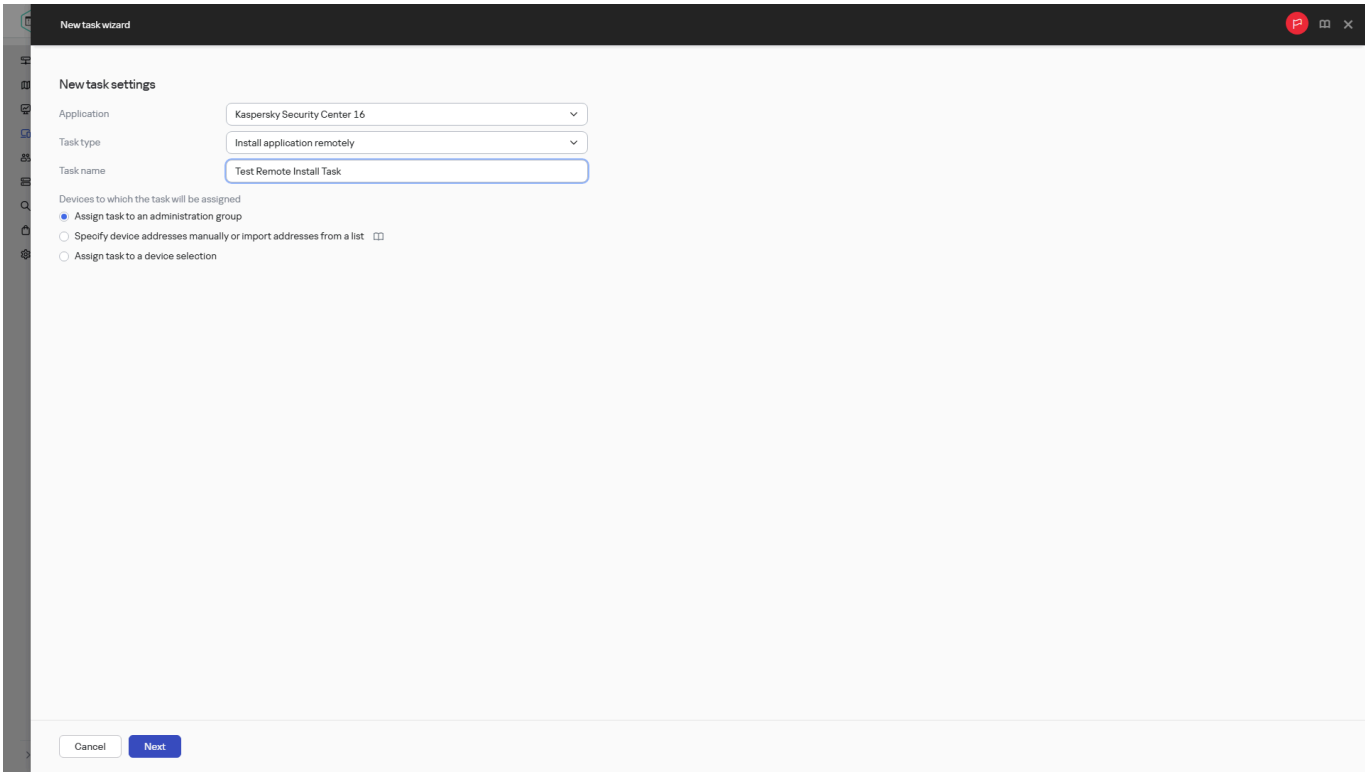
     您可能要使用该选项以对特定子网执行任务。例如，您可能要安装特定应用程序到会计设备，或者扫描疑似被感染子网中的设备。

   - **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。

*远程安装应用程序*任务为指定设备创建。如果您选择了“**分配任务到管理组**”选项，则任务是组任务。




创建远程安装应用程序任务

5. 在**任务范围**步骤，指定管理组、具有特定地址的设备或设备分类。
   可用设置取决于在上一步中选择的选项。

6. 在**安装包**步骤中，指定以下设置：

   - 在“**选择安装包**”字段中，选择要安装的应用程序的安装包。
   - 在“**强制下载安装包**”设置组中，指定如何将安装程序所需的文件分发到客户端设备中。

     - **使用网络代理**

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

     - **通过分发点使用操作系统资源**

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

       - 选择此选项。
       - 确保为目标客户端设备分配了分发点。
       - 确保分发点基于 Windows。

- **通过管理服务器使用操作系统资源**

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

  默认情况下已启用该选项。

- 在**同时下载的最大数量**字段中，指定管理服务器可以同时向其传输文件的最大允许客户端设备数。

- 在**安装尝试最大数量**字段中，指定安装程序运行的最大允许次数。

  如果超过参数中指定的尝试次数，Kaspersky Security Center Linux 将不再在设备上启动安装程序。若要重新启动*远程安装应用程序*任务，请增加**安装尝试最大数量**参数的值然后启动任务。或者，您可以创建新的"*远程安装应用程序*"任务。

- 如果您从一个卡巴斯基应用程序迁移到另一个应用程序，且当前应用程序受到密码保护，请在"**卸载当前卡巴斯基应用程序的密码**"字段中输入密码。请注意，在迁移期间，您当前的卡巴斯基应用程序将被卸载。

  仅当您在**卸载当前卡巴斯基应用程序的密码**设置组中选择了**使用网络代理**选项时，**强制下载安装包**字段才可用。

  当使用远程安装应用程序任务安装 Kaspersky Endpoint Security for Windows for Windows 时，您只能使用卸载密码来执行 Kaspersky Security for Windows Server 到 Kaspersky Endpoint Security for Windows 的迁移场景。在安装其他组件时使用卸载密码可能会导致安装错误。

  要成功完成迁移方案，请确保满足以下先决条件：

  - 您正在使用适用于 Windows 的 Kaspersky Security Center Network Agent 14.2 或更高版本。
  - 您正在运行 Windows 的设备上安装应用程序。

- 定义附加设置：

  - **如果已经安装应用程序则不再重新安装**

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

    如果禁用此选项，仍将安装应用程序。

    默认情况下已启用该选项。

  - **下载之前验证操作系统类型**

    在将文件传输到客户端设备之前，Kaspersky Security Center Linux 将检查安装实用程序设置是否适用于客户端设备的操作系统。如果设置不适用，Kaspersky Security Center Linux 不会传输文件，也不会尝试安装应用程序。例如，要将某个应用程序安装到某个管理组的设备（这些设备运行各种操作系统），可以将安装任务分配给管理组，然后启用此选项以跳过操作系统与所需设备不同的设备。

    当您在未分配的设备上远程安装网络代理时，无论**下载之前验证操作系统类型**设置如何，Kaspersky Security Center Linux 或分发点都会自动确定设备的操作系统类型。

  - **在 Active Directory 组策略中指定安装包的安装**

    如果启用此选项，安装包将使用 Active Directory 组策略进行安装。

    如果选择网络代理安装包，则该选项可用。

    默认情况下已禁用该选项。

- **提示用户关闭运行中应用程序**

  运行应用程序可能会阻止客户端设备重启。例如，如果文档在文档处理应用程序中被编辑且未被保存，则应用程序不允许设备重启。

  如果启用该选项，锁定设备上的此类应用程序在设备重启前被强制关闭。结果，用户可能丢失他们未保存的更改。

  如果禁用该选项，锁定设备不被重启。该设备上的任务状态显示设备需要重启。用户必须手动关闭所有运行在锁定设备上的应用程序并重启这些设备。

  默认情况下已禁用该选项。

- 选择要在哪些设备上安装应用程序：

  - **在所有设备上安装**

    应用程序将被安装到由其他管理服务器管理的设备。

    默认情况下已选中该选项。如果您在网络中只有一台管理服务器，您不必更改该设置。

  - **仅安装到通过该管理服务器管理的设备**

    应用程序将仅被安装到由该管理服务器管理的设备。如果您在网络中有多个管理服务器且需要避免它们之间的冲突，请选择该选项。

- 指定设备是否在安装后必须被移动到管理组：

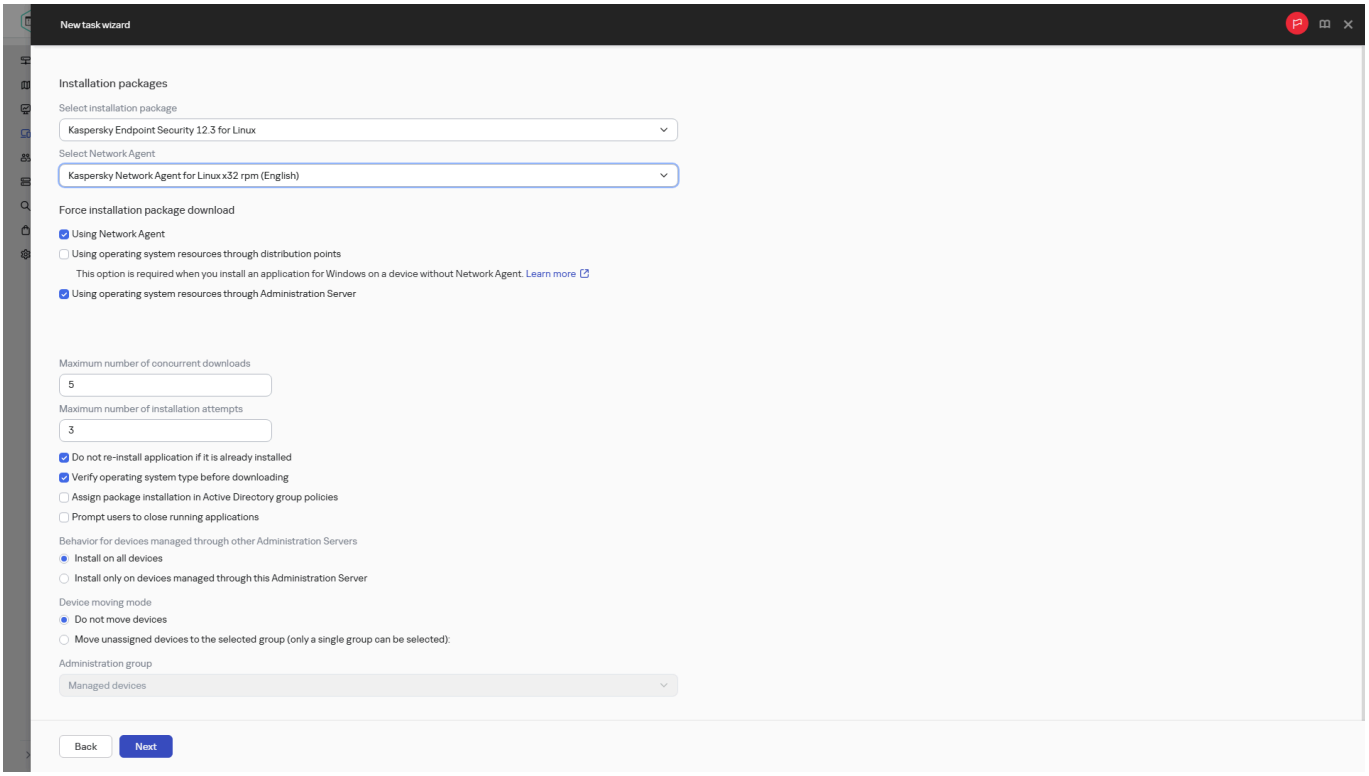
  - **不移动设备**

    设备保留在当前所在组中。未被放置在任何组的设备保持未分配。

  - **移动未分配的设备到所选组 (仅可以选择单一组)**

    设备被移动到您选择的管理组。

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




指定任务设置

7. 在向导的这一步，指定在安装应用程序期间是否必须重新启动设备：

   - **不重启设备**

     如果选择该选项，安全应用程序安装后设备不被重启。

   - **重启设备**

     如果选择该选项，安全应用程序安装后设备将被重启。

8. 如有必要，在**选择账户以访问设备**步骤，添加将用于启动*远程安装应用程序*任务的账户：

   - **不需要账户(网络代理已安装)**

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

     如果网络代理未安装在客户端设备，该选项不可用。

   - **需要账户(不使用网络代理)**

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

     - **本地或域账户**。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**本地或域账户**，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 Linux 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 Linux 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 "<用户电子邮箱>"
       ```

9. 在**完成任务创建**步骤中，单击**完成**按钮以创建任务并关闭向导。

   如果启用了“**创建完成时打开任务详情**”选项，将打开任务设置窗口。在此窗口中，您可以检查任务参数、修改它们或配置任务启动计划（如有必要）。

10. 在任务列表中，选择已创建的任务，然后单击**启动**。

    或者等待任务按照您在任务设置中指定的时间表启动。

远程安装任务完成后，选定的应用程序即安装在指定设备上。

# 在 macOS 设备上远程安装应用程序

*要使用远程安装任务在运行 macOS 的设备上安装应用程序：*

1. 创建一个由安装包和 .sh 安装脚本组成的压缩档案。
2. 在“新任务向导”中禁用“**下载之前验证操作系统类型**”选项。

或者，您可以使用**远程执行脚本**任务。以下文章介绍了如何为此任务配置文件：使用远程执行脚本任务在设备上远程安装应用程序。

# 在从属管理服务器上安装应用程序

如果您的管理服务器版本为 15.4 或更高版本，则您只能在版本为 15.4 或更高版本的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，请创建一个分发安装包**分发安装包的任务**。
3. 创建在从属管理服务器上远程安装应用程序的任务。选择**将应用程序远程安装到从属管理服务器**任务类型。

   “新任务向导”将创建一个任务，用于在特定从属管理服务器上远程安装向导中选择的应用程序。
4. 手动运行该任务，或者按照任务设置中指定的计划等待任务启动。

远程安装任务完成后，选定的应用程序即安装在从属管理服务器上。

# 在安装有网络代理的设备上远程安装应用程序

如果连接到主管理服务器（或任何其从属管理服务器）的可操作网络代理被安装到设备，您可以升级该设备上的网络代理，以及通过网络代理安装、升级或卸载支持的应用程序。

您可以在远程安装任务的属性中启用“**使用网络代理**”选项。

如果选择此选项，带有管理员定义的安装设置的安装包将被通过网络代理和管理服务器之间的通信渠道传输到目标设备。

要优化管理服务器负载和最小化管理服务器和设备之间的流量，最好为每个远程网络或每个多播域分配分发点（请参见“关于分发点”部分和“创建管理组结构和分配分发点”部分）。此种情况下，安装包和安装设置通过分发点从管理服务器分发到目标设备。

而且，您可以使用分发点来多播传送安装包，这将允许您在部署应用程序时显著降低网络流量。

当通过网络代理和管理服务器之间的通信渠道传输安装包到目标设备时，所有准备传输的安装包都将被缓存在 /var/opt/kaspersky/klnagent_srv/1093/.working/ 文件夹。当使用多个不同类型的大安装包并涉及大量分发点时，该文件夹的尺寸将显著增长。

文件不能从 FTServer 文件夹手动删除。当原始安装包被删除时，对应数据将被自动从 FTServer 文件夹删除。

分发点接收的数据保存在文件夹 /var/opt/kaspersky/klnagent_srv/1103/ 中。

文件不能从 $FTCITmp 文件夹手动删除。使用该文件夹数据的任务完成后，该文件夹的内容将被永久删除。

因为安装包从中转存储库以优化传输的格式通过管理服务器与网络代理之间的通信渠道进行分发，原始文件夹里的安装包不允许更改。这些更改将不会被管理服务器自动注册。如果您需要手动修改安装包的文件(尽管建议您避免此方案)，您必须在 Kaspersky Security Center Web Console 中编辑安装包的任何设置。在 Kaspersky Security Center Web Console 中编辑安装包的设置会导致管理服务器在目标设备传输缓存中更新安装包镜像。

在远程安装期间，服务器会向目标设备发送 ICMP 回显请求（与 ping 命令相同）。

# 在远程安装任务中管理设备重启

设备经常需要在完成应用程序远程安装时重启(尤其在 Windows)。

如果您使用 Kaspersky Security Center Linux 远程安装任务，在新任务向导或所创建任务的属性窗口（**操作系统重启**区域）中，您可以选择 Windows 设备要求重启时执行的操作：

- **不重启设备**。此种情况下，自动重启不会运行。要完成安装，您必须重启设备(例如，手动或通过设备管理任务)。所需重启的信息将被保存在任务结果和设备状态。该选项适用于在需要持续操作的服务器和其他设备上的安装任务。
- **重启设备**。此种情况下，如果完成安装需要重启，设备总是被自动重启。该选项适用于允许中断操作(关机或重启)的设备上的安装任务。
- **提示用户操作**。此种情况下，客户端设备上将显示重启提醒，提示用户手动重启设备。可以为该选项定义一些高级设置：用户消息文本、消息显示频率以及强制重启（不需要用户确认）的时间间隔。**提示用户操作**最适用于用户需要选择最合适重启时间的工作站。

# 通过 Kaspersky Security Center Linux 远程安装任务的强制部署

要执行网络代理或其他应用程序的初始部署，您可以使用 Kaspersky Security Center Linux 的远程安装任务强制安装选定的安装包，前提是每台设备都有具有本地管理员权限的用户账户。

强制安装也可以在设备无法被管理服务器直接访问时应用：例如，设备在隔离网络中，或者设备在本地网络但管理服务器在 DMZ。

初始部署时，不会安装网络代理。因此，在远程安装任务的设置中，无法选择使用网络代理安装应用程序所需的文件分发。您只能选择通过管理服务器或分发点使用操作系统资源来分发文件。

管理服务器服务必须使用在目标设备上具有管理权限的账户运行。或者，您可以在远程安装任务的设置中指定有权访问 admin$ share 的账户。

默认情况下，远程安装任务使用管理服务器运行所用账户的凭据应用到设备。需要澄清的是，这是用于访问 admin$ share 的账户，而不是运行远程安装任务的账户。安装在 LocalSystem 账户下进行。

您可以明确指定目标设备(使用列表)、通过选择它们所属的 Kaspersky Security Center Linux 管理组或通过基于指定标准创建设备分类。安装开始时间定义在任务计划中。如果任务属性中启用了**运行错过的任务**设置，任务可以在设备开启时立即运行，或设备被移动到目标管理组时立即运行。

强制安装包括传送安装包到目标设备、随后复制文件到每个目标设备的 admin$ 资源，和在这些设备上远程注册支持服务。传送安装包到目标设备通过 Kaspersky Security Center Linux 的网络交互功能运行。以下条件必须在此种情况下被满足：

- 目标设备可以从管理服务器端或分发点端访问。
- 目标设备的名称解析在网络中运行正常。
- 设备上的管理共享(admin$)保持启用。
- 以下系统服务正在目标设备上运行：
  - 服务器（LanmanServer）
    默认情况下，该服务正在运行。
  - DCOM 服务器进程启动器 (DcomLaunch)
  - RPC 端点映射器 (RpcEptMapper)
  - 远程过程调用 (RpcSs)
- TCP 445 端口在目标设备上打开，以便通过 Windows 管理工具实现远程访问。

  TCP 139、UDP 137 和 UDP 138 由较旧的协议使用，对于当前应用程序来说不再是必需的。

  防火墙必须允许动态出站访问端口，以便从管理服务器和分发点连接到目标设备。
- 在网络代理部署期间，允许 Active Directory 域策略安全设置提供 NTLM 协议的操作。
- 在运行 Microsoft Windows XP 的目标设备上，简单文件共享模式被禁用。
- 在目标设备上，访问共享和安全模型被设置为*经典 - 本地用户以自身进行身份验证*。它绝不可以是*仅限访客 – 本地用户需要以访客身份进行身份验证*。
- 目标设备是域成员，或带有管理员权限的统一账户提前在目标设备上被创建。

要成功部署网络代理或其他应用程序到未加入 Windows Server 2003 或更高版本的 Active Directory 域的设备，您必须在该设备上禁用远程 UAC。远程 UAC 是阻止本地管理账户访问 admin$ 的原因之一，这对于强制部署网络代理或其他应用程序必不可少。禁用远程 UAC 不会影响本地 UAC。

在未分配到任何 Kaspersky Security Center Linux 管理组的新设备上进行安装时，您可以打开远程安装任务属性并指定网络代理安装后设备要移动到的管理组。

当创建组任务时，记住每个组任务都影响所选组的潜逃组中的所有设备。因此，您必须避免在子组中的重复安装任务。

创建强制安装应用程序的任务的一个简化方法是自动安装。为此，您必须打开管理组属性，打开安装包列表，然后选择必须在该组中设备上安装的包。结果，所选安装包将被自动安装在该组和其所有子组中的所有设备上。包被安装的时间间隔取决于网络吞吐量和网络设备总数。

为了减轻管理服务器在向目标设备传送安装包时的负载，您可以在安装任务中选择通过分发点进行安装。注意，该安装方法给作为分发点的设备增加了大量负载。因此，建议您选择符合分布点要求的设备。如果您使用分发点，您必须确保它们存在于托管目标设备的每个隔离子网中。

使用分发点作为本地安装中心也可以用在与管理服务器具有窄通道通信的子网设备上的安装，此时子网中的通道带宽很高。

文件夹 /var/opt/kaspersky/KSC_Backups* 所在分区的磁盘剩余空间必须超过所安装应用程序的分发包的总大小的好几倍。

# 以静默模式安装应用程序

*要以静默模式安装应用程序：*

1. 在主菜单中，转到“**软件管理**” → “**安装包**”。
2. 选中所需应用程序的安装包旁边的复选框，或者为该应用程序创建一个新的安装包。

   安装包将存储于管理服务器的共享文件夹下的“安装包服务”文件夹中。每个安装包都对应一个独立的子文件夹。

3. 以下列方式之一打开所需安装包的存储文件夹：
   - 通过将相关安装包对应的文件夹从管理服务器复制到客户端设备。然后在客户端设备上打开复制的文件夹。
   - 通过从客户端设备打开对应于管理服务器预安装包的共享文件夹。

   如果共享文件位于安装了 Microsoft Windows Vista 的设备上，请为“**用户账户控制：以管理员批准模式运行所有管理员**”设置选择值“**已禁用**”（“**开始**”→“**控制面板**”→“**管理**”→“**本地安全策略**”→“**安全设置**”）。
4. 部署选择的程序，执行下面的操作：
   - 对于 Kaspersky Anti-Virus for Windows Workstations、Kaspersky Anti-Virus for Windows Servers 和 Kaspersky Security Center，打开 exec 子文件夹并用 /s 键值运行可执行文件（带 .exe 扩展名的文件）。
   - 对于其他 Kaspersky 应用程序，请在打开的文件夹中，以 /s 键值运行可执行文件（带 .exe 扩展名的文件）。

   以 `EULA=1` 和 `PRIVACYPOLICY=1` 参数运行可执行文件表示您已完全阅读、理解并接受最终用户授权许可协议和隐私策略的条款。您也知道并同意您的数据将按照隐私策略中所述进行处理和传输（包括传输到第三方国家）。授权许可协议和隐私策略的文本包含在 Kaspersky Security Center Linux 分发包中。必须接受授权许可协议和隐私策略的条款才能安装程序或升级上一版本程序。

# 准备 macOS 设备以远程安装网络代理

有以下方法可以在 macOS 受管理设备上初始安装网络代理：

- 通过在 macOS 分发点上运行远程安装任务。
- 通过发送设备用户链接到 Kaspersky Security Center Linux 生成的独立包。独立包是包含所选应用程序分发包的定义了设置的可执行模块集合。

*要准备运行 macOS 的设备以远程安装网络代理：*

1. 确保目标 macOS 设备上安装了 sudo。
2. 测试设备配置：
   a. 确保端口 22 在客户端设备上打开。为此，在“**系统偏好**”中打开“**共享**”窗格，然后确保选中“**远程登录**”复选框。

      您只能通过端口 22 来通过 Secure Shell (SSH) 连接到客户端设备。您不能更改端口号。

      您可以使用 `ssh <设备名称>` 命令远程登录到 macOS 设备。在“**共享**”窗格中，可以使用“**允许访问**”选项来设置允许访问 macOS 设备的用户范围。

   b. 禁用要连接设备的用户账户的 sudo 密码。

      在终端中使用 `sudo visudo` 命令打开 sudoers 配置文件。在打开的文件中，在“用户特权指定”条目中指定以下内容：`username ALL = (ALL) NOPASSWD: ALL`。在这种情况下，`username` 代表通过 SSH 进行设备连接的用户账户。

   c. 保存并关闭 sudoers 文件。

   d. 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. 下载并创建安装包：
   a. 使用以下方法之一下载网络代理安装包：
      - 通过使用应用程序界面
      - 从技术支持网站 https://support.kaspersky.com/ 下载相关版本的网络代理
      - 向技术支持专家索取安装包
   b. 要创建远程安装包，使用以下文件：
      - klnagent.kud
      - install.sh
      - klnagentmac.dmg

4. 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，要运行任务，请指定通过 SSH 进行设备连接的用户账户设置。

客户端设备已准备好通过您创建的相应任务远程安装网络代理。

# 虚拟基础架构

Kaspersky Security Center Linux 支持虚拟机的使用。您可以在每台虚拟机上安装网络代理和安全应用程序，并可以在虚拟机监控程序级别保护虚拟机。在第一种情况下，您可以使用标准安全应用程序或 Kaspersky Security for Virtualization Light Agent 来保护您的虚拟机。在第二种情况下，您可以使用 Kaspersky Security for Virtualization Agentless。

Kaspersky Security Center Linux 支持虚拟机回滚到先前状态。

# 降低虚拟机负载的窍门

当安装网络代理到虚拟机时，建议您禁用一些对虚拟机没有用的 Kaspersky Security Center Linux 功能。

在虚拟机或用于生成虚拟机的模版上安装网络代理时，建议执行以下操作：

- 如果要运行远程安装，则在网络代理安装包的属性窗口的"**高级**"区域中，选择"**优化 VDI 设置**"选项。
- 如果要通过向导运行交互式安装，则在向导窗口中选择"**为虚拟基础架构优化网络代理设置**"选项。

选择这些选项将改变网络代理设置，因此以下功能在默认情况下保持禁用状态（在应用策略之前）：

- 获取已安装软件的信息
- 获取硬件信息
- 获取检测到的漏洞信息
- 获取需要更新的信息

通常，这些功能对于虚拟机不必要，因为它们使用统一软件和虚拟硬件。

禁用该功能是不可逆的。如果需要任何被禁用的功能，您可以通过网络代理策略启用它，或通过网络代理本地设置。网络代理本地设置通过 Kaspersky Security Center Web Console 中相关设备的上下文菜单可用。

# 对动态虚拟机的支持

Kaspersky Security Center Linux 支持动态虚拟机。如果虚拟架构部署在组织网络，动态（临时）虚拟机可以被用在特定情况。动态虚拟机基于管理员提供的模板以独立名称创建。用户使用了虚拟机一段时间，然后关闭虚拟机，则该虚拟机将从虚拟基础架构中删除。如果 Kaspersky Security Center Linux 部署在组织网络，安装了网络代理的虚拟机将被添加到管理服务器数据库。在您关闭虚拟机后，对应的条目必须从管理服务器数据库中删除。

要运行自动删除虚拟机上的条目的功能，在动态虚拟机的模板上安装网络代理时，请选中“**启用 VDI 动态模式**”选项：

- 对于远程安装—在网络代理安装包的属性窗口（**高级**区域）
- 对于交互式安装 — 在“网络代理安装向导”中进行

> 当安装网络代理到物理设备时，不要选中“**启用 VDI 动态模式**”选项。

如果您要在删除虚拟机后将动态虚拟机的事件存储在管理服务器一段时间，那么，在管理服务器属性窗口，在“**事件存储库**”区域，选择“**设备被删除后存储事件**”选项并指定事件的最大存储期限（天）。

> 我们不建议在动态虚拟机上启用加密驱动器。

# 对虚拟机复制的支持

复制安装了网络代理的虚拟机或从安装了网络代理的模板创建虚拟机，和捕获和复制硬盘驱动器镜像的网络代理部署相同。因此，常规情况下，当复制虚拟机时，您需要执行与通过复制磁盘镜像部署网络代理时相同的操作。

然而，以下描述的两种情况展示了自动检测复制的网络代理。由于以上原因，您不必运行“通过捕获和复制设备磁盘镜像部署”中描述的复杂操作：

- “**启用 VDI 动态模式**”选项在网络代理被安装时选中：在操作系统每次重启后，该虚拟机将被认为是新设备，无论是否被复制。
- 以下 Hypervisor 之一被使用：VMware™、HyperV® 或 Xen®：网络代理通过更改的虚拟硬件 ID 检测虚拟机的复制。

> 虚拟硬件更改分析并不绝对可靠。在广泛应用该方法之前，您必须在小组虚拟机上测试您组织中使用的当前 hypervisor 版本。

# 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“**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)**

     如果在目标设备上必须指定密码才能使用 sudo 命令，则选择此选项，然后指定 root 账户的密码。Kaspersky Security Center 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 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 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。

# 监控部署

要监控 Kaspersky Security Center Linux 部署并确保受管理设备上安装了安全应用程序和网络代理，请使用监控和报告功能：

- 使用仪表板的部署小部件实时监控部署。
- 使用报告获取详细信息。

# 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“**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 Linux 提供几种卸载第三方应用程序的方法。

## 当配置应用程序远程安装时卸载不兼容应用程序

您可以在保护部署向导中配置安全应用程序远程安装时启用“**自动卸载不兼容的应用程序**”选项。当该选项被启用时，Kaspersky Security Center Linux 在安装安全应用程序到受管理设备之前卸载不兼容的应用程序。

## 通过专用任务卸载不兼容的应用程序

要卸载不兼容的应用程序，使用*远程卸载应用程序*任务。该任务应该在安全应用程序安装任务运行之前运行在设备。例如，在安装任务中，可以选择“**在完成其他任务时**”作为计划类型，其中其他任务为“*远程卸载应用程序*”。

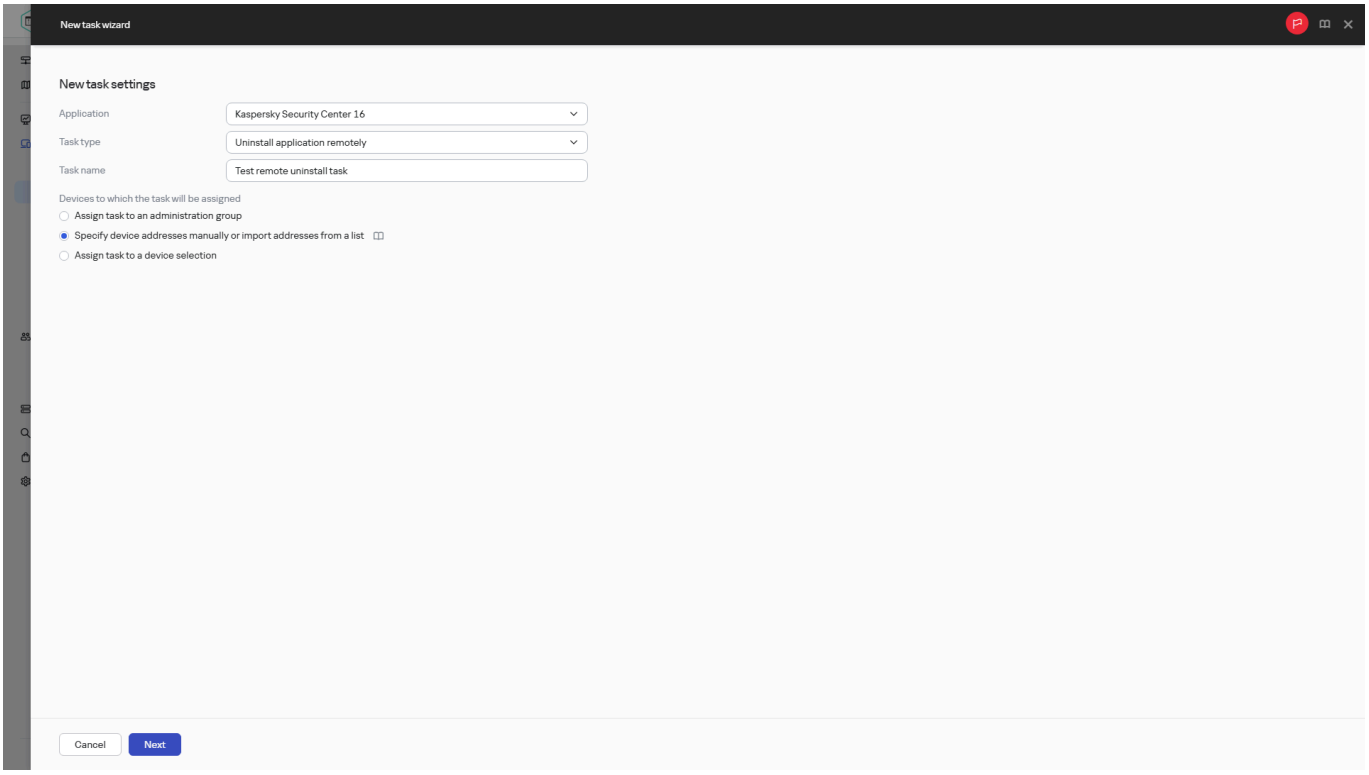
该卸载方法在安全应用程序无法正确卸载不兼容应用程序时是很有用的。

# 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：*

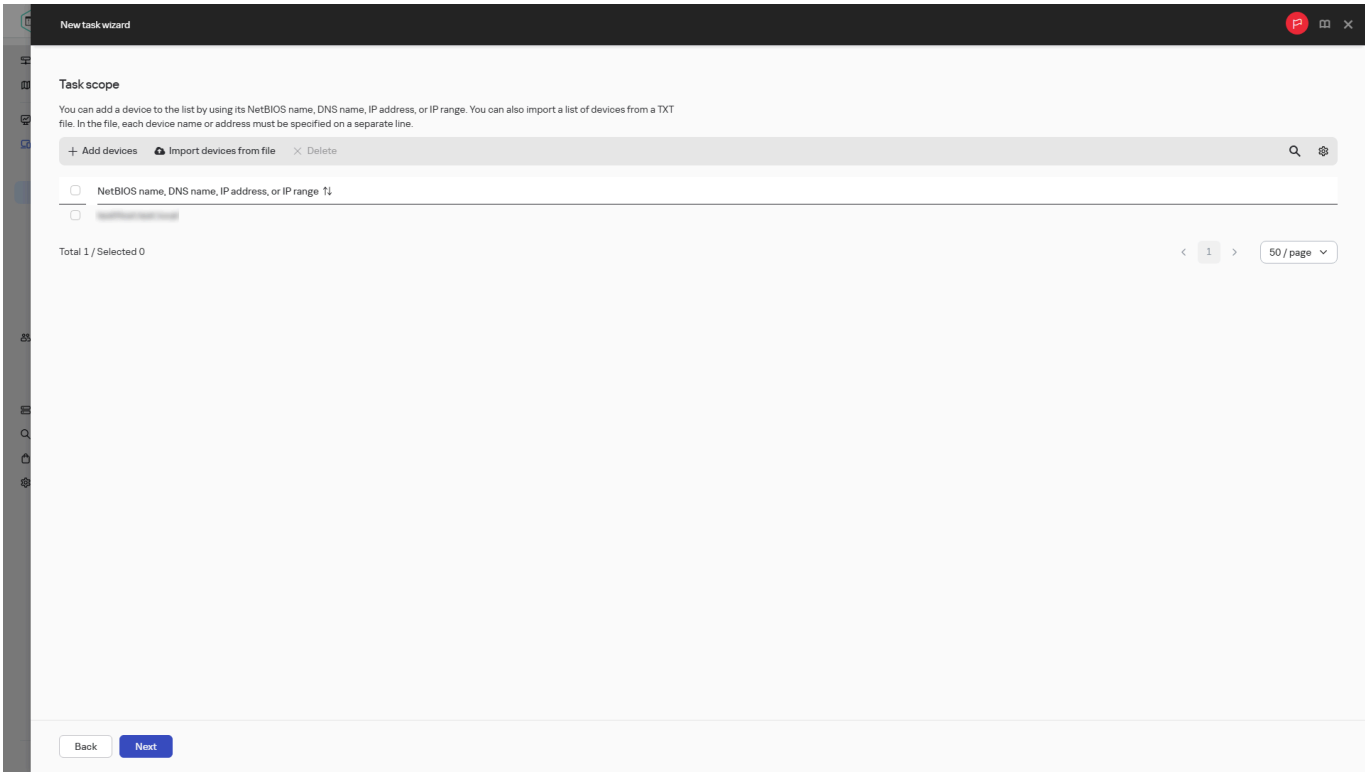
1. 在主菜单中，转到“**任务**”。
2. 单击**添加**。
   “新任务向导”启动。使用“**下一步**”按钮继续向导操作。
3. 在**应用程序**下拉列表中，选择Kaspersky Security Center。
4. 在**任务类型**列表中，选择**远程卸载应用程序**任务类型。
5. 在**任务名称**字段中，指定新任务的名称。
   任务名称不能包含多于 100 个字符并且不能包括任何特殊字符（*<>-_?:\"|）。




创建远程卸载应用程序任务

6. 选择要将任务分配到的设备。

继续执行向导的下一步。




指定任务范围

7. 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**

  显示卡巴斯基应用程序列表。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 Linux 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 Linux 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 Linux 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 Linux 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。

- **卸载指定的应用程序更新、补丁或第三方应用程序**

  显示更新、补丁和第三方应用程序的列表。选择要删除的项目。

  显示的列表是常规的应用程序和更新列表，并不对应于受管理设备上安装的应用程序和更新。选择项目之前，建议您确保在任务范围中定义的设备上安装了应用程序或更新。您可以通过属性窗口查看安装了应用程序或更新的设备列表。

  *要查看设备列表：*

  a. 单击应用程序或更新的名称。

  属性窗口打开。

  b. 打开“**设备**”区域。

  还可以在设备属性窗口中查看已安装的应用程序和更新列表。

8. 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 Linux 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 Linux 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`。设备上的安装程序每次运行返回错误时，计数器读数都会递增。

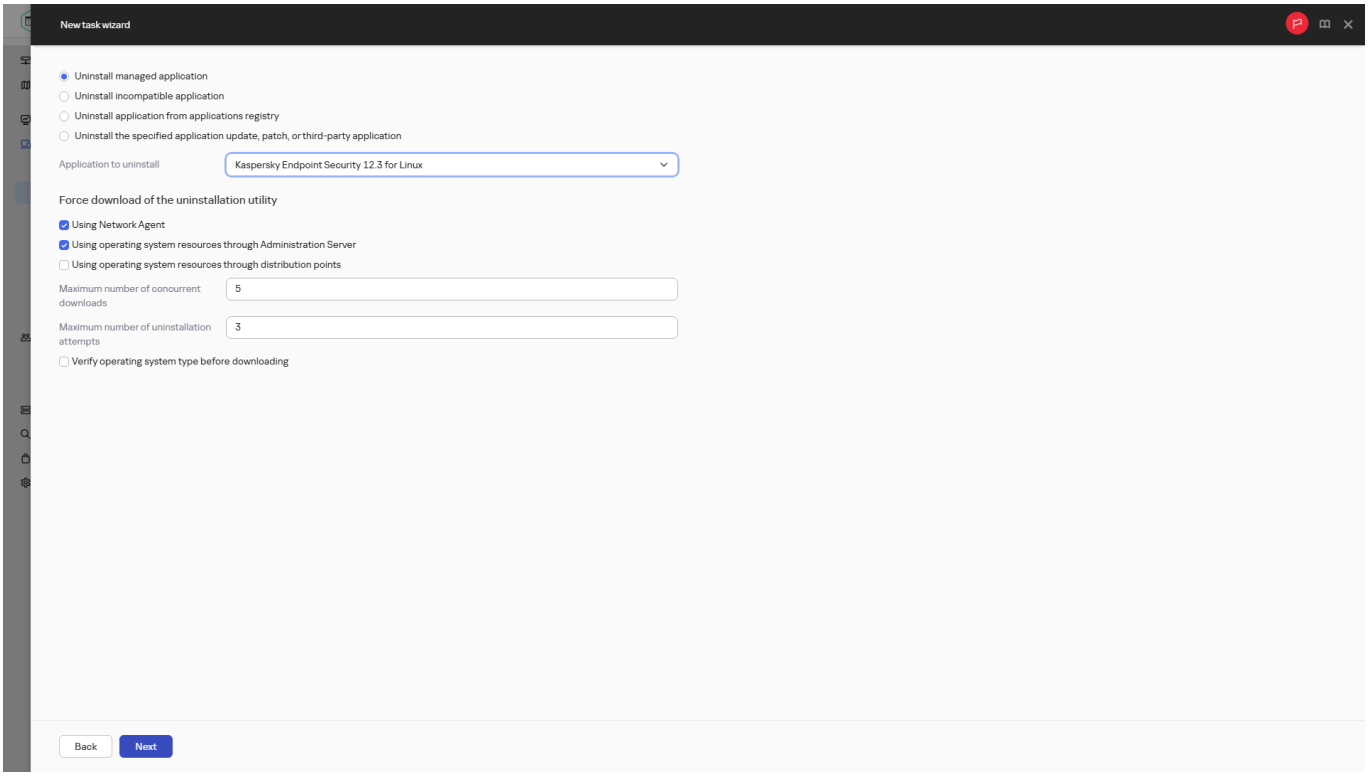
  如果已超过参数中指定的尝试次数，且设备已准备好应用程序卸载，您可以增加"**尝试卸载的最大次数**"参数的值并启动任务以卸载应用程序。或者，您可以创建新的"*远程卸载应用程序*"任务。

- **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 Linux 将检查安装实用程序设置是否适用于客户端设备的操作系统。如果设置不适用，Kaspersky Security Center Linux 不会传输文件，也不会尝试安装应用程序。例如，要将某个应用程序安装到某个管理组的设备（这些设备运行各种操作系统），可以将安装任务分配给管理组，然后启用此选项以跳过操作系统与所需设备不同的设备。

  当您在未分配的设备上远程安装网络代理时，无论**下载之前验证操作系统类型**设置如何，Kaspersky Security Center Linux 或分发点都会自动确定设备的操作系统类型。

继续执行向导的下一步。




指定任务设置

9. 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。

- **提示用户操作**

  客户端设备屏幕上将显示重启提醒，提示用户手动重启设备。可以为该选项定义一些高级设置：用户消息文本、消息显示频率以及强制重启（不需要用户确认）的时间间隔。该选项适用于用户必须可以选择最方便的时间进行重启的工作站。

  默认情况下已选定该选项。

  - **重复提示间隔(分钟)**
  - **在该时间后重启(分钟)**

- **强行关闭锁定会话中的应用程序**

  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。

继续执行向导的下一步。

10. 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证书来安装应用程序。

  - **本地或域账户**。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**本地或域账户**，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Linux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 Linux 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 Linux 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>"
    ```

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**的任务列表中。

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，所选的应用程序被从所选设备中删除。

### 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。

# 为远程安装准备 Windows 设备

远程安装应用程序到客户端设备时可能会因下列原因返回错误：

- 该任务已成功在该设备上执行。
  在此情况下，该任务无需再执行。
- 任务开始后，设备被关闭。
  在此情况下，请打开设备，然后重新启动此任务。
- 管理服务器与客户端设备上安装的网络代理之间无连接。
  要确定问题原因，请使用客户端设备的远程诊断实用程序 (klactgui)。
- 如果设备上未安装网络代理，远程安装过程中可能出现下列问题：
  - 客户端设备启用了"**禁用简单文件共享**"选项。
  - 客户端设备上未运行服务器服务。

- 客户端设备上的相关端口被关闭。
- 用于执行任务的账户权限不足。

为了避免在未安装网络代理的客户端设备上安装应用程序时可能出现的问题，您必须按照通过 Kaspersky Security Center Linux 的远程安装任务强制部署中所述进行操作。

之前使用 riprep 实用程序准备设备进行远程安装。现在这被认为是一种配置操作系统的过时方法。不建议在比 Windows XP 和 Windows Server 2003 R2 更新版本的操作系统上使用 riprep 实用程序。

# 创建“远程执行脚本”任务

您可以创建“*远程执行脚本*”任务来在客户端设备上执行安装包并远程安装应用程序。

安装包包含一个 ZIP 压缩文件，其中包含一组用于在客户端设备上执行的脚本以及一个 manifest.json 文件。在本文中了解有关创建此类安装包的更多信息。

此任务只能在具有 Linux 网络代理的设备上启动。

*要启动“远程执行脚本”任务：*

1. 转到“**新任务向导**”并选择“**远程执行脚本**”任务类型。
2. 输入任务名称并选择将分配任务的设备。单击“**下一步**”按钮。
3. 根据 ZIP 压缩文件选择一个带有 manifest.json 文件的安装包，用于远程执行。

   如果您不想在已完成该任务的设备上重新运行该任务，请打开“**不在已完成此任务的设备上启动此任务**”选项。
4. 选择账户以运行该任务。

   如果选择默认账户，则该任务将由网络代理（root 账户）执行。

   当“*远程执行脚本*”任务启动时，无法更改分配给它的账户。要更改任务分配到的账户，请在任务设置中停止任务，然后使用正确的账户详细信息重新创建任务。
5. 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。
6. 单击“**完成**”按钮。

   “*远程执行脚本*”任务创建完成并显示在任务列表。

从“*远程执行脚本*”任务接收数据后，网络代理会限制所有用户（管理员和任务设置中指定的用户除外）对接收的数据的访问。

# 根据清单文件创建安装包

*要根据清单文件创建安装包：*

1. 在主菜单中，转到“**软件管理**” → “**安装包**”。
   此时会显示管理服务器上可用的安装包的列表。
2. 单击**添加**。
   新安装包向导启动。使用“**下一步**”按钮继续向导操作。
3. 选择“**基于带有 manifest.json 文件的 ZIP 压缩包，为“远程执行脚本”任务创建一个安装包**”。
4. 指定包名称并单击“**浏览**”按钮。
   在打开的窗口中，选择一个文件来创建安装包。
5. 选择可用磁盘上的压缩文件。在本文中了解如何为此任务准备压缩文件。
   该文件开始上传至 Kaspersky Security Center Linux 管理服务器。
   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。
6. 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。
  - **版本。**应用程序版本。
  - **创建日期。**安装包创建日期。
  - **已修改。**安装包修改日期。
  - **路径。**管理服务器上自定义安装包的路径。
- 更改安装包名称和命令行参数。该功能仅适用于未根据卡巴斯基应用程序创建的安装包。

# 为“远程执行脚本”任务准备压缩文件

基于 manifest.json 文件的“*远程执行脚本*”任务的压缩文件必须满足以下要求：

- 压缩文件格式：ZIP。
- 总大小：不超过 1 GB。
- 压缩文件中的文件和文件夹的数量不受限制。
- 压缩文件的清单文件必须与下面的架构匹配，并且必须命名为 manifest.json。仅在设备上执行任务期间验证架构。

  **清单文件的 JSON 架构和数组的描述**

  JSON 架构

```
{
 "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "Schema for execute scripts task",
   "type": "object",
    "properties": {
        "version": {
            "type": "integer",
            "enum": [1]
        },
        "actions":{
            "type": "array",
            "items": {
                "type": "object",
                "properties": {
                    "type": {
                        "type": "string",
                        "enum": ["execute"]
                    },
                    "path": {
                        "type": "string"
                    },
                    "args": {
                        "type": "string"
                    },
                    "results":{
                        "type": "array",
                        "items": {
                            "type": "object",
                            "properties": {
                                "code": {
                                    "type": "integer",
                                    "minimum": -255,
                                    "maximum": 255
                                },
                                "next":{
```

```
                                    "type": "string",
                                    "enum": ["break", "continue"]
                                }
                            },
                            "required": [
                                "code",
                                "next"
                            ]
                        }
                    },
                    "default_next":{
                        "type": "string",
                        "enum": ["break", "continue"]
                    }
                },
                "required": [
                    "type",
                    "path",
                    "default_next"
                ]
            }
        }
    },
    "required": [
        "version",
        "actions"
    ]
}
```

**清单文件示例**

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "scripts/run1.cmd",
      "args": "testArg",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run2.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
```

```
      "path": "scripts/run3.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

- 压缩文件的结构必须如下：

  manifest.json

  <file1>

  <file2>

  <folder1>/<file3>

  <folder2>/<folder3>/<file4>

  ...

  <fileX>

  manifest.json 是该任务的清单文件。

  <file1>, ...., <fileX> 是包含待执行脚本的文件集。

# 使用“远程执行脚本”任务在设备上远程安装应用程序

可以使用“*远程执行脚本*”任务通过创建自定义安装包在客户端设备上远程安装应用程序。

在本文中了解如何为此任务准备压缩文件。

要创建用于在客户端设备上远程安装应用程序的安装包，您为此任务上传的压缩文件中必须包含以下文件：

- <包名称>.deb
- **install.sh**

  sudo apt-get install <包名称>.deb

- **manifest.json**

  远程安装应用程序的 JSON 架构

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "install.sh",
      "args": "<如有必要，请输入参数>",
```

```
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

数组描述

1. version—清单文件和任务的版本。

   目前唯一可接受的值是 1。

2. actions 数组的元素决定了任务中执行的脚本的组成和顺序。

   脚本的执行顺序对应于数组中元素的索引（位置）。

3. 对于 actions 数组的每个元素，定义了以下元素。

   a. type—脚本中可执行命令的类型。目前，该值始终为 execute。

   b. path—压缩文件中脚本文件的路径。

   c. args—作为可执行命令的一部分传递给脚本的参数。

   d. results—根据任务结果定义后续操作的数组。

      1. code—脚本返回的值。

      2. next—下一步要完成的操作。 continue 操作表示继续执行下一个脚本（actions 数组中的元素）；break 操作表示停止任务。

   e. default_next—如果脚本返回的值未包含在 results 中而执行的操作。

当“*远程执行脚本*”任务启动时，网络代理会将安装包与应用程序一起上传到客户端设备。当客户端设备接收到安装包后，该设备上的网络代理会解析 manifest.json 文件，并根据结果定义脚本和操作的执行顺序并开始执行。

当“*远程执行脚本*”任务完成后，应用程序将安装到客户端设备上。

# 配置“远程执行脚本”任务的通知和监控

您可以为“*远程执行脚本*”任务配置监控、事件保存行为和通知。

*要查看“远程执行脚本”任务的状态：*

1. 在主菜单中，转到“**任务**”。

   将显示任务列表。

2. 选择任务并单击“**设备历史**”。
   显示任务的进度。

*要配置事件保存行为：*

1. 在任务列表中，单击任务并转到“**设置**”选项卡。
2. 在“**通知**”部分中，单击“**设置**”按钮。
3. 选择以下选项之一来确定任务完成后应用程序的行为方式：
   - **保存所有事件**。
   - **保存任务进度相关事件**。
   - **仅保存任务执行结果**。
     事件保存在“**设备历史**”和“**事件存储库**”中。
     默认只保存任务执行结果。

     > 若选择“**保存所有事件**”，则仅保存任务执行结果。
4. 如果您要将事件保留在管理服务器数据库、管理服务器事件日志或设备上，请启用相应的选项。

在本文中了解有关配置通知的更多信息。

# 授权许可

此部分提供下列信息：

- 与 Kaspersky Security Center Linux 授权许可相关的一般概念
- 有关受管理卡巴斯基应用程序授权许可管理的说明

# Kaspersky Security Center 授权

本节介绍与 Kaspersky Security Center Linux 授权许可有关的一般概念。

## 关于最终用户授权许可协议

*最终用户授权许可协议*（授权许可协议或 EULA）是您和 AO Kaspersky Lab 之间具有约束力的合作协议，其中规定了您使用该程序应遵守的条款。

在您开始使用应用程序之前请认真阅读授权许可协议。

Kaspersky Security Center Linux 及其组件（例如网络代理）具有自己的 EULA。

您可以使用以下方法查看 Kaspersky Security Center Linux 最终用户授权许可协议的条款：

- 在 Kaspersky Security Center 安装期间。
- 如果阅读包含在 Kaspersky Security Center 分发包的 license.txt 文档。
- 如果阅读在 Kaspersky Security Center 安装文件夹的 license.txt 文档。
- 通过从卡巴斯基网站下载 license.txt 文件。

您可以使用以下方法查看 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。
- 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*

  用于试用该应用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 ID 或订单号
- 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应用程序。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*。为应用程序添加授权许可后，将在应用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，要使用应用程序，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 Linux 前阅读隐私策略。
- 隐私策略文本包含在 Kaspersky Security Center Linux 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 可以在以下模式中工作：

- **管理控制台的基本功能**

  在应用程序启动或者商业授权许可过期后，Kaspersky Security Center 以这种模式工作。在管理控制台基本功能支持下的 Kaspersky Security Center 作为保护企业网络的 Kaspersky 应用程序的一部分被传送。您也可以从卡巴斯基网站下载。

- **商业授权许可**

  如果需要不包括在管理控制台的基本功能中的其它功能，您必须购买商业授权许可。

  在管理服务器属性窗口中添加授权许可密钥时，请确保添加让您使用 Kaspersky Security Center Linux 的授权许可密钥。您可以在 Kaspersky 网站上找到此信息。每个解决方案网页都包含该解决方案包括的应用程序列表。管理服务器可接受不受支持的授权许可密钥，例如Kaspersky Endpoint Security Cloud 的授权许可密钥，但此类授权许可密钥除了管理控制台的基本功能外，不提供任何新功能。

| 功能或属性 | Kaspersky Security Center Linux 操作模式 | |
|---|---|---|
| | 没有授权许可 | 商业授权许可 |
| **管理控制台的基本功能**<br>下列功能可用：<br>• 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。<br>• 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。<br>• 远程安装应用程序。<br>• 对安装在客户端设备上的应用程序的集中配置。<br>• 控制组织的反病毒安全状态。<br>• 管理用户角色。<br>• 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。<br>• 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。<br>• "加密和数据保护"管理。<br>• 查看和手动编辑网络轮询期间发现的硬件组件列表。<br>• 查看可用于远程安装的操作系统镜像的列表。 | ✓ | ✓ |
| **漏洞和补丁管理：基本功能**<br>以下任务不需要商业授权许可：<br>• *查找漏洞和所需更新*任务<br>通过此任务，Kaspersky Security Center Linux 接收检测到的漏洞列表以及受管理设备上安装的第三方软件的所需更新列表。<br>• *修复漏洞*任务<br>"*修复漏洞*"任务使用针对 Microsoft 软件的建议修补程序和针对第三方软件的用户修补程序。要使用此任务，您必须手动为任务设置中的漏洞指定用户修补程序。 | ✓ | ✓ |
| **漏洞和补丁管理：高级功能**<br>您可以定义自动远程安装软件更新和自动修复漏洞的规则。 | – | ✓ |
| **系统管理**<br>下列功能可用：<br>• 通过名为远程桌面连接的 Microsoft® Windows® 组件远程连接到客户端设备的权限。<br>• 通过 Windows 桌面共享远程连接到客户端设备。 | – | ✓ |
| **将事件导出到 SIEM 系统：使用 Syslog 协议**<br>使用 Syslog 协议，您可以转发发生在 Kaspersky Security Center 管理服务器上和受管理设备上安装的 Kaspersky 应用程序中的任意事件。Syslog 协议是标准消息记录协议。您可以用它将事件导出到任何 SIEM 系统。 | ✓ | ✓ |
| 通过 Active Directory、KASAP 和 Kaspersky TIP Sandbox 聚合警报和执行响应操作 | – | ✓ |

# 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

传输到第三方的数据

使用软件的移动设备管理功能时，为了及时通过推送通知机制将命令传递到运行 Android 操作系统的设备，需使用 Google Firebase Cloud Messaging 服务。如果用户配置了使用 Google Firebase Cloud Messaging 服务，则用户同意以自动模式向 Google Firebase Cloud Messaging 服务提供以下信息：

- 实例 ID
- Google Firebase Cloud Messaging 服务中的软件 ID
- 安装的软件的版本
- 完整版软件
- Google Play 版本
- 软件分发包名称
- 所提供数据的方案版本
- 操作系统的版本
- 软件 ID

要阻止与 Google Firebase Cloud Messaging 服务交换信息，用户必须将 Google Firebase Cloud Messaging 服务的使用设置回滚至出厂设置值。

使用软件的移动设备管理功能时，为了及时通过推送通知机制将命令传递到运行 iOS 操作系统的设备，需使用 Apple Push Notification Service (APNs)。如果用户在 iOS MDM 服务器上安装了 APNs 证书，创建了 iOS MDM 配置文件（其中包含用于将 iOS 移动设备连接到软件的设置集合），并将此配置文件安装在移动设备上，则表示用户同意以自动模式向 APNs 提供以下信息：

- 令牌 - 设备的推送令牌。服务器在向设备发送推送通知时使用此令牌。
- PushMagic - 推送通知中必须包含的字符串。字符串值由设备生成。

### 传输到 AO Kaspersky Lab 的数据

如果用户可以使用 Kaspersky Extended Detection and Response Optimum 功能，Kaspersky Security Center Linux 会在以下情况下传输数据：

- 为了给员工分配培训课程，Kaspersky Security Center Linux 会将以下数据传输到 Kaspersky Automated Security Awareness Platform (KASAP)：用户电子邮件、备用用户电子邮件（如果有）、KASAP 中的用户 ID、培训组 ID。
- 为了使用 Kaspersky Cloud Sandbox 服务自动执行和检测恶意行为，受管理的卡巴斯基应用程序会将隔离的对象以及在执行传输对象期间创建的文件从管理服务器通过网络代理传输，然后通过 Kaspersky Security Center Web Console 传输到 Kaspersky Cloud Sandbox 服务。

### 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
- 在设备上安装卡巴斯基应用程序
- 管理已安装应用程序的设置和任务
- 管理 Kaspersky 和第三方应用程序的更新，以及查找和修复漏洞
- 在设备上激活 Kaspersky 应用程序
- 管理用户账户
- 查看设备上的卡巴斯基应用程序运行信息
- 查看报告
- 启用与卡巴斯基服务的集成

为执行其主要功能，Kaspersky Security Center Linux 可以接收、存储和处理以下信息：

- 通过扫描域控制器（Active Directory、Samba、FreeIPA 和 ALD Pro）或通过扫描 IP 间隔收到的有关组织网络上的设备的信息。管理服务器独立获取数据或从网络代理接收数据。
- 来自域控制器（Active Directory、Samba、FreeIPA 和 ALD Pro）的有关组织单位、域、用户和组的信息。管理服务器自行获取数据或从被分配充当分发点的网络代理接收数据。

- 受管理设备详细信息。网络代理将下面列出的数据从设备传输到管理服务器。用户在 Kaspersky Security Center Web Console 界面中输入设备的显示名称和说明：
  - 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、Windows 域名和类型（适用于属于 Windows 域的设备）、Windows 环境中的设备名称（适用于属于 Windows 域的设备）、DNS 域和 DNS 名称、IPv4 地址、IPv6 地址、网络位置、MAC 地址、序列号、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，以及设备是否为属于 VDI 的动态虚拟机。
  - 审计受管理设备以及决定特定补丁和更新是否适用时所需的受管理设备及其组件的其他说明：操作系统结构、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；如果设备是虚拟机，也包括虚拟机类型、管理设备的虚拟管理服务器的名称。
  - 受管理设备上的操作的详细信息：上次更新的日期和时间、设备在网络中最后一次可见的时间、重新启动等待状态以及设备打开的时间。
  - 设备用户账户及其工作会话的详细信息。
- 通过在受管理设备上运行远程诊断接收到的数据：跟踪文件、系统信息、设备上安装的卡巴斯基应用程序的详细信息、转储文件、事件日志、从卡巴斯基技术支持接收到的运行诊断脚本的结果。
- 分发点运行统计数据（如果设备是分发点）。网络代理将数据从设备传输到管理服务器。
- 用户在 Kaspersky Security Center Web Console 中输入的分发点设置。
- 将移动设备连接到管理服务器所需的数据：证书、移动连接端口、管理服务器连接地址。用户在 Kaspersky Security Center Web Console 中输入数据。
- 使用移动协议传输的移动设备详细信息。下面列出的数据从移动设备传输到管理服务器：
  - 应用程序信息：应用程序名称、应用程序的完整版本、应用程序的安装日期和时间、设备的实时保护状态、会话 ID。
  - 有关应用程序使用的授权许可密钥的信息：授权许可密钥序列号和授权许可类型、授权许可状态、授权许可密钥有效期（天数）、授权许可密钥生成和到期日期、提供授权许可的公司名称、使用订阅时的附加信息（订阅标志、到期日期和可进行订阅续费的天数、订阅提供商的网址、当前订阅状态和获取此状态的原因）、应用程序在设备上激活的日期和时间、设备上的授权许可到期的日期和时间。
  - 有关受管理设备的信息：设备名称、设备 ID、设备类型、设备 IMEI（如果可用）、设备序列号（如果可用）、设备制造商、设备 CPU 系列名称、设备所有者证书指纹、操作系统类型、操作系统版本、操作系统名称、设备上的总磁盘空间、设备所属服务器的名称、设备 IP 地址、设备组名称、用户的可分辨名称、域的可分辨名称、一次性密码或域密码。
  - 自定义命令执行结果信息：命令 ID、命令执行状态、命令执行结果；对于设备定位命令：设备的经纬度、海拔、移动速度；对于面部照片命令：尝试解锁时移动设备前置摄像头拍摄的照片。
  - 有关设备扫描的信息：上次设备扫描的日期和时间；从其开始扫描的文件系统中的完整路径；扫描的对象数量；检测到的恶意对象的数量；阻止、删除和清除的对象数量；无法清除的对象数量；验证错误的数量；终止的进程数量。
  - 有关每个应用程序组件的功能以及每个任务的执行的信息（以事件的形式呈现）：
    - 事件 ID。
    - 重要级别。
    - 事件名称和类型。

- 事件原因描述。
- 事件发生的日期和时间。
- 有关反盗窃操作事件的信息（设备解锁代码、设备坐标、命令传送方式、已删除数据列表）。
- 处理检测到的对象或操作的结果（设备上的文件名称；应用程序名称；威胁名称；威胁类型；对文件执行的操作类型；操作结果；错误代码（如果发生））。
- 有关触发的合规性规则的信息（规则标准；应用的操作；应用操作时的错误描述（如果发生））。
- 应用程序运行错误信息（应用程序版本、操作系统版本、设备名称、错误描述）。
- 有关 Samsung KNOX 错误的信息（错误代码、无法从其下载文件的 URL）。
- 有关授予应用程序的权限的信息。
- 有关受管理设备上安装的每个应用程序的信息（应用程序名称、安装状态）。
- 有关全球接受最终用户授权许可协议（EULA）的信息：EULA ID、 EULA时间戳、 EULA 文本。
- Google Firebase Cloud Messaging 设置：发件人 ID、设备注册 ID。

- 有关设备公共IP地址的信息。

- 使用 iOS MDM 协议传输的移动设备详细信息。下面列出的数据从移动设备传输到管理服务器：
  - 用于设备识别的移动设备及其组件的技术说明：设备名称、型号、操作系统名称、版本和内部版本号、设备型号、IMEI 号、电话号码、UDID、MEID、序列号、完整和可用内存数量、调制解调器固件版本、蓝牙 MAC 地址、Wi-Fi MAC 地址和 SIM 卡详细信息（作为 SIM 卡 ID 一部分的 ICCID）。
  - 受管理设备使用的移动网络详细信息：移动网络类型、当前使用的移动网络名称、家庭移动网络名称、移动网络操作员设置版本、语音漫游状态、数据漫游状态、家庭网络国家代码、居住国代码、当前使用的网络代码和加密级别。
  - 移动设备的安全设置：密码使用及其与策略设置的合规性、已安装证书、应用和配置文件列表。
  - 与管理服务器的上一次同步日期和时间以及设备管理状态。
- 使用WebRTC协议传输的移动设备数据详情：设备屏幕图像。
- 指定传输到移动设备的文件的详细信息。用户在 Kaspersky Security Center Web Console 界面中输入数据。
- 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卡巴斯基应用程序的设置：卡巴斯基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、卡巴斯基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：与受管理设备上的卡巴斯基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。
  - 卡巴斯基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。
- 将 Kaspersky Security Center Linux 与 SIEM 系统集成以进行事件导出所需的数据。用户在 Kaspersky Security Center Web Console 中输入数据。
- 将 Kaspersky Security Center Linux 与域控制器（Active Directory、Samba、FreeIPA 和 ALD Pro）集成所需的数据。用户将数据输入 Kaspersky Security Center Web Console 中。
- 用于连接 Kerberos 单点登录 (SSO) 的 Keytab 文件。用户将数据输入 Kaspersky Security Center Web Console 中。
- 配置与代理服务器连接互联网所需的数据。用户将数据输入 Kaspersky Security Center Web Console 中。
- 策略和策略配置文件中显示的 Kaspersky Security Center Linux 组件和 Kaspersky 受管理应用程序的设置。用户在 Kaspersky Security Center Web Console 界面中输入数据。
- Kaspersky Security Center Linux 组件和 Kaspersky 受管理应用程序的任务设置。用户在 Kaspersky Security Center Web Console 界面中输入数据。
- 系统管理功能处理的数据。网络代理将以下信息从设备传输到管理服务器：
  - 有关在受管理设备上检测到的硬件的信息（硬件注册表）。
    如果网络代理安装在运行 Windows 的设备上，它会向管理服务器发送有关设备硬件的以下信息：
    - RAM
    - 大容量存储设备
    - 主板
    - CPU
    - 网络适配器
    - 监控器
    - 视频适配器
    - 声卡

    如果网络代理安装在运行 Linux 或 macOS 的设备上，它会向管理服务器发送有关设备硬件的以下信息（如果该信息由操作系统提供）：
    - 总 RAM 容量
    - 大容量存储设备总容量
    - 主板
    - CPU
    - 网络适配器

- 受管理设备上安装的应用程序和补丁的详细信息（应用程序注册表）。应用程序可以与应用程序控制功能在设备上检测到的有关可执行文件的信息进行比较。
- 在受管理设备上检测到的第三方软件中的漏洞的详细信息。
- 受管理设备上安装的第三方应用程序的可用更新的详细信息。

- 在隔离的管理服务器上下载更新以修复受管理设备上的第三方软件漏洞所需的数据。用户使用管理服务器 klscflag 实用程序输入和传输数据。
- 应用程序的用户类别。用户在 Kaspersky Security Center Web Console 界面中输入数据。
- "应用程序控制"功能在受管理设备上检测到的可执行文件的详细信息。受管理应用程序通过网络代理将数据从设备传输到管理服务器。相应应用程序的帮助文件中提供了完整的数据列表。
- 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。
- 自适应异常控制规则的状态和触发的详细信息。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。
- 安装或连接到受管理设备并被"设备控制"功能检测到的外部设备（内存单元、信息传输工具、信息硬拷贝工具和连接总线）的详细信息。受管理应用程序通过网络代理将数据从设备传输到管理服务器。相应应用程序的帮助文件中提供了完整的数据列表。
- 有关加密的 Windows 设备和加密状态的信息。受管理应用程序通过网络代理将数据从设备传输到管理服务器。
- 有关设备上数据加密错误的信息。加密由卡巴斯基应用程序的加密数据功能执行。受管理应用程序通过网络代理将数据从设备传输到管理服务器。相应应用程序的在线帮助中提供了完整的数据列表。
- 受管理可编程逻辑控制器 (PLC) 列表。受管理应用程序通过网络代理将数据从设备传输到管理服务器。相应应用程序的帮助文件中提供了完整的数据列表。
- 创建威胁发展链所需的数据。受管理应用程序通过网络代理将数据从设备传输到管理服务器。相应应用程序的帮助文件中提供了完整的数据列表。
- 有关组织员工尝试访问云服务的信息。受管理应用程序通过网络代理将数据从设备传输到管理服务器。相应应用程序的帮助文件中提供了完整的数据列表。
- Kaspersky Security Center 与 Kaspersky Managed Detection and Response 服务集成（必须安装 Kaspersky Security Center Web Console 专用插件）所需的数据：集成启动令牌、集成令牌和用户会话令牌。用户在 Kaspersky Security Center Web Console 界面中输入集成启动令牌。Kaspersky MDR 服务通过专用插件传输集成令牌和用户会话令牌。
- 将 Kaspersky Security Center Linux 与 Kaspersky Cloud Sandbox 和 Kaspersky Threat Intelligence Portal 集成所需的数据（需要安装 Kaspersky Security Center Web Console 的相应插件）：集成令牌、授权令牌。用户在 Kaspersky Security Center Web Console 界面中输入集成令牌。Kaspersky Security Center Web Console 会将请求中的授权令牌传输到 Kaspersky Cloud Sandbox API。

- 将 Kaspersky Security Center Linux 与 Kaspersky Automated Security Awareness Platform (KASAP) 服务集成所需的数据：用于访问 KASAP Open API 的 API 令牌、URL（通过 Open API 访问 KASAP 的链接）。
- 输入的激活码和密钥文件的详细信息。用户在 Kaspersky Security Center Web Console 界面中输入数据。
- 用户账户：名称、描述、全名、电子邮件地址、主要电话号码、密码、管理服务器生成的 secret key 以及用于双重身份验证的一次性密码。用户在 Kaspersky Security Center Web Console 界面中输入数据。
- 管理对象的修订历史。用户在 Kaspersky Security Center Web Console 界面中输入数据。
- 用户在其上创建修订的设备 IP 地址。IP 地址由管理服务器自动定义。
- 已删除的管理对象的注册表。用户在 Kaspersky Security Center Web Console 界面中输入数据。
- 从文件创建的安装包以及安装设置。用户在 Kaspersky Security Center Web Console 界面中输入数据。
- 在 Kaspersky Security Center Web Console 中显示 Kaspersky 公告所需的数据。用户在 Kaspersky Security Center Web Console 界面中输入数据。
- Kaspersky Security Center Web Console 中的受管理应用程序插件运行所需的数据，以及这些插件在常规运行期间保存在管理服务器数据库中的数据。相应应用程序的帮助文件中介绍了提供数据的描述和方式。
- Kaspersky Security Center Web Console 用户设置：界面的本地化语言和主题、监控面板显示设置、有关通知状态（已读/未读）的信息、电子表格中的列状态（显示/隐藏）、训练模式进度。用户在 Kaspersky Security Center Web Console 界面中输入数据。
- 受管理设备与 Kaspersky Security Center Linux 组件的安全连接的证书。用户使用管理服务器 klsetsrvcert 实用程序输入和传输数据。
- 用于对组织内部 Web 资源建立信任的证书。用户在 Kaspersky Security Center Web Console 界面中输入数据。
- 用户已接受卡巴斯基法律协议条款的信息。
- 用户在 Kaspersky Security Center Web Console 或程序界面 Kaspersky Security Center OpenAPI 中输入的管理服务器数据。
- 用户在 Kaspersky Security Center Web Console 界面中输入的任何数据。

如果应用以下方法之一，则上面列出的数据可以在 Kaspersky Security Center Linux 中显示：

- 用户在 Kaspersky Security Center Web Console 界面中输入数据。
- 网络代理会自动从设备接收数据，并将其传输到管理服务器。
- 网络代理接收由 Kaspersky 受管理应用程序检索的数据，并将其传输到管理服务器。Kaspersky 受管理应用程序处理的数据列表在相应应用程序的帮助文件中提供。
- 管理服务器自行获取有关联网设备的信息，或从被分配充当分发点的网络代理接收数据。
- 通过使用 iOS MDM 协议或者移动协议，数据从移动设备传输到管理服务器。

列出的数据存储在管理服务器数据库中。密码哈希以加密形式存储。

本地处理的所有数据都只能通过 Dump 文件、跟踪文件或 Kaspersky Security Center Linux 组件的日志文件（包括安装程序和实用程序创建的日志文件）传输到 Kaspersky。

Kaspersky Security Center Linux 组件的转储文件、跟踪文件或日志文件包含管理服务器、网络代理和 Kaspersky Security Center Web Console 的任意数据。这些文件可能包含个人或机密数据。Dump 文件、跟踪文件或日志文件以非加密形式存储在设备上。Dump 文件、跟踪文件或日志文件不会自动传输到卡巴斯基，但是管理员可以在技术支持要求下手动传输数据到 Kaspersky 以便解决 Kaspersky Security Center Linux 的表现问题。

Kaspersky 按照法律和相应的 Kaspersky 规则来保护所收到的任何信息。数据均通过安全渠道传输。

单击 Kaspersky Security Center Web Console 中的链接，即表示用户同意自动传输以下数据：

- Kaspersky Security Center Linux 代码
- Kaspersky Security Center Linux 版本
- Kaspersky Security Center Linux 本地化
- 授权许可 ID
- 授权许可类型
- 授权许可是否是通过合作伙伴购买的

通过每个链接提供的数据列表取决于链接的目的和位置。

Kaspersky 以匿名形式使用接收的数据，并且只用于常规统计。摘要统计根据原始收到的信息自动生成，不包含任何个人或机密数据。一旦积累了新数据，就会擦除以前的数据（一年一次）。摘要统计无限存储。

# 关于订阅

*Kaspersky Security Center Linux 订阅*是在所选设置（订阅过期时间、受保护设备数量）下使用程序的订购。您可以和您的服务提供商（例如，互联网提供商）注册您的 Kaspersky Security Center Linux 订阅。订阅可以自动或手动续费，您也可以取消订阅。

订阅可以是限期的（例如，一年）或不限期的。如果要在限期订阅后继续使用 Kaspersky Security Center，您必须续费订阅。无限制订阅如果已经预付给服务提供商了，则会在到期日自动续费。

当受限制订阅过期时，可为您提供一个使产品继续工作的宽限期以便您及时续费。宽限期的可用性和期限由服务提供商提供。

要在订阅下使用 Kaspersky Security Center Linux，您必须应用从服务提供商收到的激活码。

您仅可以在订阅过期后或者取消订阅后为 Kaspersky Security Center Linux 申请不同的激活码。

取决于服务提供商，订阅管理可能的操作也会不同。服务提供商可以不提供订阅宽限期，因此程序会失去它的功能。

订阅激活码无法用于激活 Kaspersky Security Center 的早期版本。

在订阅下使用应用程序时，Kaspersky Security Center Linux 在指定时间间隔自动尝试访问激活服务器，直到订阅过期。如果无法使用系统 DNS 访问服务器，应用程序将使用公共 DNS 服务器。您可以在服务提供商网站续费您的订阅。

# 激活 Kaspersky Security Center Linux

您可以激活 Kaspersky Security Center Linux 以使用其额外的功能。有两种方法可以完成此任务：使用管理服务器快速启动向导或管理服务器属性。

*要激活 Kaspersky Security Center Linux：*

1. 在主菜单中，单击管理服务器名称。

   管理服务器属性窗口将打开。

2. 在“**常规**”选项卡上，选择“**授权许可密钥**”区域。

3. 在**当前授权许可**下，单击**选择**按钮。

4. 在打开的窗口中，选择要用于激活 Kaspersky Security Center Linux 的授权许可密钥。如果未列出授权许可密钥，请单击**添加新授权许可密钥**按钮，然后指定新的授权许可密钥。

5. 如有必要，您还可以添加备用授权许可密钥。为此，请在**备用授权许可密钥**下，单击**选择**按钮，然后选择现有授权许可密钥或添加新授权许可密钥。请注意，如果没有活动授权许可密钥，则无法添加备用授权许可密钥。

6. 单击“**保存**”按钮。

# 受管理卡巴斯基应用程序的授权许可

此部分描述了使用受管理 Kaspersky 应用程序的授权许可密钥时相关的 Kaspersky Security Center 功能。

Kaspersky Security Center Linux 允许您集中为客户端设备上的 Kaspersky 应用程序分发授权许可密钥、监控其使用情况，以及续订授权许可。

使用 Kaspersky Security Center 添加授权许可密钥时，该密钥的设置会保存在管理服务器上。应用程序会根据该信息生成一份授权许可密钥使用情况的报告，并通知管理员密钥属性中指定的授权许可期满日期，以及是否违反此限制。您可以在管理服务器设置内配置授权许可密钥使用情况的通知。

# 受管理应用程序的授权许可

安装到受管理设备上的 Kaspersky 应用程序必须通过将密钥文件或激活码应用到每个应用程序来获得授权。密钥文件或激活码可以按以下方法部署：

- 自动部署
- 受管理应用程序安装包
- 受管理应用程序的“添加授权许可密钥”任务
- 受管理应用程序的手动激活

您可以通过上面列出的任何方法添加新的活动或备用授权许可密钥。卡巴斯基应用程序当前使用一个活动密钥并存储一个备用密钥以在活动密钥到期后应用。您为其添加授权许可密钥的应用程序可定义密钥是活动密钥还是备用密钥。密钥定义不依赖于您用于添加新授权许可密钥的方法。

### 自动部署

如果您使用不同的受管理应用程序，且您必须将特定密钥文件或激活码部署到设备，请选择其他方法部署激活码或密钥文件。

Kaspersky Security Center 允许您自动部署可用授权许可密钥到设备。例如，三个授权许可密钥被存储在管理服务器存储库。您已对所有三个授权许可密钥启用了**自动分发的授权许可密钥**。Kaspersky 安全应用程序—例如，Kaspersky Endpoint Security for Linux— 被安装到组织设备。发现必须部署授权许可密钥的新设备。应用程序决定，例如，存储库中的两个授权许可密钥可以被部署到设备：授权许可密钥 *Key_1*和授权许可密钥 *Key_2*。这些授权许可密钥之一被部署到设备。此种情况下，无法预见两个授权许可密钥中的哪个将被部署到设备，因为自动部署授权许可密钥不提供给任何管理员活动。

当部署授权许可密钥时，设备为该授权许可密钥重新计算。您必须确保部署授权许可密钥的设备数量不超过授权许可限制。如果设备数量超过授权许可限制，所有不被授权许可覆盖的设备将被分配*严重*状态。

部署之前，密钥文件或激活码必须添加到管理服务器存储库。

说明：

- 添加授权许可密钥到管理服务器存储库
- 自动分发授权许可密钥

请注意，在以下情况下，自动分发的授权许可密钥可能不会显示在虚拟管理服务器存储库中：

- 授权许可密钥对于应用程序无效。
- 虚拟管理服务器没有受管理设备。
- 授权许可密钥已用于由另一个虚拟管理服务器管理的设备，并且已达到设备数量限制。

### 添加密钥文件或激活码到受管理应用程序安装包

对于安全应用程序，该选项不被推荐。添加到安装包的密钥文件或激活码可能被盗用。

如果您使用安装包安装受管理应用程序，您可以在该安装包中或在应用程序策略中指定激活码或密钥文件。授权许可密钥将在下一次设备与管理服务器同步时被部署到受管理应用程序。

操作说明：将授权许可密钥添加到安装包

通过为受管理应用程序添加授权许可密钥任务来进行部署

如果您选择使用为受管理应用程序添加授权许可密钥任务，您可以选择要部署到设备的授权许可密钥并以任何便捷的方法选择设备–例如，通过选择管理组或设备分类。

部署之前，密钥文件或激活码必须添加到管理服务器存储库。

说明：

- 添加授权许可密钥到管理服务器存储库
- 部署授权许可密钥到客户端设备

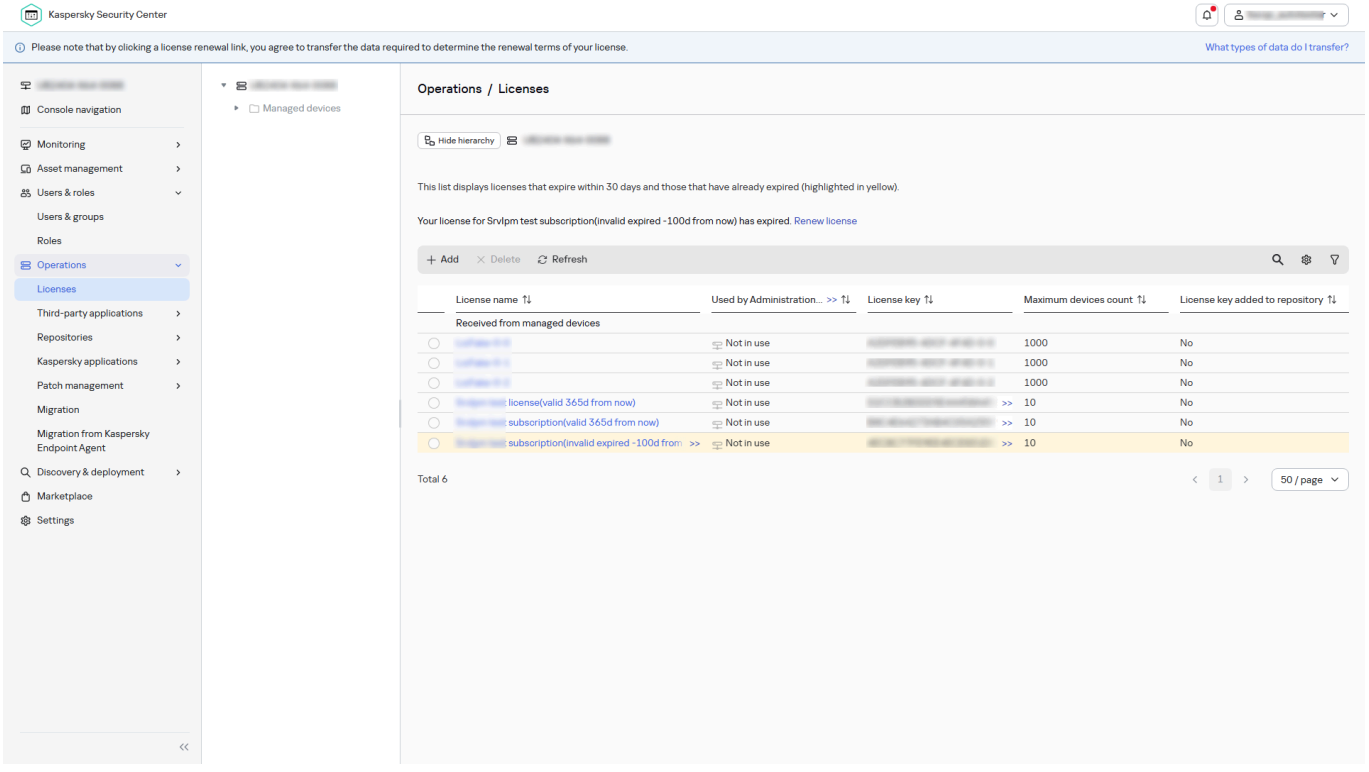
手动添加激活码或密钥文件到设备

您可以激活本地安装的 Kaspersky 应用程序，通过使用应用程序界面提供的工具。请参考已安装应用程序的文档。

# 添加授权许可密钥到管理服务器存储库

*要添加授权许可密钥到管理服务器存储库：*

1. 在主菜单中，转到“**操作**”→“**授权许可**”。



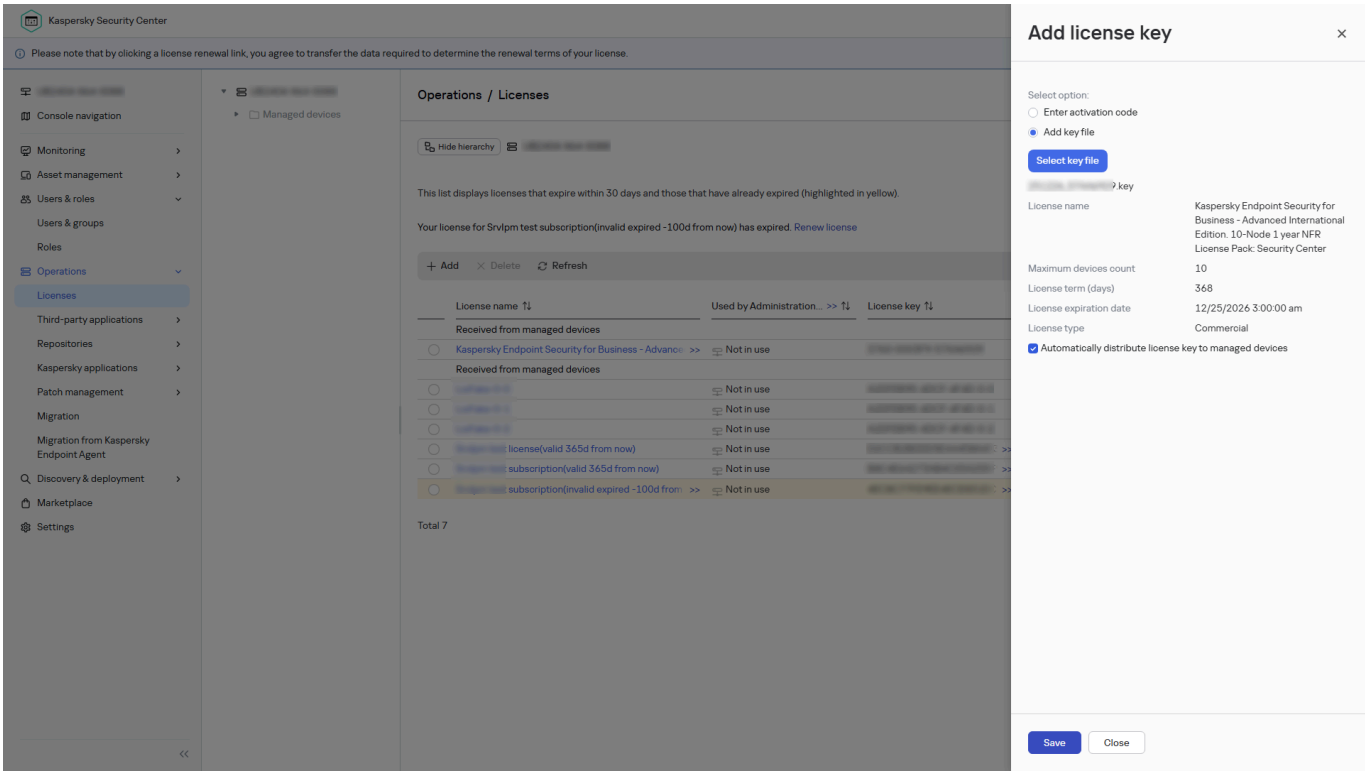

添加的卡巴斯基授权许可列表

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。




通过应用密钥文件添加授权许可密钥

- **输入激活码**

  在文本字段指定激活码并单击“**发送**”按钮。

4. 单击“**关闭**”按钮。

授权许可密钥或几个授权许可密钥被添加到管理服务器存储库。

# 部署授权许可密钥到客户端设备

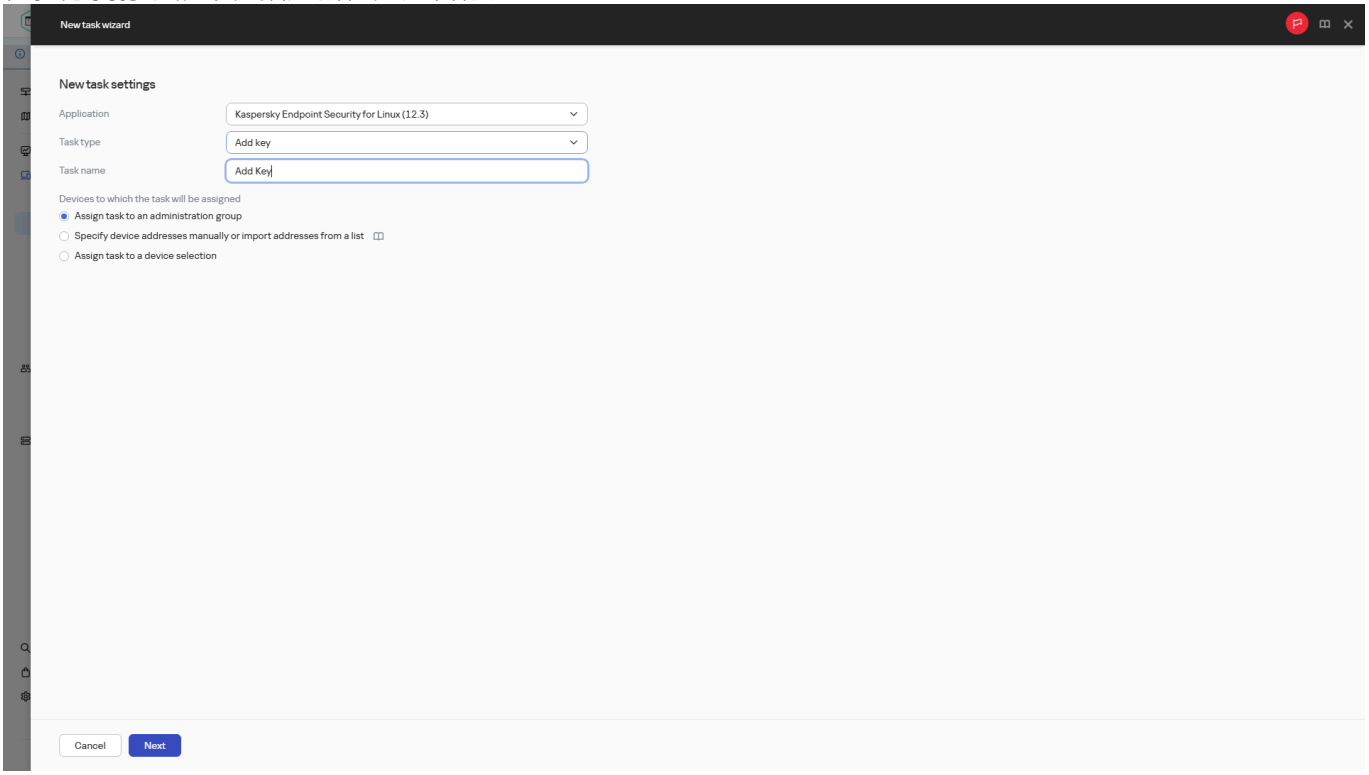
Kaspersky Security Center Web Console 允许您自动或通过“**应用程序激活**”任务将授权许可密钥分发至客户端设备。您可以使用该任务将密钥分发给特定的设备组。在通过任务分发授权许可密钥过程中，不考虑授权许可对设备数量的限制。当达到许可限制时，使用自动密钥分发自动停止授权许可密钥的分发。

如果您启用自动分发授权许可密钥，请不要创建**应用程序激活**任务来将该密钥分发给客户端设备。否则，由于频繁同步会增加管理服务器的负载。

在部署之前，请将授权许可密钥添加到管理服务器存储库。

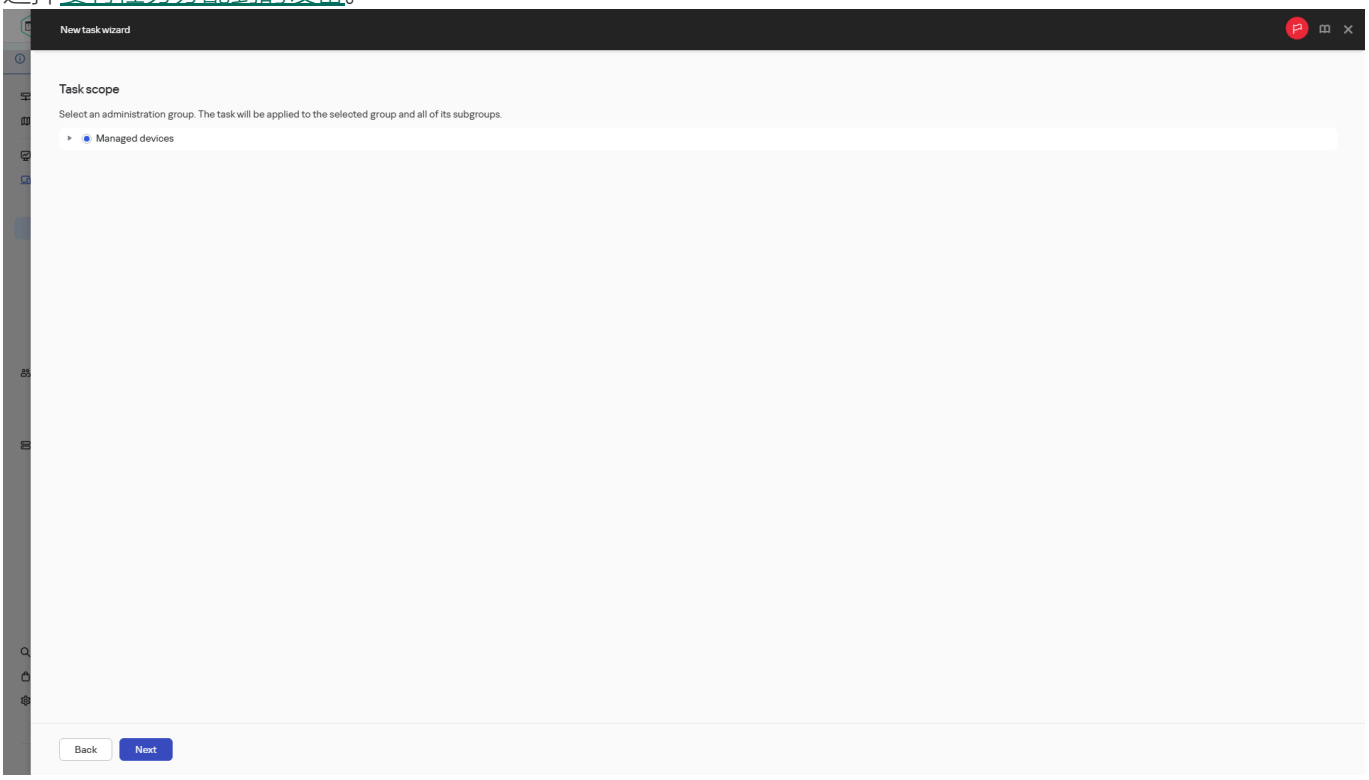
*要通过**应用程序激活**任务将授权许可密钥分发到客户端设备：*

1. 在主菜单中，转到“**任务**”。
2. 单击**添加**。
   “**新任务向导**”启动。使用“**下一步**”按钮进行向导。
3. 在**应用程序**下拉列表中，选择要为其添加授权许可密钥的应用程序。
4. 在**任务类型**列表中选择**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。




创建“添加密钥”任务

6. 选择要将任务分配到的设备。




指定任务范围

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**应用程序激活**任务之前未将授权许可密钥添加到管理服务器存储库时，才需要添加授权许可密钥。

- 选择**输入激活码**选项以输入激活码，然后执行以下操作：

  a. 指定激活码，然后单击**发送**按钮。

  有关授权许可密钥的信息将显示在密钥添加窗格中。

  b. 单击“**保存**”按钮。

  > 如果您想要自动将授权许可密钥分发到受管理设备，请启用**自动分发授权许可密钥到受管理设备**选项。

  密钥添加窗格将关闭。

- 选择**添加密钥文件**选项以添加密钥文件，然后执行以下操作：

  a. 单击**选择密钥文件**按钮。

  b. 在打开的窗口中，选择一个密钥文件，然后单击“**打开**”按钮。

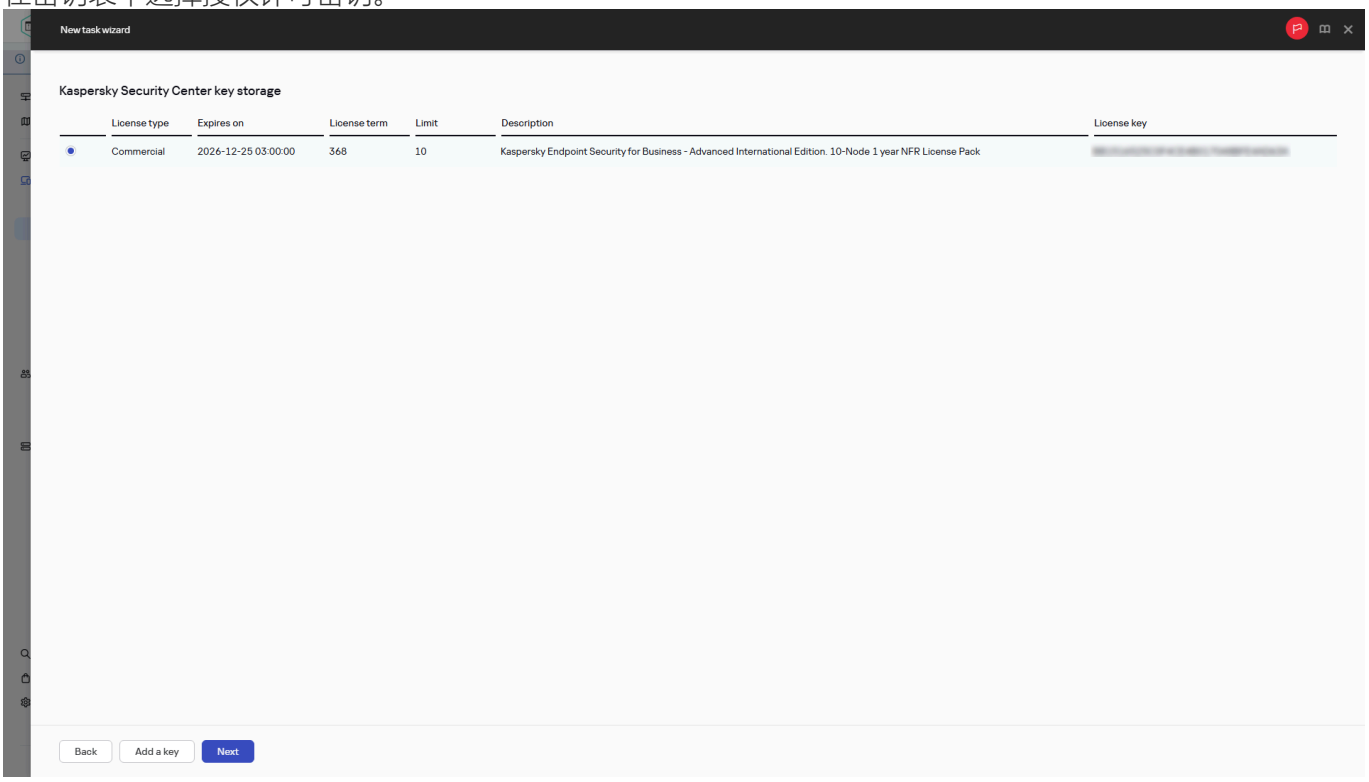
  有关授权许可密钥的信息将显示在授权许可密钥添加窗格中。

  c. 单击“**保存**”按钮。

如果您想要自动将授权许可密钥分发到受管理设备，请启用**自动分发授权许可密钥到受管理设备**选项。

密钥添加窗格将关闭。

9. 在密钥表中选择授权许可密钥。

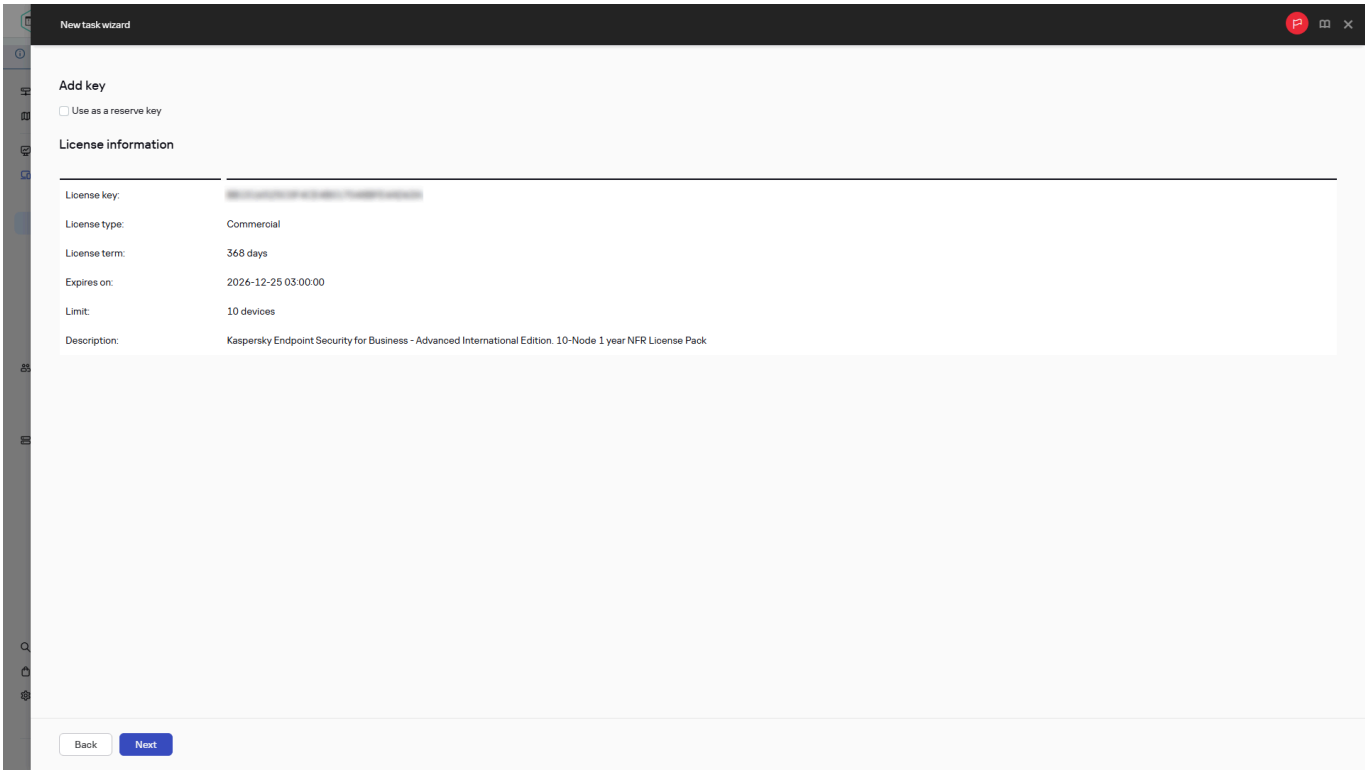



选择授权许可密钥

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。




指定备用授权许可密钥

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。

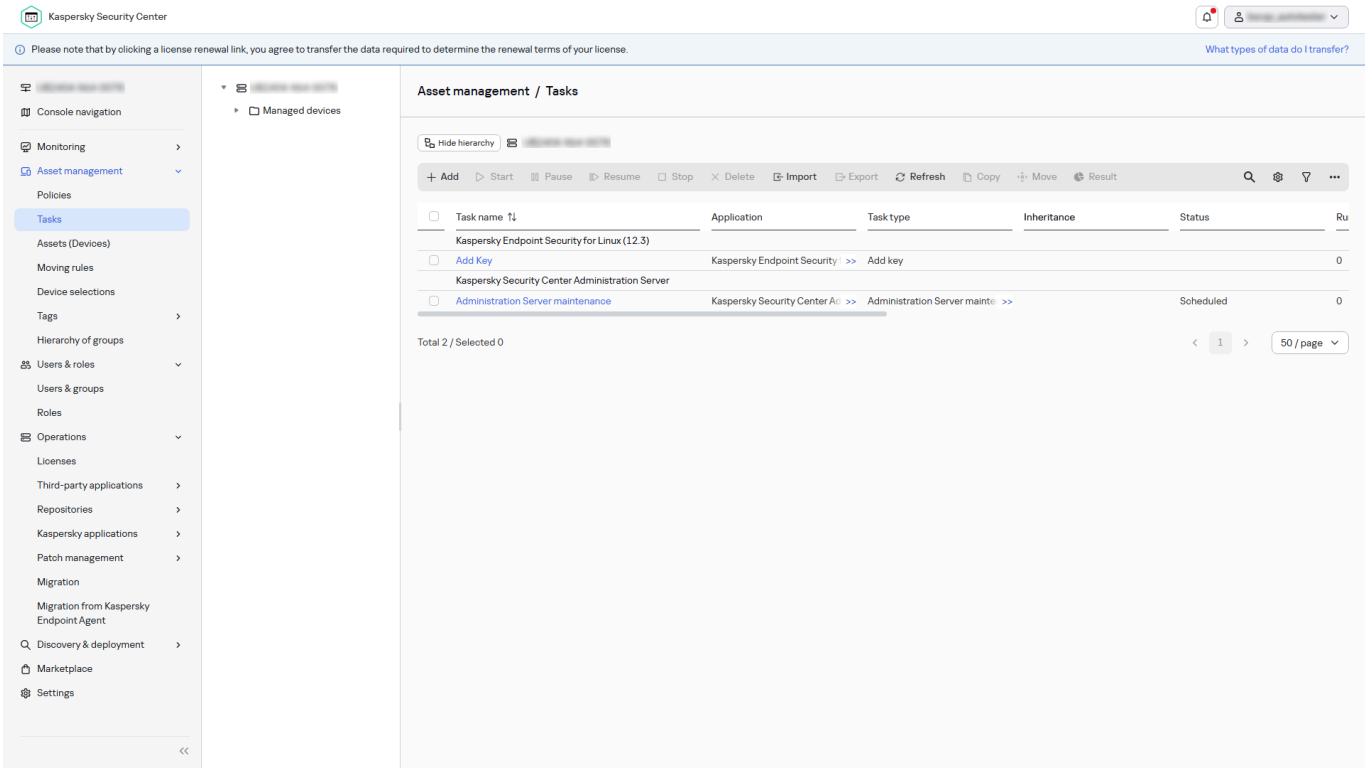
    如果您不启用该选项，任务将使用默认设置创建。您可以稍后修改默认设置。

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。




任务列表

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。

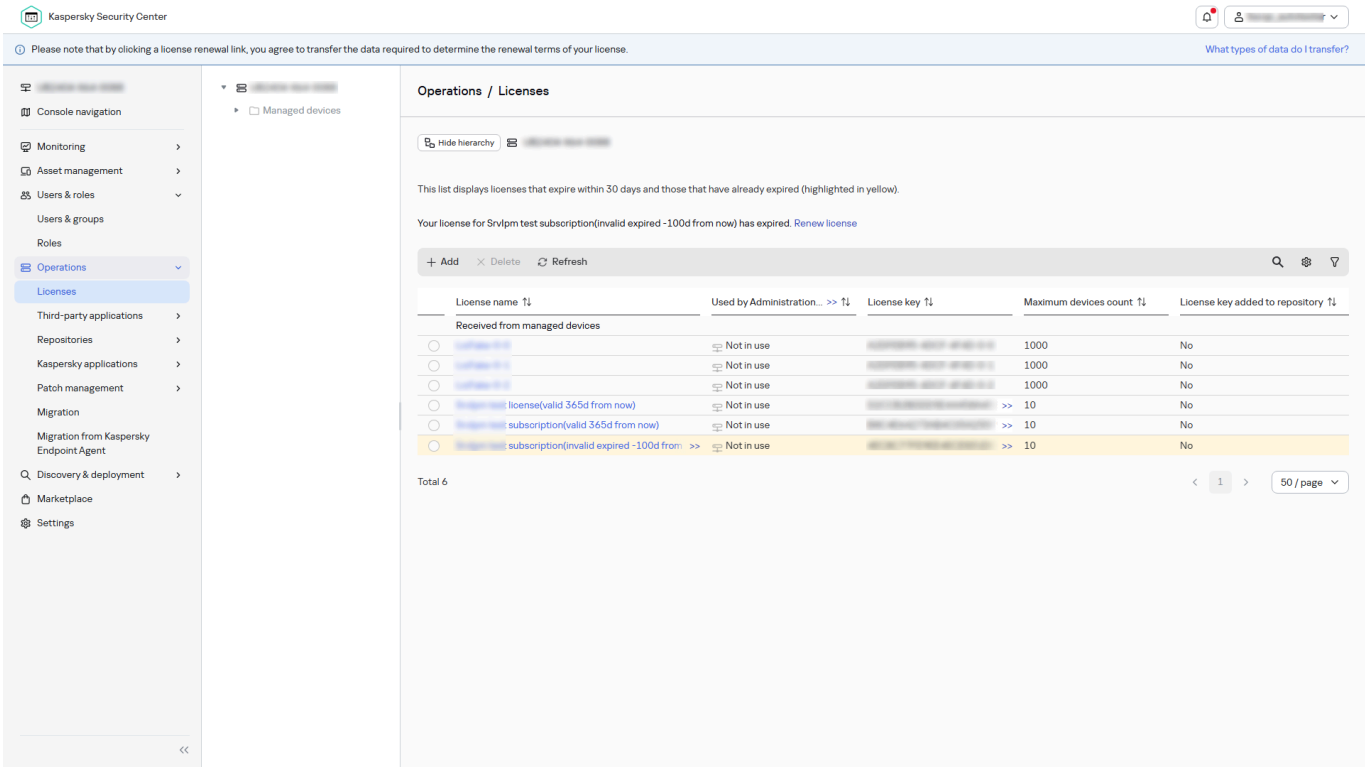
当任务完成时，授权许可密钥将被部署到所选设备。

# 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：*

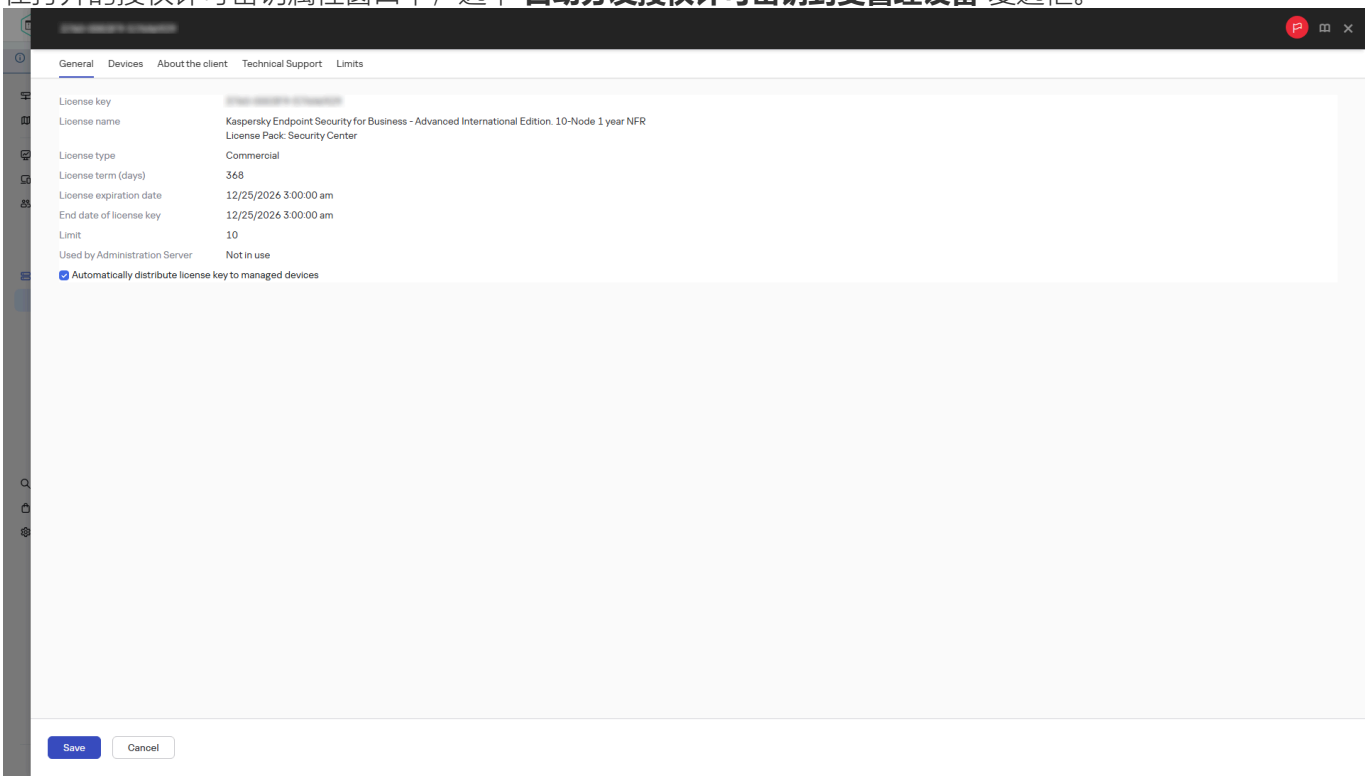
1. 在主菜单中，转到“**操作**” → “**授权许可**” → “**授权许可**”。




授权许可列表

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。




授权许可密钥属性窗口

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**” → “**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**” → “**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
- 在**限制**选项卡上 — 授权许可限制列表

  如果您在 Kaspersky Next XDR Optimum 授权许可下激活了管理服务器，则**限制** 选项卡显示具有**已启用**值的 **XDR-O**字段。

*要查看哪些授权许可密钥被部署到特定客户端设备：*

1. 在主菜单中，转到 “**资产管理**” → “**资产(设备)**”。
2. 点击所需设备的名称。
3. 在打开的设备属性窗口中，选择“**应用程序**”选项卡。
4. 点击您要查看其授权许可密钥信息的应用程序名称。
5. 在打开的应用程序属性窗口中，选择“**常规**”选项卡，然后打开“**授权许可**”区域。

将显示有关活动和备用授权许可密钥的主要信息。

为了定义虚拟管理服务器授权许可密钥的最新设置，管理服务器每天至少发送一次请求到 Kaspersky 激活服务器。如果无法使用系统 DNS 访问服务器，应用程序将使用公共 DNS 服务器。

# 超出了授权许可限制事件

Kaspersky Security Center Linux 允许您获取客户端设备上安装的 Kaspersky 应用程序的授权许可达到限制的事件信息。

授权许可达到限制的此类事件的重要级别根据以下规则定义：

- 如果当前使用单一授权许可的单元的数量达到该授权许可所覆盖的单元总数的 90% 和 100% 之间，事件等级就是**信息**重要级别。
- 如果当前使用单一授权许可的单元的数量达到该授权许可所覆盖的单元总数的 100% 和 110% 之间，事件等级就是**警告**重要级别。
- 如果当前使用单一授权许可的单元的数量超过该授权许可所覆盖的单元总数的 110%，事件等级就是**严重事件**重要级别。

# 从存储库删除授权许可密钥

当您删除部署到受管理设备上的活动授权许可密钥时，应用程序将继续工作在受管理设备。

*要从管理服务器存储库中删除密钥文件或激活码：*

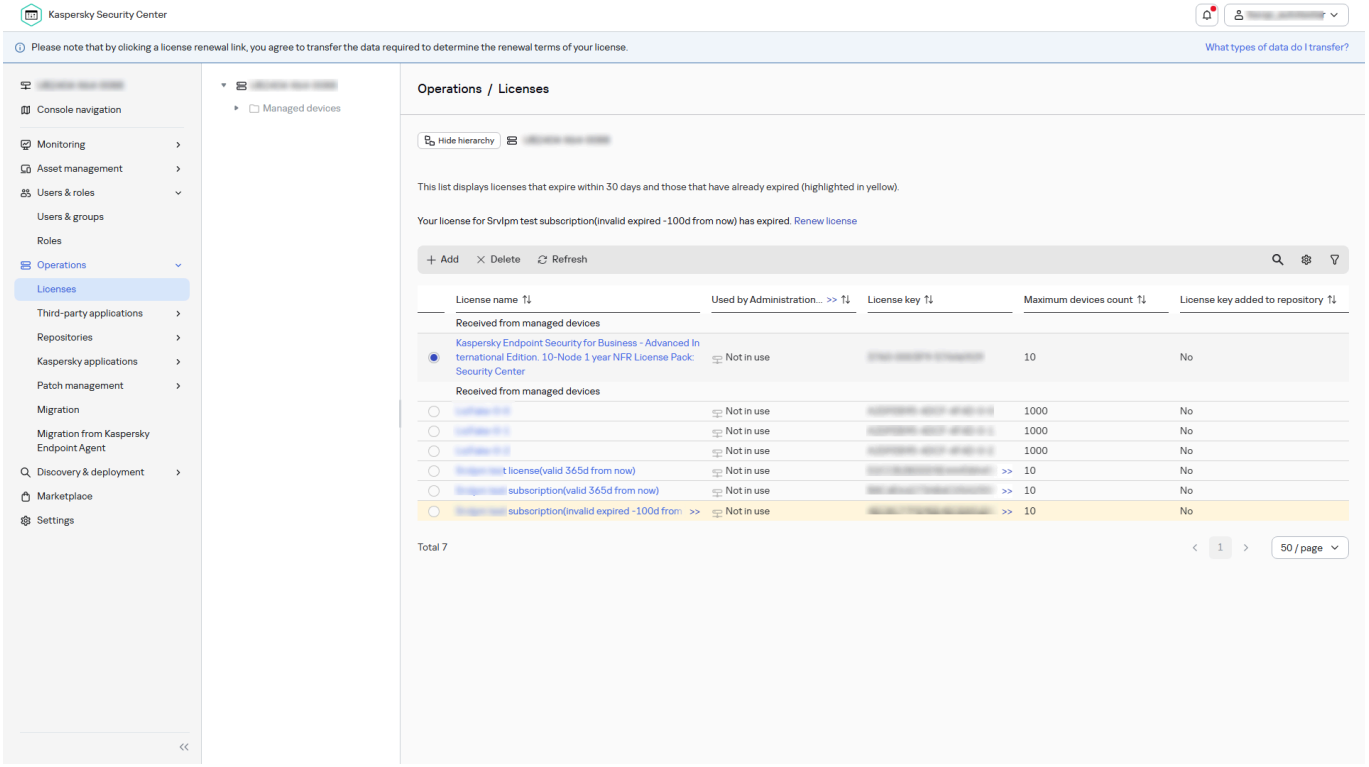
1. 检查管理服务器未使用您要删除的密钥文件或激活码。如果管理服务器使用了该密钥，则您无法删除该密钥。要执行检查：
   a. 在主菜单中，单击管理服务器名称。
      管理服务器属性窗口将打开。

b. 在“**常规**”选项卡上，选择“**授权许可密钥**”区域。

c. 如果所需的密钥文件或激活码显示在打开的区域中，请单击“**删除活动授权许可密钥**”按钮，然后确认操作。之后，管理服务器不再使用删除的授权许可密钥，但该密钥仍保留在管理服务器存储库中。如果所需的密钥文件或激活码未显示，管理服务器不会使用该密钥文件或激活码。

2. 在主菜单中，转到“**操作**”→“**授权许可**”→“**授权许可**”。

3. 选择所需的密钥文件或激活码，然后单击**删除**按钮。




授权许可列表

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。

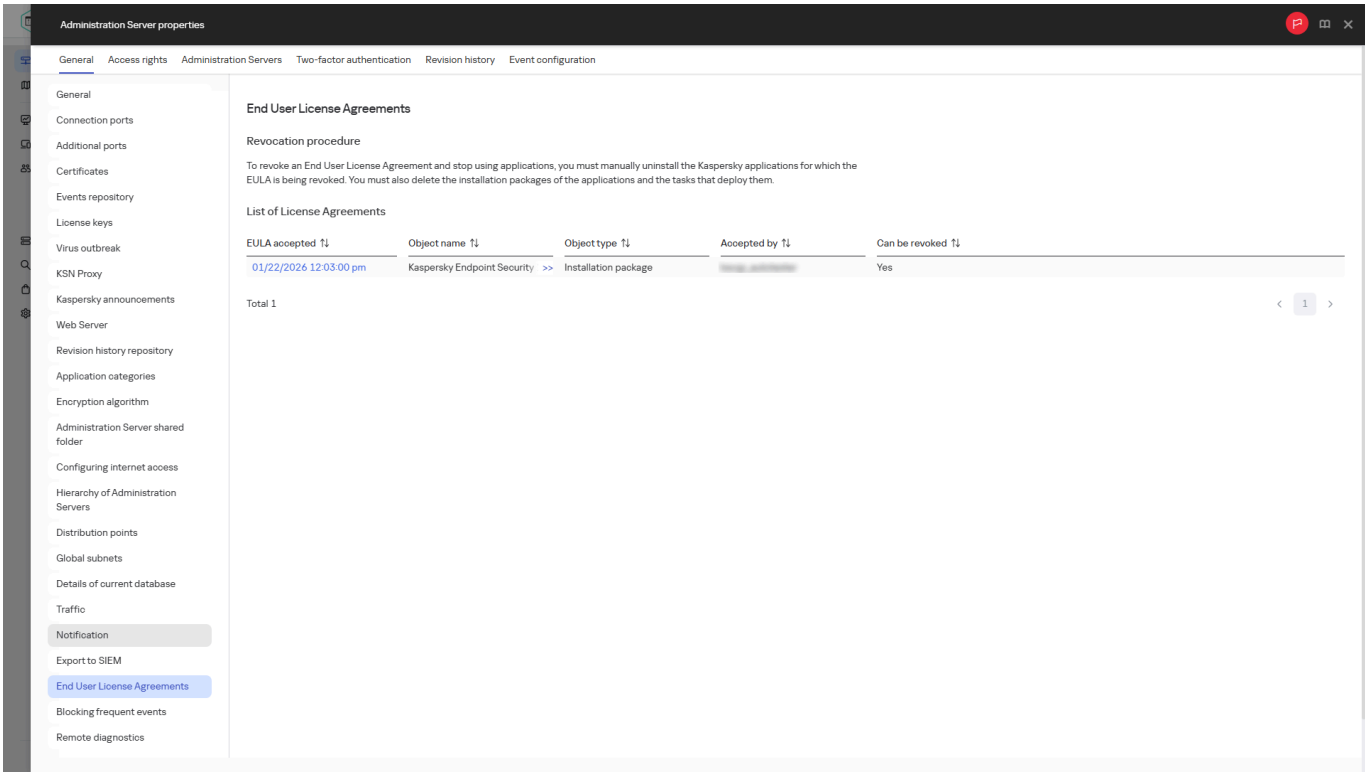
# 撤销对最终用户授权许可协议的同意

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。




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**”→“**授权许可**”。
   - 在主菜单中，转到“**监控**”→“**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。

   “**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 Linux 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 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。选择解决方案后，Kaspersky Security Center Linux 会将您重定向到 Kaspersky 网站上的相关网页，以了解有关该解决方案的更多信息。每个网页都可让您继续购买或包含有关购买过程的说明。

在“**市场**”区域中，可以使用以下条件筛选 Kaspersky 解决方案：

- 要保护的设备（端点、服务器和其他类型的资产）数量：
  - 50–250
  - 250–1000
  - 大于 1000
- 组织的信息安全团队的成熟度：
  - **基础**
    这是只有一个 IT 团队的企业的典型成熟度。自动阻止最大可能数量的威胁。
  - **最佳**
    这是在 IT 团队内具有特定 IT 安全功能的企业的典型成熟度。在此级别，所需的解决方案使公司能够应对商品威胁以及绕过现有预防机制的威胁。
  - **专家**
    这是具有复杂和分布式 IT 环境的企业的典型成熟度。IT 安全团队成熟或者公司拥有 SOC（安全运营中心）团队。所需的解决方案使公司能够应对复杂威胁和针对性攻击。
- 您要保护的资产类型：
  - **端点**：员工的工作站、物理机和虚拟机、嵌入式系统
  - **服务器**：物理和虚拟服务器
  - **云**：公有、私有或混合云环境；云服务
  - **网络**：局域网、IT 基础设施
  - **服务**：Kaspersky 提供的安全相关服务

*要查找和购买 Kaspersky 商业解决方案：*

1. 在主菜单中，转到“**市场**”。
   默认情况下，该区域显示所有可用的 Kaspersky 商业解决方案。
2. 要仅查看适合您组织的解决方案，请在筛选器中选择所需的值。
3. 点击您要购买或想要了解更多信息的解决方案。

您将被重定向到解决方案网页。您可以按照屏幕上的说明进行购买。

# 配置卡巴斯基应用程序

本部分包含有关手动配置策略和任务、用户角色、构建管理组结构和任务层级的信息。

# 方案：配置网络保护

快速启动向导使用默认设置创建策略和任务。这些设置可能不是最佳的，甚至是组织不允许的。因此，我们建议您微调这些策略和任务并，然后建其他策略和任务（如果它们对于您的网络而言是必需的）。

## 先决条件

在您开始之前，确保您已做了如下：

- 安装了 Kaspersky Security Center Linux 管理服务器
- 安装了 Kaspersky Security Center Web Console
- 完成了 Kaspersky Security Center Linux 主安装方案
- 完成了快速启动向导，或在“**受管理设备**”管理组中手动创建了以下策略和任务：
  - Kaspersky Endpoint Security 策略
  - 更新 Kaspersky Endpoint Security 的组任务
  - 网络代理策略
  - *查找漏洞和所需更新*任务

## 阶段

分阶段配置网络保护：

1. **设置和传播卡巴斯基应用程序策略和策略配置文件**

   要为安装在受管理设备上的 Kaspersky 应用程序配置和传播设置，您可以使用两种不同的安全管理方法—以设备为中心或以用户为中心。这两种方法可以被合并。

2. **配置任务以远程管理 Kaspersky 应用程序**

   检查使用快速启动向导创建的任务并按需要调整它们。

   操作说明：设置用于更新 Kaspersky Endpoint Security 的组任务、创建“查找漏洞和所需更新”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，您将通过配置卡巴斯基应用程序、任务以及管理服务器接收的事件来保护您的网络：

- 卡巴斯基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一种或两者组合。

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–具有自己的卡巴斯基应用程序设置配置。设置配置定义了哪些应用程序设置可以被用户更改以及哪些被强制设置并被管理员锁定。

通过使用以用户为中心的安全管理，您可以应用特别应用程序设置到单个用户。这可能用在员工在公司有独一角色或您要监控与个别人的设备相关的安全问题时。取决于该员工在公司的角色，您可以扩展或限制该员工更改应用程序设置的权限。例如，您可能要扩展在本地办公室管理客户端设备的系统管理员的权限。

您也可以组合以设备为中心的安全管理和以用户为中心的安全管理方法。例如，您可以为每个管理组配置特定的应用程序策略，然后为企业的一个或几个用户角色创建策略配置文件。此种情况下，策略和策略配置文件按照以下优先级进行应用：

1. 为以设备为中心的安全管理创建的策略被应用。
2. 它们根据策略配置文件属性被策略配置文件修改。
3. 策略被与用户角色关联的策略配置文件修改。

# 策略设置和传播：以设备为中心的方法

当您完成该方案后，应用程序将在所有受管理设备上被配置，与您定义的应用程序策略和策略配置文件一致。

## 先决条件

在开始之前，确保已安装 Kaspersky Security Center Linux 管理服务器和 Kaspersky Security Center Web Console。您也可能要考虑以用户为中心的安全管理作为以设备为中心的方案的附加选项。了解更多两个管理方法的详情。

## 阶段

以设备为中心的卡巴斯基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卡巴斯基应用程序设置。策略集将被传播到客户端设备。

   当您在快速启动向导中配置网络保护时，Kaspersky Security Center Linux 为以下应用程序创建默认策略：

   - Kaspersky Endpoint Security for Linux——适用于基于 Linux 的客户端设备
   - Kaspersky Endpoint Security for Windows——适用于基于 Windows 的客户端设备

   如果您通过使用该向导完成了配置过程，您不必为该应用程序创建新策略。

   如果您有几个管理服务器和/或管理组的层级结构，从属管理服务器和子管理组默认从主管理服务器继承策略。您可以强制子组和从属管理服务器的继承以防止上游策略设置的修改。如果您仅要一部分设置被强制继承，您可以在上游策略中锁定它们。剩余未锁定的设置将可以在下流策略中修改。创建的策略层级将允许您有效管理管理组中的设备。

   说明：创建一个策略

2. **创建策略配置文件（可选）**

   如果您想让单一管理组中的设备在不同策略设置下运行，为这些设备创建策略配置文件。策略配置文件是策略设置的命名子集。该子集随带策略在大设备上分发，在特别条件*配置文件激活条件*下将其补充。配置文件仅包含与"基本"策略不同的设置，并在受管理设备上活动。

   通过使用配置文件激活条件，例如，您可以将不同的策略配置文件应用到具有特定硬件配置或标记了特定标签的设备。使用标签筛选满足特别标准的设备。例如，您可以创建名为 *CentOS* 的标签，使用该标签标记所有运行 CentOS 操作系统的设备，然后指定该标签作为策略配置文件激活条件。结果，安装在所有 CentOS 设备上的卡巴斯基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卡巴斯基应用程序。

   您可以检查策略和策略配置文件是否被传送到了设备。Kaspersky Security Center Linux 在设备属性中指定传送日期和时间。

   说明：强制同步

### 结果

当以设备为中心的方案完成时，卡巴斯基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

本部分介绍以用户为中心的集中配置安装到受管理设备上的卡巴斯基应用程序的方案。当您完成该方案后，应用程序将在所有受管理设备上被配置，与您定义的应用程序策略和策略配置文件一致。

### 先决条件

在开始之前，确保已成功安装 Kaspersky Security Center Linux 管理服务器和 Kaspersky Security Center Web Console，并已完成主要部署方案。您也可能要考虑以设备为中心的安全管理作为以用于为中心的方案的附加选项。了解更多两个管理方法的详情。

### 过程

以用户为中心的卡巴斯基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卡巴斯基应用程序设置。策略集将被传播到客户端设备。

   当您在快速启动向导配置您网络的保护时，Kaspersky Security Center Linux 为 Kaspersky Endpoint Security 创建默认策略。如果您通过使用该向导完成了配置过程，您不必为该应用程序创建新策略。

   如果您有几个管理服务器和/或管理组的层级结构，从属管理服务器和子管理组默认从主管理服务器继承策略。您可以强制子组和从属管理服务器的继承以防止上游策略设置的修改。如果您仅要一部分设置被强制继承，您可以在上游策略中锁定它们。剩余未锁定的设置将可以在下流策略中修改。创建的策略层级将允许您有效管理管理组中的设备。

   说明：创建一个策略

2. **指定设备所有者**

   分配受管理设备到对应用户。

   说明：指派用户作为设备所有者

3. **为您的企业定义用户角色**

   联想您企业的员工所做的不同工作。您必须根据他们的角色划分所有员工。例如，您可以按照部门、专业或职位划分他们。之后，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卡巴斯基应用程序。

   说明：关联策略配置文件到角色

8. **传播策略和策略配置文件到受管理设备**

   默认下，Kaspersky Security Center Linux 每 15 分钟自动同步管理服务器与受管理设备。同步过程中，新的或更改的策略和策略配置文件被传播到受管理设备。您可以避免自动同步并通过使用强制同步命令手动运行同步。一旦同步完成，策略和策略配置文件被传送和应用到安装的卡巴斯基应用程序。

   您可以检查策略和策略配置文件是否被传送到了设备。Kaspersky Security Center Linux 在设备属性中指定传送日期和时间。

   说明：强制同步

## 结果

当以用户为中心的方案完成时，卡巴斯基应用程序根据指定的设置被配置并通过策略和策略配置文件层级传播。

对于新用户，您将必须创建新账户，分配一个创建的用户角色，并分配设备到用户。配置的应用程序策略和策略配置文件将被自动应用到该用户的新设备。

# 策略和策略配置文件

在 Kaspersky Security Center Web Console 中，可以为 Kaspersky 应用程序创建策略。该部分描述了策略和策略配置文件，并提供创建和修改它们的说明。

# 关于策略和策略配置文件

*策略*是应用于一个管理组和其子组的卡巴斯基应用程序设置集。您可以在管理组的设备上安装多个 Kaspersky 应用程序。Kaspersky Security Center 为管理组中的每个卡巴斯基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卡巴斯基应用程序，只能有一个策略处于活动状态。设备对卡巴斯基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：

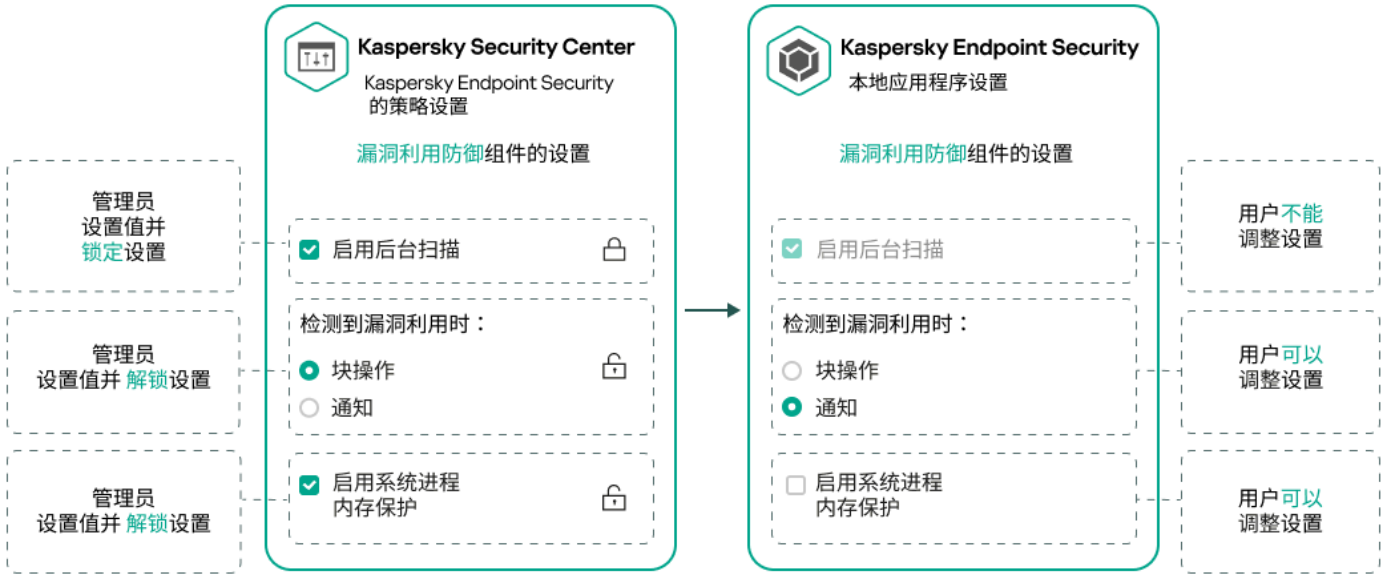
- 锁定管理子组策略的设置
- 在受管理设备上锁定本地卡巴斯基应用程序的设置

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：

- 受管理设备将应用卡巴斯基应用程序的设置值。
- 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，受管理设备上的卡巴斯基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）：




锁定和卡巴斯基应用程序设置

# 策略继承和策略配置文件

本部分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

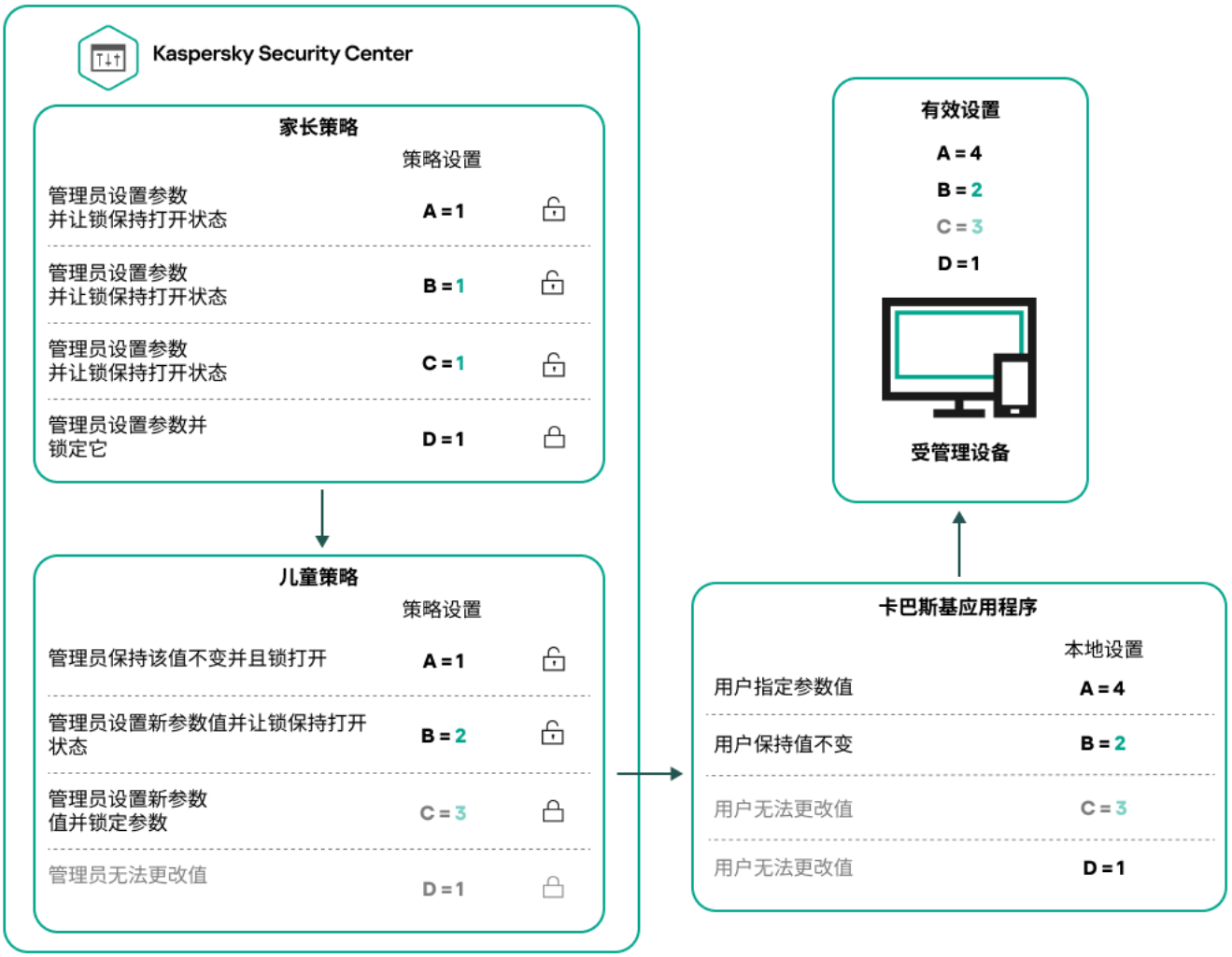
如果不同的设备需要不同的设置，则可以将设备组织到管理组中。

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）。

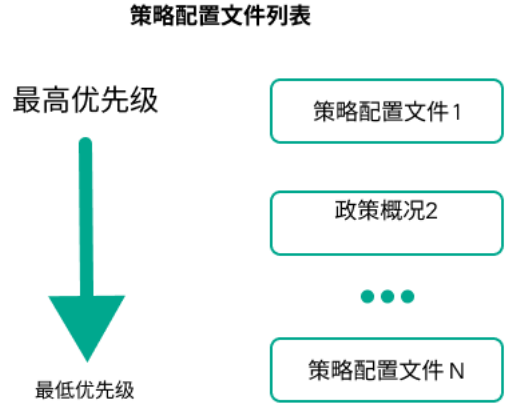



策略层级

# 策略层级中的策略配置文件

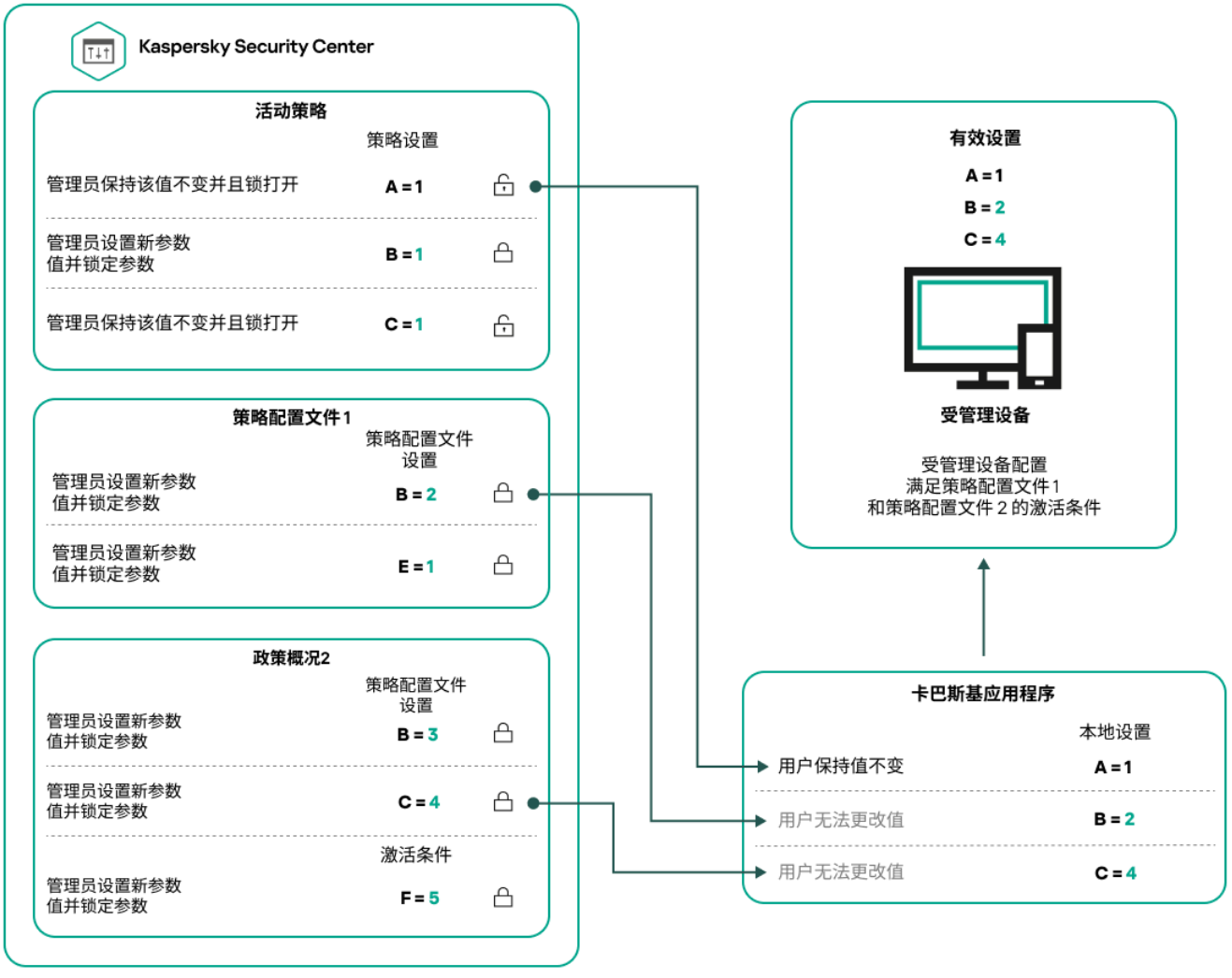
策略配置文件具有以下优先级分配条件：

- 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）。

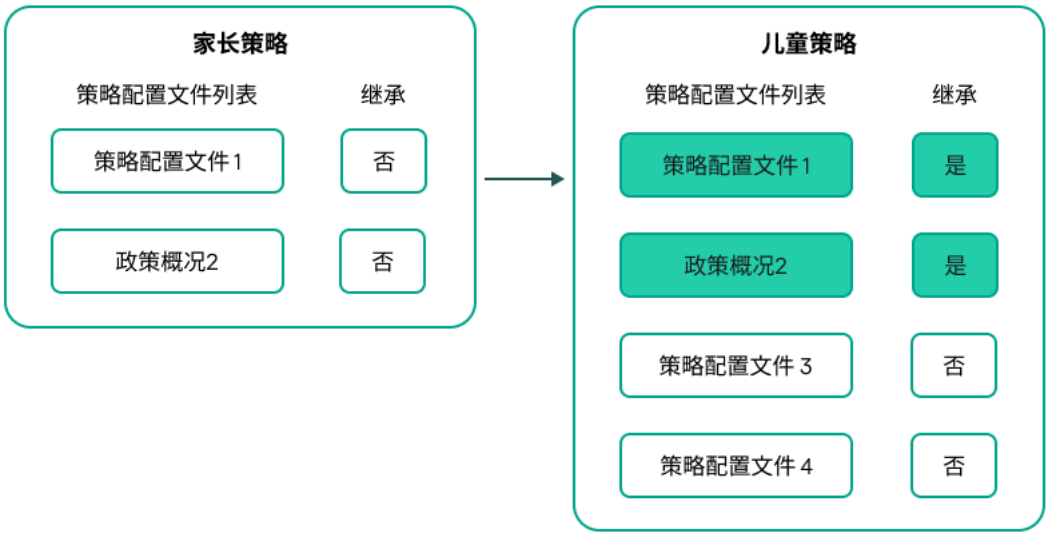



受管理设备配置满足多个策略配置文件的激活条件

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）。

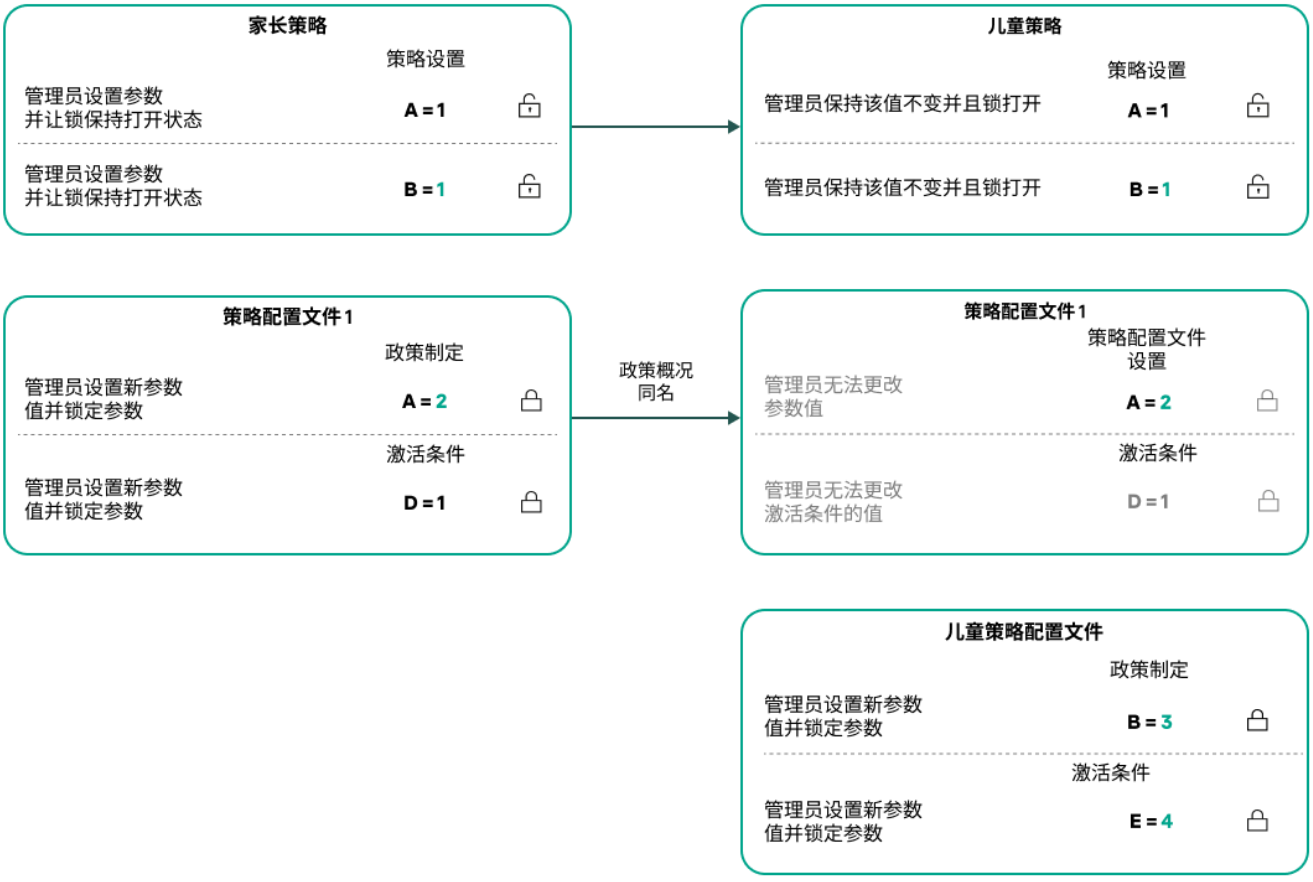



继承策略配置文件

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

本部分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“**资产管理**”→“**组层级**”。
2. 在管理组结构中，选择您要查看其策略列表的管理组。

   策略列表以表格格式出现。如果没有策略，表格为空。您可以显示或隐藏表格的列，更改它们的顺序，仅查看包含指定值的行，或者使用查找。

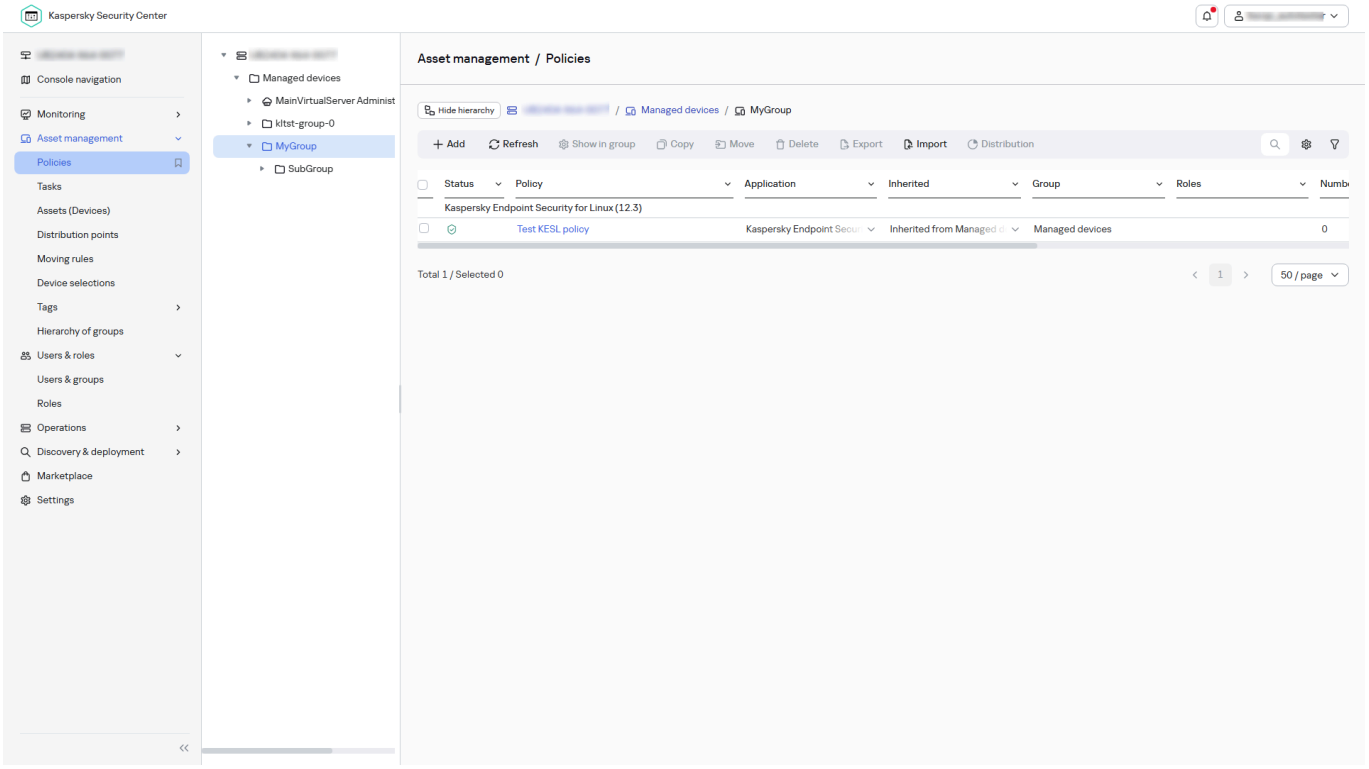
## 创建策略

您可以创建策略；您也可以修改和删除现有策略。

*要创建策略：*

1. 在主菜单中，转到“**资产管理**”→“**策略**”。
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. 单击页面顶部的“**显示层级**”按钮。
     按钮名称将更改为“**隐藏层级**”。
     b. 在打开的窗口中，单击带有所需子组的名称。

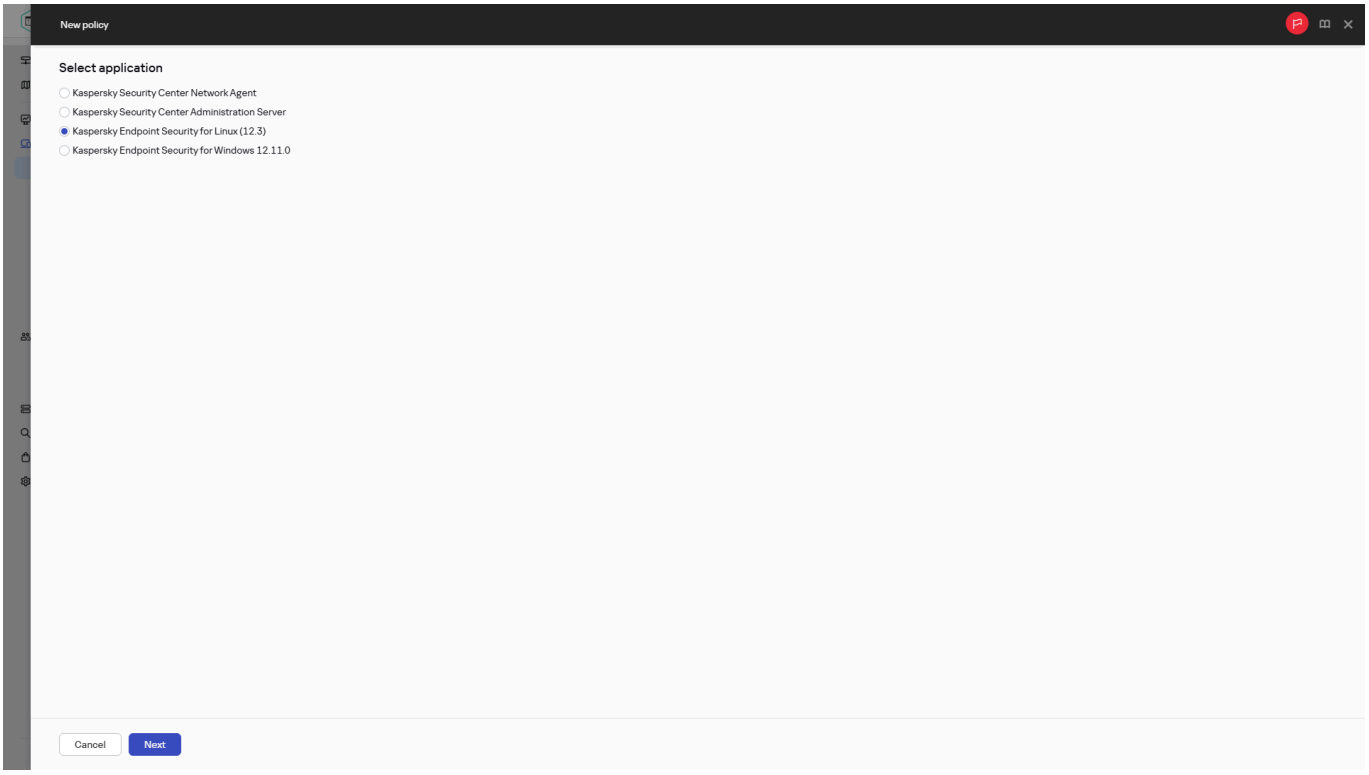
所选组的路径显示在页面顶部。如果需要，您可以单击带有管理组名称的链接前往该组。默认情况下，路径中的最后一个链接不活动。您也可以单击“**隐藏层级**”按钮关闭层次结构窗口。




策略列表

3. 单击**添加**。

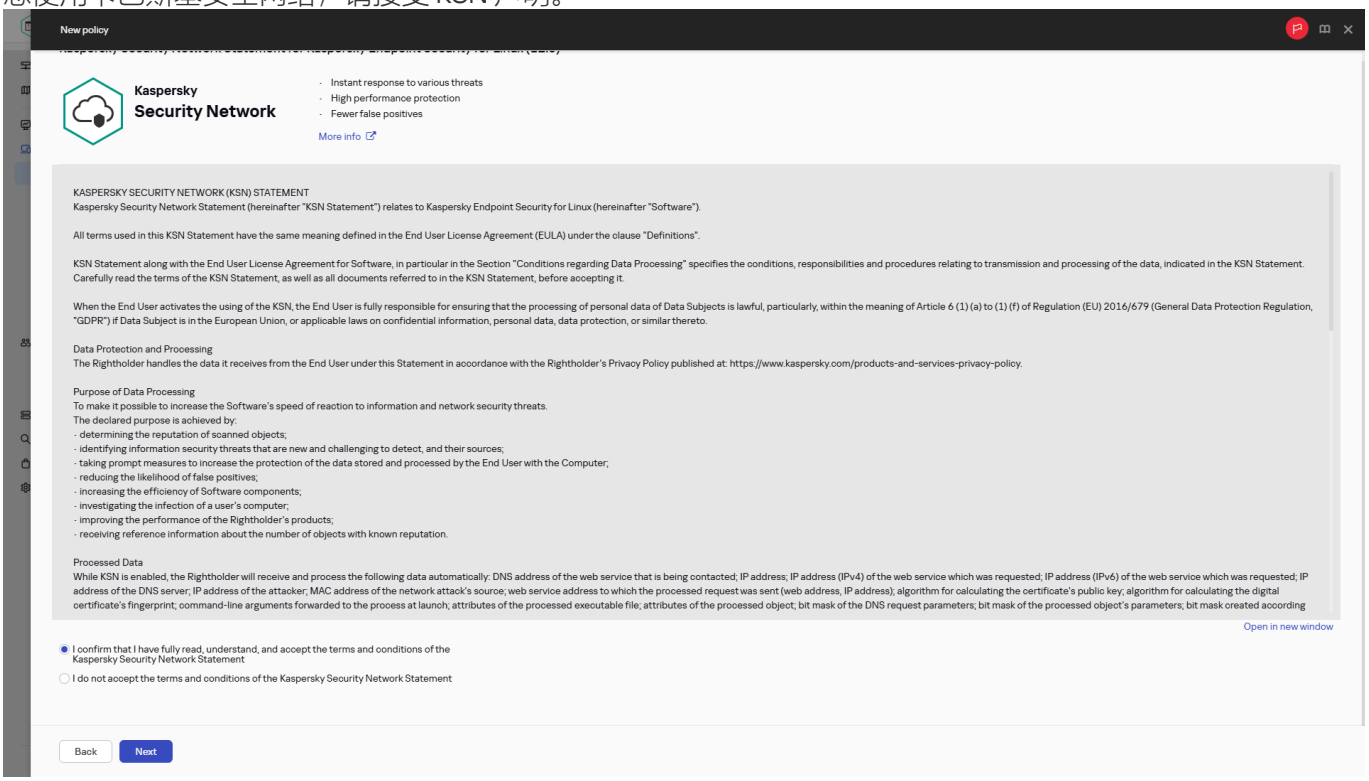
“**选择应用程序**”窗口将打开。




创建新策略

4. 选择您要为其创建策略的应用程序。

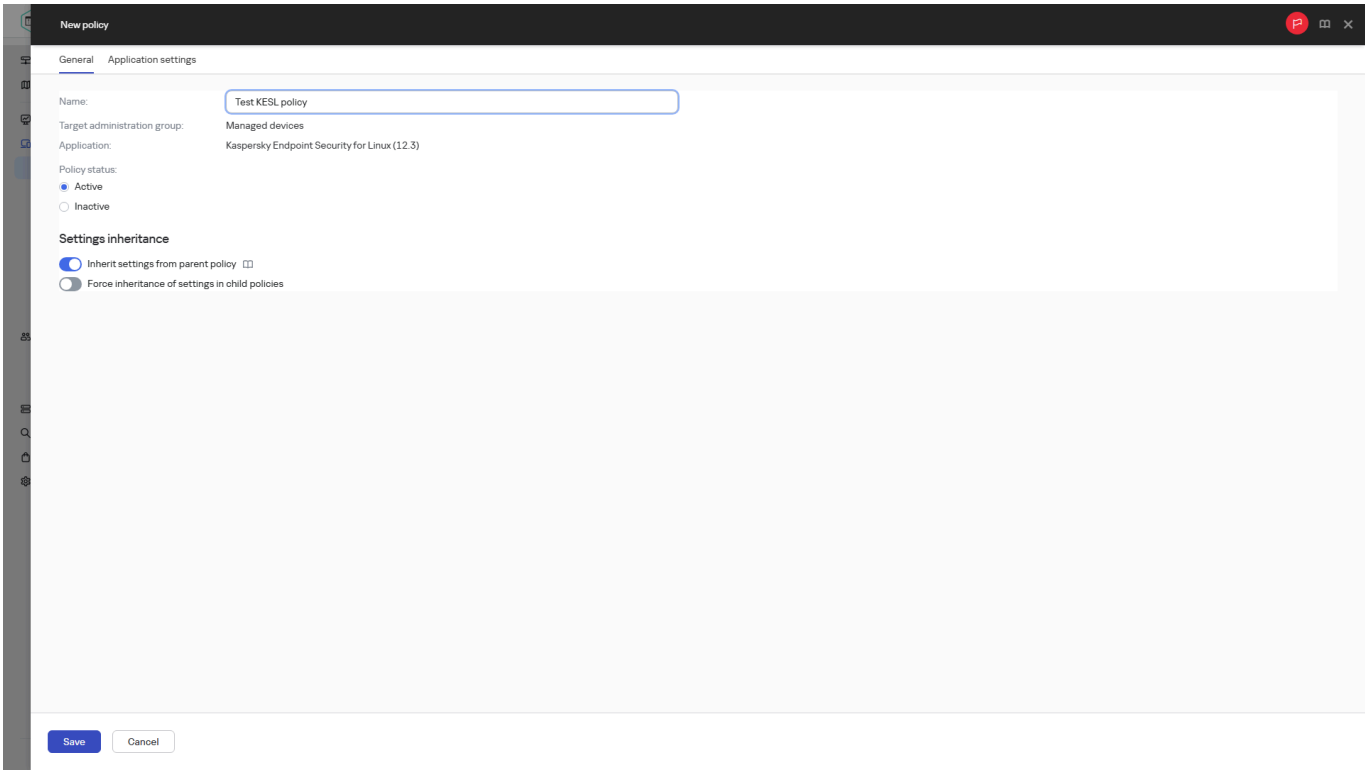
5. 如果您正在为其创建策略的卡巴斯基应用程序支持卡巴斯基安全网络，系统将提示您接受 KSN 声明。如果您想使用卡巴斯基安全网络，请接受 KSN 声明。




接受 KSN 声明

6. 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。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。




新策略设置窗口

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
   - Kaspersky Endpoint Security for Windows 帮助

   有关其他安全应用程序设置的详细信息，请参阅相应应用程序的文档。

   当编辑设置时，您可以单击“**取消**”以取消上一次操作。

9. 单击“**保存**”保存策略。

   将显示包含以下消息的通知：**正在通过管理服务器的层次结构保存和分发策略**。

   如果策略通过验证，则会显示以下通知：**策略已保存**。

   如果策略验证失败，则会显示以下通知：**通过管理服务器的层次结构保存和分发策略 失败。请联系技术支持**。您可以查看并修改策略设置，然后重试。如果问题仍然存在，请联系技术支持。

该策略显示在策略列表中。创建策略后，如果启用了此选项，则会将策略变更事件导出到 SIEM 系统。

# 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）。单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。

此外，当添加新的事件类型（例如，在应用程序的新版本中）时，**事件配置**选项卡会显示通知，并允许您通过单击**保存**或**保存并关闭**按钮来应用新设置。

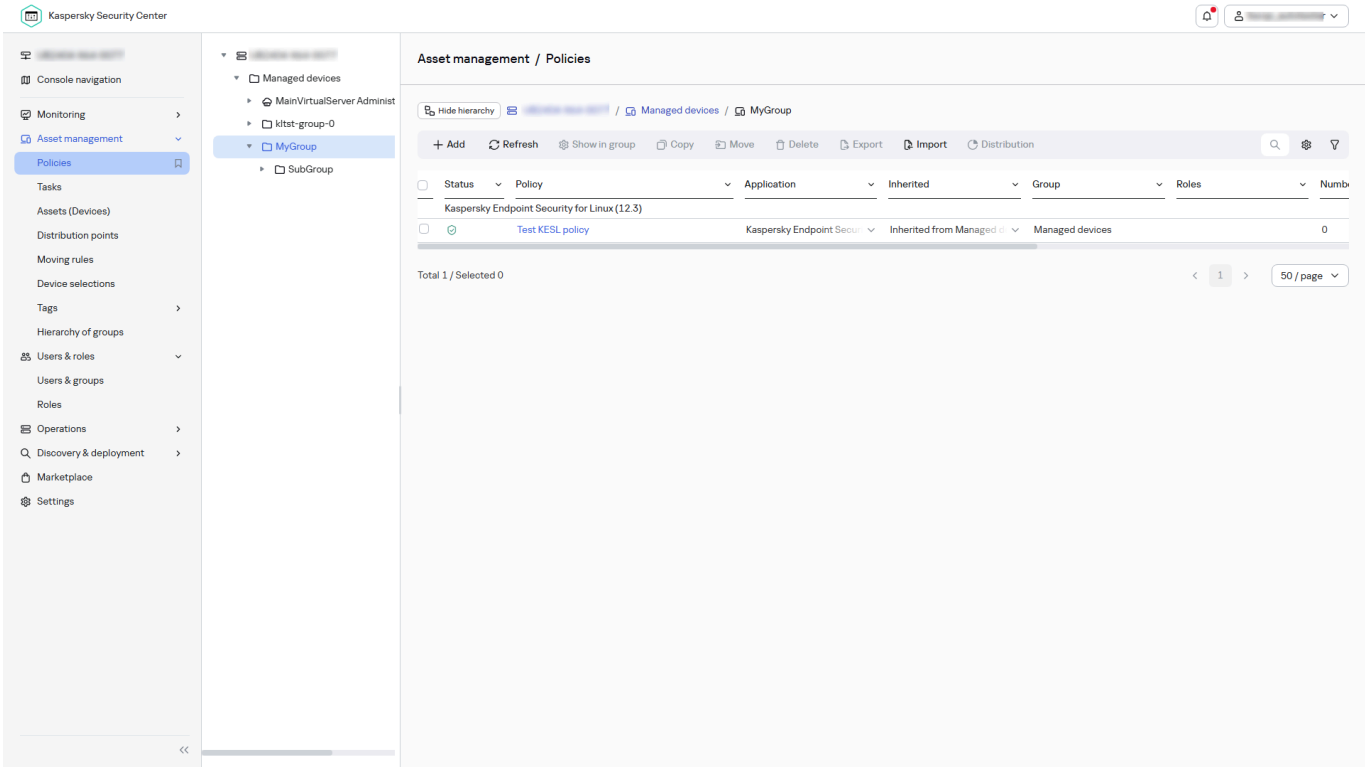
修订历史

**修订历史**选项卡允许您查看政策版本列表，比较政策版本，并在必要时恢复对政策所做的更改。

# 修改策略

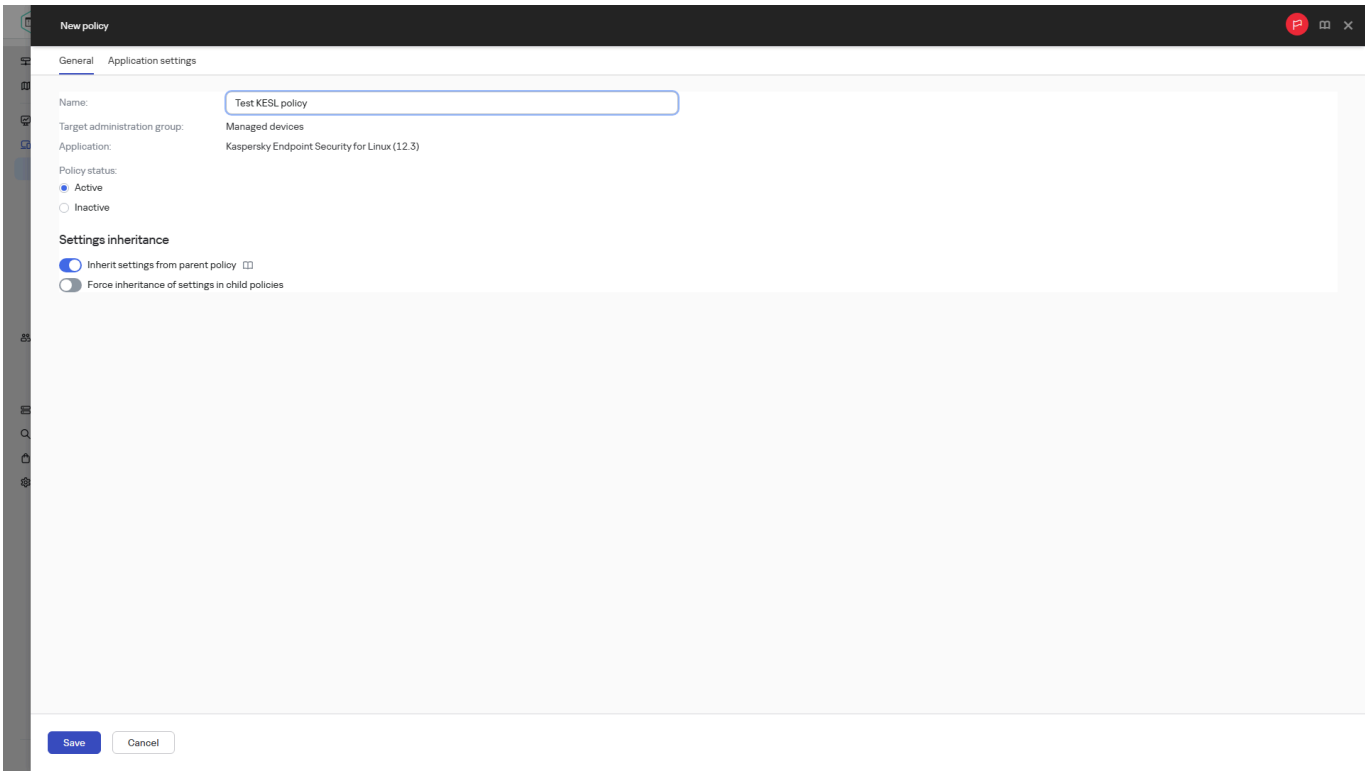
*要修改策略：*

1. 在主菜单中，转到“**资产管理**” → “**策略**”。




2. 点击您要修改的策略。

   策略设置窗口打开。




3. 指定“通用设置”和为其创建策略的应用程序的设置。有关详细信息，请参阅以下内容：

   - 管理服务器配置
   - 网络代理策略设置
   - Kaspersky Endpoint Security for Linux 帮助
   - Kaspersky Endpoint Security for Windows 帮助

   有关其他安全应用程序设置的详细信息，请参阅该应用程序的文档。

4. 点击“**保存**”。

   将显示包含以下消息的通知：**正在通过管理服务器的层次结构保存和分发策略**。

   如果策略通过验证，则会显示以下通知：**策略已保存**。

   如果策略验证失败，则会显示以下通知：**通过管理服务器的层次结构保存和分发策略 失败。请联系技术支持**。您可以查看并修改策略设置，然后重试。如果问题仍然存在，请联系技术支持。

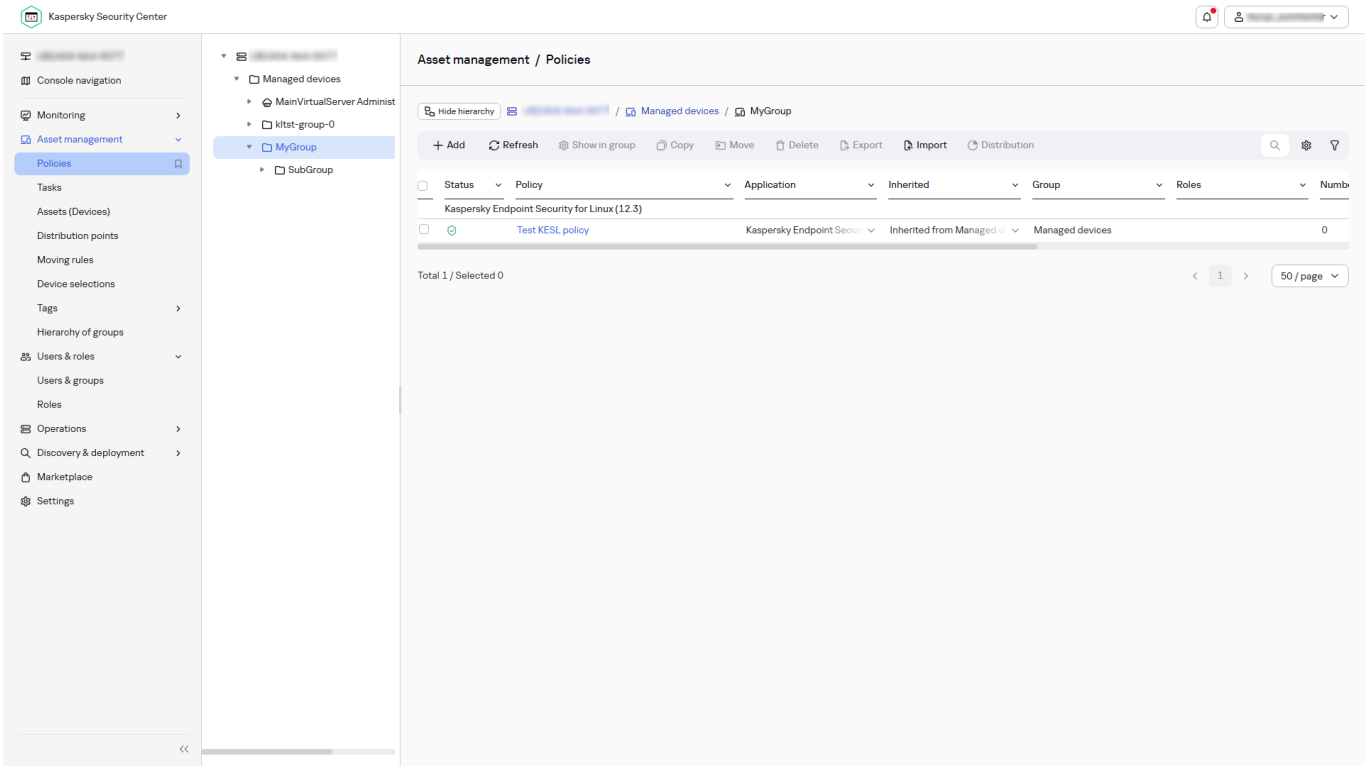
对策略所做的更改将保存在策略属性中，并将显示在“**修订历史**”区域中。策略修改后，如果已启用此选项，则会将策略更改事件导出到 SIEM 系统。

如有必要，您可以比较政策修订版本。此选项适用于管理服务器、网络代理、 Kaspersky Endpoint Security for Windows （从 14.0 Web 插件版本开始）以及 Kaspersky Endpoint Security for Mac（从 12.2.1 Patch A Web 插件版本开始）的策略。

# 启用和禁用策略继承选项

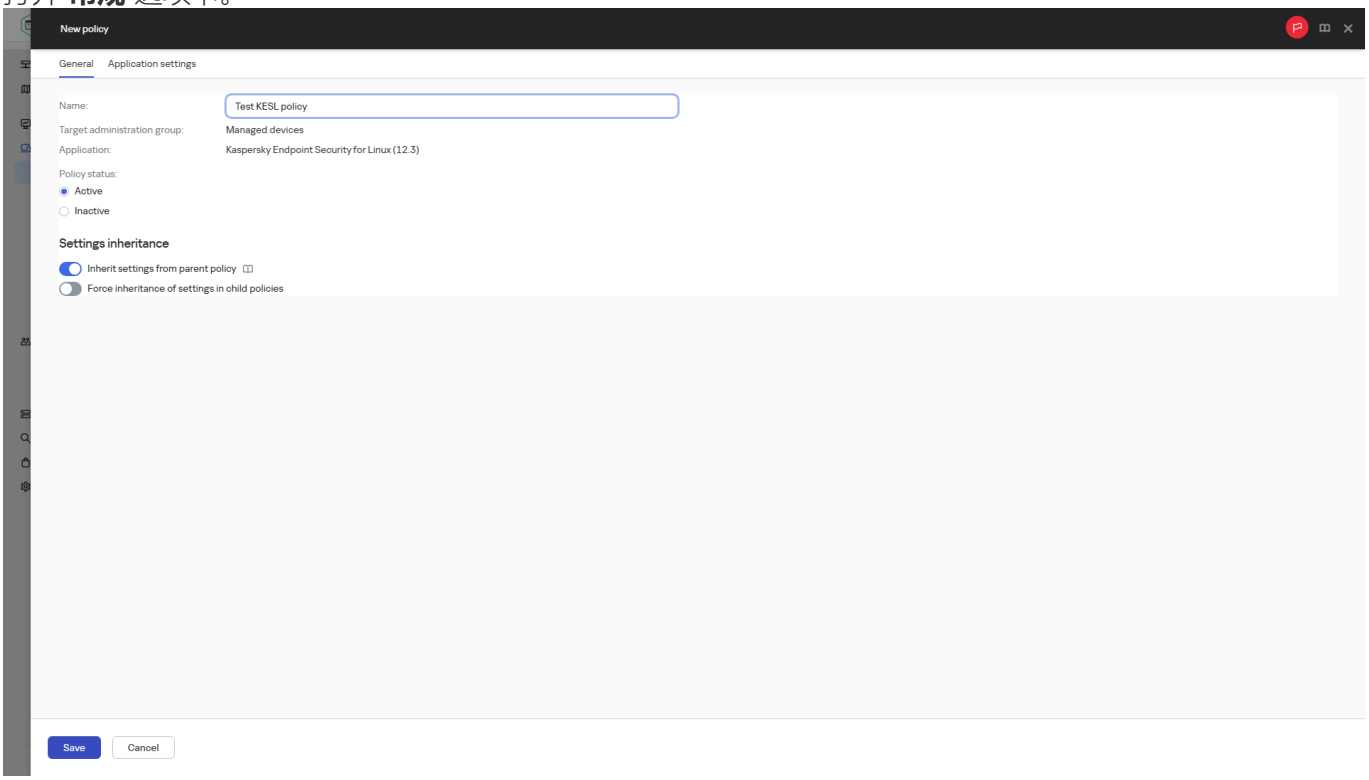
*要在策略中启用或禁用继承选项：*

1. 打开所需策略。




策略列表

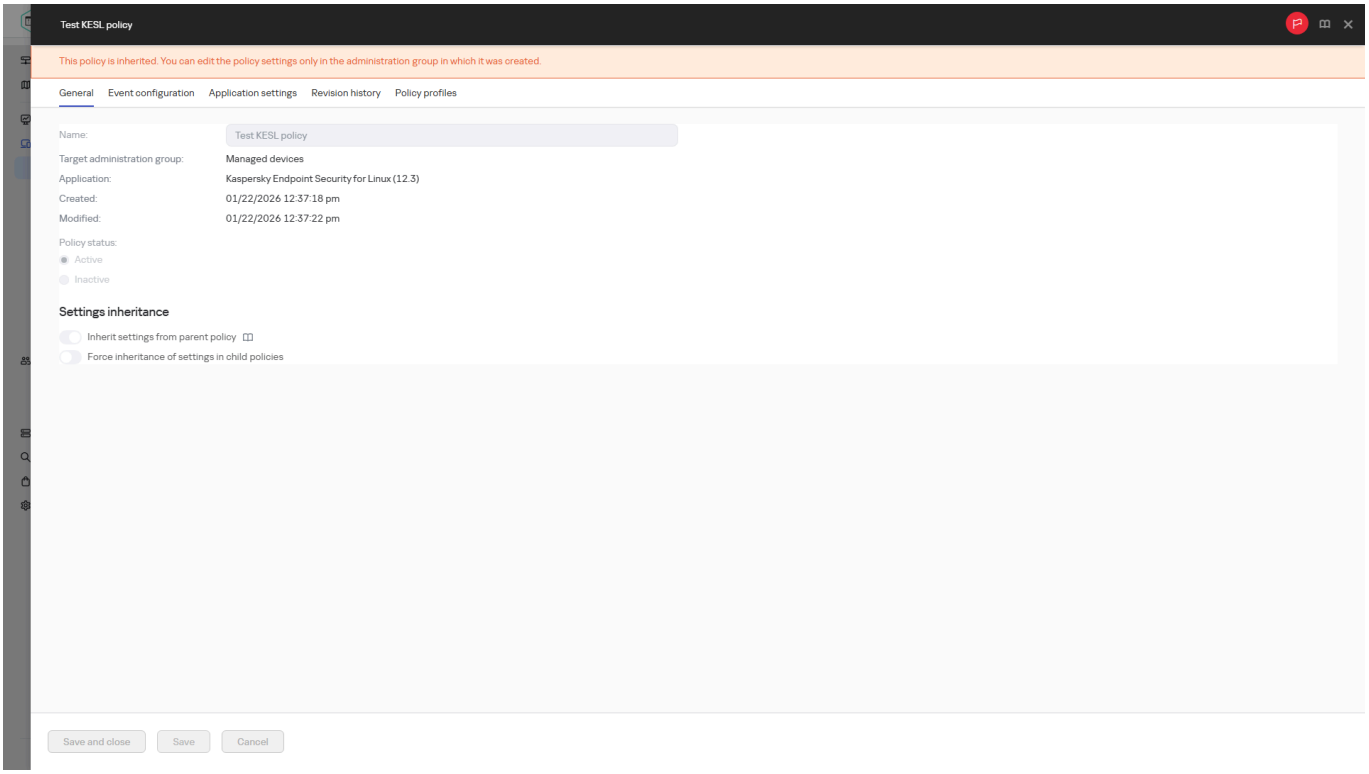
2. 打开“**常规**”选项卡。




创建新策略

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。




锁定的策略设置

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。

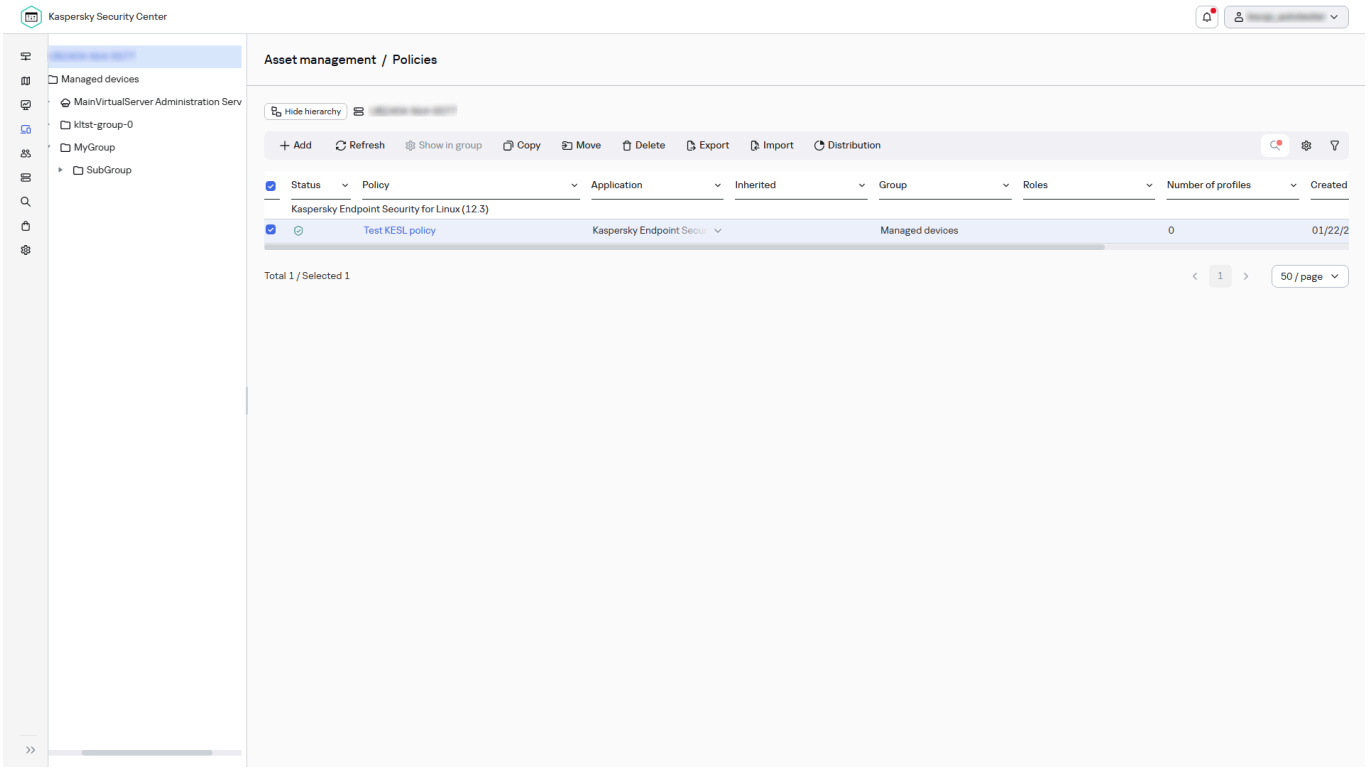
如果一个策略具有配置文件，所有子策略都继承这些配置文件。

# 复制策略

您可以从一个管理组复制策略到另一个。

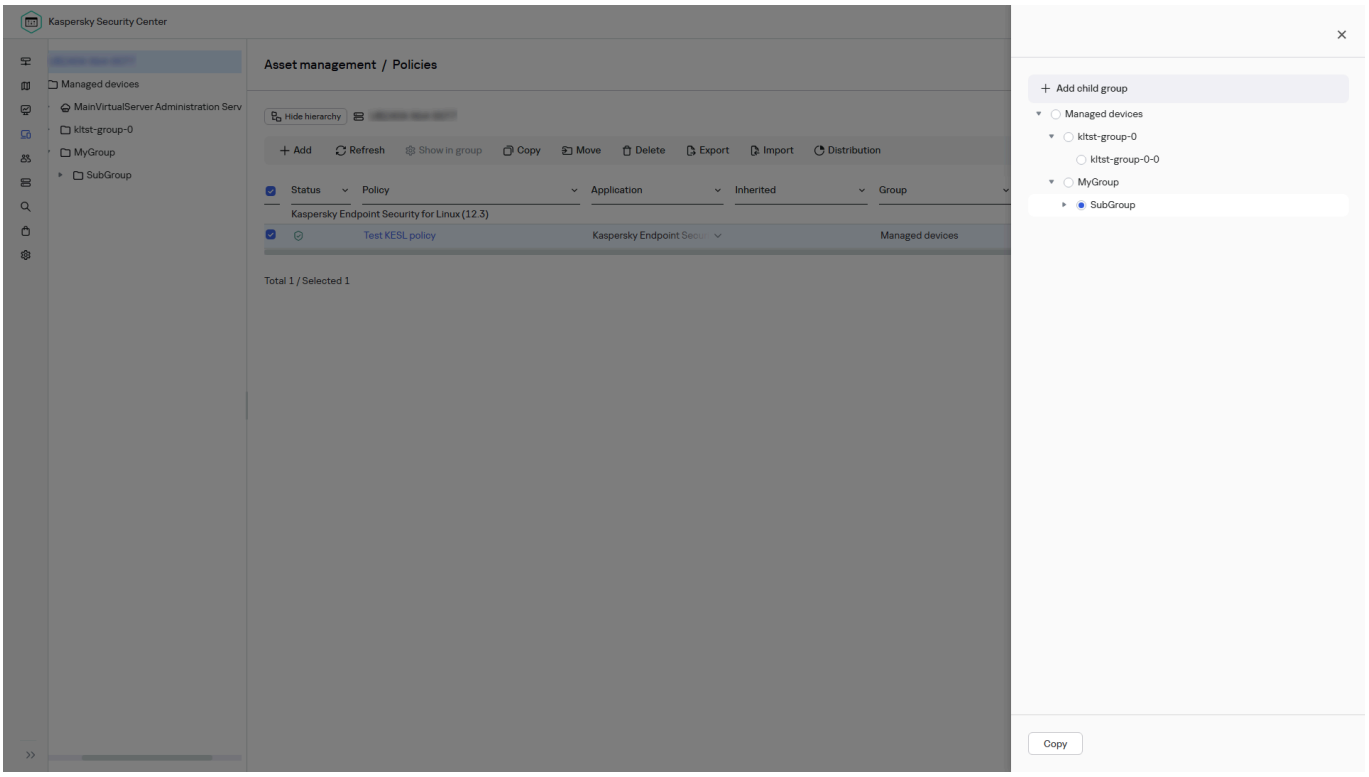
*要复制策略到其他管理组：*

1. 在主菜单中，转到“**资产管理**” → “**策略**”。
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

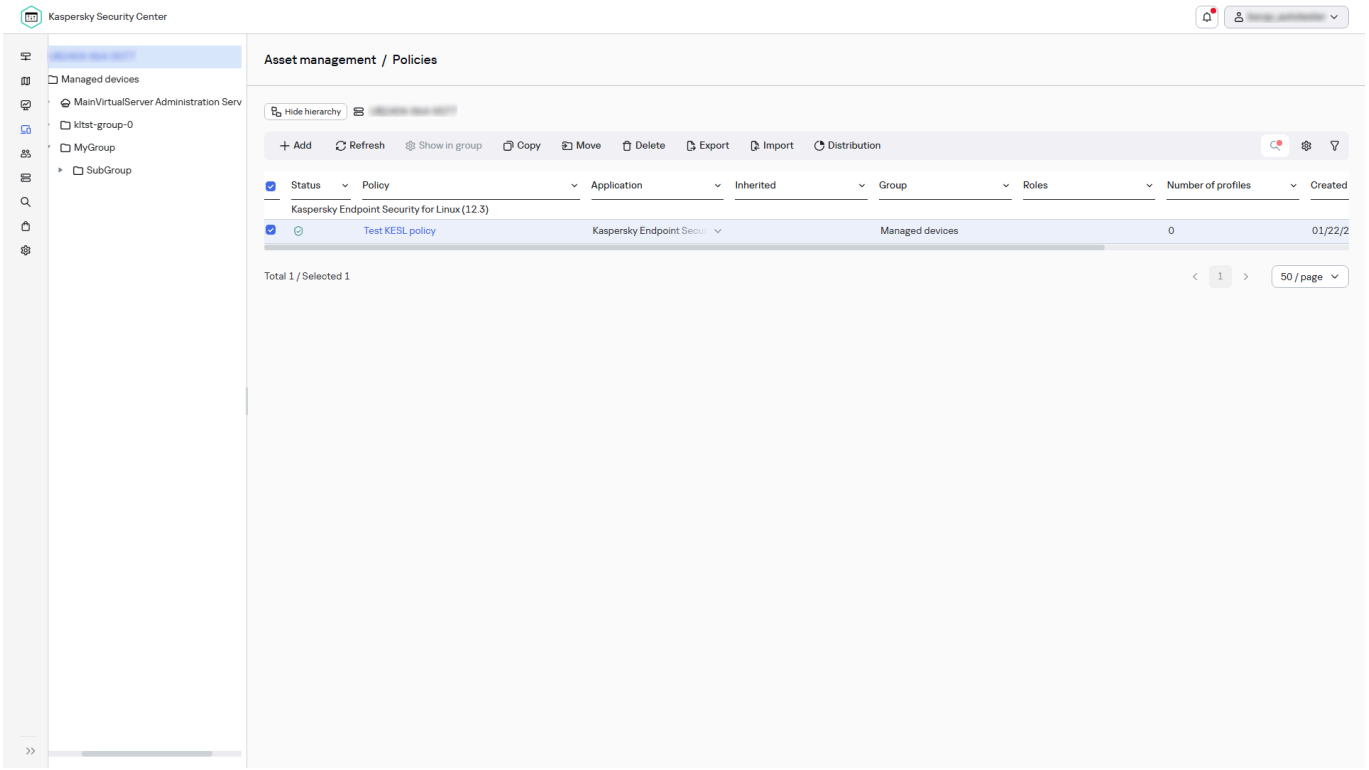
您可以从一个管理组移动策略到另一个。例如，您要删除一个组，但您要为其他组使用其策略。此种情况下，您最好在删除旧组之前将策略从旧组移动到新组。

> 将政策移动到另一个管理群组时，政策的版本历史记录将被清除。**修订历史**选项卡仅显示有关最新更改的信息。

*要移动策略到其他管理组：*

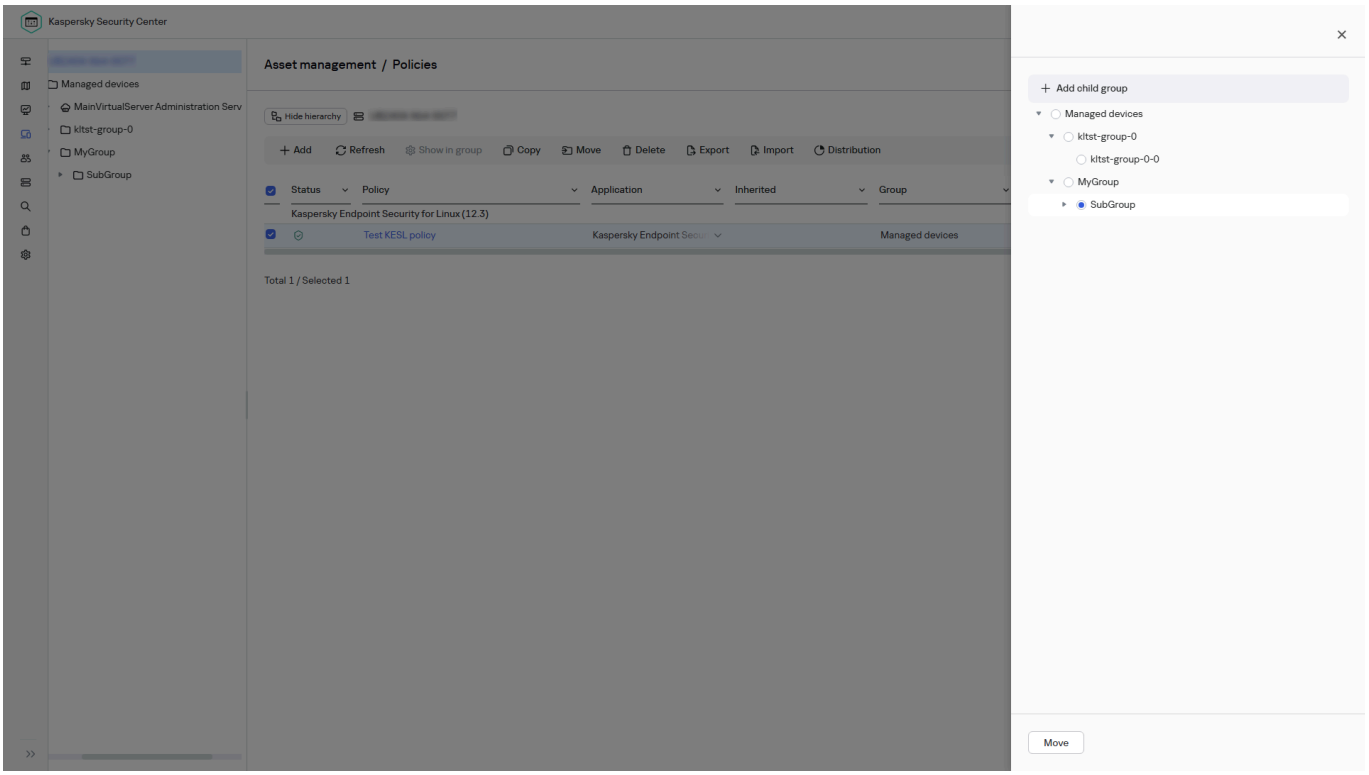
1. 在主菜单中，转到“**资产管理**”→“**策略**”。

2. 选择您要移动的策略旁边的复选框。




3. 单击“**移动**”按钮。

   在屏幕的右侧，管理组树被显示。




4. 在树中，选择目标组，即，要将策略移动到的组。

5. 单击屏幕底部的“**移动**”按钮。

6. 单击“**确定**”以确认操作。

   如果策略不是从资源组继承的，它连带所有配置文件被移动到目标组。目标组中的策略状态为“**不活动**”。您可以随时将状态更改为“**活动**”。

   如果策略是从资源组继承的，它保持在资源组。它连带所有其配置文件被复制到目标组。目标组中的策略状态为“**不活动**”。您可以随时将状态更改为“**活动**”。

如果目标组中已包含名称与新移动策略的名称一致的策略，那么会在新移动策略的名称后附加一个 （<下一个序列号>） 的索引，例如： （1） 。

# 导出策略

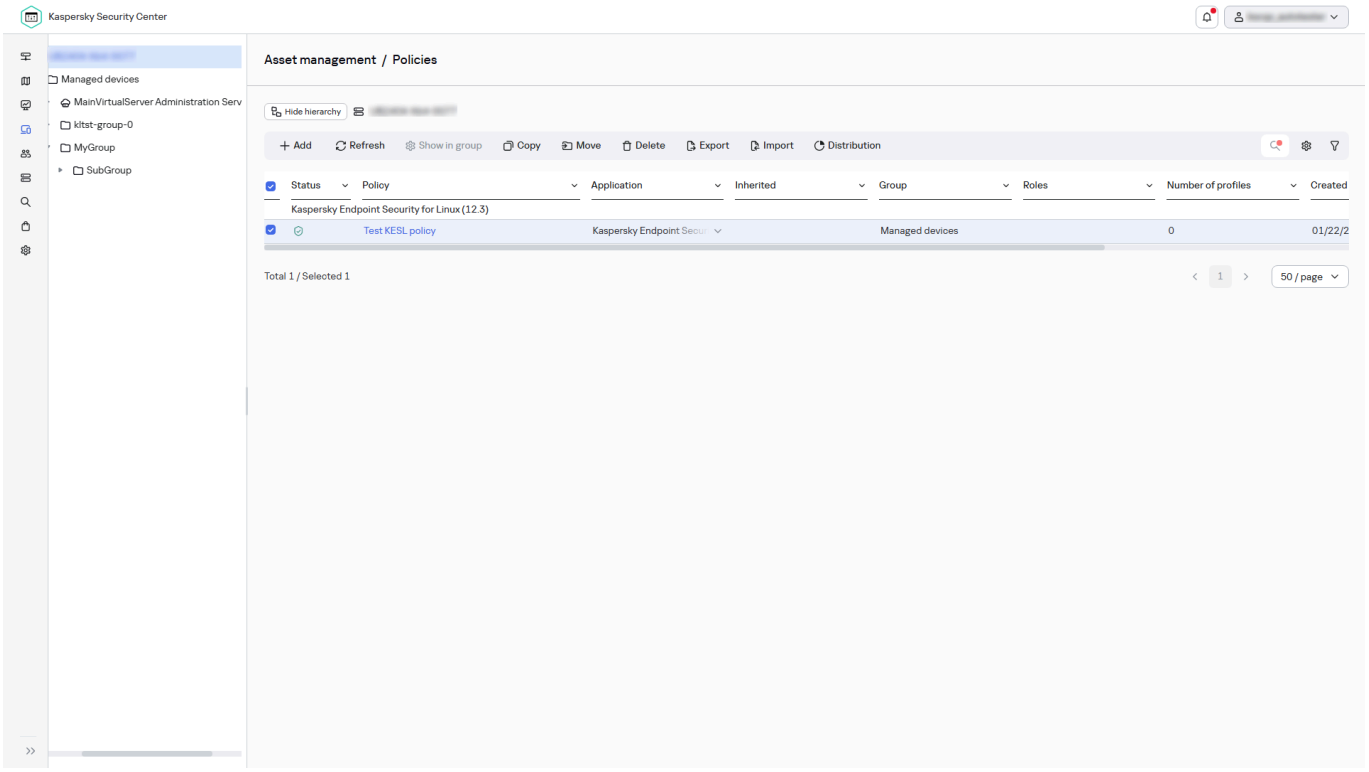
Kaspersky Security Center Linux 允许您将策略、其设置和策略配置文件保存到 KLP 文件中。您可以使用此 KLP 文件将保存的策略导入到 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux。

*要导出策略，请执行以下操作：*

1. 在主菜单中，转到“ **资产管理**” → “**策略**”。

2. 选中要导出的策略旁边的复选框。

您不能同时导出多个策略。如果您选择了多个策略，**导出**按钮将被禁用。




选择导出的策略

3. 单击“**导出**”按钮。
4. 在打开的“**另存为**”窗口中，指定策略文件的名称和路径。单击“**保存**”按钮。

   仅当您使用 Google Chrome、Microsoft Edge 或 Opera 时，才会显示“**另存为**”窗口。如果您使用其他浏览器，则策略文件会自动保存在“**下载**”文件夹。

# 导入策略

Kaspersky Security Center Linux 允许您从 KLP 文件导入策略。KLP 文件包含导出的策略、其设置和策略配置文件。

*要导入策略，请执行以下操作：*

1. 在主菜单中，转到“ **资产管理**” → “**策略**”。
2. 单击“**导入**”按钮。
3. 单击**浏览**按钮选择要导入的策略文件。
4. 在打开的窗口中，指定 KLP 策略文件的路径，然后单击“**打开**”按钮。请注意，您仅可选择一个策略文件。

   策略处理启动。
5. 策略成功处理后，选择要向其应用策略的管理组。
6. 单击**完成**按钮以完成策略导入。

出现包含导入结果的通知。如果策略成功导入，可以单击“**详细信息**”链接以查看策略属性。

成功导入后，策略会显示在策略列表中。策略的设置和配置文件也将会导入。无论导出期间选择的策略处于什么状态，导入的策略均处于非活动状态。您可以在策略属性中更改策略状态。

如果新导入的策略与现有策略有相同的名称，则导入的策略在名称后会附加一个 **(<下一个序列号>)** 索引，例如：**(1)**、**(2)**。

# 强制同步

尽管 Kaspersky Security Center Linux 自动为受管理设备同步状态、设置、任务和策略，但在某些情况下，管理员必须确切知道在某一给定时刻是否已为指定设备执行同步。

## 同步单个设备

*要强制同步管理服务器和受管理设备：*

1. 在主菜单中，转到“**资产管理**” → “**资产(设备)**”。
2. 单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：
   - 运行设备分类以查看设备列表。
   - 在主菜单中，转到**资产管理** → **资产(设备)**，然后选择包含要同步的设备的管理组：
     - 对于根组，您可以继续进行下一步。
     - 对于子组，单击页面顶部的“**显示层级**”按钮，然后在打开的窗口中，单击子组的名称。
       所选组的路径显示在页面顶部。如果需要，您可以单击带有管理组名称的链接前往该组。默认情况下，路径中的最后一个链接不活动。您也可以单击“**隐藏层级**”按钮关闭层次结构窗口。
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卡巴斯基应用程序策略后，管理员可以检查是否被更改的策略被传输到了特定受管理设备。策略可以在定期同步或者强制同步中传输。

*要查看应用程序策略被传输到受管理设备的日期和时间：*

1. 在主菜单中，转到“**资产管理**” → “**资产(设备)**”。
2. 单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。

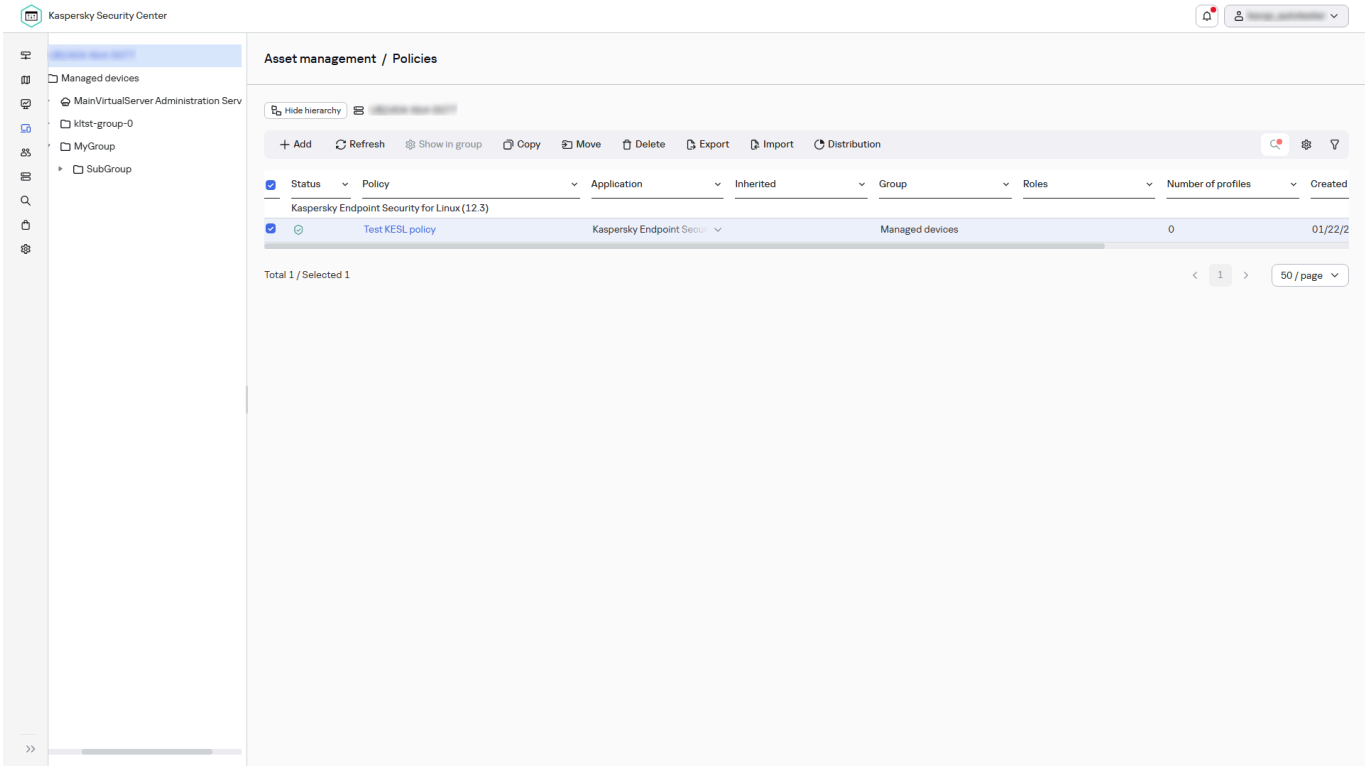
   应用程序策略窗口打开，在其中已选择“**常规**”区域并显示策略传送日期和时间。

# 查看策略分发状态图

在 Kaspersky Security Center Linux 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。

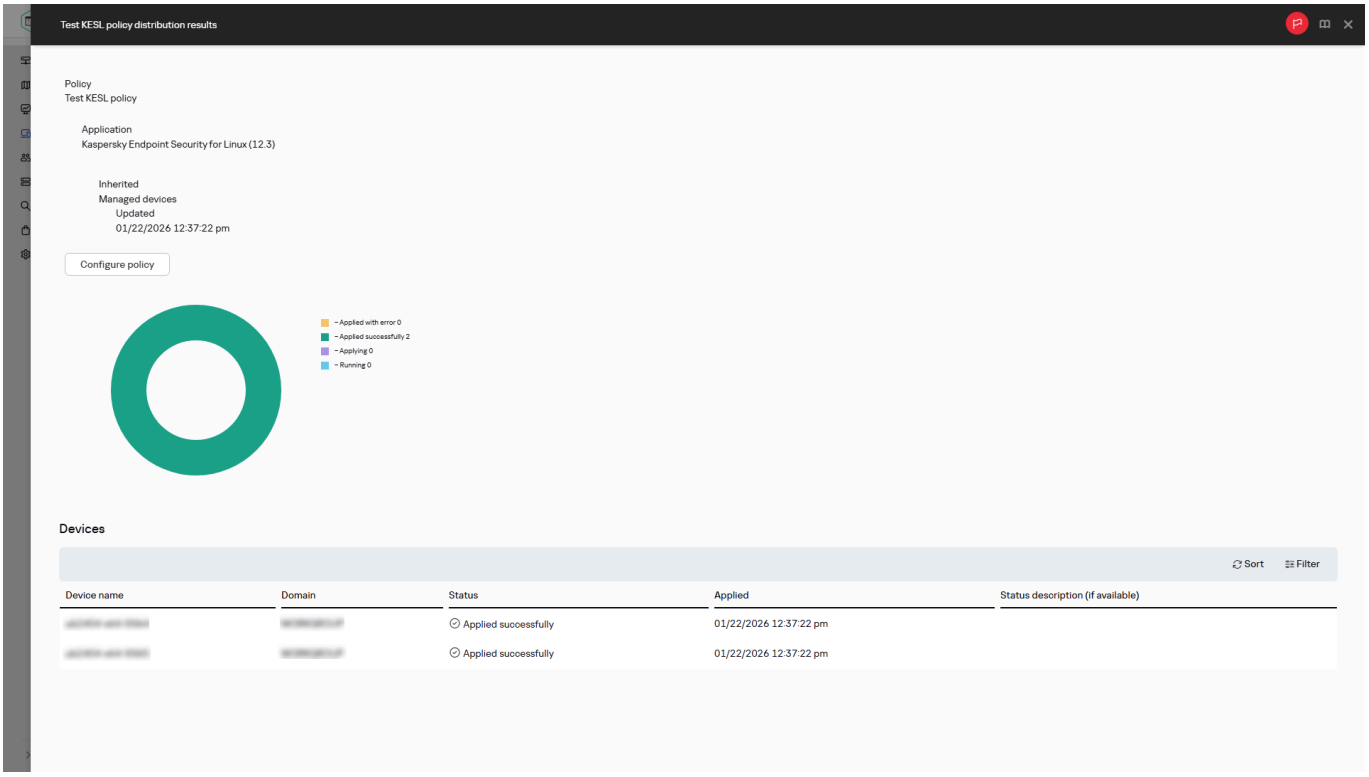
*要查看每个设备上的策略分发状态：*

1. 在主菜单中，转到“**资产管理**”→“**策略**”。
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。




策略列表

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。




策略的分发结果

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. 在主菜单中，转到“**设置**” → “**界面选项**”。
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。

## 在出现病毒爆发事件时自动激活策略

*要使策略在出现病毒爆发事件时自动激活，请执行以下操作：*

1. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口打开，**常规**选项卡被选中。
2. 选择**病毒爆发**区域。
3. 在右侧窗格中，单击“**配置在病毒爆发事件发生时要激活的策略**”链接。
   “**策略激活**”窗口将开启。
4. 在与检测病毒爆发的组件有关的区域中—用于工作站和文件服务器的反病毒、用于邮件系统的反病毒或用于周边防护的反病毒—选择所需条目旁边的选项按钮，然后单击“**添加**”。
   将打开含有“**受管理设备**”管理组的窗口。
5. 单击“**受管理设备**”旁边的 V 形图标 (>)。
   管理组层级和它们的策略被显示。
6. 在管理组层级和它们的策略中，单击策略名称或检测到病毒爆发时激活的策略的名称。
   要在列表或组中选择所有策略，选择所需名称旁边的复选框。
7. 单击“**保存**”按钮。
   管理组层级和它们的策略的窗口被关闭。

所选的策略被添加到检测到病毒爆发时激活的策略列表。所选策略在病毒爆发中被激活，无论它们是活动的还是非活动的。

如果策略在病毒爆发事件中激活，您仅可以使用手动模式返回到先前策略。

## 删除策略

如果您不再需要一个策略，您可以删除它。您仅可以删除一个在指定管理组中继承的策略。如果一个策略是继承的，您仅可以在其被创建的上级组删除它。

*要删除策略，请执行以下操作：*

1. 在主菜单中，转到“ **资产管理**” → “**策略**”。
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。策略删除后，如果启用此选项，策略更改事件将导出到 SIEM 系统。

# 管理策略配置文件

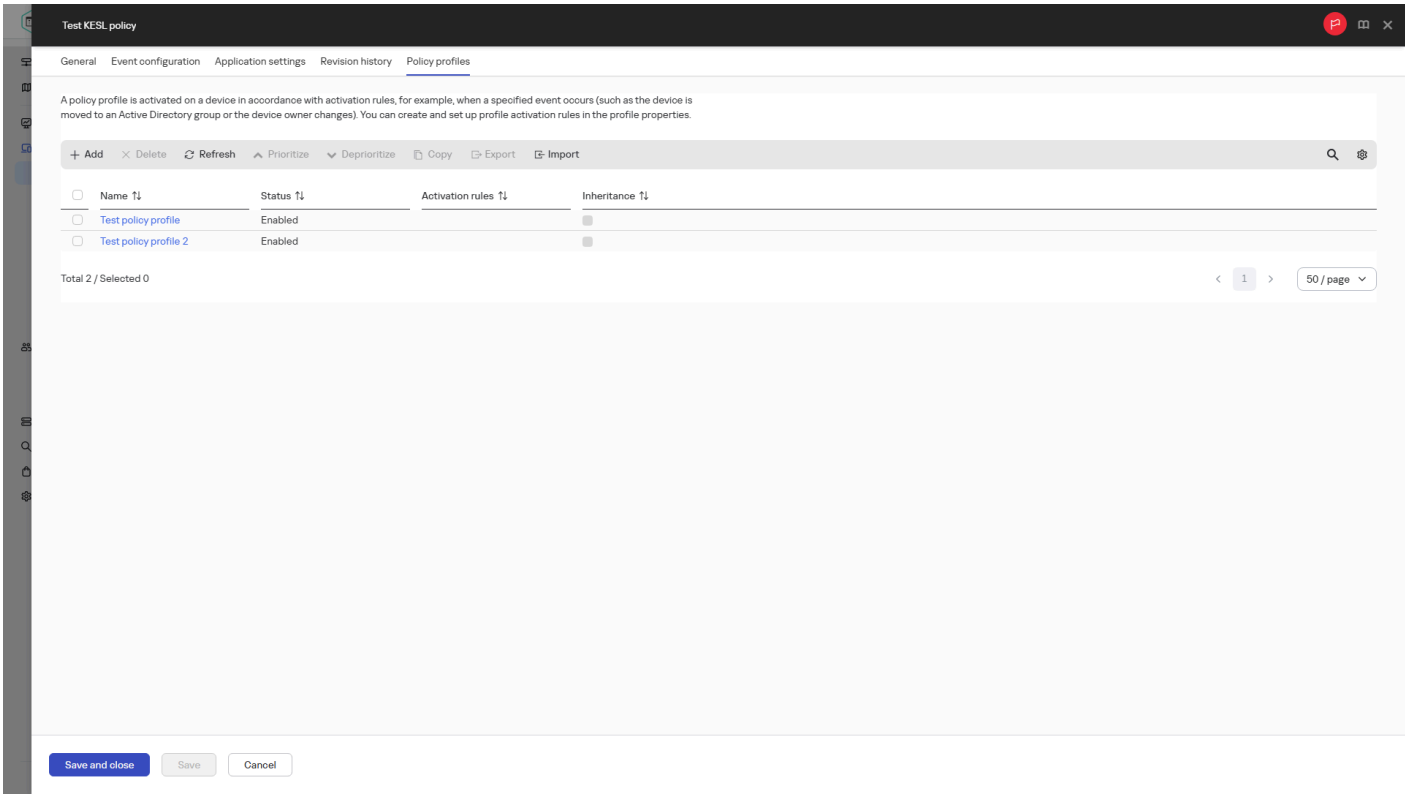
本节介绍管理策略配置文件并提供有关查看策略配置文件、更改策略配置文件优先级、创建策略配置文件、复制策略配置文件、创建策略配置文件激活规则、删除、导出和导入策略配置文件的信息。

# 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“**资产管理**” → “**策略**”。
2. 单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。

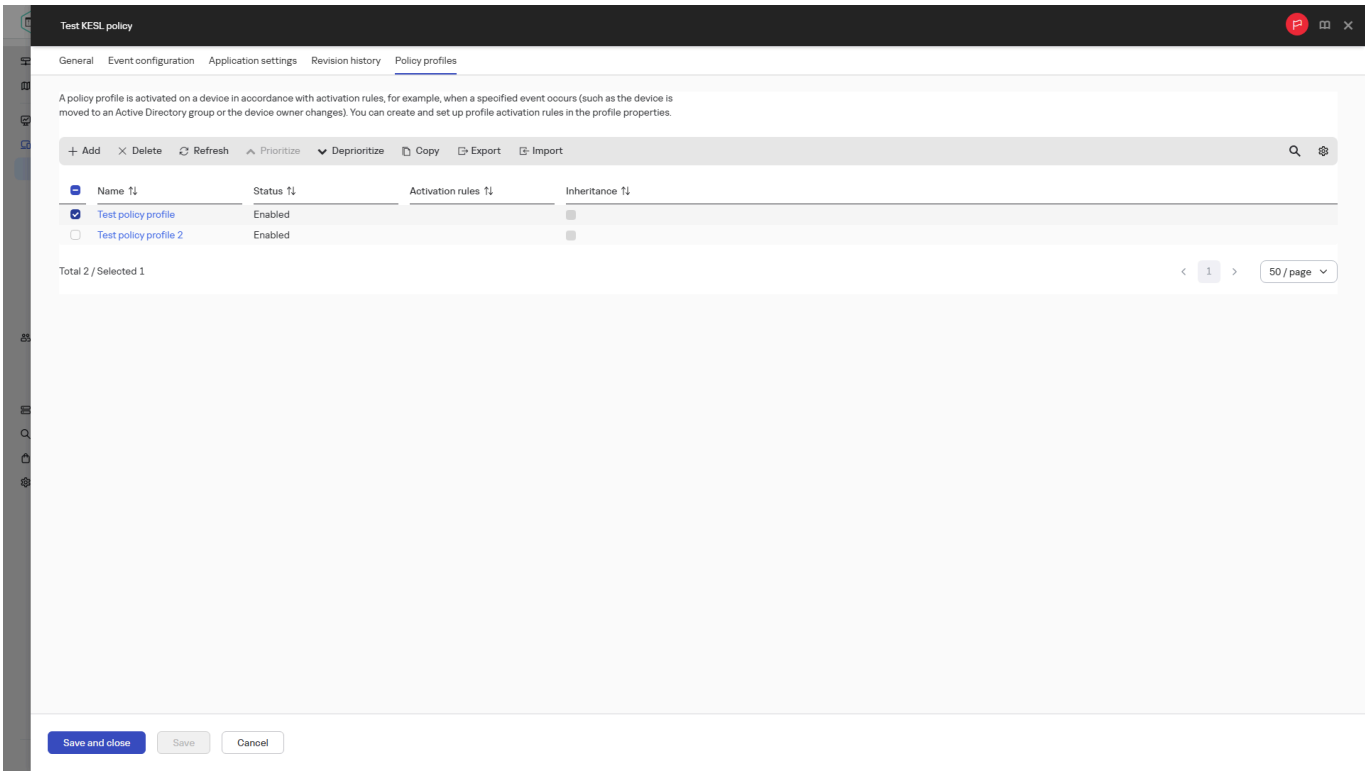



策略配置文件列表

# 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

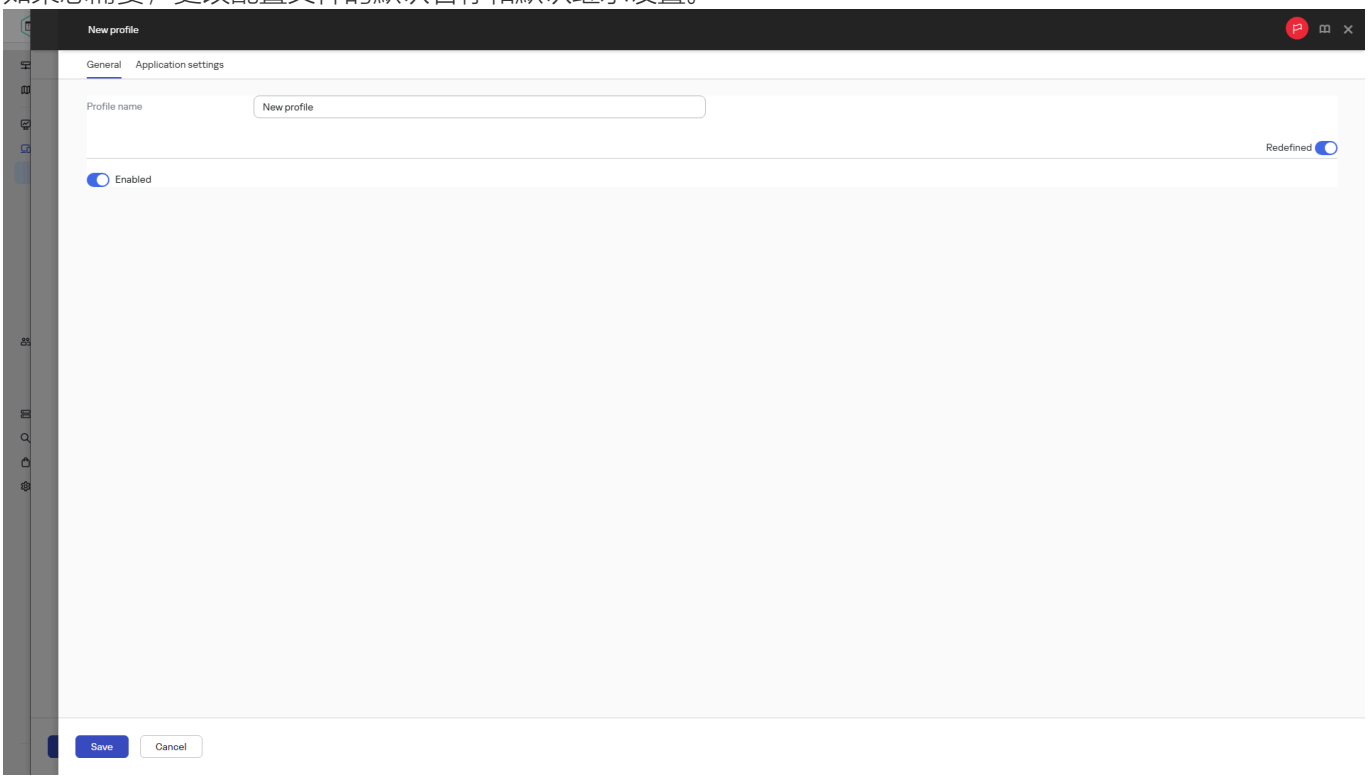
*要创建策略配置文件：*

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。



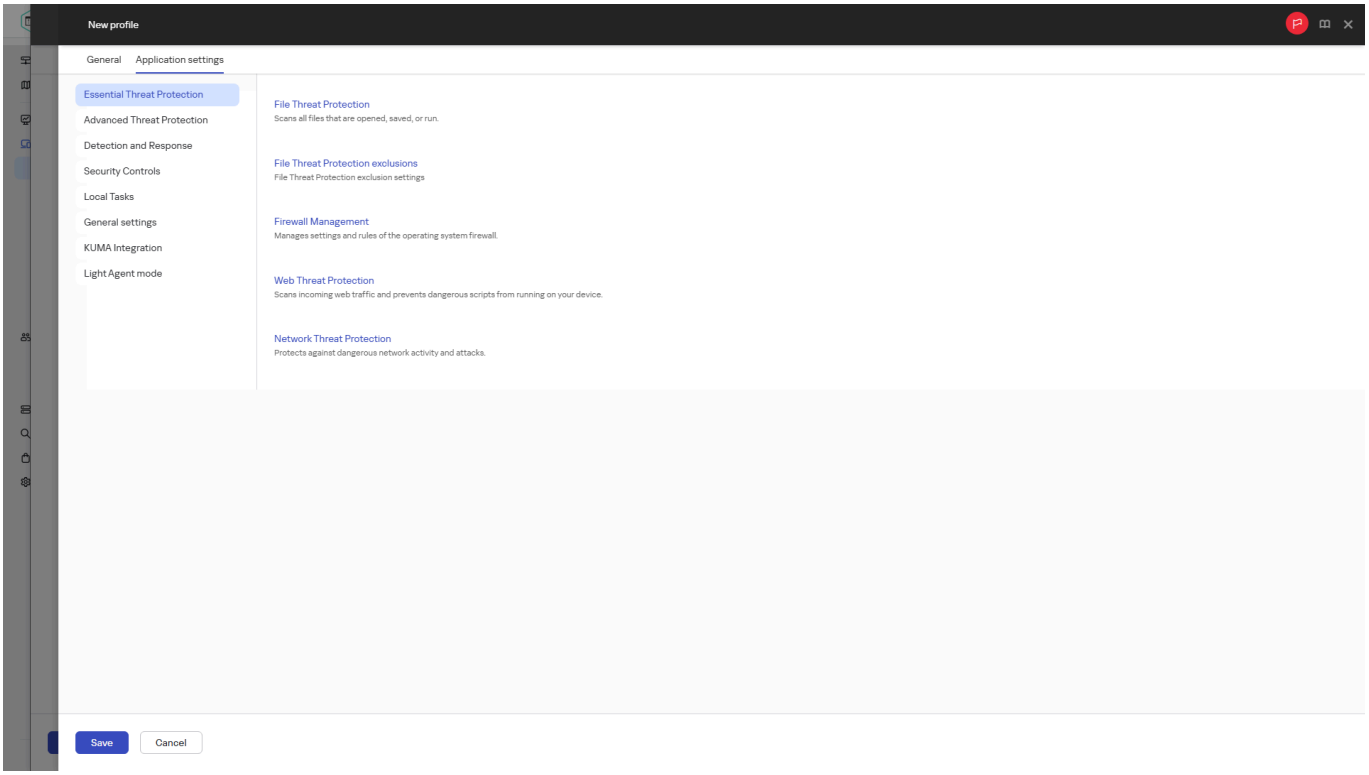

创建新策略配置文件

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。




指定策略配置文件设置

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。

- **设备的网络位置**

  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，并单击“**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。

- **Active Directory 使用规则**

  选择该复选框根据设备在活动目录组织单元中的出现或者设备在活动目录安全组中的成员关系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：

  - **在 Active Directory 安全组中的设备所有者成员关系**

    如果启用此选项，其所有者是指定安全组成员的设备上的策略配置文件将激活。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。

  - **在 Active Directory 安全组中的设备成员关系**

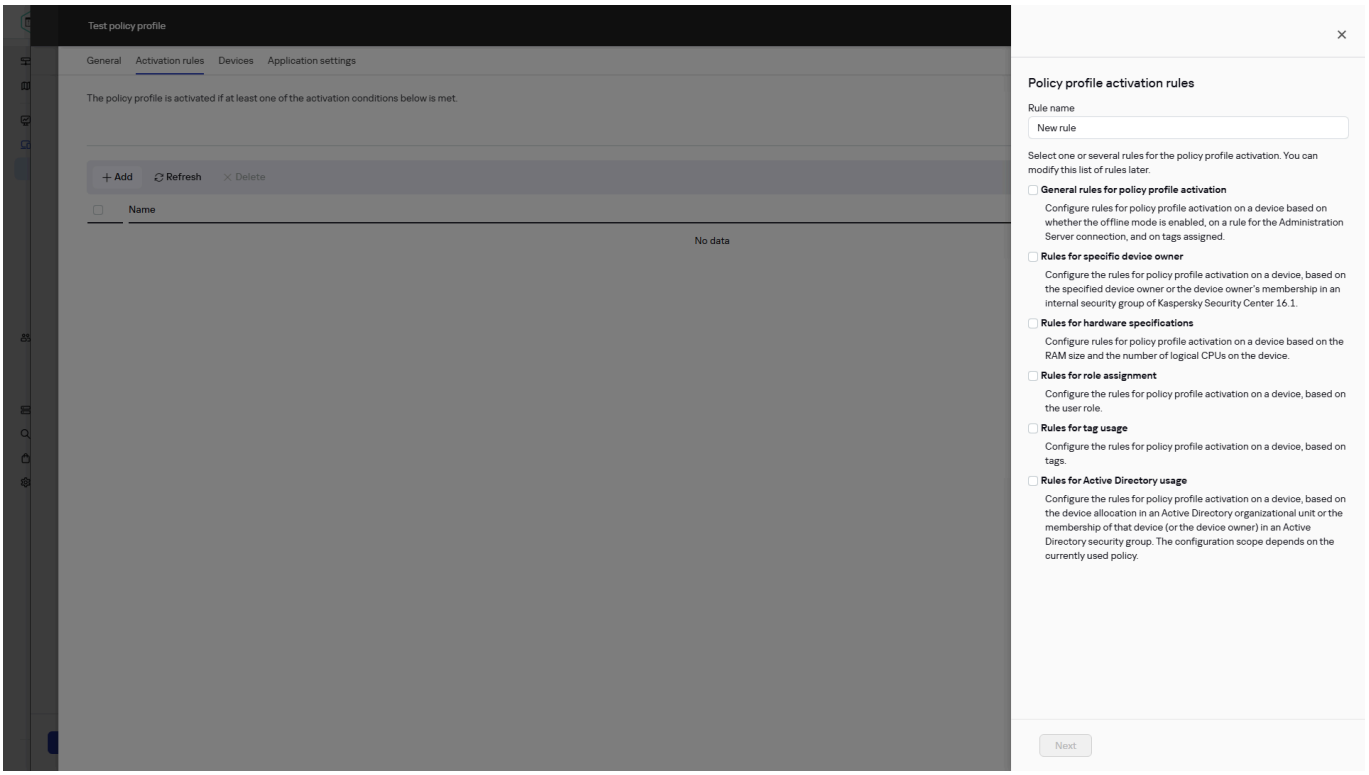
    如果启用此选项，设备上的策略配置文件将激活。如果禁用此选项，配置文件激活标准不起作用。默认情况下已禁用该选项。

  - **在 Active Directory 组织单元中的设备分配**

    如果启用此选项，指定 Active Directory 组织单元 (OU) 中包括的设备上的策略配置文件将激活。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。

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。




创建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。

## 导出和导入策略配置文件

您可以将政策配置文件保存到 KLPROF 文件，而无需导出政策，然后使用此 KLPROF 文件将保存的配置配置文件导入到政策中。

这样，您可以快速恢复策略配置文件设置，而无需重新配置。

政策配置文件会被导入到与从其导出该配置文件的应用程序版本相同的应用程序的政策中。对于支持政策向后兼容的应用程序（例如，Kaspersky Endpoint Security for Windows），此操作也适用。您可以将政策配置文件导入到不同版本的政策中。

*要导出政策配置文件：*

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，单击要导出的政策配置文件。
3. 在工具栏上，单击**导出**按钮。
4. 在打开的窗口中，指定要保存包含政策配置文件的文件的目录。
   如有必要，您可以更改文件名。
5. 单击“**保存**”按钮。

如果操作成功完成，屏幕上将显示相应的消息。否则，将显示错误消息。

*要导入政策配置文件：*

1. 转到您要的政策的配置文件列表。
   将出现政策配置文件列表。
2. 在工具栏上，单击**导入**按钮。

3. 在打开的窗口中，选择包含所需政策配置文件的 KLPROF 文件，然后单击**打开**按钮。
   导入文件的最大大小是 4 MB。

如果操作成功完成，屏幕上将显示相应的消息。否则，将显示错误消息。

策略配置文件会以导出时的名称导入，而不是以 KLPROF 文件的名称导入。
无论导出前策略配置文件的优先级如何，该文件都会以**已禁用**状态和最低优先级导入。

以下情况无法执行导入：

- 政策中已存在同名配置文件；
- 政策中的配置文件数量为 100。

# 网络代理策略设置

*若配置网络代理程序政策：*

1. 在主菜单中，转到“**资产管理**”→“**策略**”。
2. 单击网络代理程序政策的名称。
   网络代理程序政策的属性窗口打开。属性窗口包含如下所述的选项卡和设置。

请参阅比较表格，它详细介绍了根据使用的操作系统类型如何应用以下设置。

## 常规

在该选项卡上，您可以修改策略名称、策略状态并指定策略设置的继承：

- 在“**名称**”字段中，您可以修改策略名称。
- 在“**策略状态**”块，您可以选择以下策略模式之一：
  - **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。
  - **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

在该选项卡上，您可以配置事件记录和事件通知。事件根据重要性级别分布在以下部分：

- **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“**发生了安全问题**”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“**发生了安全问题**”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安全问题，您可以使用受管理设备的设置管理此问题。

### 应用程序设置

### 设置

在“**设置**”区域，您可以配置网络代理策略：

- **仅通过分发点分发文件**

  如果启用此选项，则受管理设备上的网络代理只从分发点检索更新。

如果禁用此选项，则受管理设备上的网络代理从分发点或管理服务器检索更新。

请注意，受管理设备上的安全应用程序从每个安全应用程序的更新任务中设置的源检索更新。如果启用“**仅通过分发点分发文件**”选项，请确保在更新任务中将 Kaspersky Security Center Linux 设置为更新源。

默认情况下已禁用该选项。

- **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的名称。
  - 策略传输至受管理设备时漫游策略的名称（对于Linux 版网络代理不可用）。
  - 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。
  - 策略传输至受管理设备时包含其名称和优先级的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。

- **保护网络代理服务免遭非授权的卸载或终止，并防止设置更改**

  当启用该选项时，网络代理被安装到受管理设备之后，没有所需权限组件无法被卸载或重新配置。网络代理服务无法被停止。此选项对域控制器没有影响。

  启用此选项可保护以本地管理员权限操作的工作站上的网络代理。

  默认情况下已禁用该选项。

- **使用卸载密码**

  如果启用此选项，则单击“**修改**”按钮可以指定用于 klmover 实用程序和 Windows 设备上网络代理远程卸载的密码。

  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：

- **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。

- **包括补丁信息**

  有关在客户端设备上安装的应用程序补丁的信息将发送到管理服务器。启用此选项可能会增加管理服务器和 DBMS 的负载，并导致数据库数据量的增加。

  默认情况下已启用该选项。它仅适用于 Windows。

- **Windows Update 更新详情**

  如果启用此选项，则有关客户端设备上必须安装的 Microsoft Windows Update 更新的信息将发送至管理服务器。

  默认情况下已启用该选项。它仅适用于 Windows。

  有关 Microsoft Windows 可选更新的信息未发送至管理服务器。

- **软件漏洞和对应更新的详情**

  如果启用此选项，则将有关在受管理设备上检测到的第三方软件（包括 Microsoft 软件）中的漏洞信息以及有关修复第三方漏洞（不包括 Microsoft 软件）的软件更新信息发送到管理服务器。

  选择此选项（**软件漏洞和对应更新的详情）**会增加网络负载、管理服务器磁盘负载和网络代理资源消耗。

  默认情况下已启用该选项。它仅适用于 Windows。

  要管理 Microsoft 软件的软件更新，请使用“**Windows Update 更新详情**”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。

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。

## 软件更新和漏洞

在“**软件更新和漏洞**”区域，您可以启用对可执行文件的漏洞扫描：

- **当运行可执行文件时扫描其漏洞**

  如果启用此选项，系统将在运行可执行文件时扫描漏洞。

  默认情况下已启用该选项。

## 重启管理

如果受管理设备的操作系统必须重启才能正确使用、安装或卸载应用程序，您可以在“**重启管理**”区域指定要执行的操作：

- **不重启操作系统**

  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。

- **如有必要，自动重启操作系统**

  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。

- **提示用户操作**

  客户端设备屏幕上将显示重启提醒，提示用户手动重启设备。可以为该选项定义一些高级设置：用户消息文本、消息显示频率以及强制重启（不需要用户确认）的时间间隔。该选项适用于用户必须可以选择最方便的时间进行重启的工作站。

  默认情况下已选定该选项。

  - **重复提示间隔(分钟)**

    如果启用该选项，应用程序以指定频率提示用户重启操作系统。

    默认情况下已启用该选项。默认时间间隔为 5 分钟。可用值介于 1 和 1440 分钟之间。

    如果禁用该选项，提示仅显示一次。

  - **在该时间后强制重启(分钟)**

    提示用户之后，应用程序在指定时间间隔后强制操作系统重启。

    默认情况下已启用该选项。默认延时是 30 分钟。可用值介于 1 和 1440 分钟之间。

  - **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。

## 管理补丁和更新

在“管理补丁和更新”区域，您可以配置受管理设备的更新下载和分发以及补丁的安装：

- **对未定义状态的组件自动安装可应用更新和补丁**

  如果启用此选项，带有*未定义*批准状态的卡巴斯基应用程序在从更新服务器下载后将被自动安装在受管理设备。

  如果禁用此选项，被下载和标注为*未定义*状态的 Kaspersky 补丁将仅在您改变其状态为*已批准*是被安装。

  默认情况下已启用该选项。

- **提前从管理服务器下载更新和反病毒数据库(推荐)**

  如果启用此选项，离线模式更新下载被使用。当管理服务器接收更新时，它通知网络代理(安装网络代理的设备)将用于受管理应用程序的更新。当网络代理接收更新的信息后，它提前从管理服务器下载相关文件。在第一次连接网络代理时，管理服务器发起更新下载。网络代理下载所有更新到客户端设备后，更新对该设备上的应用程序可用。

  当客户端设备上的受管理应用程序尝试访问网络代理以更新时，该网络代理检查其是否具有所有的更新。如果在受管理应用程序请求更新之前 25 小时内，更新已从管理服务器收到，则网络代理不连接到管理服务器，而是从本地缓存提供更新给受管理应用程序。当网络代理提供更新到客户端设备上的应用程序时，到管理服务器的连接可能不被建立，但是更新不需要连接。

  如果禁用此选项，离线模式更新下载不被使用。更新根据更新下载任务的计划被分发。

  默认情况下已启用该选项。

## 连接

“**连接**”区域包含三个子区域：

- **网络**
- **连接配置文件**
- **连接计划**

在“**网络**”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。

  - **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。

- **在 Microsoft Windows 防火墙中打开网络代理端口**

  如果启用此选项，网络代理工作所需的端口将添加到 Microsoft Windows 防火墙排除列表中。

  默认情况下已启用该选项。

- **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。

- **使用分发点强制连接到管理服务器**

  如果在分发点设置窗口中选择了“**将此分发点用作推送服务器**”选项，则选择此选项。否则，分发点不会用作推送服务器。

在“**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**

  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

- **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：

- **Windows 网络**

  此选项仅适用于基于 Windows 的分发点。

  如果启用此选项，则管理服务器将按照所配置的计划自动轮询网络，单击“**设置快速轮询计划**”和“**设置完整轮询计划**”链接可配置轮询计划。

  如果禁用此选项，管理服务器将以**网络轮询频率(分钟)**字段中指定的时间间隔轮询网络。

  可以在“**Windows 域的轮询频率(分钟)**（适用于快速 Windows 网络轮询）和 **网络轮询频率(分钟)**（适用于完整 Windows 网络轮询）”字段中配置网络代理版本的设备发现间隔。

  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。

- **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。

- **域控制器**

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

  如果禁用此选项，则分发点将不轮询域控制器。

对于 10.2 版之前的网络代理，可在“**轮询间隔(分钟)**”字段中配置域控制器轮询频率。如果启用此选项，则字段可用。

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。

## KSN 代理(分发点)

在“**KSN 代理(分发点)**”区域，您可以配置应用程序使用分发点从受管理设备转发 Kaspersky Security Network (KSN) 请求：

- **在分发点端启用 KSN 代理**

  KSN 代理服务运行在用作分发点的设备上。使用该功能重新分发和优化网络流量。

  分发点发送列在Kaspersky Security Network声明中的KSN统计信息到卡巴斯基。

  默认情况下已禁用该选项。启用该选项仅在**使用管理服务器作为代理服务器** 和 **我同意使用卡巴斯基安全网络** 选项在管理服务器属性窗口中被启用时起作用。

  您可以分配活动被动集群节点到分发点并在该节点上启用 KSN 代理服务器。

- **转发 KSN 请求到管理服务器**

  分发点从受管理设备转发 KSN 请求到管理服务器。

  默认情况下已启用该选项。

- **通过互联网直接访问 KSN 云/KPSN**

  分发点从受管理设备转发 KSN 请求到 KSN 云或 KPSN。分发点本身上生成的 KSN 请求也直接发送到 KSN 云或 KPSN。

- **TCP 端口**

  受管理设备将用于连接到 KSN 代理服务器的 TCP 端口号。默认端口号是 13111。

- **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。

- **HTTPS 端口**

  如果您需要受管理设备通过 HTTPS 端口连接到 KSN 代理服务器，请启用“**使用 HTTPS**”选项，然后在“**HTTPS 端口**”字段中指定端口号。默认情况下已禁用该选项。连接到 KSN 代理服务器的默认 HTTPS 端口是 17111。

## 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。

## 本地账户管理(仅限 Linux)

“**本地账户管理(仅限 Linux)**”部分包括三个子部分：

- **用户证书管理**
- **添加或编辑适用的本地管理员组**
- **上传参考文件以保护用户设备上的 sudoers 文件以防更改**

在“**用户证书管理**”子部分中，您可以指定要安装的根证书。例如，这些证书可用于验证网站或网络服务器的真实性。

- **安装根证书**

  如果启用此选项，则添加到表中的证书将安装在指定的设备上。

  如果禁用此选项，则不会在指定设备上安装任何证书。

  默认情况下已禁用该选项。

- **添加**

  单击此按钮会打开一个窗口，您可以在其中添加证书。

  证书必须小于 10 MB。

  Kaspersky Security Center 支持具有 CER、CRT、CERT、PEM 和 KEY 扩展名的证书。

在“**添加或编辑适用的本地管理员组**”子部分中，您可以管理本地管理员组。例如，在撤销本地管理员权限时会使用这些组。您还可以使用“**特权设备用户报告(仅限 Linux)**”检查特权用户账户列表。

- **添加**

  单击此按钮会打开一个窗口，您可以在其中添加本地管理员组。

- **编辑**

  单击此按钮会打开一个窗口，您可以在其中编辑本地管理员组。

  如果选中本地管理员组旁边的复选框，则此按钮可用。

- **删除**

  单击此按钮会从表中删除所选的本地管理员组。

  如果选中本地管理员组旁边的复选框，则此按钮可用。

在“**上传参考文件以保护用户设备上的 sudoers 文件以防更改**”子部分中，您可以配置对 sudoers 文件的控制。特权组和设备用户由设备上的 sudoers 文件定义。sudoers 文件位于 `/etc/sudoers`。您可以上传参考 sudoers 文件，以保护 sudoers 文件以防更改。这可以防止对 sudoers 文件进行不必要的更改。

无效的参考 sudoers 文件可能会导致用户的设备出现故障。

- **控制 sudoer 文件**

  如果启用此选项，sudoers 文件将由当前参考 sudoers 文件替换。

  如果禁用此选项，sudoers 文件将保持不变。

  默认情况下已禁用该选项。

- **参考 sudoer 文件**

  此字段显示上传的参考 sudoers 文件的名称。

- **上传**

  单击此按钮会打开一个窗口，您可以在其中上传参考 sudoers 文件。

- **当前参考 sudoer 文件**

  单击此按钮会显示当前 sudoers 文件的内容。

## 修订历史

在“**修订历史**”选项卡上，您可以：

- 查看和保存策略修订的历史记录。
- 回滚至策略修订。
- 添加和编辑策略修订描述。
- 比较策略修订。

# Windows、Linux 和 macOS 网络代理的使用：比较

网络代理的使用取决于设备的操作系统。网络代理策略和安装包设置也根据操作系统不同而不同。下表比较了适用于 Windows、Linux 和 macOS 操作系统的网络代理的功能和使用方案。

网络代理功能比较

| 网络代理功能 | Windows | Linux | macOS |
|---|---|---|---|
| **安装** | | | |
| 通过使用第三方工具克隆带有操作系统和网络代理的管理员硬盘驱动器镜像进行安装 | ✓<br>限制：不受适用于 Arm 架构 Microsoft Windows 的网络代理的支持。 | ✓ | ✓ |
| 使用用于远程安装应用程序的第三方工具进行安装 | ✓ | ✓ | ✓ |
| 通过在设备上运行应用程序安装程序来手动安装 | ✓ | ✓ | ✓ |
| 在静默模式下安装网络代理 | ✓ | ✓ | ✓ |
| 手动连接客户端设备至管理服务器。klmover 实用程序 | ✓ | ✓ | ✓ |
| 自动安装 Kaspersky Security Center 组件的更新和补丁 | ✓ | ✓ | — |
| 自动分发密钥 | ✓ | ✓ | ✓ |
| 强制同步 | ✓ | ✓ | ✓<br>推送服务器除外 |
| **分发点** | | | |
| 用作分发点 | ✓<br>限制：不受适用于 Arm 架构 Microsoft Windows 的网络代理的支持。 | ✓ | ✓ |
| 计算分发点的数量和配置 | ✓<br>限制：不受适用于 Arm 架构 Microsoft Windows 的网络代理的支持。 | ✓<br>不使用网络定位感知 (NLA)。 | ✓<br>不使用网络定位感知 (NLA)。 |
| 离线模式更新下载 | ✓<br>限制：不受适用于 Arm 架构 Microsoft Windows 的网络代理的支持。 | ✓ | ✓ |
| 网络轮询 | ✓<br>• IP 范围轮询<br>• 域控制器轮询（Microsoft Active Directory）<br>限制：不受适用于 Arm 架构 Microsoft Windows 的网络代理的支持。 | ✓<br>IP 范围轮询<br>Zeroconf 轮询<br>域控制器轮询（Microsoft Active Directory、Samba 4 Active Directory、FreeIPA, ALD Pro） | — |
| 在分发点端运行 KSN 代理服务 | ✓<br>限制：不受适用于 Arm 架构 Microsoft Windows 的网络代理的支持。 | ✓ | — |

| 网络代理功能 | Windows | Linux | macOS |
| --- | --- | --- | --- |
| 通过卡巴斯基更新服务器将更新下载到将更新分发到受管理设备的分发点存储库 | ✓<br>限制：不受适用于 Arm 架构 Microsoft Windows 的网络代理的支持。 | ✓ | –<br>（如果一个或多个运行 Linux 或 macOS 的设备在“将更新下载至分发点存储库”任务范围内，则该任务将以“失败”状态完成，即使该任务在所有 Windows 设备上均已成功完成。） |
| 推送应用程序安装 | ✓<br>限制：不受适用于 Arm 架构 Microsoft Windows 的网络代理的支持。 | 受限制：无法使用 Linux 分发点在 Windows 设备上执行推送安装。 | 受限制：无法使用 macOS 分发点在 Windows 设备上执行推送安装。 |
| 用作推送服务器 | ✓<br>限制：不受适用于 Arm 架构 Microsoft Windows 的网络代理的支持。 | ✓ | – |
| **处理第三方应用程序** | | | |
| 在设备上远程安装应用程序 | ✓ | ✓ | ✓<br>请参阅以下文章了解详细信息：在 macOS 设备上远程安装应用程序。 |
| 在网络代理策略中配置操作系统更新 | ✓<br>限制：不受适用于 Arm 架构 Microsoft Windows 的网络代理的支持。 | – | – |
| 查看软件漏洞信息 | ✓<br>限制：不受适用于 Arm 架构 Microsoft Windows 的网络代理的支持。 | – | – |
| 扫描应用程序以查找漏洞 | ✓<br>限制：不受适用于 Arm 架构 Microsoft Windows 的网络代理的支持。 | – | – |
| 软件更新 | ✓<br>限制：不受适用于 Arm 架构 Microsoft Windows 的网络代理的支持。 | – | – |
| 清查设备上所安装的软件 | ✓ | ✓ | – |
| **虚拟机** | | | |
| 在虚拟机上安装网络代理 | ✓ | ✓ | ✓ |
| 虚拟桌面基础架构 (VDI) 的优化设置 | ✓<br>限制：不受适用于 Arm 架构 Microsoft Windows 的网络代理的支持。 | ✓ | ✓ |
| 对动态虚拟机的支持 | ✓<br>限制：不受适用于 Arm 架构 Microsoft Windows 的网络代理的支持。 | ✓ | ✓ |
| **其他** | | | |
| 使用 Windows 桌面共享来审核远程客户端设备上的操作 | ✓ | – | – |
| 监控反病毒保护状态 | ✓ | ✓ | ✓ |
| 管理设备重启 | ✓ | – | – |
| 支持文件系统回滚 | ✓ | ✓ | ✓ |
| 使用网络代理作为连接网关 | ✓ | ✓ | ✓ |
| 连接管理器 | ✓ | ✓ | ✓ |
| 漫游用户的连接配置文件 | ✓ | ✓ | ✓ |

| 网络代理功能 | Windows | Linux | macOS |
| --- | --- | --- | --- |
| 网络代理从一个管理服务器切换到另一个管理服务器（根据网络位置自动切换） | ✓ | ✓ | ✓ |
| 检查客户端设备与管理服务器之间的连接。klnagchk 实用程序 | ✓ | ✓ | ✓ |
| 远程连接至客户端设备桌面 | ✓ | ✓ | ✓<br>通过使用虚拟网络计算 (VNC) 系统。 |
| 通过迁移向导下载独立安装包 | ✓ | ✓ | ✓ |
| 查看客户端设备硬件的信息 | ✓ | ✓<br>安装在这些设备上的网络代理发送给管理服务器的 Linux 设备硬件信息仅限于受管理设备设置描述中指定的信息。 | ✓<br>安装在这些设备上的网络代理发送给管理服务器的 macOS 设备硬件信息仅限于受管理设备设置描述中指定的信息。 |

# 按操作系统比较网络代理设置

下表显示了可用的网络代理策略设置，具体取决于安装了网络代理的受管理设备的操作系统。

网络代理设置：按操作系统比较

| “设置”区域 | Windows | Linux | macOS |
| --- | --- | --- | --- |
| **常规** | ✓ | ✓ | ✓ |
| **事件配置** | ✓ | ✓ | ✓ |
| **设置** | ✓ | ✓<br>下列选项可用：<br>• **仅通过分发点分发文件**<br>• **事件队列的最大大小(MB)**<br>• **应用程序被允许在设备上检索策略扩展数据** | ✓ |
| **存储库** | ✓ | ✓<br>下列选项可用：<br>• **已安装应用程序详情**<br>• **硬件注册表的详细信息** | ✓<br>“**硬件注册表的详细信息**”选项可用。 |
| **连接→网络** | ✓ | ✓<br>除了**在 Microsoft Windows 防火墙中打开网络代理端口**选项之外。 | ✓ |
| **连接→连接配置文件** | ✓ | ✓ | ✓ |
| **连接→连接计划** | ✓ | ✓ | ✓ |
| **通过分发点的网络轮询** | ✓<br>下列选项可用：<br>• **Windows 网络**<br>• **IP 范围**<br>• **域控制器** | ✓<br>下列选项可用：<br>• **Zeroconf**<br>• **IP 范围**<br>• **域控制器** | — |
| **分发点网络设置** | ✓ | ✓ | ✓ |
| **KSN 代理(分发点)** | ✓ | ✓ | — |
| **更新(分发点)** | ✓ | ✓ | — |
| **修订历史** | ✓ | ✓ | ✓ |

# 启用和禁用网络代理的低资源消耗模式

在低资源消耗模式下，您可以限制安装在客户端设备上的网络代理的 RAM 使用量。默认情况下，低资源消耗模式被禁用。

在低资源消耗模式下，无法执行以下功能：

- 无法指定网络代理作为分发点（无论是手动还是自动）。
- 网络代理不会在单独的文本文件中记录有关网络代理状态的信息。
- 网络代理不支持离线模式的更新下载。
- 以下组件和进程被禁用：
  - 获取有关第三方更新和漏洞的信息。
  - 在分发点端运行 KSN 代理。
  - 将更新上传到分发点存储库。
  - 绕过 DNS 服务器阻止。
  - 获取有关可用磁盘空间的信息。

禁用低资源消耗模式后，组件和进程会恢复运行。

*要启用低资源消耗模式：*

1. 在客户端设备上的命令行中执行以下命令：

   ```
   sudo /opt/kaspersky/klnagent64/sbin/klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 1
   ```

2. 使用以下命令重新启动网络代理：

   ```
   sudo service klnagent64 restart
   ```

3. 在操作系统日志中，检查**Kaspersky Security Center 网络代理正在低资源消耗模式下工作**项是否显示。

   低资源消耗模式已启用。

*要禁用低资源消耗模式：*

1. 在客户端设备上的命令行中执行以下命令：

   ```
   sudo /opt/kaspersky/klnagent64/sbin/klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 0
   ```

2. 使用以下命令重新启动网络代理：

   ```
   sudo service klnagent64 restart
   ```

   低资源消耗模式被禁用。

您还可以使用*远程执行脚本任务*远程启用低资源消耗模式。

# 配置受管理应用程序的保护

若要配置受管理卡巴斯基应用程序的保护设置，您可以使用策略。

有关配置 Kaspersky Endpoint Security 策略的更多信息，请参阅相应帮助：

- Kaspersky Endpoint Security for Windows 帮助
- Kaspersky Endpoint Security for Linux 帮助
- Kaspersky Endpoint Security for Mac 帮助

# 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）。

# 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。

# 卡巴斯基安全网络 （KSN）

该部分描述如何使用卡巴斯基安全网络 (KSN) 的在线服务基础架构。该部分提供了关于 KSN 的详细描述，介绍了如何启用 KSN，配置对 KSN 的访问，并查看 KSN 代理服务器的使用统计。

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。

# 关于 KSN

卡巴斯基安全网络 (KSN) 是一种在线服务的基础架构，可提供对 Kaspersky 在线知识库的访问，其中包含与文件信誉、网络资源和软件相关的信息。使用卡巴斯基安全网络的数据，可确保卡巴斯基应用程序更快地响应威胁，提高某些保护组件的有效性，并降低误报风险。KSN 允许您使用 Kaspersky 的信誉数据库检索有关安装在受管理设备上的应用程序信息。

一旦加入 KSN，即表示您同意以自动模式将通过 Kaspersky Security Center Linux 管理的客户端设备上安装的 Kaspersky 程序的相关操作信息发送到 Kaspersky。依照当前KSN 访问设置发送信息。

Kaspersky Security Center Linux 支持以下 KSN 基础架构解决方案：

- *全球 KSN* 是一种允许您与 Kaspersky Security Network 交换信息的解决方案。一旦加入 KSN，即表示您同意以自动模式将通过 Kaspersky Security Center Linux 管理的客户端设备上安装的卡巴斯基应用程序的操作相关信息发送到 Kaspersky。依照当前KSN 访问设置发送信息。卡巴斯基分析师还分析收到的信息，并将其包含在卡巴斯基安全网络的信誉数据库和统计数据库中。Kaspersky Security Center Linux 默认使用此解决方案。

- *卡巴斯基私有安全网络 (KPSN)* 是一种解决方案，允许安装了卡巴斯基应用程序的设备用户访问卡巴斯基安全网络的信誉数据库和其他统计数据，而无需从用户自己的设备向全球 KSN 发送数据。KPSN 用于由于以下原因无法参与卡巴斯基安全网络的企业客户：

  - 用户设备未连接到互联网。

  - 法律或企业安全策略禁止传输任何数据到国家/地区以外或企业局域网以外。

  您可以在管理服务器属性窗口的 **KSN 代理**区域对卡巴斯基私人安全网络设置访问设置。

在运行快速启动向导时，应用程序会提示您加入 KSN。您可以在使用应用程序的任何时间启用或者停止 KSN。

您将根据您在启用 KSN 时阅读并接受的 KSN 声明来使用 KSN。如果 KSN 声明有更新，当您升级管理服务器的版本时会向您显示。您可以接受更新的 KSN 声明，也可以拒绝。如果您拒绝，您将根据之前接受的 KSN 声明的先前版本继续使用 KSN。

启用 KSN 后，Kaspersky Security Center Linux 会检查 KSN 服务器是否可访问，以确保受管理设备的安全级别得到维护。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。

管理服务器管理的客户端设备通过 KSN 代理服务器与 KSN 交互。KSN 代理服务器提供以下功能：

- 即使无法直接访问互联网，客户端设备也可以向 KSN 发送请求、从 KSN 获取信息以及向 KSN 传送信息。

- KSN 代理可缓存处理后的数据，从而减少发送通道的工作负荷以及为等待客户端设备所请求的信息而花费的时间。

您可以在管理服务器的属性窗口的“**KSN 代理**”部分配置 KSN 代理服务器。

# 设置对 KSN 的访问

您可以在管理服务器和分发点上设置到卡巴斯基安全网络 (KSN) 的访问。

*要设置管理服务器到 KSN 的访问：*

1. 在主菜单中，单击管理服务器名称。

   管理服务器属性窗口将打开。

2. 在“**常规**”选项卡上，选择“**KSN 代理**”区域。

3. 将切换按钮切换到“**在管理服务器上启用 KSN 代理 已启用**”位置。

   如果启用此选项，KSN 代理服务器会将数据发送到 KSN，以提高 Kaspersky Security Center 组件的效率并改善卡巴斯基应用程序的性能。数据被从客户端设备发送到 KSN，与在这些客户端设备上活动的 Kaspersky Endpoint Security 策略一致。如果此切换按钮被禁用，则数据不会通过 Kaspersky Security Center Linux 从管理服务器以及客户端设备发送到 KSN。但是，客户端设备能够根据其设置直接将数据发送到 KSN（绕过 Kaspersky Security Center Linux）。在客户端设备上活动的 Kaspersky Endpoint Security 策略决定了哪些数据将被直接从那些设备发送到 KSN（绕过 Kaspersky Security Center Linux）。

4. 选择 KSN 基础设施解决方案。

   在**参与 KSN** 子部分中，执行以下操作之一：

   - 如果使用的是全球 KSN，请将切换按钮切换到“**使用卡巴斯基安全网络已启用**”位置。

     启用此选项时，请确保阅读并接受 KSN 声明的条款。

   - 如果要使用 KPSN，请将切换按钮切换到“**使用卡巴斯基私人安全网络已启用**”位置，然后单击“**选择 KSN 代理设置文件**”按钮以下载 KPSN 设置（带有 pkcs7 和 pem 扩展名的文件）。下载完设置之后，界面会显示提供商的名称和联系人，以及 KPSN 设置文件的创建日期。

   将切换按钮切换到“**使用卡巴斯基私人安全网络已启用**”位置时，将显示一条消息，其中包含有关 KPSN 的详细信息。

   以下卡巴斯基应用程序支持 KPSN：

   - Kaspersky Security Center Linux
   - Kaspersky Endpoint Security for Linux
   - Kaspersky Endpoint Security for Windows

   如果您在 Kaspersky Security Center Linux 中启用 KPSN，这些应用程序将接收支持 KPSN 的相关信息。在应用程序设置窗口，在**高级威胁保护**区域的**卡巴斯基安全网络**子区域中，将显示有关选定 KSN 提供者的信息：KSN 或 KPSN。

   > 如果在管理服务器属性窗口的“**KSN 代理**”区域中配置了 KPSN，则 Kaspersky Security Center Linux 不发送任何统计数据到卡巴斯基安全网络。

5. 如果您在管理服务器属性中配置了代理服务器设置，但您的网络架构要求您直接使用 KPSN，请启用“**当连接到 KPSN 时忽略代理服务器设置**”选项。否则，从受管理应用程序的请求无法到达 KPSN。

6. 配置管理服务器到 KSN 代理服务的连接：

   - 在“**连接设置**”下，对于“**TCP 端口**”，指定用于连接到 KSN 代理服务器的 TCP 端口号。连接到 KSN 代理的默认端口是 13111。
   - 如果您要让管理服务器通过 UDP 端口连接到 KSN 代理服务器，请启用“**使用 UDP 端口**”选项，并为“**UDP 端口**”指定端口号。默认情况下，此选项为禁用状态，并且使用 TCP 端口。如果启用此选项，默认将使用 UDP 端口 15111 连接到 KSN 代理服务器。
   - 如果您要让管理服务器通过 HTTPS 端口连接到 KSN 代理服务器，请启用“**使用 HTTPS**”选项，并为“**HTTPS 端口**”指定端口号。默认情况下，此选项为禁用状态，并且使用 TCP 端口。如果启用此选项，默认将使用 HTTPS 端口 17111 连接到 KSN 代理服务器。

7. 将切换按钮切换到**通过主管理服务器连接从属管理服务器到 KSN 已启用**位置。

   如果启用此选项，从属管理服务器使用主管理服务器作为 KSN 代理服务器。如果禁用此选项，从属管理服务器自己连接到 KSN。该情况下，受管理设备使用从属管理服务器作为 KSN 代理服务器。

   > 如果在从属管理服务器属性的“**KSN 代理**”区域的右侧面板中将切换按钮切换到“**在管理服务器上启用 KSN 代理 已启用**”位置，则从属管理服务器将使用主管理服务器作为代理服务器。

8. 单击“**保存**”按钮。

KSN 访问设置将被保存。

您也可以设置分发点访问 KSN，例如，如果您想降低管理服务器负载。作为 KSN 代理服务器的分发点从受管理设备直接发送 KSN 请求到 Kaspersky，不使用管理服务器。

*要设置分发点到卡巴斯基安全网络（KSN）的访问：*

1. 确保分发点是手动分配。
2. 在主菜单中，单击管理服务器名称。

   管理服务器属性窗口将打开。
3. 在“**常规**”选项卡上，选择“**分发点**”区域。
4. 单击分发点的名称以打开其属性窗口。
5. 在分发点属性窗口的“**KSN 代理**”区域中，启用“**在分发点端启用 KSN 代理**”选项，然后启用“**通过互联网直接访问 KSN 云/KPSN**”选项。
6. 单击“**确定**”。

该分发点将作为 KSN 代理服务器。

> 请注意，分发点不支持使用 NTLM 协议进行受管理设备身份验证。

# 启用和禁用 KSN 的使用

*要启用 KSN，请执行以下操作：*

1. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**KSN 代理**”区域。
3. 将切换按钮切换到“**在管理服务器上启用 KSN 代理 已启用**”位置。

KSN 代理服务器被启用并将数据发送到 KSN，以提高 Kaspersky Security Center 组件的效率并改善卡巴斯基应用程序的性能。

1. 根据您使用的KSN 基础设施解决方案，启用相应的切换按钮。
   - 如果使用的是全球 KSN，请将切换按钮切换到“**使用卡巴斯基安全网络已启用**”位置。
     现在可以将数据发送到 KSN。启用此选项时，您必须阅读并接受 KSN 声明的条款。
   - 如果使用的是 KPSN，请将切换按钮切换到“**使用卡巴斯基私人安全网络已启用**”位置，然后单击“**选择 KSN 代理设置文件**”按钮以下载 KPSN 设置（带有 pkcs7 和 pem 扩展名的文件）。下载完设置之后，界面会显示提供商的名称和联系人，以及 KPSN 设置文件的创建日期。
     将切换按钮切换到“**使用卡巴斯基私人安全网络已启用**”位置时，将显示一条消息，其中包含有关 KPSN 的详细信息。
2. 单击“**保存**”按钮。

*要禁用 KSN，请执行以下操作：*

1. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**KSN 代理**”区域。
3. 将切换按钮切换到**在管理服务器上启用 KSN 代理 已禁用**位置，以禁用 KSN 代理服务。
4. 单击“**保存**”按钮。

# 查看已接受的 KSN 声明

启用卡巴斯基安全网络 (KSN) 时，必须阅读并接受 KSN 声明。您可以随时查看已接受的 KSN 声明。

*要查看已接受的 KSN 声明：*

1. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口将打开。

2. 在“**常规**”选项卡上，选择“**KSN 代理**”区域。

3. 单击**查看卡巴斯基安全网络声明**链接。

在打开的窗口中，可以查看已接受的 KSN 声明的文本。

# 接受更新的 KSN 声明

您将根据您在启用 KSN 时阅读并接受的 KSN 声明来使用 KSN。如果 KSN 声明有更新，当您升级管理服务器的版本时会向您显示。您可以接受更新的 KSN 声明，也可以拒绝。如果您拒绝，您将根据之前接受的 KSN 声明的版本继续使用 KSN。

升级管理服务器版本后，将自动显示更新的 KSN 声明。如果您拒绝更新的 KSN 声明，您仍然可以在以后查看并接受它。

*要查看然后接受或拒绝更新的 KSN 声明：*

1. 单击应用程序主窗口右上角的“**查看通知**”链接。

“**通知**”窗口打开。

2. 单击“**查看更新的 KSN 声明**”链接。

**卡巴斯基安全网络声明更新**窗口打开。

3. 阅读 KSN 声明，然后单击以下按钮之一做出决定：

- **我接受更新的 KSN 声明**
- **在旧声明下使用 KSN**

根据您的选择，KSN 会按照当前或更新的 KSN 声明的条款继续工作。您可以随时在管理服务器的属性中查看接受的 KSN 声明的文本。

# 检查分发点是否充当 KSN 代理服务器

在分配为充当分发点的受管理设备上，可以启用 Kaspersky Security Network (KSN) 代理。当 ksnproxy 服务在设备上运行时，受管理设备充当 KSN 代理服务器。您可以在设备上本地检查、打开或关闭此服务。

您可以将基于 Windows 或基于 Linux 的设备分配为分发点。检查分发点的方法取决于该分发点的操作系统。

*要检查基于 Linux 的分发点是否充当 KSN 代理服务器：*

1. 在分发点设备上，运行`ps aux`命令以显示正在运行的进程列表。

2. 在正在运行的进程列表中，检查 `/opt/kaspersky/klnagent64/sbin/ksnproxy` 进程是否正在运行。

如果 `/opt/kaspersky/klnagent64/sbin/ksnproxy` 进程正在运行，则设备上的网络代理会参与卡巴斯基安全网络，并充当分发点范围内包括的受管理设备的 KSN 代理服务器。

*要检查基于 Windows 的分发点是否充当 KSN 代理服务器：*

1. 在分发点设备上的 Windows 中，打开“**服务**”（“**所有程序**”→“**管理工具**”→“**服务**”）。
2. 在服务列表，检查 ksnproxy 服务是否正在运行。

   如果 ksnproxy 服务正在运行，则设备上的网络代理会参与卡巴斯基安全网络，并充当分发点范围内包括的受管理设备的 KSN 代理服务器。

如果您想，您可以关闭 ksnproxy 服务。在这种情况下，分发点上的网络代理停止参与卡巴斯基安全网络。该需要本地管理员权限。

# 查看 KSN 代理服务器的统计信息

Kaspersky Security Center Web Console 可让您查看 KSN 代理服务器的使用统计信息。

统计信息包括以下参数：

- 与 KSN 的连接状态
- 缓存记录数
- 缓冲中处理的包数
- 收到的数据包数量

如果您使用 KPSN 作为基础设施解决方案，则会显示 KPSN 的使用统计信息。

*查看统计信息：*

1. 在主菜单中，单击管理服务器名称。

   管理服务器属性窗口将打开。
2. 在**常规**选项卡上，选择**KSN 代理**部分，然后打开**统计**选项卡。

   该选项卡将显示 KSN 代理服务器使用的实际统计。统计数据每 15 秒刷新一次。

您可以通过单击**复制到剪贴板**按钮来复制统计数据。

# 管理任务

本节介绍 Kaspersky Security Center Linux 使用的任务。

# 关于任务

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

特定应用程序的任务可以使用 Kaspersky Security Center Web Console 创建，仅在该应用程序的管理插件安装在 Kaspersky Security Center Web Console 服务器上时。

任务可以在管理服务器和设备上执行。

管理服务器上执行的任务包含以下：

- 自动分发报告
- 将更新下载至存储库
- 备份管理服务器数据
- 数据库维护

以下类型的任务在设备上执行：

- *本地任务* — 在特定设备上执行的任务。

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

- *组任务* — 在特定组的所有设备上执行的任务。

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

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

您可以为每个应用程序创建不管多少个组任务、全局任务或本地任务。

您可以更改任务设置、查看任务进度、复制、导出、导入和删除任务。

仅当为其创建任务的应用程序在运行时，才能在设备上启动任务。

任务执行结果保存在每台设备的操作系统事件日志、管理服务器上的操作系统事件日志和管理服务器数据库中。

不在任务设置中包括私人数据。例如，避免指定域管理员密码。

# 关于任务范围

*任务范围*是执行任务的设备集合。范围的类型包括以下：

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

当创建*全局任务*时，您可以使用以下方法指定范围：

- 手动指定特定设备。

  您可以使用 IP 地址（或 IP 范围）或 DNS 名称作为设备地址。您还可以选择由管理服务器检测到的联网设备。

- 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：*

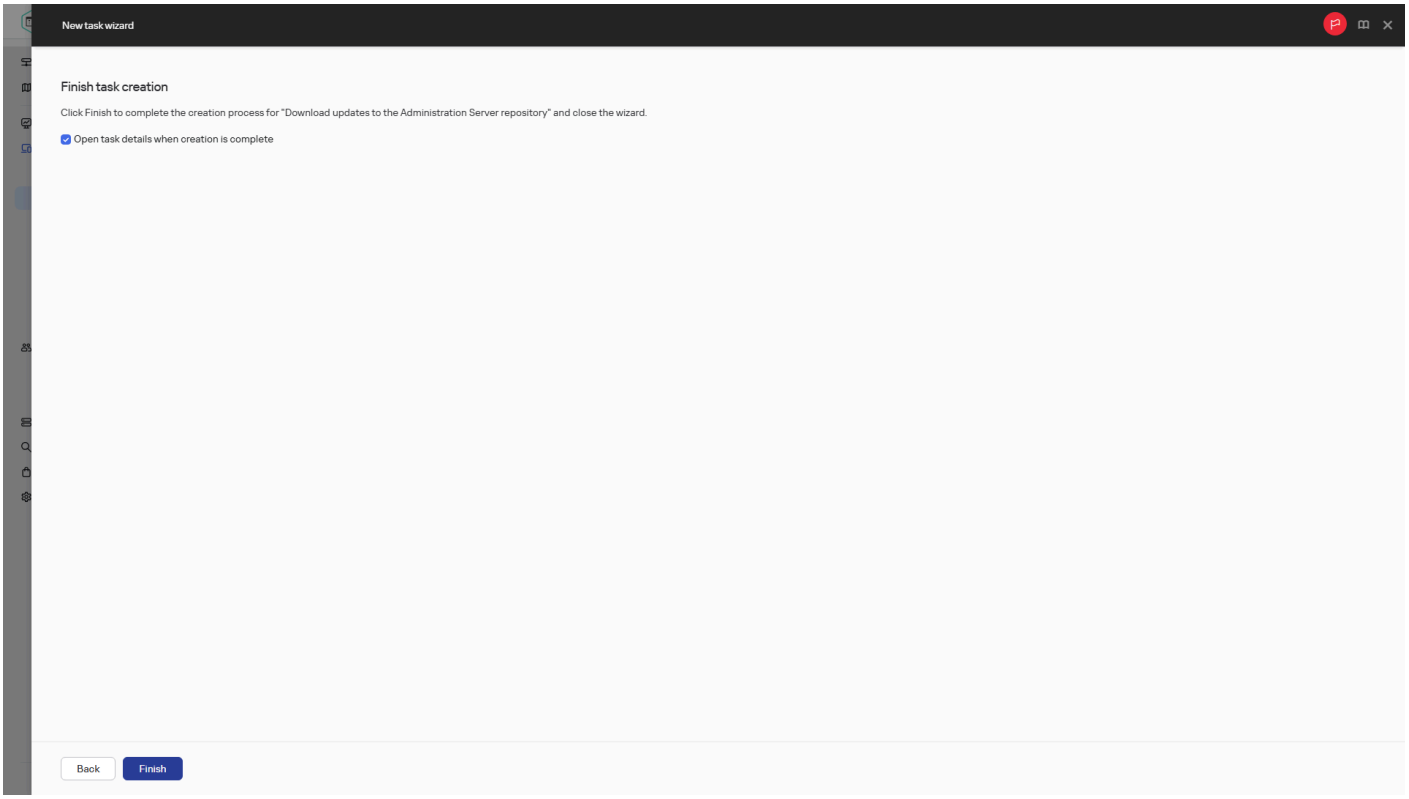
1. 在主菜单中，转到“**任务**”。
2. 单击**添加**。

   “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。




完成任务创建

*要创建分配给所选设备的新任务：*

1. 在主菜单中，转到“**资产管理**”→“**资产(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。

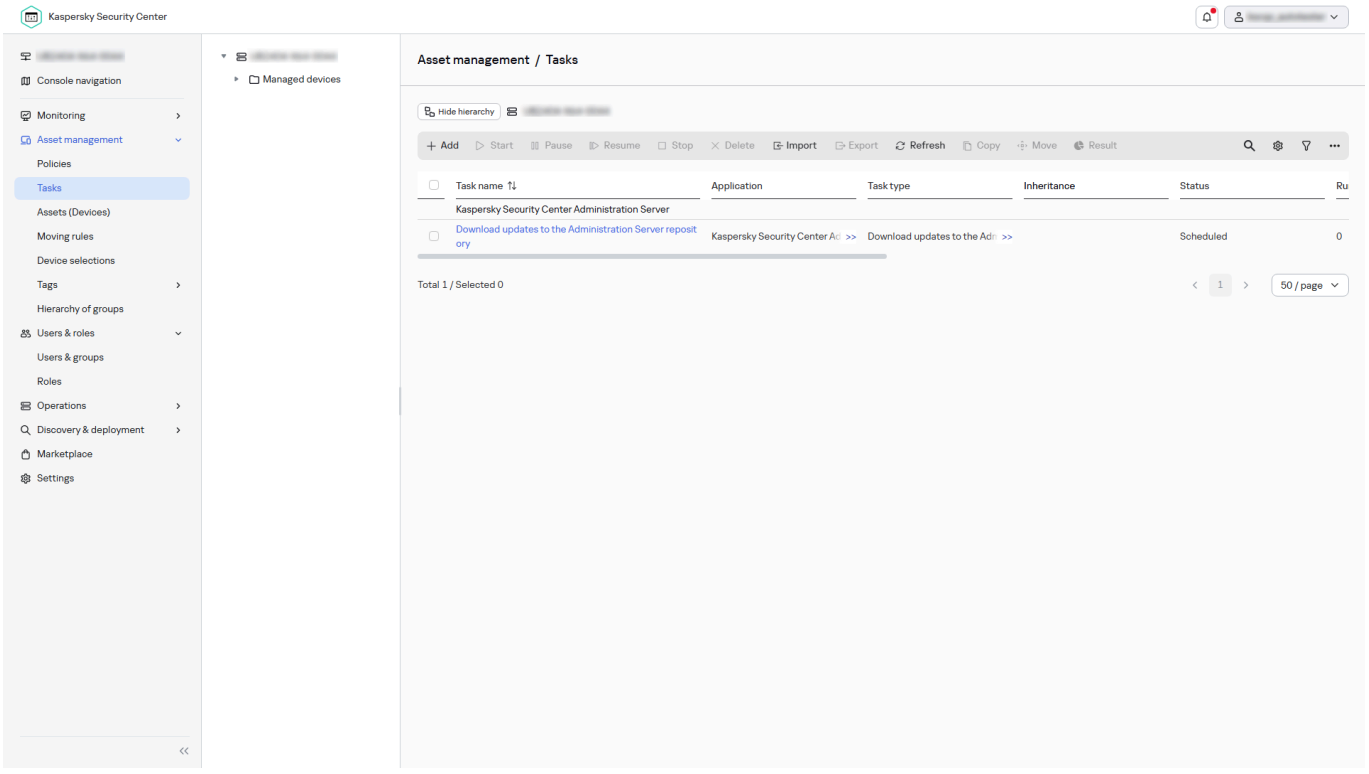
任务为选定的设备创建。

# 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“**资产(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“**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。




从任务列表中启动任务

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。

# 为选择的设备执行任务

您可以在设备列表中选择一台或多台客户端设备，然后启动之前为它们创建的任务。这可让您运行之前为一组特定设备创建的任务。

这会将任务被分配到的设备更改到您在运行任务时选择的设备列表。

*要为选择的设备启动任务：*

1. 在主菜单中，转到**资产管理 → 资产(设备)**。将显示受管理设备列表。
2. 在受管理设备列表中，使用复选框选择要为其运行任务的设备。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**应用现有任务**。

   现有任务列表将得到显示。
4. 所选设备显示在任务列表上方。如有必要，您可以从此列表中删除设备。除一台设备之外您可以删除所有设备。

5. 在列表中选择所需的任务。您可以使用列表上方的搜索框按名称搜索所需的任务。只能选择一项任务。

6. 单击**保存并启动任务**。

所选任务立即为所选设备启动。任务中的计划启动设置不会更改。

# 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，*

在主菜单中，转到“**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。

*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

本部分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：

> 计划的类型可能根据任务而有所不同。

> 某些类型的计划可能不适用于其他卡巴斯基应用程序。

  - **启动任务设置：**

    - **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 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。

    - **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。

    - **一次**

      该任务在指定的日期和时间运行一次（默认情况下，在创建任务的当天）。

- **立即**

  任务在设置保存后立即运行。

- **每月在所选工作日**

  任务定期运行，在指定月日的指定时间。

  默认情况下，开始时间为18:00，且未选择任何日期。

  > 请注意，您选择的是当月的星期几，而不是具体的日期，也不是具体的周数（例如，当月的第一周或第二周）。例如，如果您将光标设置在第一行的**周二**单元格中，这意味着任务将在每月的**第一周**星期二运行。

  您可以选择一周中的多个日期。

- **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。仅当两个任务被分配给同一设备时，此选项才可用。例如，您可能想使用“***Turn on the device***”选项运行开启设备任务，在它完成后，运行*病毒扫描*任务作为触发任务。

  您必须从表中选择触发任务以及该任务必须完成的状态（**成功完成**或**失败**）。

  如有必要，您可以按如下方式搜索、排序和过滤表中的任务：

  - 在搜索栏中输入任务名称，即可根据名称搜索任务。
  - 单击排序图标可按名称对任务进行排序。

    默认情况下，任务按字母顺序升序排列。
  - 单击过滤器图标，在打开的窗口中按组过滤任务，然后单击**应用**按钮。

- **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卡巴斯基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。

- **使用任务启动自动随机延迟间隔**

  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：
  - **使用 Wake-On-LAN 功能在任务启动之前开启设备**

    设备上的操作系统在任务开始之前的指定时间启动。默认时间段为五分钟。

    如果您想要任务在任务范围内的所有客户端设备上运行，包括任务要启动时关闭的设备，则启用该选项。

    如果您希望在任务完成后自动关闭设备，请启用“**任务完成后关闭设备**”选项。可以在同一窗口中找到此选项。

    默认情况下已禁用该选项。

  - **任务完成后关闭设备**

    例如，您可能想为每周五工作时间后安装更新到客户端设备的更新安装任务启用该选项，然后在周末关闭这些设备。

    默认情况下已禁用该选项。

  - **如果任务运行超过该时间则停止**

    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，请单击“**设置**”链接。

    默认下，所有通知方法被禁用。

  - **仅通知错误**

    如果该选项被启用，管理员仅在任务执行完成但带有错误时被通知。

    如果该选项被禁用，管理员在每次任务执行完成后被通知。

    默认情况下已启用该选项。

- 安全设置。
- 任务范围设置。

取决于任务范围决定的方式，以下设置被展现：

- **设备。**

  如果任务范围由管理组决定，您可以查看该组。这里不可以更改。然而，您可以设置**任务范围排除项**。

  如果任务范围由设备列表决定，您可以通过添加和删除设备修改该列表。

- **设备分类**

  您可以更改应用程序任务的设备分类。

- **任务范围排除项**

  您可以指定应用任务的设备组。要排除的组仅可以是应用任务的管理组的子组。

- **修订历史**。

# 导出任务

Kaspersky Security Center Linux 允许您将任务及其设置保存到 KLT 文件。您可以使用此 KLT 文件将保存的任务导入到 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux。

*要导出任务，请执行以下操作：*

1. 在主菜单中，转到“**任务**”。
2. 选中要导出的任务旁边的复选框。
   您不能同时导出多个任务。如果您选择了多个任务，**导出**按钮将被禁用。管理服务器任务也将无法导出。
3. 单击“**导出**”按钮。
4. 在打开的“**另存为**”窗口中，指定任务文件的名称和路径。单击“**保存**”按钮。
   仅当您使用 Google Chrome、Microsoft Edge 或 Opera 时，才会显示“**另存为**”窗口。如果您使用其他浏览器，则任务文件会自动保存在“**下载**”文件夹。

# 导入任务

Kaspersky Security Center Linux 允许您从 KLT 文件导入任务。KLT 文件包含导出的任务及其设置。

为了正确导入卡巴斯基应用程序任务，您必须安装相应的管理插件。

*要导入任务，请执行以下操作：*

1. 在主菜单中，转到“**任务**”。
2. 单击“**导入**”按钮。
3. 单击**浏览**按钮选择要导入的任务文件。

4. 在打开的窗口中，指定 KLT 任务文件的路径，然后单击“**打开**”按钮。请注意，您仅可选择一个任务文件。
   任务处理启动。

5. 任务成功处理后，选择要向其分配任务的设备。为此，请选择以下选项之一：

   - **分配任务到管理组**

     任务被分配到包含在管理组中的设备。您可以指定现有组之一或者创建新组。

     例如，您可能要使用该选项运行发送消息到用户任务，如果消息针对包含在特定管理组中的设备。

     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。

6. 指定任务范围。

7. 单击**完成**按钮以完成任务导入。

出现包含导入结果的通知。如果任务成功导入，可以单击“**详细信息**”链接以查看任务属性。

成功导入后，任务会显示在任务列表中。任务设置和时间表也会一起导入。任务将根据其时间表启动。

> 如果新导入的任务与现有任务具有相同的名称，则导入的任务在名称后会附加一个 **(<下一个序列号>)** 索引，例如：**(1)**、**(2)**。

# 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. 在主菜单中，转到“**任务**”。

2. 单击**管理启动任务的账户凭证**。

   遵照向导的说明操作。

## 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 Linux 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 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 Linux 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。

*要查看任务结果：*

1. 在任务属性窗口中，选择“**常规**”部分。
2. 单击“**结果**”链接打开“**任务结果**”窗口。

*要查看从属管理服务器的任务结果：*

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。
3. 单击“**从属服务器的统计信息**”。
4. 选择要显示“**任务结果**”窗口的从属服务器。

# 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] 标签并将其分配给所有浏览器（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“**软件管理** ”→“**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“**软件管理**” → “**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“**软件管理**”→“**第三方应用程序**”→“**应用程序注册表**”。

2. 单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“**软件管理**”→“**第三方应用程序**”→“**应用程序注册表**”。

2. 单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“**软件管理**” → “**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。

# 使用 klscflag 实用程序开放端口 13291

您可以使用 klbackup 实用程序来实现 Kaspersky Security Center Linux 的自动化运行。klakaut 实用程序及其帮助系统位于 Kaspersky Security Center Linux 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。

# 在 Kaspersky Security Center Web Console 中注册 Kaspersky Industrial CyberSecurity for Networks 应用程序

要开始通过 Kaspersky Security Center Web Console 使用 Kaspersky Industrial CyberSecurity for Networks Web 应用程序，您必须首先在 Kaspersky Security Center Web Console 中注册它。

*要注册 Kaspersky Industrial CyberSecurity for Networks 应用程序：*

1. 确保完成以下操作：

   - 您已下载并安装 Kaspersky Industrial CyberSecurity for Networks Web 插件。

     您可以稍后在等待 Kaspersky Industrial CyberSecurity for Networks Server 与管理服务器同步时执行此操作。下载并安装插件后，**KICS for Networks**部分将显示在 Kaspersky Security Center Web Console 主菜单中。

   - 在 Kaspersky Industrial CyberSecurity for Networks 网页界面中，配置并启用了与 Kaspersky Security Center 的交互。详情请参阅 Kaspersky Industrial CyberSecurity for Networks 在线帮助。

2. 将安装有 Kaspersky Industrial CyberSecurity for Networks Server 的设备从未分配设备组移动到受管理设备组：

   a. 在主菜单中，转到“**Asset management**” → “**Unassigned devices**”。

   b. 选中安装有 Kaspersky Industrial CyberSecurity for Networks Server 的设备旁边的复选框。

   c. 单击**移动到组**按钮。

   d. 在管理组的层次结构中，选中**受管理设备**组旁边的复选框。

   e. 单击“**移动**”按钮。

3. 打开安装了 Kaspersky Industrial CyberSecurity for Networks Server 的设备的属性窗口。

4. 在设备属性页面的 **General** 部分，选择“**不要断开与管理服务器的连接**”选项，然后单击“**保存**”按钮。

5. 在设备属性页面，选择**应用程序**区域。

6. 在**应用程序**区域，选择 Kaspersky Security Center 网络代理。

7. 如果应用程序的当前状态是“*已停止*”，等到它变为“*正在运行*”。

   这最多需要 15 分钟。如果您尚未安装 Kaspersky Industrial CyberSecurity for Networks Web 插件，您可以立即安装。

8. 如果想查看 Kaspersky Industrial CyberSecurity for Networks 的统计信息，您可以在仪表板上添加小部件。要添加小部件，请执行以下操作：

   a. 在主菜单中，转到“**监控**”→“**仪表板**”。

   b. 在仪表板上，单击“**添加或恢复网页小部件**”按钮。

   c. 在打开的小部件菜单中，选择“**其它**”。

   d. 选择您要添加的小部件：

      - KICS for Networks 部署图
      - 有关 KICS for Networks Servers 的信息
      - KICS for Networks 的最新活动
      - KICS for Networks 中存在问题的设备
      - KICS for Networks 中的关键事件
      - KICS for Networks 中的状态

9. 要继续访问 Kaspersky Industrial CyberSecurity for Networks Web 界面，请执行以下操作：

   a. 在主菜单中，转至**KICS for Networks** →**搜索**。

   b. 单击**查找事件或设备**按钮。

   c. 在打开的**查询参数**窗口中，单击**服务器**字段。

   d. 从与 Kaspersky Security Center 集成的服务器下拉列表中选择 Kaspersky Industrial CyberSecurity for Networks 服务器，然后单击**查找**按钮。

   e. 单击 Kaspersky Industrial CyberSecurity for Networks 服务器名称旁边的**转至服务器**链接。

      Kaspersky Industrial CyberSecurity for Networks 登录页面将显示。

      要登录 Kaspersky Industrial CyberSecurity for Networks Web 界面，您需要提供应用程序用户账户凭据。

# 管理用户和用户角色

该部分描述了用户和用户角色，并提供创建和修改它们、分配角色和组到用户以及关联策略配置文件到角色的说明。

# 关于用户账户

Kaspersky Security Center Linux 允许您管理用户账户以及安全组。应用程序支持三种账户类型：

- 组织员工的账户。在轮询组织的域控制器时管理服务器检索数据的域用户的账户。
- 本地用户账户。受管理设备上的本地账户，以及安装了管理服务器的设备上的本地账户。
- Kaspersky Security Center Linux 内部用户的账户。您可以创建内部用户账户。这些账户仅在 Kaspersky Security Center Linux 内使用。

kladmins 组不能被用来在 Kaspersky Security Center Linux 中存取 Kaspersky Security Center Web Console。kladmins 组只能包含被用来启动 Kaspersky Security Center Linux 服务的账户。

*查看用户账户和安全组表：*

1. 在主菜单中，转至“**用户和角色**” → “**用户和组**”。
2. 选择**用户**或**组**选项卡。

用户或安全组表将打开。如果要查看仅包含内部用户或组或仅包含本地用户或组的表，请将**账户类型**过滤条件分别设置为**内部**或**本地**。

如果用户表包含超过 50,000 个用户，则仅显示前 50,000 个用户，其余用户将不显示。

# 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卡巴斯基应用程序设置关联。您可以分配角色到用户集，或者到管理组层级的任何级别、管理服务器或特定对象级别的安全组集。

如果您通过包含虚拟管理服务器的管理服务器层级来管理设备，请注意，您仅可从物理管理服务器创建、修改或删除用户角色。这样，您可以将用户角色传输到从属管理服务器，包括虚拟服务器。

您可以关联用户角色到策略配置文件。如果用户被分配角色，用户将获得执行工作职能所需的安全设置。

一个用户角色可以与特定管理组中的设备用户关联。

### 用户角色范围

*用户角色范围*是用户和管理组的组合。与用户角色关联的设置仅应用到属于该角色用户的设备，以及仅在这些设备属于与该角色关联的组（包括子组）时。

### 使用角色的好处

使用角色的好处之一是您不必为每个受管理设备或用户指定安全设置。公司中的用户和设备数量可能太大，但是需要不同安全设置的不同工作的数量相对较小。

### 与使用策略配置文件的不同点

策略配置文件是为每个卡巴斯基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**、**写入**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** | **写入** | • 将设备添加到管理组：**写入**<br>• 从管理组中删除设备：**写入**<br>• 将管理组添加到另一个管理组：**写入**<br>• 将管理组从另一个管理组中删除：**写入** | 无 | 无 | 无 |

| 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**：**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 | **常规功能：访问对象而不考虑它们的 ACLs** 功能区域用于审计目的。当用户被授予此功能区域的**读取**权限时，他们将获得对所有对象的完全**读取**权限，并能够以本地管理员权限（Linux 的 root 权限）在通过网络代理连接到管理服务器的设备上执行任何创建的任务。我们建议谨慎地将这些权限授予有限数量的用户，这些用户需要这些权限来履行工作职责。<br>即使其他权限禁止对特定对象的读取访问，访问权限也会被授予。 |
| **常规功能**：**基本功能** | • **读取**<br>• **写入**<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）：**写入**、**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：**写入**<br>• 查看组的访问控制列表：**读取**<br>• 查看操作系统日志：**读取**<br>• 查看用于恢复对 BitLocker 加密的硬盘的访问权限的恢复密钥：**执行** | • “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>• “已安装的邮件系统保护应用程序汇总报告”<br>• “已安装的工作站保护应用程序和 Windows Server 保护应用程序汇总报告”<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报告”<br>• “受感染的设备用户报告”<br>• “安全问题报告”<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>• “漏洞报告”<br>• “禁止的应用程序报告”<br>• “Web 控制报告”<br>• “受管理设备加密状态报告”<br>• “大容量存储设备加密状态报告”<br>• “加密驱动器访问权限报告”<br>• “文件加密错误报告”<br>• “加密文件访问被阻止报告”<br>• “有效用户权限报告”<br>• “权限报告” | 无 |
| **常规功能**：**已删除对象** | • **读取**<br>• **写入** | • 查看回收站中的已删除对象：**读取**<br>• 删除回收站中的对象：**写入** | 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>• **写入** | • 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 |

| 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**：**对管理服务器的操作** | • **读取**<br>• **写入**<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：**写入**<br>• 指定在管理服务器上启动的激活代理端口：**写入**<br>• 指定在管理服务器上启动的移动激活代理端口：**写入**<br>• 指定用于分发独立安装包的 Web 服务器端口：**写入**<br>• 指定用于分发 MDM 配置文件的 Web 服务器端口：**写入**<br>• 指定用于通过 Web 控制台连接的管理服务器 SSL 端口：**写入**<br>• 指定用于移动连接的管理服务器端口：**写入**<br>• 指定管理服务器数据库中存储的最大事件数量：**写入**<br>• 指定管理服务器可以发送的最大事件数量：**写入**<br>• 指定管理服务器可以发送事件的时间段：**写入** | • “备份管理服务器数据”<br>• “数据库维护” | 无 | 无 |
| **常规功能**：**Kaspersky 软件部署** | • **管理 Kaspersky 补丁**<br>• **读取**<br>• **写入**<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：<br>"Kaspersky" |
| **常规功能**：**密钥管理** | • **导出密钥文件**<br>• **写入** | • 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：**写入** | 无 | 无 | 无 |
| **常规功能**：**强制报告管理** | • **读取**<br>• **写入** | • 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** | 无 | 无 | 无 |

| 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 |
| --- | --- | --- | --- | --- | --- |
| | | • 管理安全组：**修改对象** ACL<br>• 管理别名：**修改对象** ACL | | | |
| **常规功能**：**虚拟管理服务器** | • **管理虚拟管理服务器**<br>• **读取**<br>• **写入**<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 |

| 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**：**加密密钥管理** | **写入** | 导入加密密钥：**写入** | 无 | 无 | 无 |
| **移动设备管理**：**常规** | • **连接新设备**<br>• **仅发送信息命令到移动设备**<br>• **发送命令到移动设备**<br>• **管理证书**<br>• **读取**<br>• **写入** | • 获取密钥管理服务还原数据：**读取**<br>• 删除用户证书：**管理证书**<br>• 获取用户证书的公开部分：**读取**<br>• 检查是否启用了公钥基础结构：**读取**<br>• 检查公钥基础结构账户：**读取**<br>• 获取公钥基础结构模板：**读取**<br>• 通过扩展密钥用法证书获取公钥基础结构模板：**读取**<br>• 检查公钥基础结构证书是否被吊销：**读取**<br>• 更新用户证书发行设置：**管理证书**<br>• 获取用户证书发行设置：**读取**<br>• 按应用程序名称和版本获取软件包：**读取**<br>• 设置或取消用户证书：**管理证书**<br>• 续订用户证书：**管理证书**<br>• 设置用户证书标签：**管理证书**<br>• 运行 MDM 安装包的生成；取消生成 MDM 安装包：**连接新设备** | 无 | 无 | 无 |
| **系统管理**：**连接性** | • **开始 RDP 会话**<br>• **连接到现有 RDP 会话**<br>• **启动隧道**<br>• **将设备中的文件保存到管理员工作站**<br>• **读取**<br>• **写入**<br>• **执行**<br>• **对设备分类执行操作** | • 创建桌面共享会话：**创建桌面共享会话的权限**<br>• 创建 RDP 会话：**连接到现有 RDP 会话**<br>• 创建隧道：**启动隧道**<br>• 保存内容网络列表：**将设备中的文件保存到管理员工作站** | 无 | “设备用户报告” | 无 |
| **系统管理**：**漏洞和补丁管理** | • **读取**<br>• **写入**<br>• **执行**<br>• **对设备分类执行操作** | • 查看第三方补丁属性：**读取**<br>• 更改第三方补丁属性：**写入** | • “修复漏洞”<br>• “安装所需更新并修复漏洞” | “软件更新报告” | 无 |
| **系统管理**：**远程执行脚本** | • **读取**<br>• **写入**<br>• **执行**<br>• **对设备分类执行操作** | 用户可以查看任务属性：**读取** | “远程执行脚本” | 无 | 无 |

| 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 |
| --- | --- | --- | --- | --- | --- |
| | | 用户可以创建、删除或修改安装包：**写入**<br><br>用户可以运行任务：**写入**。在客户端 Linux 设备上，脚本以 root 权限执行。<br><br>用户可以运行任务或安排其运行：**执行**<br>用户可以在所选设备上运行任务：**在所选设备上执行操作** | | | |

# 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。

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。

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。当创建新角色时，您必须自己设置角色范围并分配对 Kaspersky Security Center Linux 功能的访问权限。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 | 允许在通过网络代理以本地管理员权限（Linux 为 root）连接到管理服务器的选定设备上执行所有查看操作和执行任何创建的任务。<br><br>我们建议谨慎地将该角色指派给有限数量的用户，这些用户需要它们来履行工作职责。 |
| 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。

预定义用户角色的访问权限

| 角色 | 描述 |
| --- | --- |
| 管理服务器管理员 | 允许在以下功能区域的所有操作：<br>• **常规功能**：<br>  • **基本功能**<br>  • **加密密钥管理**<br>  • **事件处理**<br>  • **管理服务器层级**<br>  • **虚拟管理服务器**<br>• **系统管理**：<br>  • **连接**<br>  • **硬件清单**<br>  • **软件清查** |
| 管理服务器操作员 | 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>  • **加密密钥管理**<br>  • **虚拟管理服务器**<br>• **系统管理**：<br>  • **连接**<br>  • **硬件清单**<br>  • **软件清查** |
| 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 | 允许在以下功能区域的所有操作：<br>• **常规功能：**<br>  • **基本功能**<br>  • **卡巴斯基应用程序部署**<br>  • **授权许可密钥管理**<br>• **系统管理：**<br>  • **操作系统部署**<br>  • **漏洞和补丁管理**<br>  • **远程安装**<br>  • **软件清查**<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。 |

| 角色 | 描述 |
| --- | --- |
| 安装操作员 | 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>  • **卡巴斯基应用程序部署**（也授予在该区域的**管理 Kaspersky 补丁**权限）<br>  • **虚拟管理服务器**<br>• **系统管理：**<br>  • **操作系统部署**<br>  • **漏洞和补丁管理**<br>  • **远程安装**<br>  • **软件清查** |
| 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**<br>• **常规功能：加密密钥管理**<br>• **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**（如果适用）权限：<br>• **常规功能：基本功能**<br>• **常规功能：加密密钥管理**<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>  • **加密密钥管理**<br>  • **管理服务器上的操作**<br>  • **设备标签**<br>  • **卡巴斯基应用程序部署**<br>  • **应用程序整合**<br>  • **虚拟管理服务器**<br>• **移动设备管理**区域，包括所有功能<br>• **系统管理**区域，包括所有功能<br>• **Kaspersky Endpoint Security** 区域，包括所有功能 |
| “移动设备管理”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**<br>• **移动设备管理**区域，包括所有功能<br>在**常规功能：授权许可密钥管理**中授予**导出密钥文件**权限。<br><br>在**系统管理：漏洞和补丁管理**中授予**读取**权限。 |
| “移动设备管理”操作员 | 在“**常规功能：基本功能**”中授予“**读取**”和“**执行**”权限。<br><br>在**移动设备管理**中授予**读取**和**仅向移动设备发送信息命令**权限：<br>• **常规**<br>• **Self Service Portal** |
| 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>在**系统管理：连接**功能区中授予以下权限：**读取**、**写入**、**执行**、**将文件从设备保存到管理员工作站**以及**对设备分类执行操作**。<br><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。 |

| 角色 | 描述 |
| --- | --- |
| 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。 |
| “漏洞和补丁管理”管理员 | 允许在“**常规功能**：**基本功能**”和“**系统管理**”（包括所有功能，*除了***远程执行脚本**）功能区域的所有操作。 |
| “漏洞和补丁管理”操作员 | 授予在“**常规功能**：**基本功能**”和“**系统管理**”（包括所有功能，*除了***远程执行脚本**功能）功能区域的**读取**和**执行**（如果适用）权限。 |

# 分配对特定对象的访问权限

除了分配服务器级别的访问权限，您还可以配置对特定对象的访问，例如对特定任务的访问。该应用程序允许您指定对以下对象类型的访问权限：

- 管理组
- 任务
- 报告
- 设备分类
- 事件分类

*要分配对特定对象的访问权限：*

1. 根据对象类型，在主菜单中转到相应区域：
   - **资产管理 → 组层级**
   - **任务**
   - **监控→报告**
   - **资产管理→设备分类**
   - **监控→事件分类**
2. 打开要为其配置访问权限的对象的属性。

   要打开管理组或任务的属性窗口，单击对象名称。其他对象的属性可以使用工具栏上的按钮打开。
3. 在属性窗口中，打开**访问权限**部分。

   用户列表将打开。列出的用户和安全组具有对象的访问权限。默认情况下，如果您使用管理组或服务器的层级，则列表和访问权限是从父管理组或主服务器继承的。
4. 为了能够修改列表，启用**使用自定义权限**选项。

5. 配置访问权限：

   - 使用**添加**和**删除**按钮修改列表。
   - 指定用户或安全组的访问权限。执行以下操作之一：
     - 如果要手动指定访问权限，请选择用户或安全组，单击“**访问权限**”按钮，然后指定访问权限。
     - 如果要分配一个用户角色到用户或安全组，请选择用户或安全组，单击“**角色**”按钮，然后选择要分配的角色。

6. 单击“**保存**”按钮。

配置对象的访问权限。

# 向用户和安全组分配访问权限

您可以授予用户和安全组访问权限，以使用管理服务器的不同功能，例如 Kaspersky Endpoint Security for Linux。

*为用户或安全组分配访问权限：*

1. 在主菜单中，单击管理服务器名称。

   管理服务器属性窗口将打开。

2. 在“**访问权限**”选项卡上，选中要分配权限的用户或安全组名称旁边的复选框，然后单击“**访问权限**”按钮。

   您不能同时选择多个用户或安全组。如果您选择了多个条目，“**访问权限**”按钮将被禁用。

3. 配置用户或组的权限集：

   a. 使用管理服务器或其他卡巴斯基应用程序的功能扩展节点。

   b. 选择所需功能或访问权限旁边的**允许**或**拒绝**复选框。

   *示例 1：* 选中**应用程序集成**节点旁边的**允许**复选框，向用户或组授予对应用程序集成功能（**读取**、**写入**和**执行**）的所有可用访问权限。

   *示例 2：* 展开**加密密钥管理**节点，然后选中写入权限旁边**的允许**复选框，以授予用户或组对加密密钥管理功能的**写入**访问权限。

4. 配置访问权限集后，单击**确定**。

用户或用户组的权限集将被配置。

管理服务器（或管理组）的权限被分成以下部分：

- 常规功能：
  - 管理组的管理
  - 访问对象而不考虑它们的 ACLs
  - 基本功能

    - 已删除对象
    - 加密密钥管理
    - 事件处理
    - 在管理服务器上的操作（仅位于管理服务器的属性窗口中）
    - 设备标签
    - 卡巴斯基应用程序部署
    - 授权许可密钥管理
    - 应用程序整合
    - 强制报告管理
    - 管理服务器层级
    - 用户权限
    - 虚拟管理服务器
- 移动设备管理：
    - 常规
    - Self Service Portal
- 系统管理：
    - 连接
    - 远程执行脚本
    - 硬件清单
    - 网络访问控制
    - OS 部署
    - 漏洞和补丁管理
    - 远程安装
    - 软件清单

如果没有为访问权限选择“**允许**”或“**拒绝**”，则该访问权限被认为*未定义*：它将被拒绝，直到被用户明确拒绝或允许为止。

用户权限是以下各项的集合：

- 用户自己的权限
- 分配给该用户的所有角色的权限

- 用户所属的所有安全组的权限
- 分配到用户所属安全组的所有角色的权限

如果至少一个权限集对权限“**拒绝**”，那么用户被拒绝该权限，即便其他集允许它或保持未定义。

您还可以将用户和安全组添加至用户角色范围，以使用管理服务器的不同功能。与用户角色关联的设置只应用到属于拥有该角色的用户的设备，并且这些设备只属于与该角色关联的组，包括子组。

# 添加内部用户账户

如果您想要添加用户账户，请确保您的账户在常规功能：用户权限功能区域中具有修改对象 ACL权限。

*要向 Kaspersky Security Center Linux 添加新的内部用户账户：*

1. 在主菜单中，转至**用户和角色** → **用户和组**，然后选择**用户**选项卡。
2. 单击**添加**。
3. 在打开的“**添加用户**”窗口中，指定新用户账户设置：
   - **名称**。
   - 连接到 Kaspersky Security Center Linux 的用户的**密码**。
     密码必须符合以下规则：
     - 密码的字符长度必须是 8 到 256 位。
     - 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，请单击。
     您可以启用**用户必须在首次登录时更改密码**选项，以在第一次用户身份验证时强制更改密码。
4. 保存更改以完成新用户账户的创建。

新的用户账户将被添加到用户列表中。

要使用已创建的内部用户账户登录 Kaspersky Security Center Web Console，您必须为该帐户分配一个角色。登录前，请确保该内部用户账户已分配角色。否则，将会出现登录错误。

# 创建安全组

*要创建安全组：*

1. 在主菜单中，转至“**用户和角色**” → “**用户和组**”，然后选择“**组**选项卡。
2. 单击**添加**。
3. 在打开的**创建安全组**窗口中，为新安全组指定以下设置：
   - **组名称**
   - **描述**
4. 单击“**保存**”保存设置。

新的安全组已被添加到组列表中。

# 编辑内部用户账户

如果您想要编辑用户账户，请确保您的账户在常规功能：用户权限功能区域中具有修改对象 ACL权限。

*要编辑 Kaspersky Security Center Linux 的内部用户账户：*

1. 在主菜单中，转至**用户和角色** → **用户和组**，然后选择**用户**选项卡。
2. 单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：
   - **用户账户**

     如果必要，将切换按钮切换到“**不活动**”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。
   - 描述
   - **完整名称**
   - **邮件地址**
   - **主电话**

- **密码**

  如有必要，您可以按如下方式为用户连接到 Kaspersky Security Center Linux 设置新密码：

  a. 单击**更改密码**按钮，然后为用户账户设置新密码。
  密码必须符合以下规则：

  - 密码的字符长度必须是 8 到 256 位。
  - 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，请单击。

  b. 如有必要，启用**用户必须在首次登录时更改密码**选项，以在下次用户身份验证时强制更改密码。

  c. 如果用户账户受到保护以防止未经授权的修改，您必须确认您有更改此账户的权限。在**账户保护**窗口中，指定在常规功能：用户权限功能区域中具有修改对象 ACL权限的账户的凭据。

4. 在“**双重身份验证**”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. 保存更改以完成用户账户的编辑。

更新的用户账户出现在用户列表中。

# 编辑安全组

*要编辑安全组：*

1. 在主菜单中，转至**用户和角色** → **用户和组**，然后选择**组**选项卡。
2. 单击您要编辑的安全组名称。

3. 在打开的组设置窗口中，更改安全组设置：
   - 在“**常规**”选项卡上，您可以更改“**名称**”和“**描述**”设置。这些设置仅适用于内部安全组。
   - 在“**用户**”选项卡上，可以添加用户到安全组。此设置仅适用于内部用户和内部安全组。
   - 在“**角色**”选项卡上，可以分配角色到安全组。
4. 单击“**保存**”保存设置。

更改将应用于安全组。

# 为用户或安全组分配角色

*为用户或安全组分配角色：*

1. 在主菜单中，转至**用户和角色→用户和组**，然后选择**用户**或**组**选项卡。
2. 选择要向其分配角色的用户或安全组的名称。
   您可以选择多个名称。
3. 在菜单项目上，单击“**分配角色**”按钮。
   角色分配向导启动。
4. 按照向导的说明进行操作：选择要分配给所选用户或安全组的角色，然后选择角色的范围。
   *用户角色范围*是用户和管理组的组合。与用户角色关联的设置仅应用到属于该角色用户的设备，以及仅在这些设备属于与该角色关联的组（包括子组）时。

拥有一组管理服务器使用权限的角色将被指派给用户（或多个用户，或安全组）。在用户或安全组列表中，**已分配角色**列中会出现一个复选框。

# 添加用户账户到内部安全组

> 您仅可以添加内部用户账户到内部安全组。

*要添加用户账户到内部安全组：*

1. 在主菜单中，转至**用户和角色 → 用户和组**，然后选择**用户**选项卡。
2. 选择您要添加到安全组的用户账户旁边的复选框。
3. 单击“**分配组**”按钮。
4. 在打开的“**分配组**”窗口中，选择要将用户账户添加到的安全组。
5. 单击“**保存**”按钮。

用户账户被添加到安全组。您还可以使用组设置将内部用户添加到安全组。

# 将用户指定为设备所有者

有关如何将用户指定为移动设备所有者的信息，请参阅Kaspersky Secure Mobility Management帮助文档。

*要指派用户作为设备所有者：*

1. 如果要分配连接到虚拟管理服务器的设备的所有者，请先切换到虚拟管理服务器：
   a. 在主菜单中，单击当前管理服务器名称右侧的 V 形图标 ()。
   b. 选择所需的管理服务器。
2. 在主菜单中，转至**用户和角色** → **用户和组**，然后选择**用户**选项卡。
   系统打开一个用户列表。如果您当前连接到虚拟管理服务器，则该列表包括来自当前虚拟管理服务器和主管理服务器的用户。
3. 单击您要分配为设备所有者的用户账户名称。
4. 在打开的用户设置窗口中，选择“**设备**”选项卡。
5. 单击**添加**。
6. 从设备列表中，选择您要分配给用户的设备。
7. 单击“**确定**”。

   所选的设备被添加到分配给用户的设备列表。

您可以在“**资产管理**”→“**资产(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。

# 安装网络代理期间将用户指定为设备所有者

若要在通过安装包安装网络代理时将用户指定为设备所有者，请将下表中指定的变量添加到网络代理安装包设置中。

| 变量名称 | 是否必需 | 描述 | 可能值 |
|---|---|---|---|
| KLNAGENT_DEVICEOWNER_REGISTRATION_START | 否 | 允许在安装网络代理后运行该实用程序，将用户注册为设备所有者。如果禁用，则用户无法注册为设备所有者。 | 1 – 安装网络代理后，用于将用户注册为设备所有者的实用程序将启动。<br>其他 – 该实用程序不可用。 |

| | | | |
|---|---|---|---|
| KLNAGENT_DEVICEOWNER_LOGIN | 否<br>是的，如果您输入密码 | 包含将注册为设备所有者的用户的登录信息。 | Kaspersky Security Center Linux 用户列表中指定的用户登录信息。 |
| KLNAGENT_DEVICEOWNER_PASSWORD | 否<br>是的，如果您输入登录信息 | 包含将注册为设备所有者的用户的加密密码。 | 用户的密码。 |

网络代理将在安装 Kaspersky Security Center Linux 期间解密指定的登录名和密码，并将用户注册为设备所有者。

您还可以在使用响应文件以静默模式安装网络代理时将用户指定为设备所有者。

*在使用响应文件以静默模式安装网络代理时将用户指定为设备所有者：*

1. 将 KLNAGENT_DEVICEOWNER_REGISTRATION_START 参数添加到响应文件并将其设置为 1。
   安装网络代理后，用于将用户注册为设备所有者的实用程序将启动。
2. 在客户端设备的命令行中输入登录名和密码。
   该用户将被指定为设备所有者。

如果用户包含在内部安全组中，则登录信息必须包含用户名。

如果用户包含在活动目录安全组中，则登录信息必须包含用户名和域名。

您必须从应用中输入基于时间的一次性密码 (TOTP) 以进行双重身份验证。

# 安装网络代理后将用户指定为 Linux 设备所有者

*允许用户注册为 Linux 设备所有者：*

1. 在卡巴斯基安全管理中心云控制台中，转到 **软件管理** → **安装包**。
   安装包列表将打开。
2. 点击网络代理的安装包。
   此时将打开安装包的属性窗口。
3. 在安装包属性窗口中，单击“**设置**”→“**高级**”。
4. 在“**用户注册为设备所有者(仅限 Linux)**”部分中，打开“**允许在安装网络代理后运行用户注册实用工具**”选项，然后单击“**保存**”。

将用户注册为设备所有者的实用程序可以通过客户端设备上的命令行来运行。

*要在客户端设备上将用户注册为 Linux 设备所有者：*

1. 在客户端设备上的命令行中执行以下命令：
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner
   ```
2. 如果出现提示，请输入登录名和密码。
   如果网络代理的应答文件或安装包中包含登录名和密码，请在客户端设备上的命令行中执行以下命令：
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner -unattended
   ```

如果用户包含在内部安全组中，则登录信息必须包含用户名。

如果用户包含在活动目录安全组中，则登录信息必须包含用户名和域名。

您必须从应用中输入基于时间的一次性密码 (TOTP) 以进行双重身份验证。

该用户将被注册为设备所有者。

# 删除用户的设备所有者角色

*要在客户端设备上删除作为设备所有者的用户：*

1. 在客户端设备上的命令行中执行以下命令：

   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -remove_owner
   ```

2. 输入用户名和密码。

如果用户包含在内部安全组中，则登录信息必须包含用户名。

如果用户包含在活动目录安全组中，则登录信息必须包含用户名和域名。

您必须从应用中输入基于时间的一次性密码 (TOTP) 以进行双重身份验证。

该用户作为设备所有者的身份将被删除。

# 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，转至**用户和角色** → **用户和组**，然后选择**用户**选项卡。
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“**双重身份验证**”选项卡。
4. 如果您想在每次更改或修改帐户设置时请求双重身份验证的登录凭证和一次性安全码，在**双重身份验证**选项卡上，请选择**请求身份验证以验证修改用户账户的权限**。否则，请选择“**允许用户修改该账户而不需要附加身份验证**”选项。
5. 保存更改。

# 配置双重身份验证

从管理服务器版本16.1开始，双重身份验证将自动启用。不支持禁用双重身份验证的全局选项。本方案提供了在首次登录时配置双重身份验证以及在管理服务器上配置双重身份验证设置的步骤。

## 阶段

分阶段配置双重身份验证：

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。

   在俄罗斯可用：

   - Bitrix24 OTP
   - Yandex ID
   - Avanpost 验证器
   - Aladdin 2FA
   - Rutoken OTP

   全球可用（包括俄罗斯）：

   - Google Authenticator
   - Microsoft Authenticator

   要检查 Kaspersky Security Center Linux 是否支持您要使用的身份验证应用，请为所有用户或特定用户启用双重身份验证。

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

   > 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身份验证应用。

2. **将安装了认证应用的设备的时间与安装了管理服务器的设备的时间同步**

   确保已安装认证应用的设备上的时间和已部署管理服务器的设备上的时间与 UTC 同步。为了提高准确性，建议在整个基础架构中使用相同的 NTP 服务器。否则，在配置双重身份验证时可能会出现故障。

3. **在用户账户登录 Web Console 时，为其配置双重身份验证**

   登录云控制台并配置双重身份验证。

   如果您无法配置双重身份验证，请联系具有常规功能：用户权限功能区域中**修改对象**ACL权限且已配置双重身份验证的用户，将您的帐户添加到双重身份验证允许列表中。

4. **在管理服务器上配置双重身份验证设置**

如果您已配置双重身份验证并具有常规功能**常规功能**用户权限**用户权限修改对象**ACL权限，则可以按如下方式在管理服务器上配置双重身份验证设置：

1. 查看可在登录时配置双重身份验证的用户列表：

   - 对于全新安装管理服务器16.1的用户：将所需用户添加到双重身份验证允许列表中，以便他们能够在首次登录时配置双重身份验证。
   - 升级或恢复到管理服务器 16.1 时：查看双重身份验证允许列表，并删除不应有权访问管理服务器的账户。

2. 排除不需要启用双重身份验证的用户账户（可选）

   将用户账户从双重身份验证中排除，允许这些账户即使未配置双重身份验证，也能登录管理服务器。对于在身份验证期间无法提供安全代码的集成账户，可能有必要从双重身份验证中排除这些账户。集成账户用于通过 OpenAPI 运行脚本。

3. 重置或删除双重身份验证 secret key（可选）

   当用户无法访问其双重身份验证设备或需要在新设备上设置双重身份验证时，您可以重置双重身份验证的密钥。您还可以重置自己账户的 secret key。

   您可以删除 secret key，从而完全阻止用户登录 Web Console 和访问管理服务器。

4. 编辑安全码颁发者的名称（可选）

   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码颁发者名称，以便更好地识别不同的管理服务器。

结果

完成此方案后：

- 您的用户账户和另一个需要访问管理服务器的用户账户均已配置双重身份验证。
- 集成账户即从双重身份验证中排除。

# 关于账户的双重身份验证

Kaspersky Security Center Linux为Kaspersky Security Center云控制台用户提供双重身份验证。双重身份验证基于RFC 6238标准（TOTP：基于时间的一次性密码算法）。

每次登录Kaspersky Security Center云控制台时，您都需要输入用户名、密码以及额外的一次性安全码。若要接收一次性安全码，移动设备或电脑上必须安装了身份验证应用。

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。为了生成一次性安全码，您必须将安装了认证应用的设备上的时间与管理服务器设备上的时间同步。为了提高准确性，我们建议在整个基础设施中使用相同的NTP服务器。

若要检查Kaspersky Security Center Linux是否支持您要使用的身份验证应用，请尝试使用此身份验证应用配置双重身份验证。

其中一个步骤建议您指定由身份验证应用程序生成的一次性安全码。如果成功，则 Kaspersky Security Center Linux 支持所选的身份验证器。

**使用身份验证应用生成验证码**

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。

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。下次登录后，新的安全码颁发者名称会被分配给管理服务器。安全码为一次性，有效期最长为 30 秒（具体时间可能会有所不同）。

我们强烈建议您保存密钥或二维码，并将其保管在安全的地方。如果您无法使用身份验证应用程序访问设备，这将帮助您恢复对Kaspersky Security Center云控制台的访问。

双重身份验证具有以下功能：

- 从管理服务器版本 16.1 开始，双重身份验证默认自动启用，并默认禁用登录时配置双重身份验证的选项。登录时配置双重身份验证仅适用于包含在双重身份验证允许列表中的用户。
- 用户只能为自己的账户配置双重身份验证。
- 您可以从双重身份验证中排除指定账户。对于无法接收一次性安全码进行身份验证的集成账户，此功能可能非常重要。集成账户用于通过 OpenAPI 运行脚本。
- 若要重新生成双重身份验证的密钥，用户必须重置其自身帐户的密钥。
- 若要重置或删除其他用户帐户的双重身份验证的密钥，用户必须拥有已配置双重身份验证的帐户，并且在常规功能**常规功能**用户权限**用户权限修改对象**ACL权限。
- 要将其他用户的账户从双重身份验证中排除或修改双重身份验证允许列表，用户必须拥有已配置双重身份验证的账户，并且在**常规功能**：**用户权限**功能区中拥有修改对象ACL权限。
- 应该始终至少有一个用户配置了双重身份验证，以便该用户可以管理双重身份验证允许列表和排除列表。
- 双重身份验证仅在管理服务器 16.1 版本中自动启用。如果其他主要管理服务器或从属管理服务器运行的是版本 16 或更早版本，则它们的双重身份验证设置将保持不变。
- 虚拟管理服务器会继承物理管理服务器的双重身份验证设置，因此，如果物理管理服务器启用了双重身份验证，虚拟管理服务器也会启用该功能。您无法在虚拟管理服务器上配置双重身份验证设置。
- 要使双重身份验证正常运行，您需要将管理服务器和云控制台升级到16.1或更高版本。

若要通过双重身份认证实现全面保护，不仅需要对管理服务器采取安全防护措施，还需保障其部署设备的安全性。为此，请参照强化指南中的建议。

# 在 Kaspersky Next Expert View 登录时配置双重身份验证密钥

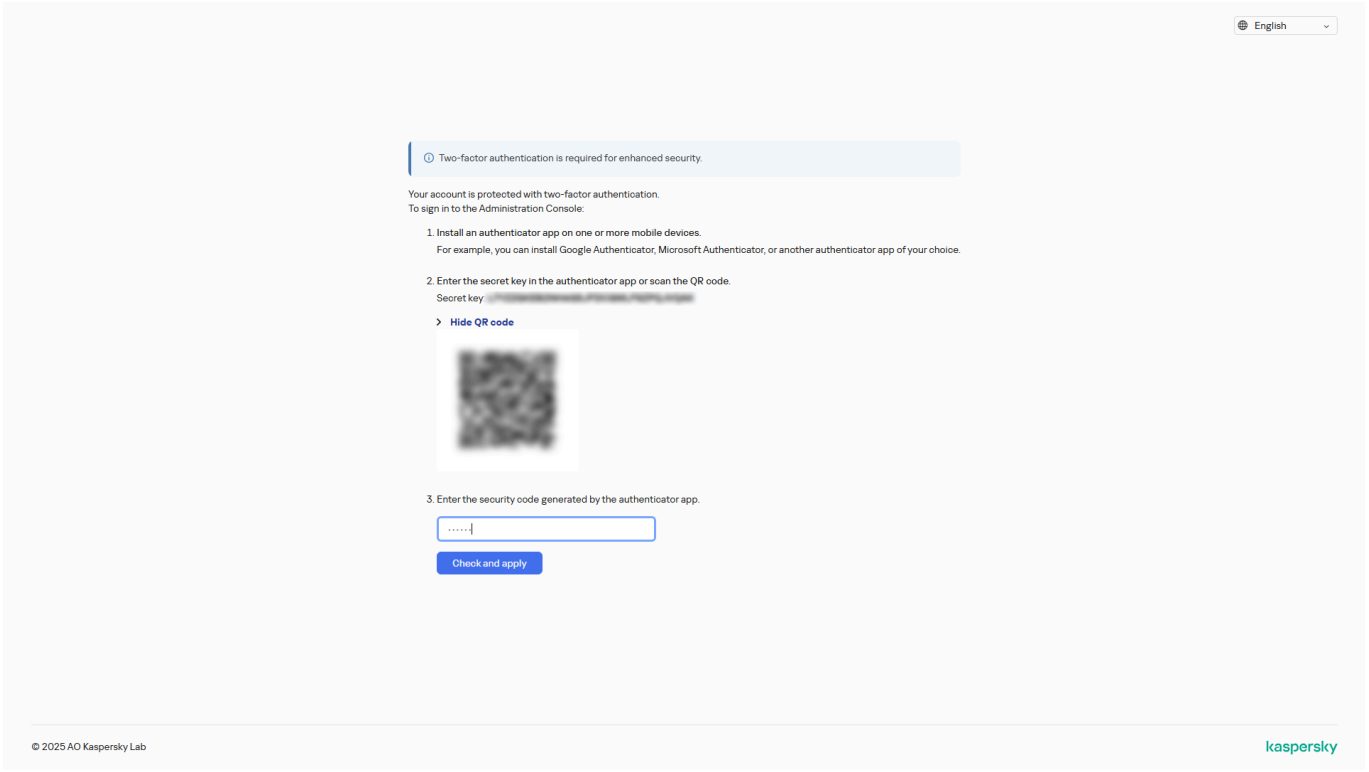
首次登录Kaspersky Security Center Linux 16.1或更高版本时，将打开配置双重身份验证的窗口。

*要为您的账户配置双重身份验证：*

1. 请在移动设备或计算机上安装任何支持基于时间的一次性密码算法的应用程序，例如：
   - Google Authenticator
   - Microsoft Authenticator
   - Bitrix24 OTP
   - Yandex ID
   - Avanpost 验证器
   - Aladdin 2FA
   - Rutoken OTP

   强烈建议不要将认证应用安装在对管理服务器进行管理的同一台设备上。
2. 确保已安装认证应用的设备上的时间和已部署管理服务器的设备上的时间与 UTC 同步。为了提高准确性，建议在整个基础架构中使用相同的 NTP 服务器。
3. 使用移动设备或计算机上的认证应用来生成一次性安全码。为此，请执行以下操作之一：
   - 在认证应用中手动输入双重身份验证 secret key。
   - 单击**查看二维码**并使用身份验证器应用扫描二维码。

移动设备上将显示一个 6 位数的一次性安全码。




在 Kaspersky Next Expert View 登录时配置双重身份验证密钥

4. 在“**双重身份验证**”窗口中，指定由认证应用生成的一次性安全码，然后单击“**检查和应用**”按钮。

**Rutoken OTP 配置**

如果您使用 Rutoken OTP，则需要一台安装了 Rutoken OTP 应用程序的 Android 移动设备。Android 移动设备必须满足以下要求：

- 操作系统是 Android 7 或更高版本。
- NFC 模块可用且已启用。

在 Rutoken OTP 应用程序中，您必须配置以下参数：

- 扫描两步配置向导中显示的二维码。
- 将时间间隔设置为 30 秒。
- 选择 SHA1 作为算法。

*要配置 Rutoken OTP：*

1. 将 Rutoken OTP 设备放在带有 NFC 模块的移动设备旁边。
2. 在 Rutoken OTP 应用程序中，按下“**连接令牌**”。
3. 在 Rutoken OTP 应用程序中，按下“**配置设置**”，然后按下“**保存 secret key**”。

如果令牌成功连接到移动设备，Rutoken OTP 应用程序将显示以下状态消息：

- **令牌已连接。**
- **设置已配置。**
- **密钥已保存。**

4. 在 Rutoken OTP 设备上，按下按钮。
   设备上会显示一个安全码。
5. 在 Kaspersky Security Center Web Console 的两步验证窗口中，输入安全码。

您的账户已配置双重身份验证。您可以根据您的权限访问管理服务器。

如果您无法配置双重身份验证，请联系在**常规功能**： **用户权限**功能区域中拥有修改对象ACL权限且已配置双重身份验证的用户，将您的账户添加到双重身份验证允许列表中。

# 允许用户配置双重身份验证

双重身份验证允许列表是允许在登录云控制台时初始配置双重身份验证的用户列表。此列表包含未配置双重身份验证的用户账户。默认情况下，新用户账户不会包含在双重身份验证允许列表中，必须由管理员添加到该列表中。如果新帐户是用于运行OpenAPI脚本的集成帐户，则必须将其从双重身份验证中排除。

当用户帐户配置了双重身份验证或被排除在双重身份验证之外时，用户帐户将自动从允许双因素身份验证列表中删除。

对于已配置双重身份验证且在常规功能**常规功能**用户权限**用户权限修改对象**ACL权限的帐户，可以手动修改双重身份验证允许列表。

*若要手动将用户账户添加到双重身份验证允许列表：*

1. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口将打开。
2. 在属性窗口的**双重身份验证**选项卡中，在**允许生成 Secret 密钥的用户**表中，单击**添加**按钮。
3. 在打开的窗口中：
   a. 选择要添加的用户账户。
      只有未被排除在双重身份验证之外且没有双重身份验证密钥的用户才能添加到双重身份验证允许列表中。
   b. 如果用户账户受到保护以防止未经授权的修改，您必须确认您有更改此账户的权限。在“**账户保护**”窗口中，指定您自己的账户凭证和用于双重身份验证的一次性安全码。
   c. 保存更改。

选定的用户账户将被添加到双重身份验证允许列表中。下次登录时，用户将能够生成密钥。

在为该用户账户配置双重身份验证之前，可以从双重身份验证允许列表中删除该用户账户。

*若要手动从双重身份验证允许列表中删除用户账户：*

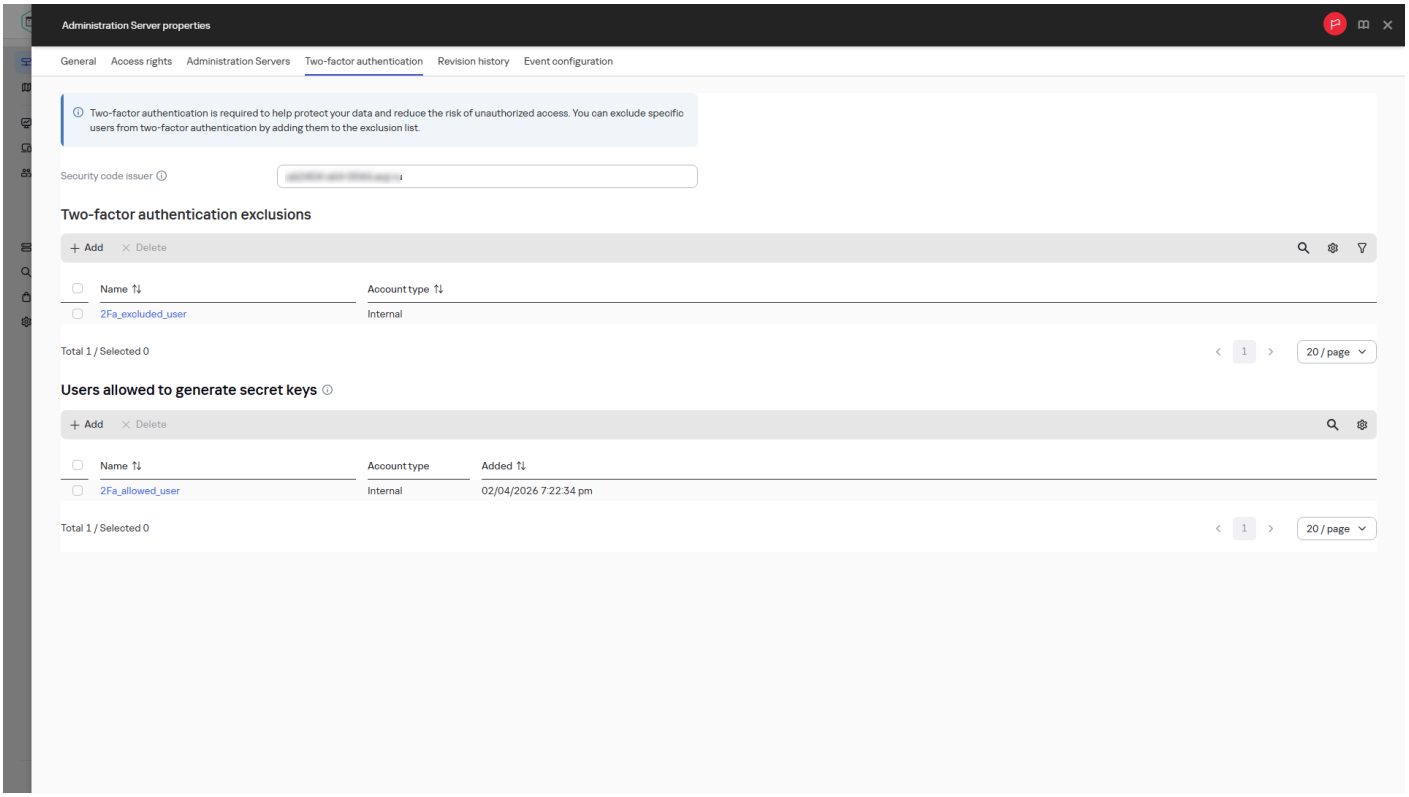
1. 在主菜单中，单击管理服务器名称。

   管理服务器属性窗口将打开。

2. 在属性窗口的**双重身份验证**选项卡上的**允许生成 Secret 密钥的用户**表中，选择要删除的用户账户，然后单击**删除**。

3. 如果用户账户受到保护以防止未经授权的修改，您必须确认您有更改此账户的权限。在“**账户保护**”窗口中，指定您自己的账户凭证和用于双重身份验证的一次性安全码。

所选用户账户被从双重身份验证允许列表中删除。




配置双重身份验证允许列表

如果在管理服务器上的活动会话期间，您的双重身份验证密钥被其他用户删除，或者您自行重置了密钥但未创建新密钥，则修改双重身份验证允许列表的功能将被阻止。

用户账户也可以自动添加到双重身份验证允许列表或从中删除。

重置其他帐户的双重身份验证密钥时，这些帐户会自动添加到允许列表中，以便它们可以生成新密钥。

将管理服务器从版本 16 或更早版本升级到版本 16.1 或更高版本，以及在管理服务器 16 或更早版本上创建数据备份并将其还原到管理服务器 16.1 或更高版本时，如果满足以下所有条件，则用户账户将自动添加到双重身份验证允许列表中：

- 用户在*常规功能功能区域中具有“读取”权限：基本功能*直接分配给用户（而不是通过安全组）。具有此权限的用户和角色范围必须包含所有已管理和未分配的设备，并且必须在管理服务器级别设置。
- 该用户未被排除在双重身份验证之外。

- 该用户没有双重身份验证密钥。
- 更早版本的管理服务器上并非所有用户都启用了双重身份验证。

即使未能满足其中一项条件，用户也无法被添加到双重身份验证允许列表中。

> 升级或恢复后，我们建议确保双重身份验证允许列表中仅包含必须有权访问管理服务器的用户账户。查看双重身份验证允许列表，并从中删除任何其他帐户。将用于通过OpenAPI运行脚本的集成帐户添加到排除项列表中，以防止脚本运行失败。

如果满足以下所有条件，则用户帐户在升级或恢复后将失去对管理服务器的访问权限：

- 用户在*常规功能功能区拥有"读取"权限：基本功能*是通过安全组分配的（不是直接分配给用户），或者根本没有此权限。
- 该用户未被排除在双重身份验证之外。
- 该用户没有双重身份验证密钥。
- 为更早版本的管理服务器上的所有用户启用了双重身份验证。

如有需要，可手动将这些帐户添加到双重身份验证允许列表中。

# 重置和删除双重身份验证密钥

当用户无法访问其双重身份验证设备或需要在新设备上设置双重身份验证时，您可以重置密钥。重置密钥后，用户可以再次登录云控制台并生成新密钥。

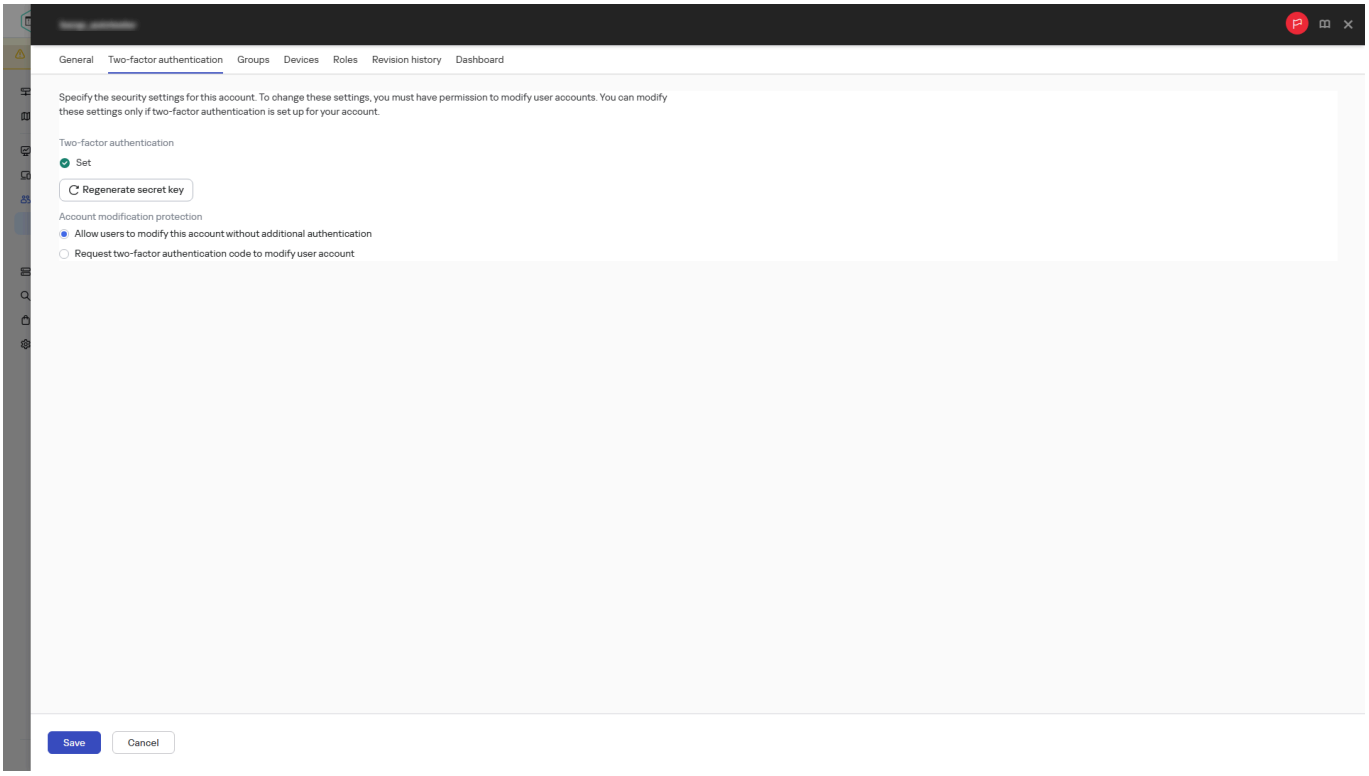
> 只有当您已配置双重身份验证，并且在**常规功能**：**用户权限**功能区域中拥有修改对象ACL权限时，才能重置或删除其他用户的双重身份验证密钥。您也可以重新生成自己的密钥。

*要重置某个帐户的密钥：*

1. 在主菜单中，转至"**用户和角色**" → "**用户和组**"，然后选择"**用户**"选项卡。
2. 单击要重置密钥的用户账户名称。

3. 如果要重置自己帐户的密钥：

a. 在**双重身份验证**选项卡上，单击**重新生成 Secret 密钥**按钮。

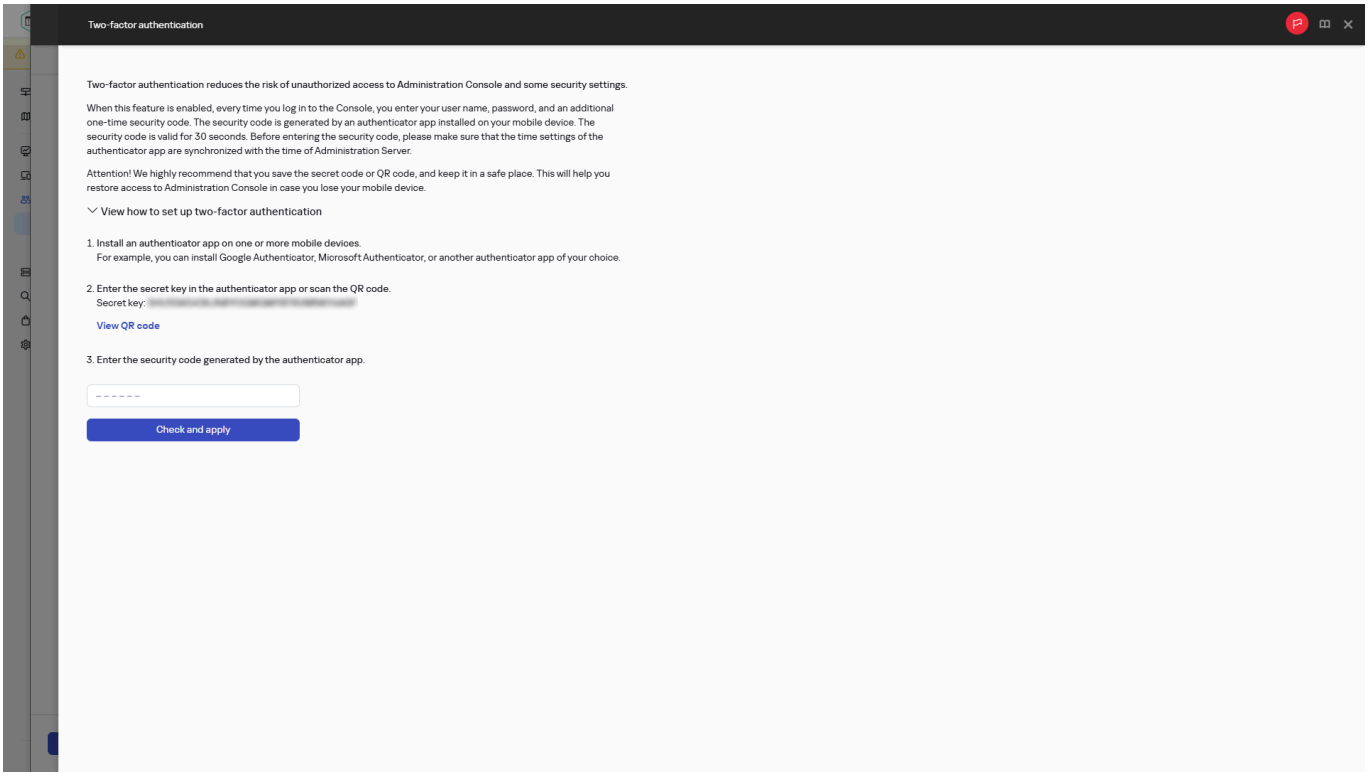



为当前用户账户重新生成双重身份验证密钥

a. 如果您的账户受到保护以防止未经授权的修改，您必须确认您有更改此账户的权限。在**账户保护**窗口中，指定您自己帐户的登录凭据和双重身份验证安全码。

b. 在**双重身份验证**窗口中，点击**查看如何建立双重身份验证**，然后点击**查看二维码**。

c. 使用移动设备上的身份验证应用扫描二维码并接收一次性安全码。



a. 在**双重身份验证**窗口中，指定由身份验证应用生成的安全码，然后单击**检查和应用**按钮。

**Rutoken OTP 配置**

如果您使用 Rutoken OTP，则需要一台安装了 Rutoken OTP 应用程序的 Android 移动设备。Android 移动设备必须满足以下要求：

- 操作系统是 Android 7 或更高版本。
- NFC 模块可用且已启用。

在 Rutoken OTP 应用程序中，您必须配置以下参数：

- 扫描两步配置向导中显示的二维码。
- 将时间间隔设置为 30 秒。
- 选择 SHA1 作为算法。

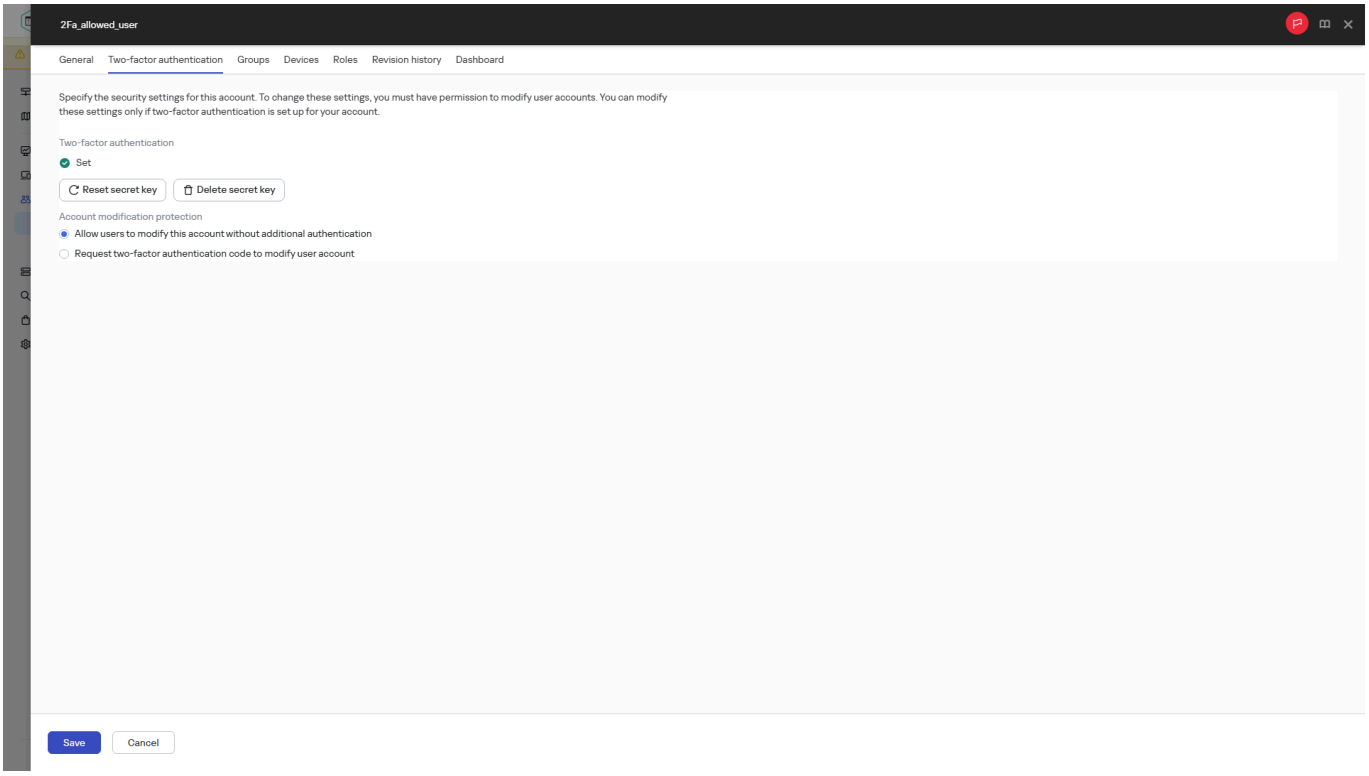
*要配置 Rutoken OTP：*

1. 将 Rutoken OTP 设备放在带有 NFC 模块的移动设备旁边。
2. 在 Rutoken OTP 应用程序中，按下“**连接令牌**”。
3. 在 Rutoken OTP 应用程序中，按下“**配置设置**”，然后按下“**保存 secret key**”。
   如果令牌成功连接到移动设备，Rutoken OTP 应用程序将显示以下状态消息：
   - **令牌已连接。**
   - **设置已配置。**
   - **密钥已保存。**
4. 在 Rutoken OTP 设备上，按下按钮。
   设备上会显示一个安全码。
5. 在 Kaspersky Security Center Web Console 的两步验证窗口中，输入安全码。

您的帐户密钥已更改。

4. 若要重置其他帐户的密钥：

   a. 在**双重身份验证**选项卡上，单击**重置 Secret 密钥**按钮。




重置另一个用户账户的双重身份验证密钥

   a. 如果用户账户受到保护以防止未经授权的修改，您必须确认您有更改此账户的权限。在**账户保护**窗口中，指定您自己帐户的登录凭据和双重身份验证的一次性安全码。

   b. 确认重置密钥，然后保存更改。

   当您为另一个账户重置密钥时，现有密钥将被删除，并且该用户账户将被添加到管理服务器属性中的双重身份验证允许列表中。下次登录时，该用户将能够生成新密钥。

   用户账户的密钥将被重置。

您可以删除 secret key，从而完全阻止用户登录 Web Console 和访问管理服务器。

*若要删除密钥：*

1. 在主菜单中，转至“**用户和角色**” → “**用户和组**”，然后选择“**用户**”选项卡。

2. 单击要删除密钥的内部用户帐户的名称。

   您无法删除自己帐户的密钥。

3. 在**双重身份验证**选项卡上，单击**删除 Secret 密钥**按钮。

4. 如果用户账户受到保护以防止未经授权的修改，您必须确认您有更改此账户的权限。在**账户保护**窗口中，指定您自己帐户的登录凭据和双重身份验证的一次性安全码。

5. 确认删除密钥，然后保存更改。

   用户账户的密钥将被删除。

您可以通过将用户添加到管理服务器属性中的双重身份验证允许列表中来恢复访问权限。在这种情况下，用户下次登录时将能够生成新密钥。

# 从双重身份验证中排除账户

您可以将用户账户从双重身份验证中排除，允许这些账户即使未配置双重身份验证，也能登录管理服务器。对于在身份验证期间无法提供一次性安全码的集成账户，从双重身份验证中排除这些账户可能是有必要的。集成账户用于通过 OpenAPI 运行脚本。

> 如果您的帐户已配置双重身份验证，并且您在常规功能**常规功能**用户权限**用户权限修改对象**ACL权限，则可以修改排除项列表。

*要从双重身份验证中排除某个用户账户：*

1. 在主菜单中，单击管理服务器名称。

   管理服务器属性窗口将打开。

2. 在属性窗口的“**双重身份验证**”选项卡上，在“**双重身份验证排除项**”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. 如果用户账户受到保护以防止未经授权的修改，您必须确认您有更改此账户的权限。在“**账户保护**”窗口中，指定您自己的账户凭证和用于双重身份验证的一次性安全码。

   c. 保存更改。

选定的用户账户将被排除在双重身份验证之外，若其 secret key 已存在，则会被一并删除。在管理服务器16.1上还原备份或将管理服务器升级到16.1 或更高版本时，排除的帐户列表不会更改。如果排除项列表中的账户在管理服务器的先前版本中使用了 secret key，则这些 secret key 将在 16.1 版本中被删除。

您可以从排除项列表中删除用户账户，以完全阻止用户登录 Web Console 和访问管理服务器。

*要从排除项列表中删除用户账户：*

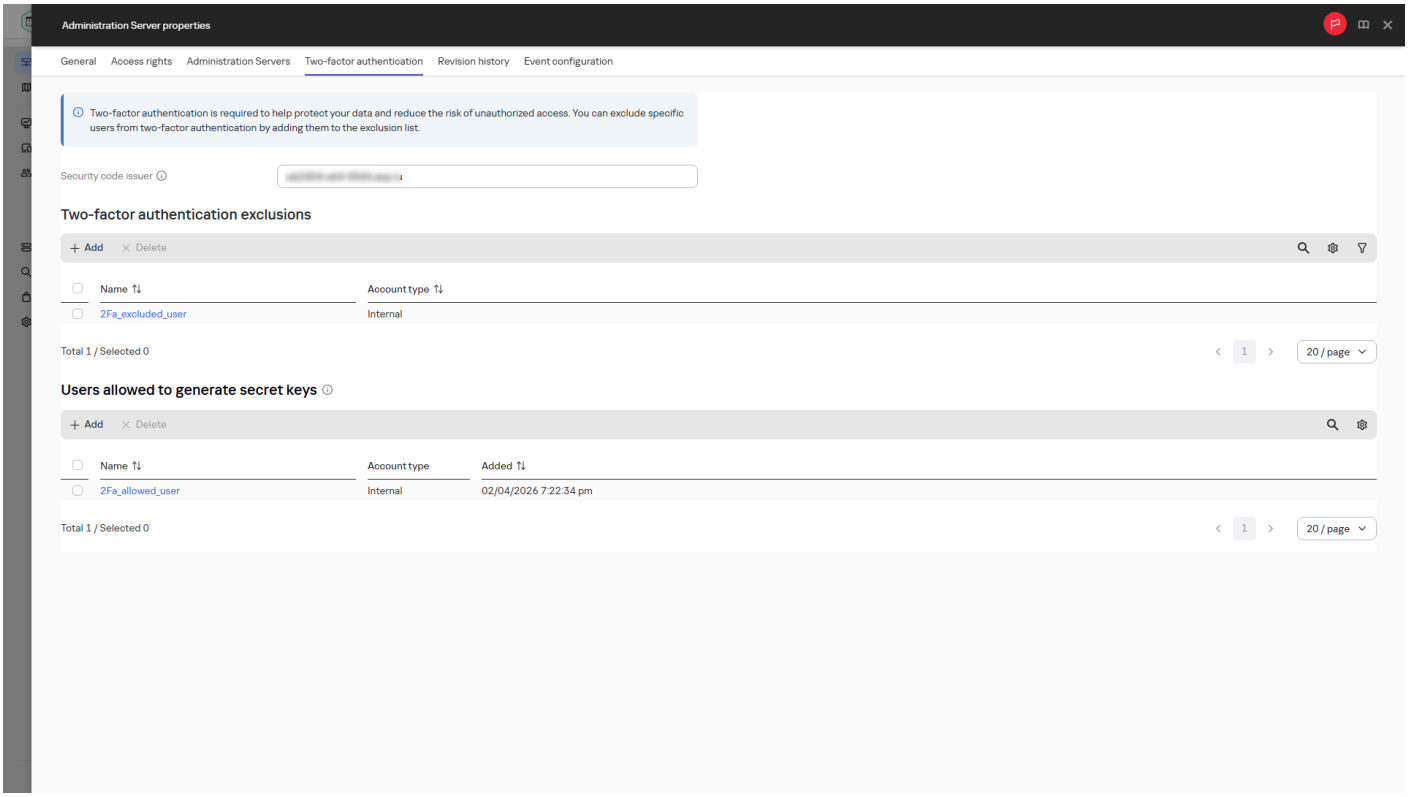
1. 在主菜单中，单击管理服务器名称。

   管理服务器属性窗口将打开。

2. 在属性窗口的“**双重身份验证**”选项卡上的**双重身份验证排除项**表中，选择要删除的用户账户，然后单击“**删除**”。

3. 如果用户账户受到保护以防止未经授权的修改，您必须确认您有更改此账户的权限。在“**账户保护**”窗口中，指定您自己的账户凭证和用于双重身份验证的一次性安全码。

选定的用户账户将从排除项列表中删除。




配置双重身份验证排除列表

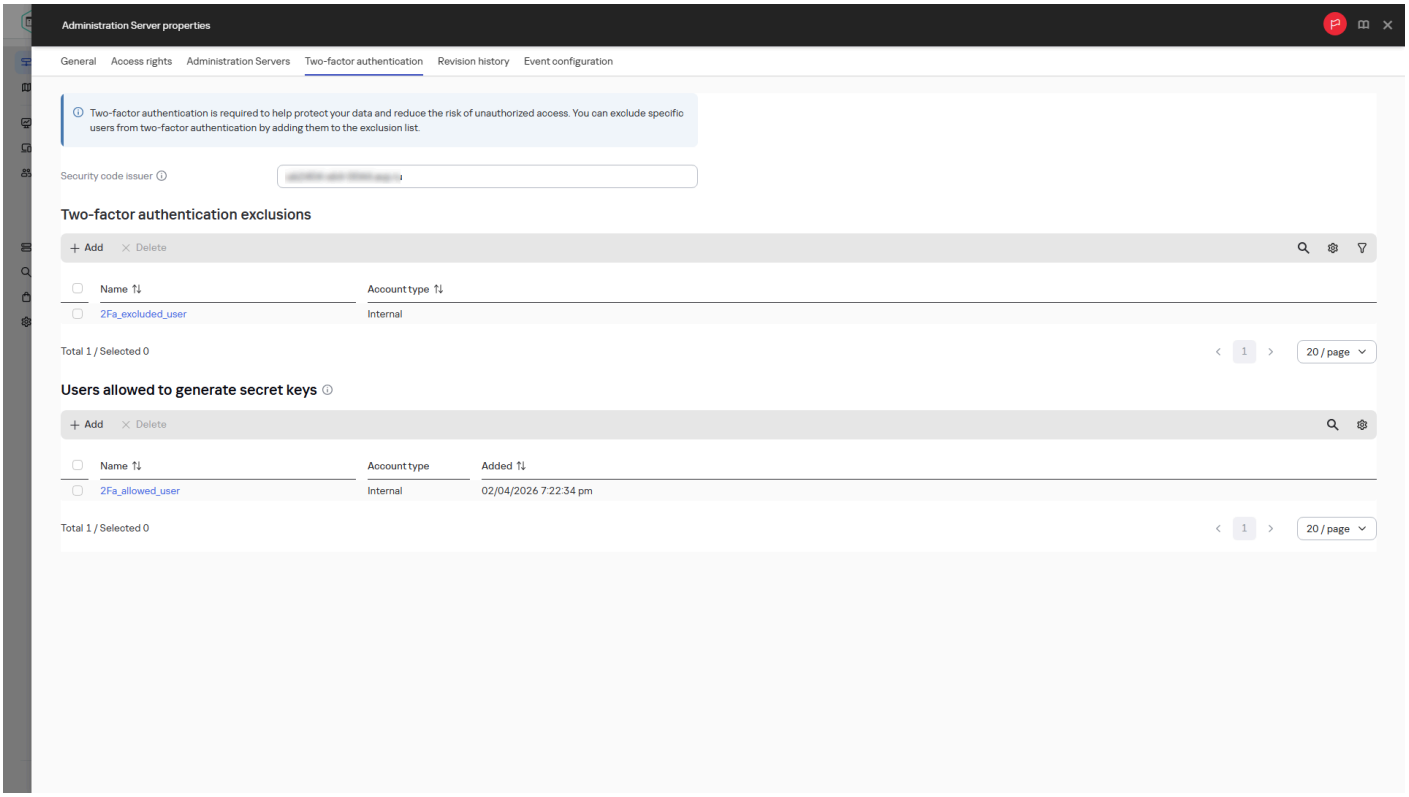
# 编辑安全码签发者名称

您可以为不同的管理服务器配置多个不同标识符（称为颁发者）。您可以更改安全码颁发者的名称，例如，当该管理服务器与其他管理服务器使用的安全码颁发者名称相似时。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。

*要指定安全代码颁发者的新名称：*

1. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口将打开。
2. 在属性窗口的“**双重身份验证**”选项卡中，在“**安全码发布者**”字段中输入新名称，然后保存更改。

下次登录后，新的安全码颁发者名称会被分配给管理服务器。




指定安全码签发者的名称

# 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。

# 删除用户或安全组

> 您仅可以删除内部用户或内部安全组。

*要删除用户或安全组：*

1. 在主菜单中，转至“**用户和角色**” → “**用户和组**”，然后选择“**用户**”或“**组**”选项卡。
2. 选择您要删除的用户或安全组旁边的复选框。

   > 应该始终至少有一个用户配置了双重身份验证，以便该用户可以管理双重身份验证允许列表和排除列表。

3. 单击**删除**。
4. 在打开的窗口中，单击“**确定**”。

   用户或安全组被删除。

# 更改用户账户的密码

如果当前密码即将过期或者您想将其更改为更安全的密码，则可能需要更改您自己账户或其他用户账户的密码。

密码必须符合以下规则：

- 密码的字符长度必须是 8 到 256 位。
- 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。

## 更改您自己账户的密码

*要编辑您的账户密码：*

1. 在上方窗格中，单击您的账户名称，以转到账户菜单。
2. 从下拉列表中，选择“**更改密码**”。
3. 在打开的右侧窗格中，输入当前密码，然后指定用于连接到 Kaspersky Security Center Linux 的新密码。
   要查看输入的密码，请单击。
4. 如果您的账户受到保护以防止未经授权的修改，您必须确认您有更改此账户的权限。在**账户保护**窗口中，指定您自己的账户或者在**常规功能**：**用户权限**功能区域中具有修改对象ACL权限的账户的登录凭证。
5. 使用移动设备上的身份验证应用来生成一次性安全码。

## 更改内部用户账户的密码

*要编辑内部用户账户的密码：*

1. 在主菜单中，转至**用户和角色** → **用户和组**，然后选择**用户**选项卡。
2. 单击您要编辑的用户账户名称。
3. 在打开的用户设置窗口的**常规**选项卡上，单击**更改密码**按钮。
4. 为连线到 Kaspersky Security Center Linux 的用户的Set new password。
   要查看输入的密码，请单击。
5. 如有必要，启用**用户必须在首次登录时更改密码**选项，以在下次用户身份验证时强制更改密码。
6. 如果用户账户受到保护以防止未经授权的修改，您必须确认您有更改此账户的权限。在**账户保护**窗口中，指定在**常规功能**：**用户权限**功能区域中具有修改对象ACL权限的账户的凭据。
7. 使用移动设备上的身份验证应用来生成一次性安全码。

## 使用服务器标志配置更改密码的选项

您可以使用 klscflag 实用程序通过以下命令来配置更改密码：

- 配置密码轮换期限（ `LP_SplPwdChangePeriodDays`标志）

  ```
  klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangePeriodDays -t d -v <rotation_period>
  ```

  其中 `<rotation_period>`是用户密码过期后的时间段（以天为单位）。可能的值：0–730。如果参数值为 0，则禁用密码轮换。

- 配置需要更改密码的初次警告时间（LP_SplPwdChangeNotificationHours标志）

  klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangeNotificationHours -t d -v <warning_time>

  其中<warning_time>是用户密码过期之前的时间段（以小时为单位）。在此期间，会显示需要更改密码的通知。可能的值：0–17520。如果参数值为 0，则警告时间为密码轮换周期的 25%。

- 指定**用户必须在首次登录时更改密码**选项的默认值（ LP_SplPwdForceChange标志）

  klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdForceChange -t d -v <值>

  其中< value >标志的可能值为：

  1 — **用户必须在首次登录时更改密码**选项已启用。

  0 — **用户必须在首次登录时更改密码**选项被禁用。

要查看当前标志值，请运行以下命令：

klscflag -fget -pv .core/.independent -s KLLIM -n <标志> -t d

其中<标志>是LP_SplPwdChangePeriodDays、 LP_SplPwdChangeNotificationHours或LP_SplPwdForceChange标志。

# 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“**确定**”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，编辑卡巴斯基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. 单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，编辑卡巴斯基应用程序的访问权限。
4. 单击“**保存**”保存设置。

更新的角色出现在用户角色列表。

# 编辑用户角色范围

*用户角色范围*是用户和管理组的组合。与用户角色关联的设置仅应用到属于该角色用户的设备，以及仅在这些设备属于与该角色关联的组（包括子组）时。

*要添加用户、安全组和管理组到用户角色范围，您可以使用以下方法之一：*

*方法 1：*

1. 在主菜单中，转至**用户和角色→用户和组**，然后选择**用户**或**组**选项卡。
2. 选择您要添加到用户角色范围的用户或安全组旁边的复选框。
3. 单击“**分配角色**”按钮。
   角色分配向导启动。使用“**下一步**”按钮继续向导操作。
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**”按钮关闭窗口。

所选用户或安全组和所选管理组被添加到用户角色范围。

*方法 2:*

1. 在主菜单中，转到“**用户和角色**”→“**角色**”。
2. 单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**”按钮继续向导操作。
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**”按钮关闭窗口。
8. 单击“**关闭**”按钮（✕）以关闭角色属性窗口。

所选用户或安全组和所选管理组被添加到用户角色范围。

*方法 3:*

1. 在主菜单中，单击管理服务器名称。
   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，然后应用并保存更改。
   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“**确定**”。

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**”区域。
4. 单击**编辑**。
5. 要关联角色到：
   - **现有策略配置文件** – 单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. 在主菜单中，单击管理服务器名称。
   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。

# 修改账户密码

您可以更改本地账户密码，例如当用户忘记本地账户密码或要执行计划的密码更改时。

即使用户尚未登录账户，密码更改也将生效。您还可以更改本地根账户的密码。

> 此任务只能在 Linux 设备上执行。

*要更改特定设备上的本地账户密码：*

1. 在主菜单中，转到“**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“**更改账户密码(仅限 Linux)**”。
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。

为指定设备创建“*更改账户密码（仅限 Linux）*”任务。如果您选择了“**分配任务到管理组**”选项，则任务是组任务。

5. 在**任务范围**步骤，指定管理组、具有特定地址的设备或设备分类。

   可用设置取决于在上一步中选择的选项。

6. 在“**输入账户名和新密码**”步骤中，指定以下设置：

   - 在“**账户名**”字段中，指定要更改密码的账户名称。
   - 在“**新密码**”字段中，指定将要为前一个字段中所指定的账户设置的密码。

     要查看您输入的字符，请单击并按住“**显示**”按钮。
   - 如有必要，请选中“**设置为一次性密码(用户必须在首次登录后更改密码)**”复选框。

     - **设置为一次性密码(用户必须在首次登录后更改密码)**

       如果选中此复选框，则在用户首次登录后，系统将提示用户设置新密码。

       如果清除此复选框，则在用户首次登录后，系统将不会提示用户设置新密码。

       默认情况下已清除该选框。

7. 在**完成任务创建**步骤中，单击**完成**按钮以创建任务并关闭向导。

   如果启用了“**创建完成时打开任务详情**”选项，将打开任务设置窗口。在此窗口中，您可以检查任务参数、修改它们或配置任务启动计划（如有必要）。

8. 在任务列表中，选择已创建的任务，然后单击**启动**。

   或者等待任务按照您在任务设置中指定的时间表启动。

更改账户密码任务完成后，会更改指定设备上的指定本地账户的密码。

> 为了确保正确运行更改账户密码任务，必须在用户设备上禁用 SELinux。

# 撤销本地管理员权限

您可以从账户中撤销本地管理员权限。这为您提供了对用户账户的额外控制。例如，您可以在一次性分配完成后撤销本地管理员权限。

运行此任务时，会检查指定的本地账户是否属于本地管理员组。这些组在网络代理策略设置中定义。您可以在网络代理策略设置中自定义本地管理员组列表。您还可以使用“**特权设备用户报告(仅限 Linux)**”检查特权用户账户列表。

> 此任务只能在 Linux 设备上执行。

*要撤销特定设备上的本地管理员权限：*

1. 在主菜单中，转到“**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“**撤销本地管理员权限(仅限 Linux)**”。
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。

   为指定设备创建“*撤销本地管理员权限（仅限 Linux）*”任务。如果您选择了“**分配任务到管理组**”选项，则任务是组任务。
5. 在**任务范围**步骤，指定管理组、具有特定地址的设备或设备分类。

   可用设置取决于在上一步中选择的选项。
6. 在向导的该步骤，指定以下设置：

   - 在“**操作模式**”设置组中，选择操作模式：

     - **从列出的账户中撤销本地管理员权限**

       如果选择此选项，将会从指定的本地账户撤销本地管理员权限。

       默认情况下已选定该选项。

     - **从本地管理员权限撤销中排除列出的账户**

       如果选择此选项，将会从指定账户外的所有本地账户撤销本地管理员权限。

默认情况下未选定该选项。

- 指定本地账户：
  - 单击**添加**。
  - 在打开的窗口中，执行以下操作：
    - 在“**账户名**”字段中，指定本地账户的名称。
    - 在“**账户操作**”设置组（仅当选择“**从列出的账户中撤销本地管理员权限**”选项时可用）中，选择操作。
    - **保留账户**

      如果选择此选项，则撤销本地管理员权限后不会删除本地账户。
      默认情况下已选定该选项。
    - **删除账户**

      如果选择此选项，无论本地账户是否具有本地管理员权限，都将被删除。
      默认情况下未选定该选项。

7. 在**完成任务创建**步骤中，单击**完成**按钮以创建任务并关闭向导。
   如果启用了“**创建完成时打开任务详情**”选项，将打开任务设置窗口。在此窗口中，您可以检查任务参数、修改它们或配置任务启动计划（如有必要）。
8. 在任务列表中，选择已创建的任务，然后单击**启动**。
   或者等待任务按照您在任务设置中指定的时间表启动。

当撤销本地管理员权限任务完成后，会从指定设备上的指定本地账户撤销本地管理员权限。

# 配置 Kerberos 域身份验证

Kaspersky Security Center Linux 允许您通过 Kerberos 协议使用域身份验证。域身份验证可让您在 Kaspersky Security Center Web Console 中启用安全身份验证，而无需在公司网络上重新输入密码（单点登录）。

您必须首先配置域控制器以使用 Kerberos 并生成 keytab 文件。要了解更多信息，请参阅您的域控制器的文档。

Microsoft Active Directory支持SCRIL（交互式登录需要智能卡）。

## 为 FreeIPA 和 AldPro 生成 keytab 文件

*要生成 keytab 文件，请执行以下操作：*

1. 创建一个用户账户，供 IAM 用于访问域控制器。
2. 如果管理服务器位于 FreeIPA/AldPro 域之外，请添加 DNS 记录条目和主机条目：

   ```
   ipa dnsrecord-add <zoneName> <recordName> --a-rec <管理服务器 IP 地址>
   ipa host-add --password=<password> <管理服务器主机地址>
   ```

3. 为管理服务器创建 HTTP 服务时，请指定 PAC 类型：

   ```
   ipa service-add HTTP/< 管理服务器主机 FQDN >@< 域名用大写字母书写 > --ok-to-auth-as-delegate=true --pac-type PAD
   ```

4. 指定用于身份验证的用户账户：

   ```
   ipa service-allow-retrieve-keytab HTTP/< 管理服务器主机地址 >@< 域名用大写字母书写 > --user=<user>
   ```

5. 导出 keytab 文件：

   ```
   ipa-getkeytab -s < 域控制器地址 > -p HTTP/< 管理服务器主机地址 >@< 域名用大写字母书写 > -k /tmp/h.keytab
   ```

## 为 Microsoft Active Directory 生成 keytab 文件

*要生成 keytab 文件，请执行以下操作：*

1. 创建一个用户账户，供 IAM 用于与域控制器通讯。

2. 为该用户账户启用以下选项：

   - **用户无法更改密码**
   - **Kerberos AES 256 位加密**

   您可以启用**密码永不过期**选项，以避免每次密码过期时都重新发放 keytab 文件。

3. 为用户账户添加服务主体名称 (SPN)：

   ```
   setspn -S HTTP/< 管理服务器主机 FQDN > < 域名用大写字母书写 >\<user>
   ```

4. 导出 keytab 文件：

   ```
   ktpass -out C:\<folder>\< keytab 文件名 > -princ HTTP/< 管理服务器主机 FQDN >@< 域名用大写字母书写 > -mapuser < 域名用大写字母书写 >\<user> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass <password> -mapop set
   ```

## 为 Samba 生成 keytab 文件

*要生成 keytab 文件，请执行以下操作：*

1. 创建一个用户账户，供 IAM 用于与域控制器通讯：

   ```
   samba-tool user add <user>
   ```

2. 将 SPN 添加到用户账户：

   ```
   samba-tool spn add HTTP/< 管理服务器主机 FQDN > <user>
   ```

3. 导出 keytab 文件：

   ```
   samba-tool domain exportkeytab /tmp/file.keytab --principal=HTTP/< 管理服务器主机 FQDN >
   ```

## 启用 Kerberos 域身份验证

*要启用 Kerberos 域身份验证：*

1. 执行域控制器轮询。
2. 在主菜单中，转到“**设置**”→“**单点登录**”。
3. 启用“**Kerberos 身份验证**”选项。
4. 上传 keytab 文件。
5. 为域用户分配角色，以授予对 Kaspersky Security Center Web Console 的访问权限。
   已为域用户启用 Kerberos 域身份验证。

# 更新 Kaspersky 数据库和应用程序

该部分描述了定期更新以下内容必须采取的步骤：

- Kaspersky 数据库和软件模块
- 已安装的 Kaspersky 应用程序，包括 Kaspersky Security Center Linux 组件和安全应用程序

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

本部分提供定期更新 Kaspersky 数据库、软件模块和应用程序的方案。在您完成配置网络保护方案后，您必须维持保护系统的可靠性以确保管理服务器和受管理设备保持受保护状态以防范各种威胁，包括病毒、网络攻击和钓鱼攻击。

网络保护通过更新以下内容保持最新：

- Kaspersky 数据库和软件模块
- 已安装的 Kaspersky 应用程序，包括 Kaspersky Security Center Linux 组件和安全应用程序

当您完成方案时，您可以确保：

- 您的网络被最新的卡巴斯基软件保护，包括 Kaspersky Security Center Linux 组件和安全应用程序。
- 对网络安全至关重要的反病毒数据库和其他 Kaspersky 数据库始终保持最新。

## 先决条件

受管理设备必须连接到管理服务器。如果未建立连接，请考虑手动更新 Kaspersky 数据库和软件模块，或者直接从 Kaspersky 更新服务器更新。

管理服务器必须连接到互联网。

在您开始之前，确保您已做了如下：

1. 根据通过 Kaspersky Security Center Web Console 部署 Kaspersky 应用程序的方案将 Kaspersky 安全应用程序部署到受管理设备。
2. 创建了配置了所有所需策略、策略配置文件和任务，根据网络保护配置方案。
3. 分配了适当数量的分发点，与受管理设备和网路拓扑一致。

更新 Kaspersky 数据库和应用程序分阶段进行：

1. **选择更新 scheme**

   您可以使用多种方案来安装安全应用程序的更新。选择一个或多个满足您网络需求的 scheme。

2. **创建管理服务器的“将更新下载至存储库”任务**

   该任务由 Kaspersky Security Center 快速启动向导自动创建。如果您未运行向导，立即创建任务。

   此任务需要从 Kaspersky 更新服务器下载更新到管理服务器的存储库，以及为 Kaspersky Security Center Linux 更新 Kaspersky 数据库和软件模块。更新被下载后，它们可以被传播到受管理设备。

   如果您的网络被分配了分发点，更新被从管理服务器存储库自动下载到分发点存储库。此种情况下，分发点所在范围的受管理设备从分发点存储库下载更新，而不是从管理服务器存储库。

   使用说明：创建管理服务器的“将更新下载至存储库”任务

3. **创建“将更新下载至分发点存储库”任务（可选）**

   默认下，更新被从管理服务器下载到分发点。您可以配置 Kaspersky Security Center Linux 直接从 Kaspersky 更新服务器下载更新到分发点。您可以下载到分发点存储库，例如，如果管理服务器和分发点之间的流量比分发点和 Kaspersky 更新服务器之间的流量贵，或者如果您的管理服务器没有互联网访问。

   当您的网络已分配分发点并已创建“*将更新下载至分发点存储库*”任务时，分发点从 Kaspersky 更新服务器下载更新，而不是从管理服务器存储库下载。

   操作说明：创建将更新下载至分发点存储库的任务

4. **配置分发点**

   当您的网络已分配分发点时，确保在所有所需分发点的属性中启用“**已启用**”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。

7. **批准和拒绝受管理的卡巴斯基应用程序的更新**

   默认下，下载的软件更新具有*未定义*状态。您可以更改状态到*已批准*或*已拒绝*。批准的更新总是被安装。如果更新受管理的卡巴斯基应用程序时需要查看和接受最终用户授权许可协议的条款，则您需要先接受这些条款。此后，更新可以被传播到受管理设备。您设置了*已拒绝*状态的更新将不被安装到设备。如果受管理应用程序被拒绝的更新先前被安装，Kaspersky Security Center Linux 将尝试从所有设备上卸载该更新。

   批准和拒绝更新仅适用于安装在 Windows 和 Linux 客户端设备上的网络代理和受管理的卡巴斯基应用程序。不支持管理服务器、Kaspersky Security Center Web Console 和管理 Web 插件的无缝更新。

   操作说明：批准和拒绝软件更新

   有时，网络代理更新后，您可能会被提示重新启动受管理设备。如果显示所需重启通知，单击通知中的**查看设备**链接，选中要重新启动的设备旁边的复选框，然后单击**重新启动**按钮以完成网络代理更新。

结果

方案完成后，Kaspersky Security Center Linux 配置为在更新下载到管理服务器的存储库后更新卡巴斯基数据库。您然后可以继续监控网络状态。

# 关于更新 Kaspersky 数据库、软件模块和应用程序

为了确保管理服务器和受管理设备的保护是最新的，您必须提供以下内容的定期更新：

- Kaspersky 数据库和软件模块

  在下载卡巴斯基数据库和软件模块之前，Kaspersky Security Center Linux 会检查卡巴斯基服务器是否可访问。如果无法使用系统 DNS 访问服务器，应用程序将使用公共 DNS 服务器。这对于确保更新反病毒数据库并保持受管理设备的安全级别是必要的。

- 已安装的 Kaspersky 应用程序，包括 Kaspersky Security Center Linux 组件和安全应用程序

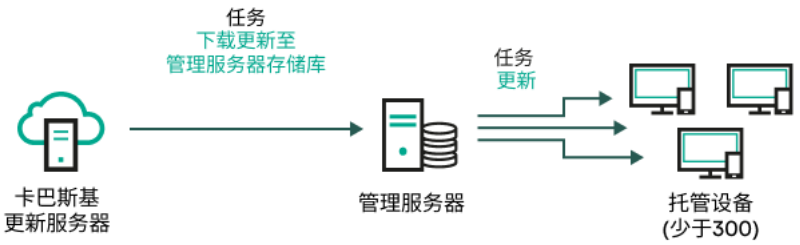
  通过 Kaspersky Security Center Linux，您可以自动更新安装在 Windows 和 Linux 客户端设备上的网络代理和卡巴斯基应用程序。不支持管理服务器、Kaspersky Security Center Web Console 和管理 Web 插件的无缝更新。要更新这些组件，您必须从卡巴斯基网站下载最新版本，然后手动进行安装。

取决于您网络的配置，您可以使用以下方案来下载和分发所需更新到受管理设备：

- 通过使用单个任务：*将更新下载至管理服务器存储库*
- 通过使用两个任务：
  - “*将更新下载至管理服务器存储库*”任务
  - 创建“*将更新下载至分发点存储库*”任务
- 通过本地文件夹、共享文件夹或 FTP 服务器手动
- 直接从卡巴斯基更新服务器到受管理设备上的 Kaspersky Endpoint Security
- 如果管理服务器没有互联网连接，则通过本地或网络文件夹

## 使用“将更新下载至管理服务器存储库”任务

在此方案中，Kaspersky Security Center Linux 通过“*将更新下载至管理服务器存储库*”任务来下载更新。在单一网段包含少于 300 台受管理设备或每个网段包含少于 10 台受管理设备的小网络中，更新直接从管理服务器存储库被分发到受管理设备（参见下图）。



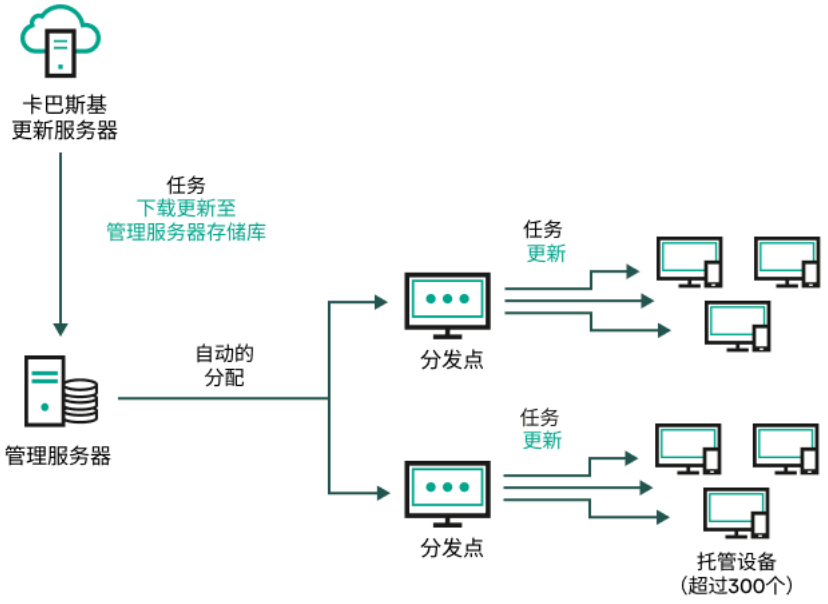

通过使用“*将更新下载至管理服务器存储库*”任务更新，而不使用分发点

更新源不仅可以是 Kaspersky 更新服务器，还可以是本地或网络文件夹。

默认下，管理服务器与 Kaspersky 更新服务器通信并使用 HTTPS 协议下载更新。您可以配置管理服务器使用 HTTP 协议，而不是 HTTPS。

如果您的网络中的单一网段包含 300 台或更多受管理设备，或者每个网段包含多于 9 台受管理设备，我们建议您使用分发点传播更新到受管理设备（参见下图）。分发点降低管理服务器负载并优化管理服务器和受管理设备之间的流量。您可以计算数字并配置您网络所需的分发点。

此种方案中，更新被从管理服务器存储库自动下载到分发点存储库。分发点所在范围的受管理设备从分发点存储库下载更新，而不是从管理服务器存储库。




通过使用“*将更新下载至管理服务器存储库*”任务更新，并使用分发点

“*将更新下载至管理服务器存储库*”任务完成后，Kaspersky Endpoint Security 的 Kaspersky 数据库和软件模块的更新即下载到管理服务器存储库。这些更新通过Kaspersky Endpoint Security *更新*任务安装。

> “*将更新下载至管理服务器存储库*”任务在虚拟管理服务器上不可用。虚拟管理服务器的存储库将显示已下载至主管理服务器的更新。

您可以配置在测试设备集上进行更新的操作和错误验证。如果验证成功，更新被分发到其他受管理设备。

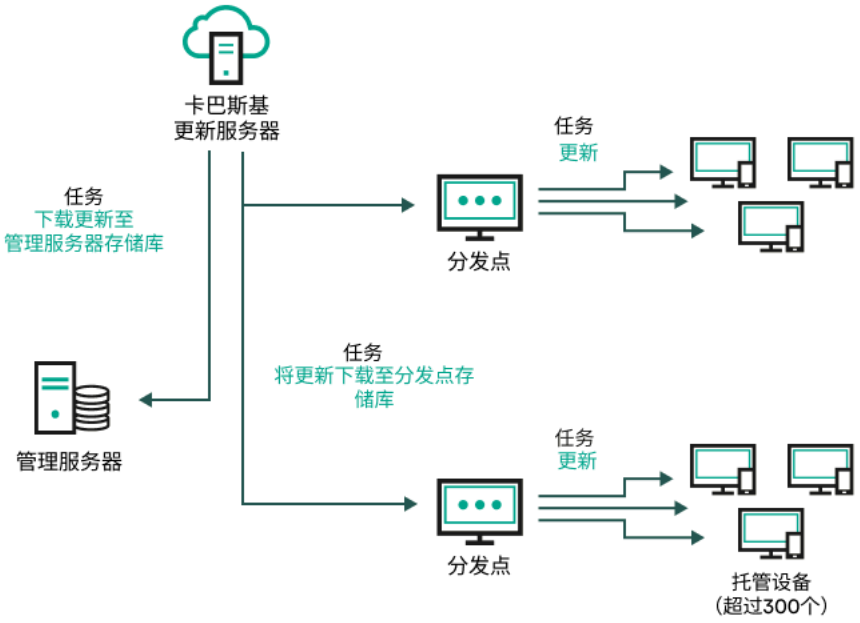
每个卡巴斯基应用程序都从管理服务器请求所需更新。管理服务器集合这些更新并仅下载应用程序请求的更新。这确保了相同更新不被下载多次，且不必要更新不被下载。当运行“*将更新下载至管理服务器存储库*”任务时，管理服务器自动发送以下信息到 Kaspersky 更新服务器以便确保相关版本的 Kaspersky 数据库和软件模块的下载：

- 应用程序 ID 和版本
- 应用程序启动 ID
- 活动密钥 ID
- “*将更新下载至管理服务器存储库*”任务运行 ID

传输的信息都不包含个人数据或其他机密数据。AO Kaspersky Lab 依照法律需求保护信息。

使用两个任务：“将更新下载至管理服务器存储库”任务和“将更新下载至分发点存储库”任务

您可以直接从 Kaspersky 更新服务器下载更新到分发点存储库，而不是从管理服务器存储库，然后分发更新到受管理设备（参见下图）。您可以下载到分发点存储库，例如，如果管理服务器和分发点之间的流量比分发点和 Kaspersky 更新服务器之间的流量贵，或者如果您的管理服务器没有互联网访问。




通过使用“*将更新下载至管理服务器存储库*”任务和“*将更新下载至分发点存储库*”任务更新

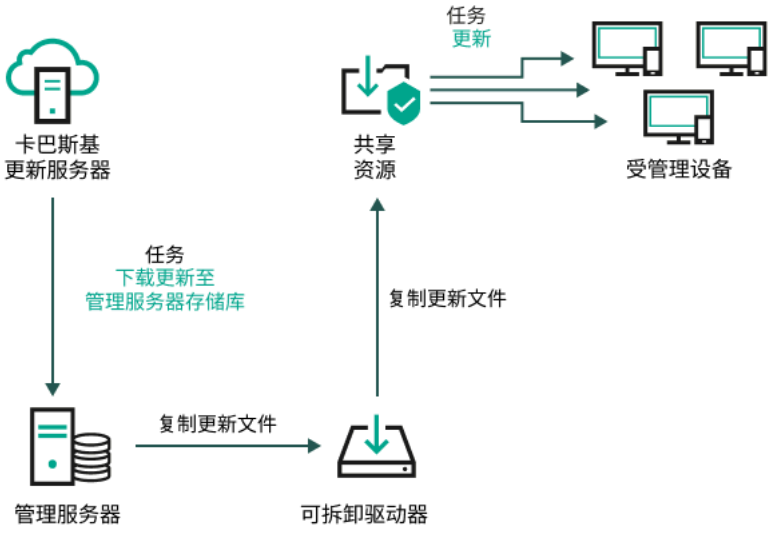
默认下，管理服务器和分发点与 Kaspersky 更新服务器通信并使用 HTTPS 协议下载更新。您可以配置管理服务器和/或分发点使用 HTTP 协议，而不是 HTTPS。

要实施此方案，除了“*将更新下载至管理服务器存储库*”任务外，请创建“*将更新下载至分发点存储库*”任务。此后，分发点将从 Kaspersky 更新服务器下载更新，而不是从管理服务器存储库。

此方案也需要“*将更新下载至管理服务器存储库*”任务，因为该任务被用于下载 Kaspersky 数据库和 Kaspersky Security Center Linux 软件模块。

### 通过本地文件夹、共享文件夹或 FTP 服务器手动

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



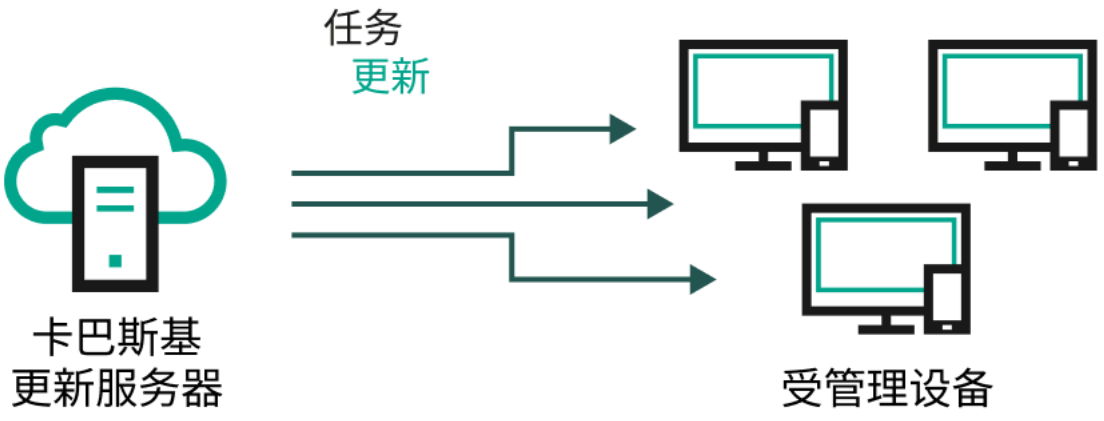

通过本地文件夹、共享文件夹或 FTP 服务器更新

有关 Kaspersky Endpoint Security 中更新源的更多信息，请参见以下帮助文档：

- Kaspersky Endpoint Security for Linux 帮助
- Kaspersky Endpoint Security for Windows 帮助

### 直接从卡巴斯基更新服务器到受管理设备上的 Kaspersky Endpoint Security

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




直接从 Kaspersky 更新服务器更新安全应用程序

在此方案中，安全应用程序不使用 Kaspersky Security Center Linux 提供的存储库。要直接从 Kaspersky 更新服务器接收更新，请在安全应用程序中指定 Kaspersky 更新服务器作为更新源。有关这些设置的详细信息，请参见以下帮助文档：

- Kaspersky Endpoint Security for Linux 帮助
- Kaspersky Endpoint Security for Windows 帮助

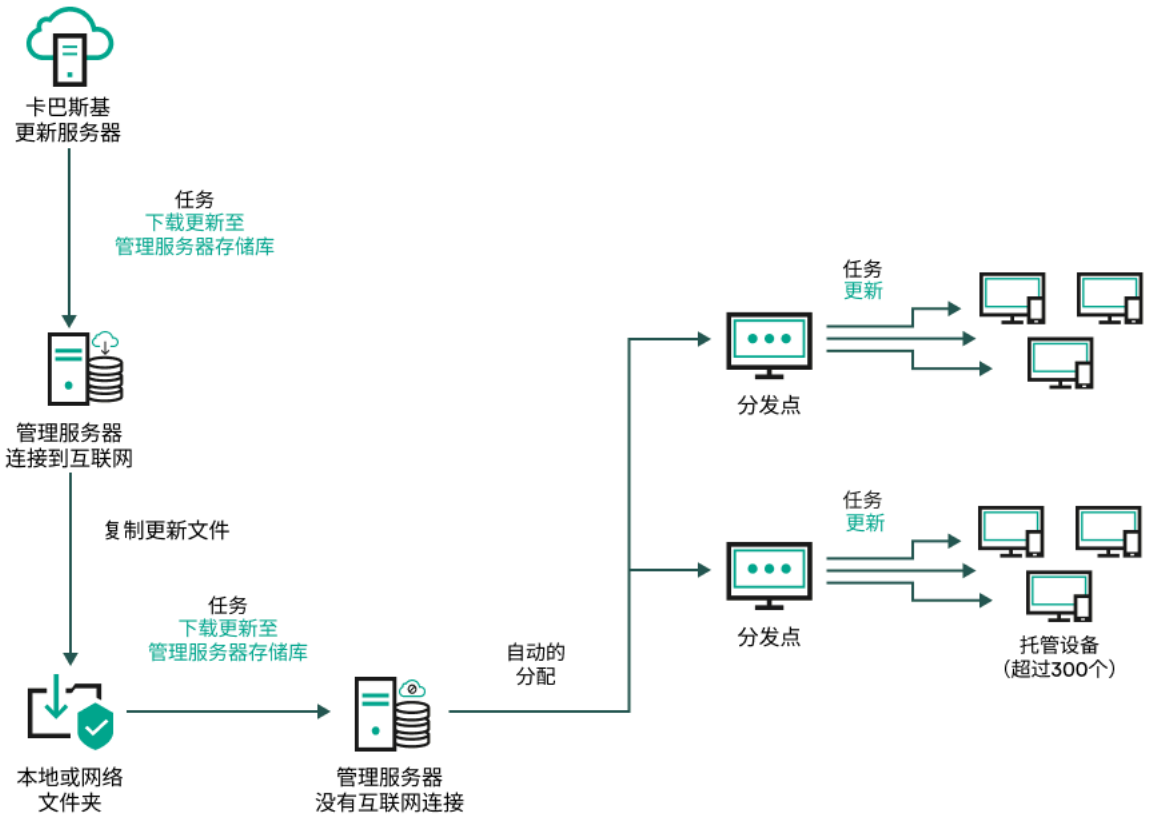
## 如果管理服务器没有互联网连接，则通过本地或网络文件夹

如果管理服务器没有互联网连接，您可以配置“*将更新下载至管理服务器存储库*”任务以从本地或网络文件夹下载更新。在这种情况下，必须不时地将所需的更新文件复制到指定文件夹。例如，您可以从以下来源之一复制所需的更新文件：

- 具有互联网连接的管理服务器（请参见下图）

  由于管理服务器只下载安全应用程序请求的更新，管理服务器管理的安全应用程序集（有互联网连接的应用程序和没有互联网连接的应用程序）必须匹配。

  如果用于下载更新的管理服务器版本为 13.2 或更早，请打开“*将更新下载至管理服务器存储库*”任务的属性，然后启用“**使用旧方案下载更新**”选项。




如果管理服务器没有互联网连接，则通过本地或网络文件夹更新

- 卡巴斯基更新实用程序

  由于此实用程序使用旧方案下载更新，请打开“*将更新下载至管理服务器存储库*”任务，然后启用“*使用旧方案下载更新*”选项。如有必要，您还可以配置*自动下载更新请求文件*选项，以便卡巴斯基更新实用程序仅下载所需的更新。

# 创建“将更新下载至管理服务器存储库”任务

“*将更新下载至管理服务器存储库*”任务允许您将卡巴斯基安全应用程序的数据库和软件模块的更新从卡巴斯基更新服务器下载到管理服务器存储库。

Kaspersky Security Center 快速启动向导会自动创建管理服务器的“*将更新下载至管理服务器存储库*”任务。任务列表中只能有一个“*将更新下载至管理服务器存储库*”任务。如果该任务已从管理服务器的任务列表中删除，您可以再次创建该任务。

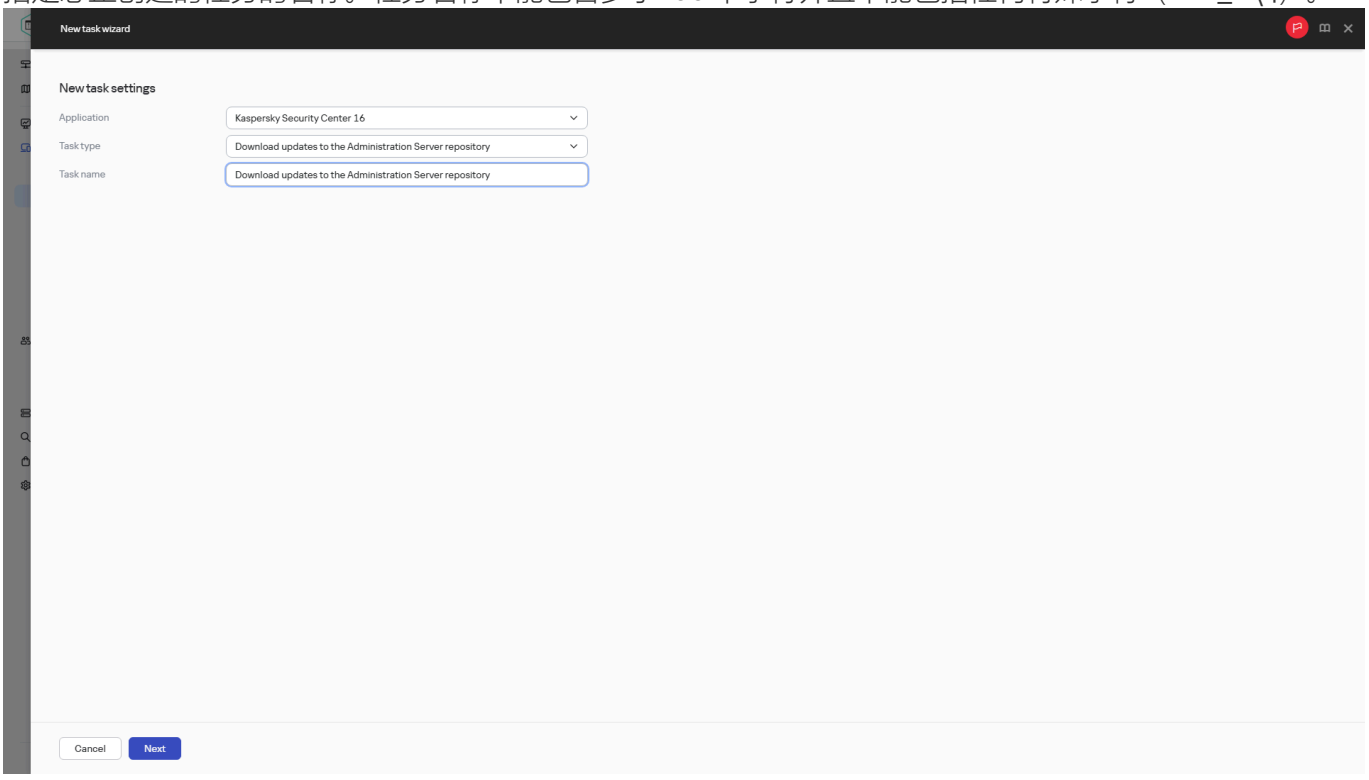
完成“*将更新下载至管理服务器存储库*”任务并下载更新后，可以将它们传播到受管理设备。

在向受管理设备分发更新之前，可以运行“*更新验证*”任务。这样可以确保管理服务器将正确安装下载的更新，并且安全级别不会由于更新而降低。要在分发更新之前对其进行验证，请配置“*将更新下载至管理服务器存储库*”任务设置中的“**运行更新验证**”选项。

*要创建“将更新下载至管理服务器存储库”任务：*

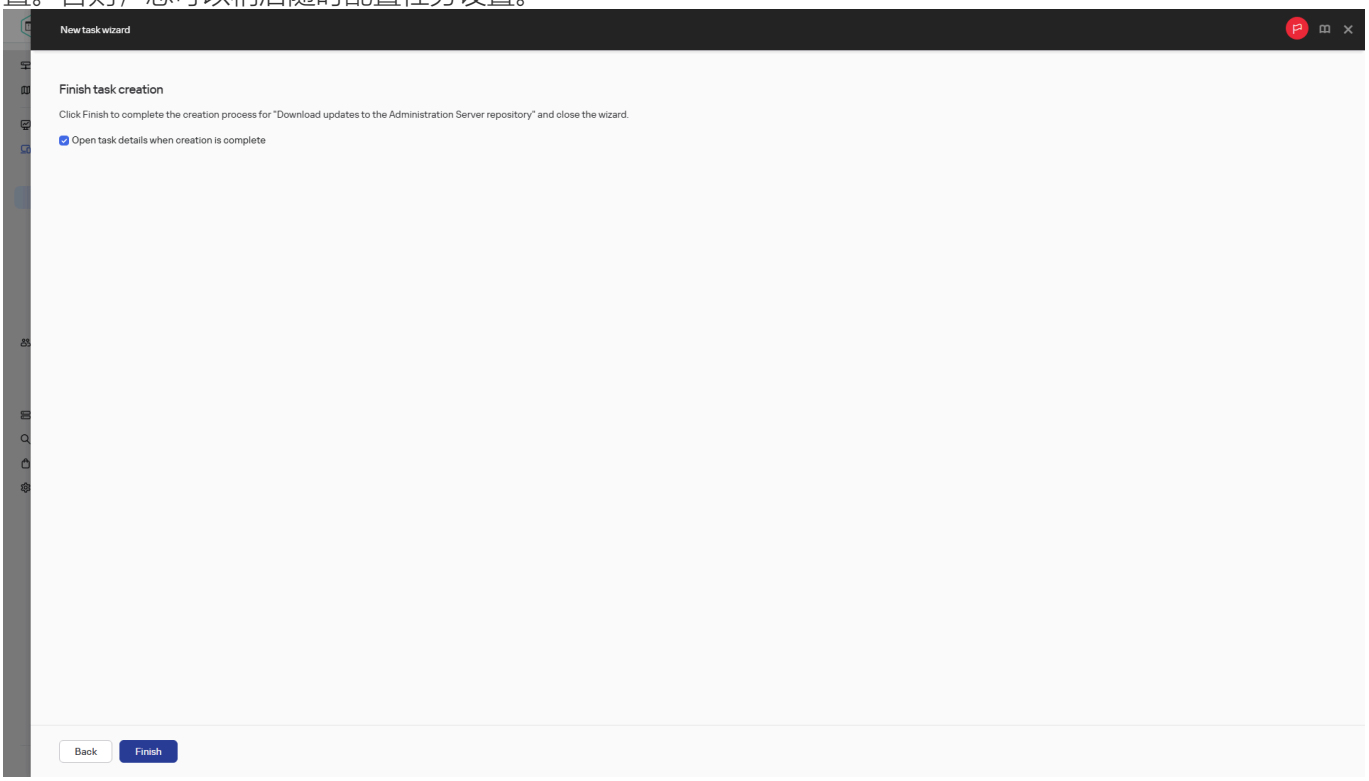
1. 在主菜单中，转到“**任务**”。
2. 单击**添加**。

   “新任务向导”启动。遵照向导的说明操作。
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（*<>-_?:\"|）。




创建“将更新下载至管理服务器存储库”任务

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。




完成任务创建

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**

     作为更新源，您可以使用：

     - 卡巴斯基更新服务器（默认选中）
     - 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。

       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。文件夹路径取决于设备的操作系统。由于本地文件夹位于基于 Linux 的管理服务器上，因此您必须指定 POSIX 路径，例如 /path/to/dir。

       选择 SMB 网络文件夹作为更新源时，请先将该文件夹挂载到安装了管理服务器的设备上，然后再选择该文件夹。然后使用其本地文件系统路径指定已挂载文件夹的路径。通过 SMB 协议提供对该文件夹的访问。

用作更新源的本地或网络文件夹、FTP 或 HTTP 服务器必须包含一种文件夹结构，该结构与卡巴斯基更新服务器上的文件夹结构相匹配。您可以使用卡巴斯基更新实用程序获取此结构。

在“*将更新下载至管理服务器存储库*”任务和“*将更新下载至分发点存储库*”任务中，如果选择受密码保护的本地或网络文件夹作为更新源，则用户身份验证不起作用。要解决此问题，首先挂载受密码保护的文件夹，然后指定所需的凭据，例如，通过操作系统。之后，您可以选择此文件夹作为更新下载任务中的更新源。Kaspersky Security Center Linux 不会要求您输入凭据。

- **更新存储文件夹**

  用于存储已保存更新的指定文件夹的路径。您可以将指定的文件夹路径复制到剪贴板。您不能更改组任务的指定文件夹的路径。

- **强制从属管理服务器更新**

  如果启用该选项，当新更新下载后管理服务器立刻在从属管理服务器上启动更新任务。更新任务通过使用在从属管理服务器上的任务属性中配置的更新源来启动。

  如果禁用此选项，从属管理服务器上的更新任务将根据计划启动。

  默认情况下已禁用该选项。

- **复制下载的更新到附加文件夹**

  管理服务器接收更新后，它复制它们到指定文件夹。如果您想要在您的网络上手动管理更新的分发，则使用该选项。

  例如，您可能要在以下情况下使用该选项：您组织的网络包含几个独立子网，且每个子网的设备不能访问其他子网。然而，所有子网中的设备都可以访问通用网络共享。此种情况下，您在子网之一设置管理服务器从 Kaspersky 更新服务器下载更新，启用该选项，然后指定该网络共享。对于其他管理服务器的“将更新下载至存储库”任务中，指定与更新源相同的网络共享。

  如果您选择将下载的更新复制到本地文件夹，则必须在已安装管理服务器的设备上指定文件夹。文件夹路径取决于设备的操作系统。由于本地文件夹位于基于 Linux 的管理服务器上，因此您必须指定 POSIX 路径，例如 /path/to/dir。

  选择位于基于 Linux 的管理服务器上的网络文件夹时，您必须预先确保已安装管理服务器的设备可以通过挂载该文件夹来访问该网络文件夹。对文件夹的访问使用 SMB 协议执行。

  默认情况下已禁用该选项。

- **下载差异文件**

  该选项启用下载 diff 文件功能。

  默认情况下已禁用该选项。

- **使用旧方案下载更新**

  从版本 14 开始，Kaspersky Security Center Linux 使用新方案下载数据库和软件模块的更新。要使应用程序使用新方案下载更新，更新源包含的更新文件必须具有与新方案兼容的元数据。如果更新源包含的更新文件的元数据仅与旧方案兼容，请启用“**使用旧方案下载更新**”选项。否则，更新下载任务将失败。

  例如，当指定本地或网络文件夹为更新源，并且此文件夹中的更新文件已被以下应用程序之一下载时，您必须启用此选项：

  - 卡巴斯基更新实用程序

    此实用程序使用旧方案下载更新。

- Kaspersky Security Center 13 Linux

  例如，您的管理服务器 1 没有互联网连接。在这种情况下，您可以使用具有互联网连接的管理服务器 2 下载更新，然后将更新放置到本地或网络文件夹以将其用作管理服务器 1 的更新源。如果管理服务器 2 的版本为 13 或更低，请在管理服务器 1 的任务中启用“**使用旧方案下载更新**”选项。

默认情况下已禁用该选项。

- **运行更新验证**

  管理服务器从源下载更新并将其保存到临时存储库，然后运行“**更新验证任务**”字段中定义的任务。如果任务成功完成，则将更新从临时存储库复制到管理服务器上的共享文件夹，然后分发到所有将管理服务器作为更新源的设备（启动具有“**当新更新下载至存储库时**”计划类型的任务）。只有在执行“*更新验证*”任务之后，将更新下载至存储库的任务才完成。

  默认情况下已禁用该选项。

- **自动下载更新请求文件**

  如果您想要卡巴斯基更新实用程序仅下载具有适当配置的所需更新，请启用此选项并指定 Kaspersky Security Center Linux 将创建更新请求文件的路径，其中包含有关要下载的更新的信息。更新请求文件包含用于版本控制的时间戳和 MD5 哈希。

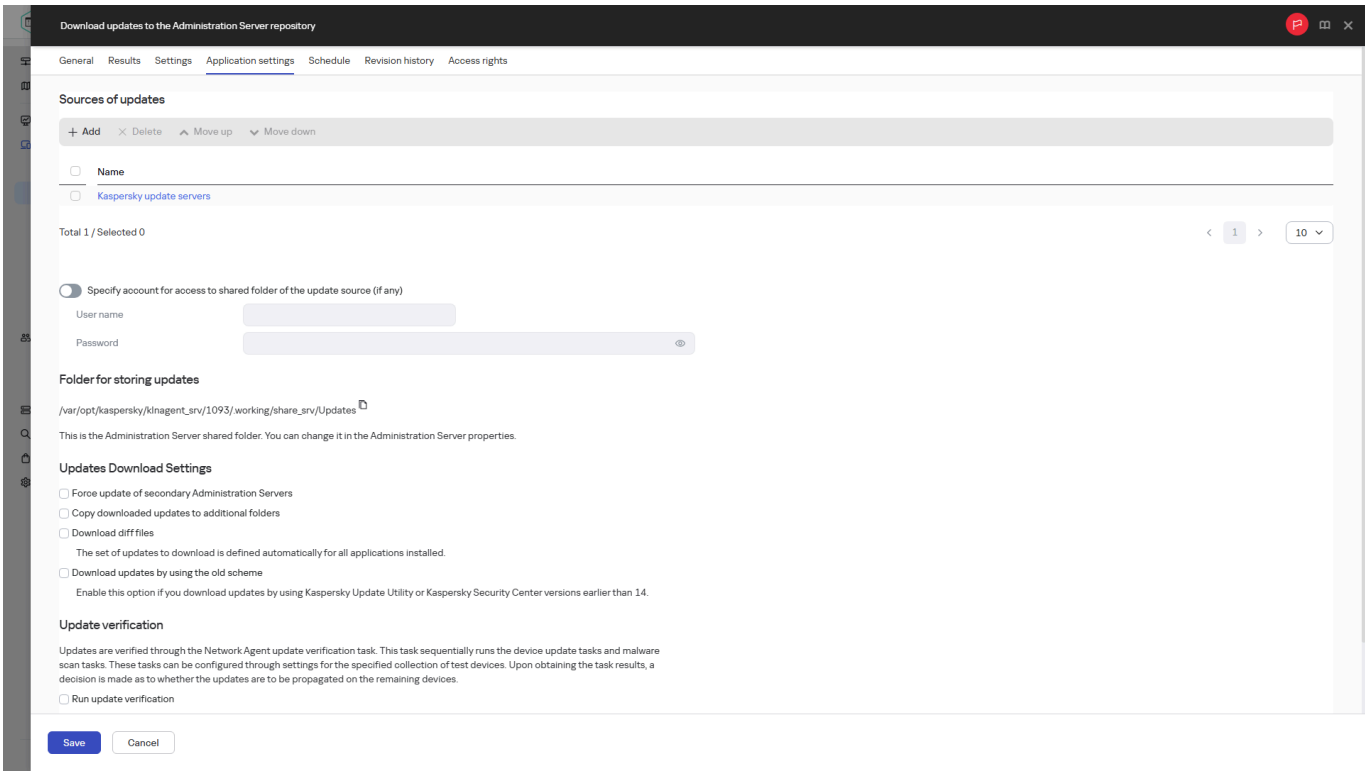
  请确保禁用**使用旧方案下载更新**选项。

  此外，必须配置卡巴斯基更新实用程序中的更新下载。

  默认情况下指定以下路径：/var/opt/kaspersky/klnagent_srv/1093/.working/share_srv/retranslation_request.xml。如有必要，您可以更改默认名称（retranslation_request）和路径。

  > 请求文件可以放在本地或共享文件夹中。使用共享文件夹时，您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。

  执行*将更新下载到管理服务器存储库*任务时，Kaspersky Security Center Linux 会在您指定的路径处创建 .xml 格式的更新请求文件。卡巴斯基更新实用程序自动从请求文件中获取信息，然后仅下载所需的更新。如果卡巴斯基更新实用程序无法自动获取信息（例如，卡巴斯基更新实用程序无权访问 Kaspersky Security Center Linux 在其中创建请求文件的文件夹），您必须使用第三方工具传输该文件。




指定"将更新下载到管理服务器存储库"任务的属性

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：

- **启动任务**：
  - **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。
  - **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。

- **每月在所选工作日**

  任务定期运行，在指定月日的指定时间。

  默认情况下，开始时间为18:00，且未选择任何日期。

  > 请注意，您选择的是当月的星期几，而不是具体的日期，也不是具体的周数（例如，当月的第一周或第二周）。例如，如果您将光标设置在第一行的**周二**单元格中，这意味着任务将在每月的**第一周**星期二运行。

  您可以选择一周中的多个日期。

- **在完成其他任务时**

  当前任务在其他任务完成后启动。仅当两个任务被分配给同一设备时，此选项才可用。例如，您可能想使用“***Turn on the device***”选项运行开启设备任务，在它完成后，运行*病毒扫描*任务作为触发任务。

  您必须从表中选择触发任务以及该任务必须完成的状态（**成功完成**或**失败**）。

  如有必要，您可以按如下方式搜索、排序和过滤表中的任务：

  - 在搜索栏中输入任务名称，即可根据名称搜索任务。
  - 单击排序图标可按名称对任务进行排序。

    默认情况下，任务按字母顺序升序排列。
  - 单击过滤器图标，在打开的窗口中按组过滤任务，然后单击**应用**按钮。

- 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卡巴斯基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。

- **使用任务启动自动随机延迟间隔**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

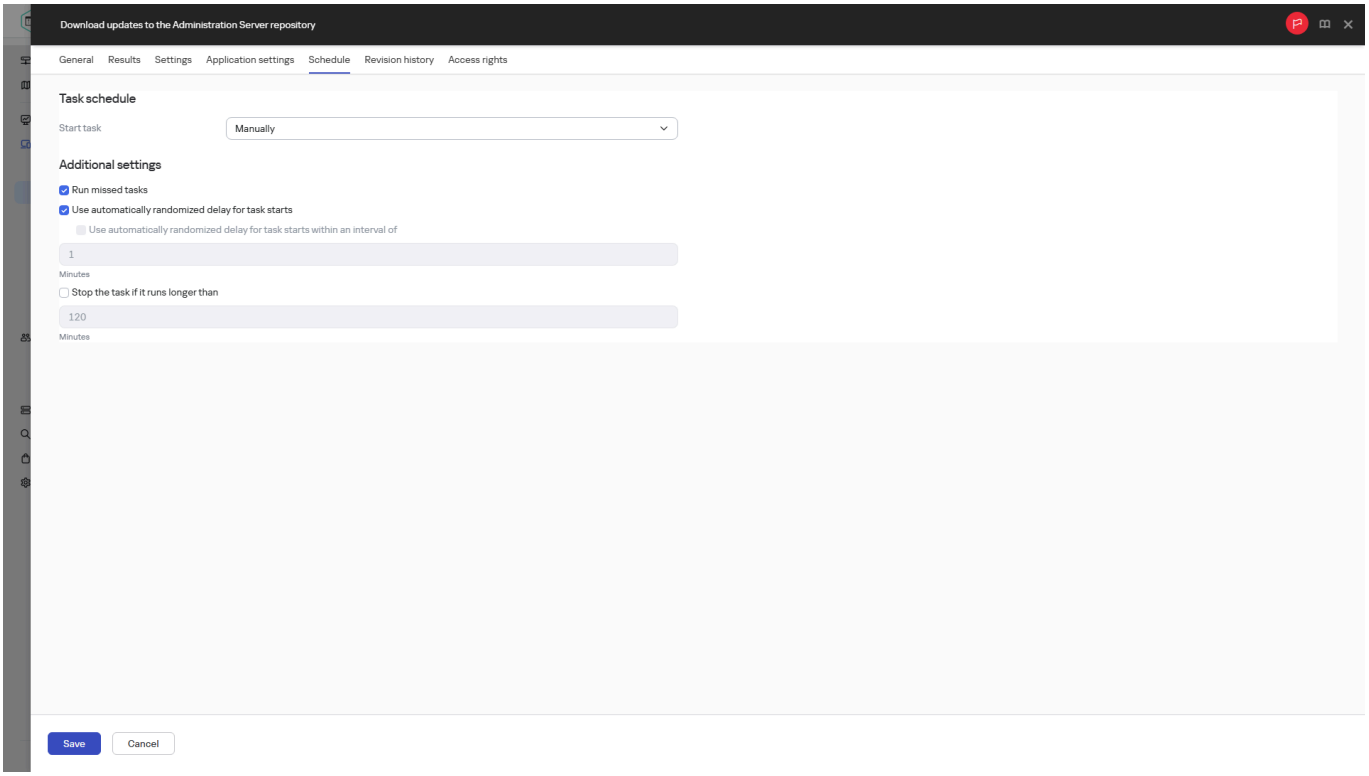
  默认情况下已禁用该选项。默认时间间隔为一分钟。

- **如果任务运行超过该时间则停止**

  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。

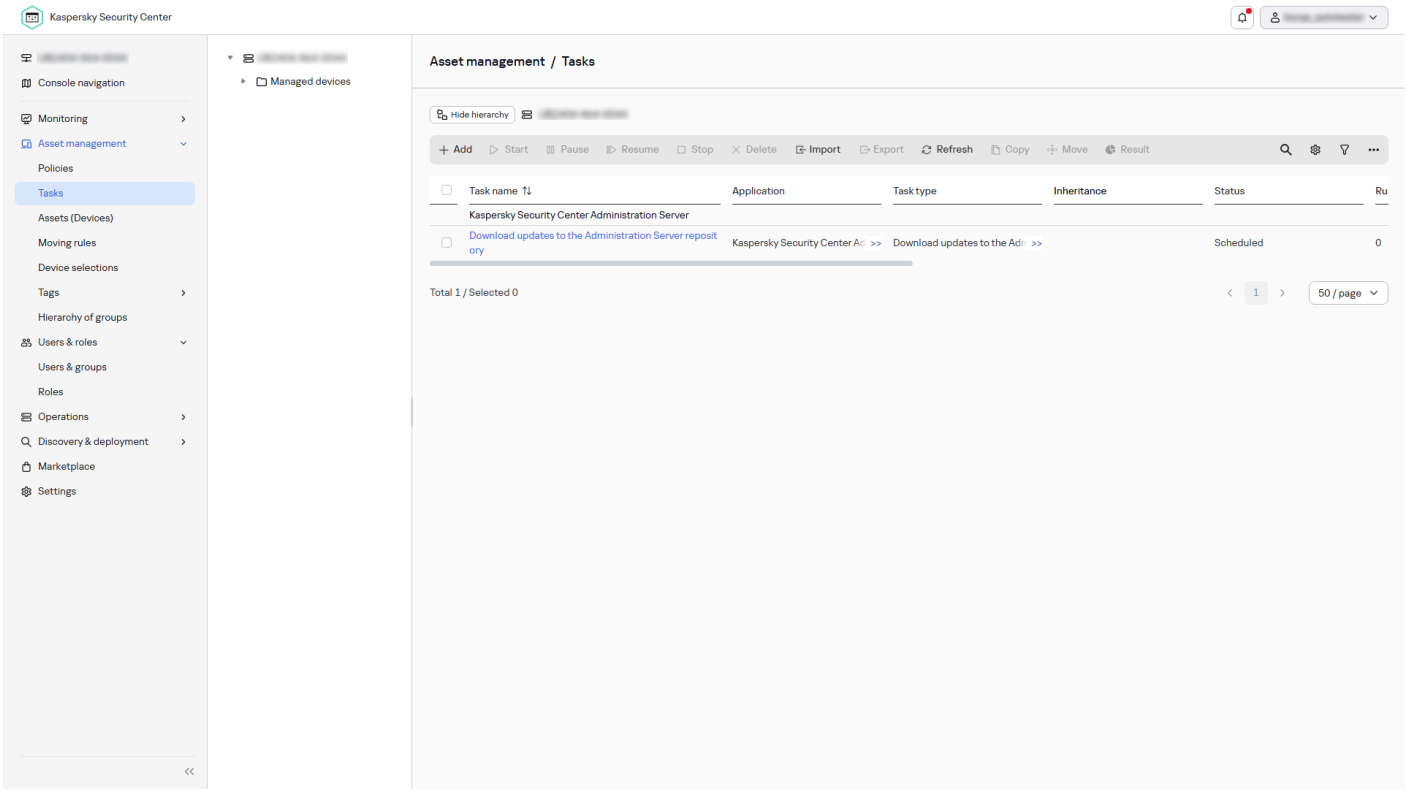
  默认情况下已禁用该选项。默认任务执行时间是 120 分钟。




指定"将更新下载至分发点存储库"任务的计划

10. 单击"**保存**"按钮。

任务被创建和配置。




任务列表

当管理服务器执行“*将更新下载至管理服务器存储库*”任务时，数据库和软件模块的更新将从更新源下载并存储在管理服务器的共享文件夹中。如果您为管理组创建此任务，它将仅被应用到包含在指定管理组中的网络代理。

这些更新将从管理服务器共享文件夹分发至客户端设备和从属管理服务器。

# 验证已下载的更新

安装更新到受管理设备之前，您可以先通过“*更新验证*”任务检查更新。作为“*将更新下载至管理服务器存储库*”任务的一部分，“*更新验证*”任务会自动执行。管理服务器从更新源下载更新，将其保存在临时存储库并执行“*更新验证*”任务。如果任务成功完成，更新将从临时存储库复制到管理服务器共享文件夹。它们被分发到所有以该管理服务器为更新源的客户端设备。

如果“*更新验证*”任务的结果显示位于临时存储库中的更新是错误的，或“*更新验证*”任务发生错误，这些更新不会被复制到共享文件夹。管理服务器保留之前的更新集。此外，计划类型为“**当新更新下载至存储库时**”的任务也不会启动。如果新更新扫描成功完成，在下次启动“*将更新下载至管理服务器存储库*”任务时将执行这些操作。

如果在一台或多台测试设备上出现以下情况，那么更新集合就被认为是无效的：

- 发生了更新任务错误。
- 安全应用程序的实时保护状态在应用更新后更改。
- 运行按需扫描任务过程中发现了一个被感染的对象。
- Kaspersky 程序出现运行时错误。

如果在任何测试设备上未出现以上情况，该更新集就被认为是有效的，“*更新验证*”任务被认为已成功完成。

在开始创建“*更新验证*”任务之前，请执行先决条件：

1. 创建包含多台测试设备的管理组。您将需要此组来验证更新。

   建议使用网络中具有最可靠的保护和最常用的应用程序配置的设备。这种方法可提高扫描期间病毒检测的质量和可能性，并将误报的风险降至最低。如果在测试设备上检测到病毒，“*更新验证*”任务将被视为不成功。

2. 为 Kaspersky Security Center 支持的应用程序（例如 Kaspersky Endpoint Security for Linux）创建更新和病毒软件扫描任务。创建更新和恶意软件扫描任务时，请指定具有测试设备的管理组。

   “*更新验证*”任务会在测试设备上依次运行更新和恶意软件扫描任务，以检查所有更新是否有效。此外，在创建“*更新验证*”任务时，您需要指定更新和恶意软件扫描任务。

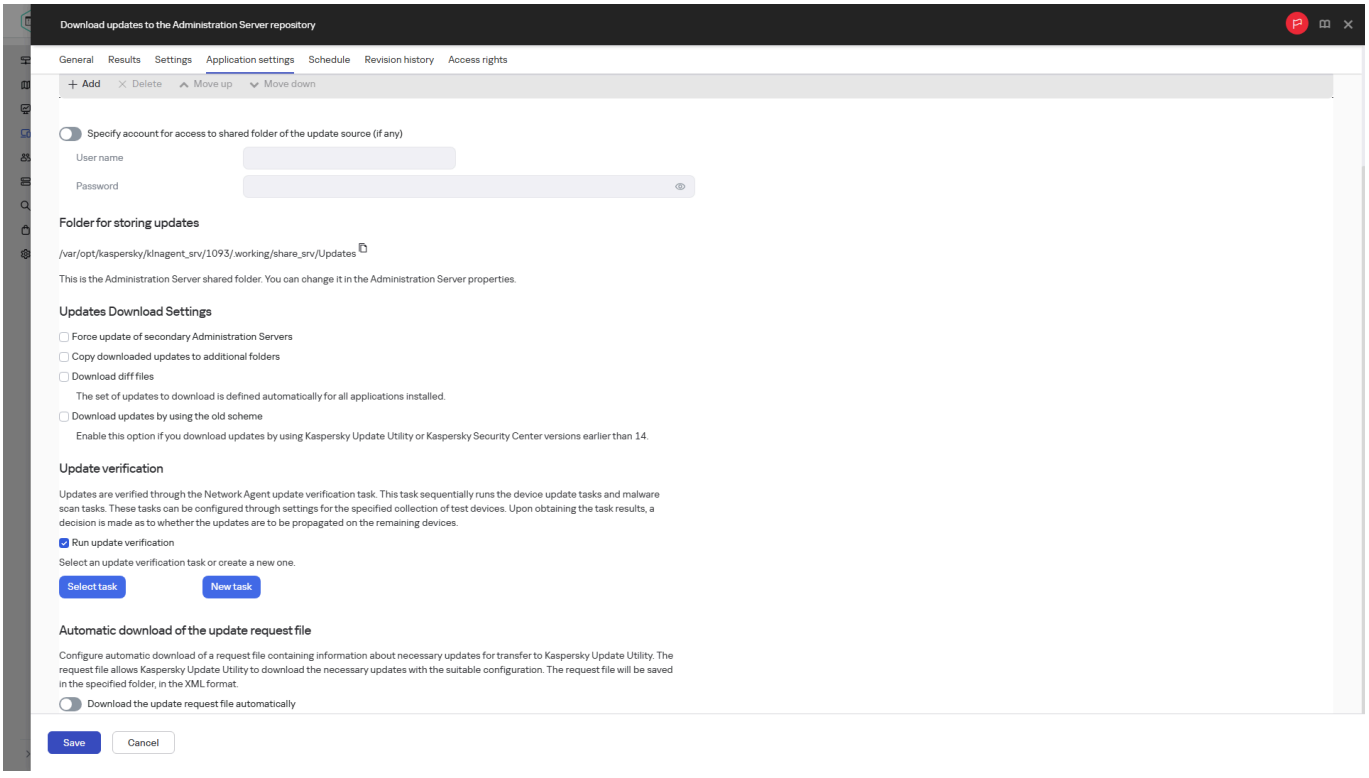
3. 创建“*将更新下载至管理服务器存储库*”任务。

*要让 Kaspersky Security Center Linux 将更新分发至客户端设备前对下载的更新进行验证，请执行以下操作：*

1. 在主菜单中，转到“**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。



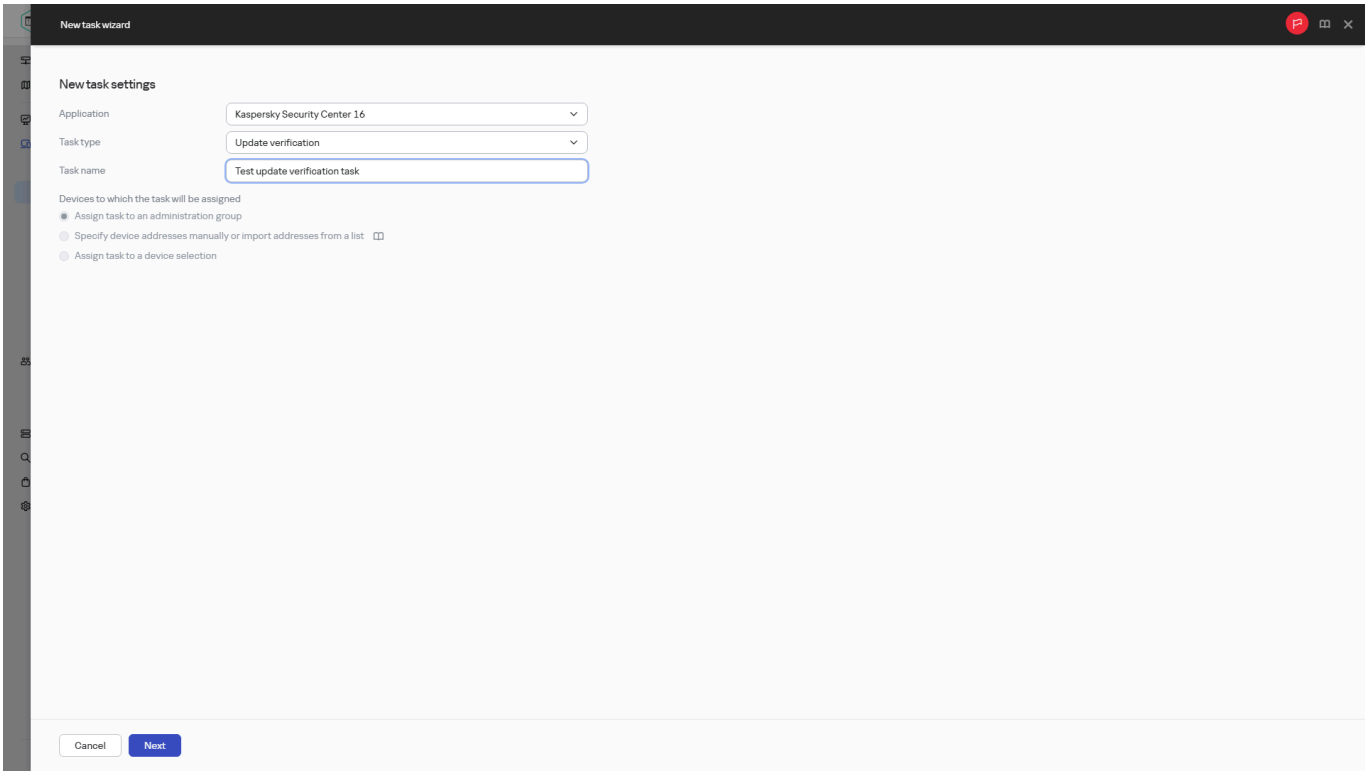

“将更新下载至管理服务器存储库”任务的属性

4. 如果“*更新验证*”任务存在，请单击“**选择任务**”按钮。在打开的窗口中，在具有测试设备的管理组中选择“*更新验证*”任务。

5. 如果您先前未创建“*更新验证*”任务，请执行以下操作：

a. 单击“**新任务**”按钮。

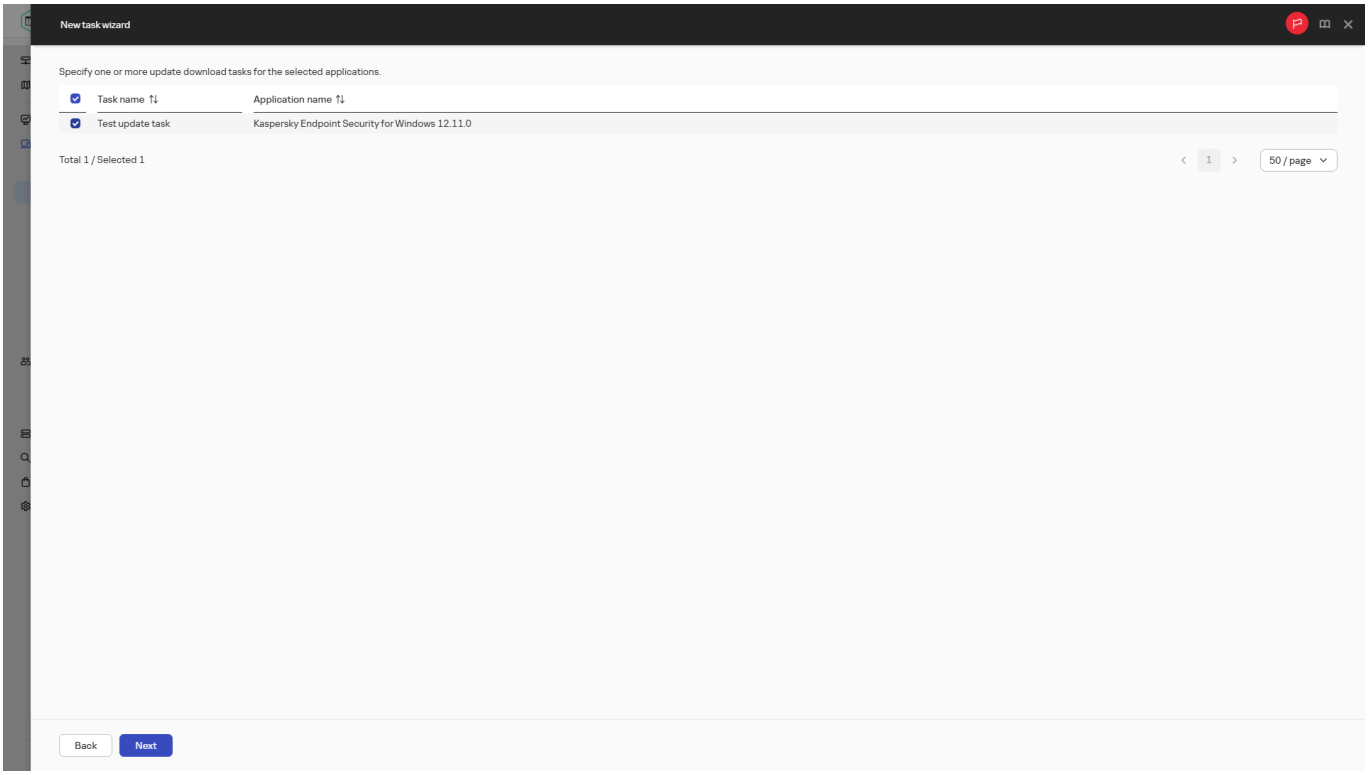
b. 如果要更改预设名称，则在打开的“新任务向导”中指定任务名称。




创建“更新验证”任务

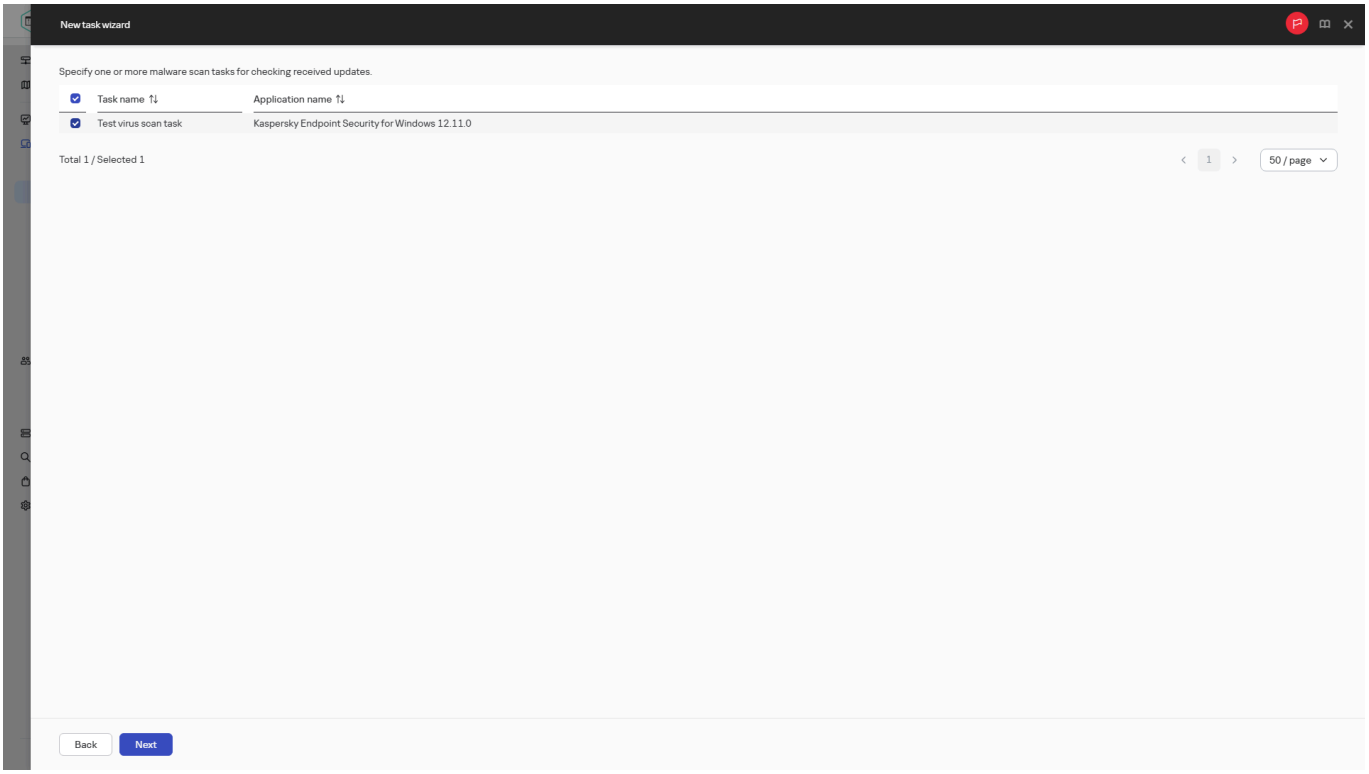
a. 选择您先前创建的具有测试设备的管理组。

b. 选择 Kaspersky Security Center Linux 支持的所需应用程序的更新任务。




选择应用程序更新任务

a. 选择 Kaspersky Security Center Linux 支持的所需应用程序的恶意软件扫描任务。




选择恶意软件扫描任务

之后，会出现以下选项。我们建议将这些选项保持启用状态：

- **在数据库更新后重启设备**

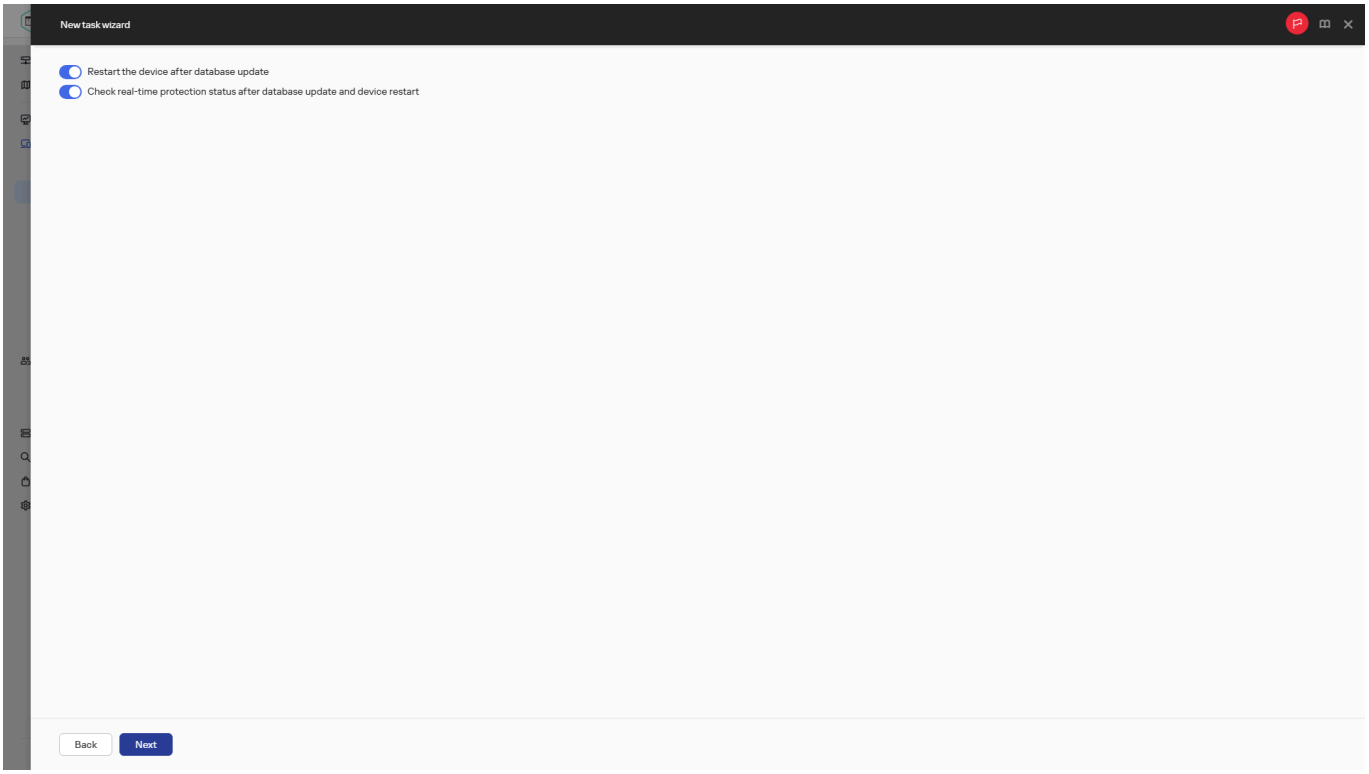
  在设备上更新反病毒数据库后，建议重新启动设备。

  默认情况下已启用该选项。

- **在数据库更新和设备重启后检查实时保护状态**

  如果启用此选项，则“*更新验证*”任务将检查下载到管理服务器存储库的更新是否有效，以及在反病毒数据库更新和设备重启后保护级别是否降低。

默认情况下已启用该选项。




指定任务设置

a. 指定运行“*更新验证*”任务将使用的账户。您可以使用您的账户并保持“**默认账户**”选项为启用状态。或者，您可以指定另一个用于运行该任务并具有必要访问权限的账户。为此，请选择“**指定账户**”选项，然后输入该账户的凭据。

6. 单击“**保存**”关闭“*将更新下载至管理服务器存储库*”任务的属性窗口。

自动更新验证被启用。现在，您可以运行“*将更新下载至管理服务器存储库*”任务，它将从更新验证开始。

# 创建“将更新下载至分发点存储库”任务

您可以为管理组创建“*将更新下载至分发点存储库*”任务。该任务将为包含在指定管理组中的分发点运行。

您可以使用该任务，例如，如果管理服务器和分发点之间的流量比分发点和 Kaspersky 更新服务器之间的流量贵，或者如果您的管理服务器没有互联网访问。

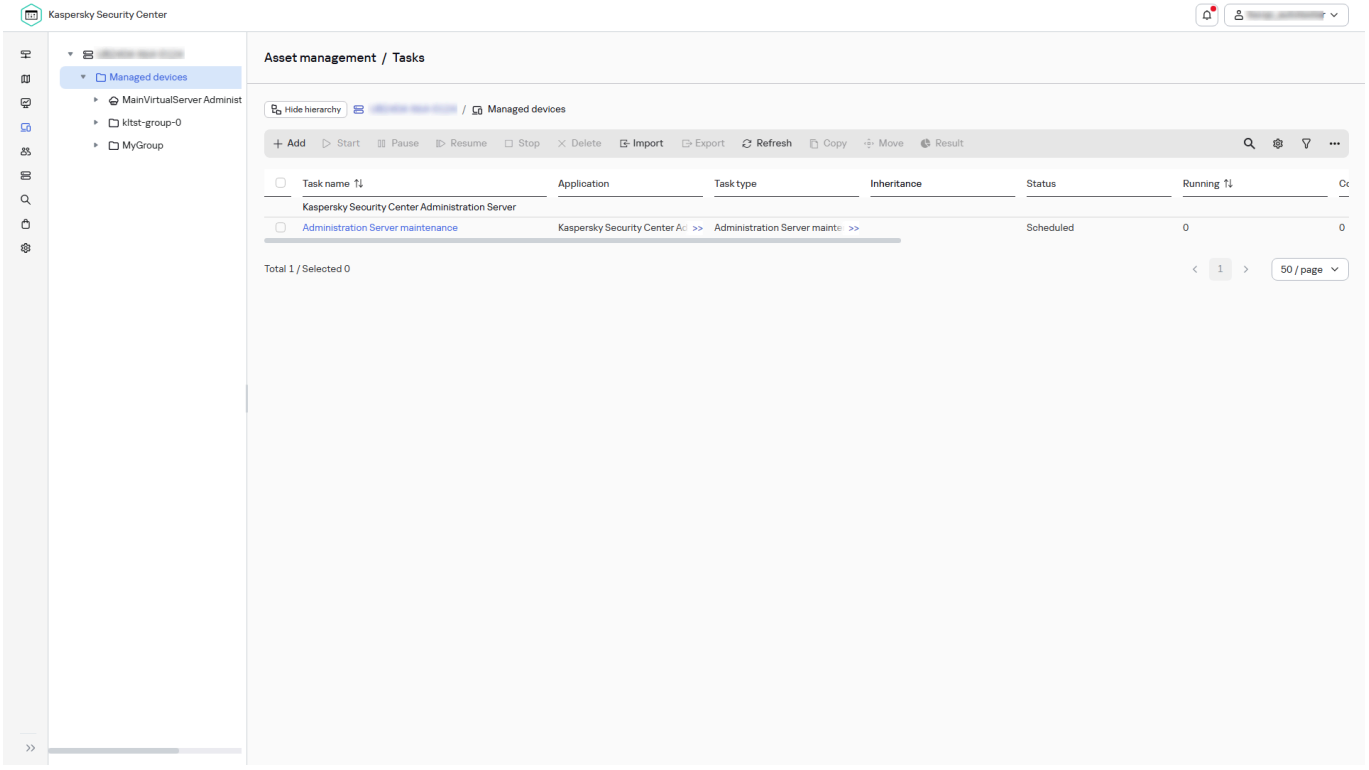
此任务需要从 Kaspersky 更新服务器下载更新到分发点的存储库。更新列表包含：

- Kaspersky 安全应用程序的数据库和软件模块的更新
- Kaspersky Security Center 组件更新
- Kaspersky 安全应用程序更新

更新被下载后，它们可以被传播到受管理设备。

*要创建“**将更新下载至分发点存储库**”任务，对于选定的管理组：*

1. 在主菜单中，转到“**任务**”。



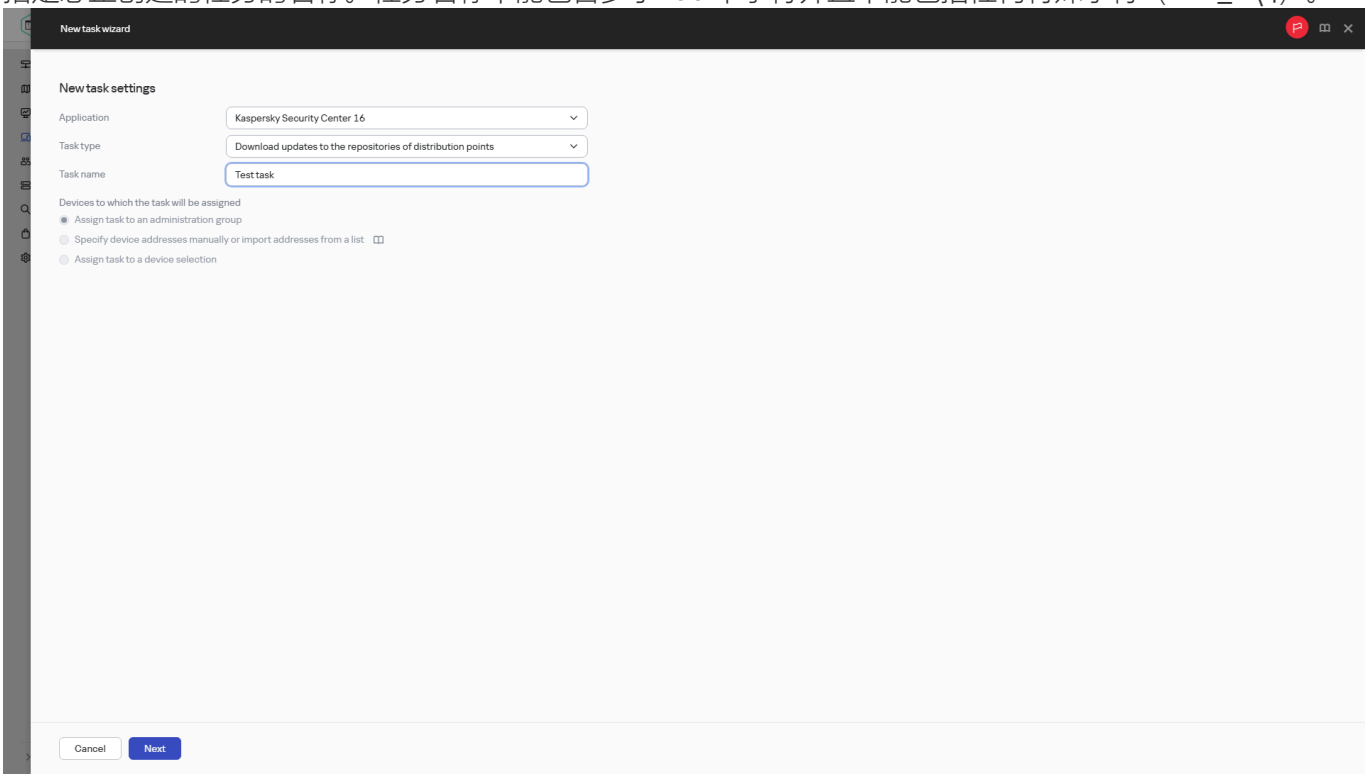

任务 部分

2. 单击“**添加**”按钮。

   “新任务向导”启动。遵照向导的说明操作。

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（*<>-_?:\"|）。




创建“将更新下载至分发点存储库”任务

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。

     - 本地或网络文件夹

       包含最新更新的本地或网络文件夹。只有已安装的 SMB 共享才能用作网络文件夹。在选择本地文件夹时，您必须在安装了管理服务器的设备上指定一个文件夹。

       > 在“*将更新下载至管理服务器存储库*”任务和“*将更新下载至分发点存储库*”任务中，如果选择受密码保护的本地或网络文件夹作为更新源，则用户身份验证不起作用。要解决此问题，首先挂载受密码保护的文件夹，然后指定所需的凭据，例如，通过操作系统。之后，您可以选择此文件夹作为更新下载任务中的更新源。Kaspersky Security Center Linux 不会要求您输入凭据。

   - **更新存储文件夹**

     用于存储已保存更新的指定文件夹的路径。您可以将指定的文件夹路径复制到剪贴板。您不能更改组任务的指定文件夹的路径。

   - **下载差异文件**

     该选项启用下载 diff 文件功能。

     默认情况下已禁用该选项。

   - **使用旧方案下载更新**

     从版本 14 开始，Kaspersky Security Center Linux 使用新方案下载数据库和软件模块的更新。要使应用程序使用新方案下载更新，更新源包含的更新文件必须具有与新方案兼容的元数据。如果更新源包含的更新文件的元数据仅与旧方案兼容，请启用“**使用旧方案下载更新**”选项。否则，更新下载任务将失败。

     例如，当指定本地或网络文件夹为更新源，并且此文件夹中的更新文件已被以下应用程序之一下载时，您必须启用此选项：

     - 卡巴斯基更新实用程序

       此实用程序使用旧方案下载更新。

     - Kaspersky Security Center 13 Linux

       例如，分发点配置为从本地或网络文件夹获取更新。在这种情况下，您可以使用具有互联网连接的管理服务器下载更新，然后将更新放置到分发点的本地或网络文件夹。如果管理服务器的版本为 13 或更低，请在“*将更新下载至分发点存储库*”任务中启用“**使用旧方案下载更新**”选项。

默认情况下已禁用该选项。

10. 为任务启动创建计划。如果必要，指定以下设置：

- **启动任务**：
  - **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。

  - **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。

  - **每月在所选工作日**

    任务定期运行，在指定月日的指定时间。

    默认情况下，开始时间为18:00，且未选择任何日期。

    > 请注意，您选择的是当月的星期几，而不是具体的日期，也不是具体的周数（例如，当月的第一周或第二周）。例如，如果您将光标设置在第一行的**周二**单元格中，这意味着任务将在每月的**第一周**星期二运行。

    您可以选择一周中的多个日期。

- **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。仅当两个任务被分配给同一设备时，此选项才可用。例如，您可能想使用"***Turn on the device***"选项运行开启设备任务，在它完成后，运行*病毒扫描*任务作为触发任务。

  您必须从表中选择触发任务以及该任务必须完成的状态（**成功完成**或**失败**）。

  如有必要，您可以按如下方式搜索、排序和过滤表中的任务：

  - 在搜索栏中输入任务名称，即可根据名称搜索任务。
  - 单击排序图标可按名称对任务进行排序。

    默认情况下，任务按字母顺序升序排列。
  - 单击过滤器图标，在打开的窗口中按组过滤任务，然后单击**应用**按钮。

- **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卡巴斯基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。

- **使用任务启动自动随机延迟间隔**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

  默认情况下已禁用该选项。默认时间间隔为一分钟。

11. 单击"**保存**"按钮。

任务被创建和配置。

除了您在任务创建过程中指定的设置，您还可以更改所创建任务的其他属性。

执行“*将更新下载至分发点存储库*”任务时，数据库和软件模块的更新从更新源下载并存储在共享文件夹。下载的更新将仅被包含在指定管理组的分发点和没有更新下载任务的更新代理使用。

# 添加“将更新下载至管理服务器存储库”任务的更新源

在创建或使用“将更新下载至管理服务器存储库”任务时，可以选择以下更新源：

- Kaspersky 更新服务器
- 主管理服务器

  此资源适用于为从属或虚拟管理服务器创建的任务。
- 本地或网络文件夹

> 在“*将更新下载至管理服务器存储库*”任务和“*将更新下载至分发点存储库*”任务中，如果选择受密码保护的本地或网络文件夹作为更新源，则用户身份验证不起作用。要解决此问题，首先挂载受密码保护的文件夹，然后指定所需的凭据，例如，通过操作系统。之后，您可以选择此文件夹作为更新下载任务中的更新源。Kaspersky Security Center Linux 不会要求您输入凭据。

默认使用 Kaspersky 更新服务器，但您也可以从本地或网络文件夹下载更新。如果您的网络没有互联网访问权限，您可能希望使用文件夹。在这种情况下，您可以从 Kaspersky 更新服务器手动下载更新并将下载的文件放在所需的文件夹中。您只能指定一个本地或网络文件夹路径。

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。文件夹路径取决于设备的操作系统。由于本地文件夹位于基于 Linux 的管理服务器上，因此您必须指定 POSIX 路径，例如 /path/to/dir。

只有已安装的 SMB 共享才能用作网络文件夹。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。

*要添加更新源：*

1. 在主菜单中，转到“**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**”表中，单击“**添加**”按钮。
5. 在打开的窗口中，添加必要的来源，然后单击“**保存**”按钮。

   如果选中“**本地或网络文件夹**”复选框，则指定文件夹的路径。
6. 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。

如果您同时添加卡巴斯基更新服务器和本地或网络文件夹，则可以设置更新的优先级。为此，在“**更新源**”表中，选中要更改优先级的更新旁边的复选框，然后单击“**上移**”或“**下移**”按钮。

# 批准和拒绝软件更新

更新安装任务的设置可能需要对要安装的更新进行批准。您可以批准必须安装的更新并拒绝不能安装的更新。

例如，您可能想先在测试环境中检查更新安装以确保它们不干预设备操作，仅在这之后允许安装这些更新到客户端设备。

批准和拒绝更新仅适用于安装在 Windows 客户端设备上的网络代理和受管理应用程序。不支持管理服务器、Kaspersky Security Center Web Console 和管理 Web 插件的无缝更新。要更新这些组件，您必须从卡巴斯基网站下载最新版本，然后手动进行安装。

*要批准或拒绝一个或几个更新：*

1. 在主菜单中，前往**软件管理→卡巴斯基应用程序→无缝更新**。

   可用更新列表被显示。

   受管理应用程序的更新可能需要安装 Kaspersky Security Center 的特定最低版本。如果此版本高于当前版本，则会显示这些更新，但无法批准。此外，在升级 Kaspersky Security Center 之前，无法从此类更新创建安装包。系统会提示您将 Kaspersky Security Center 实例升级到所需的最低版本。

2. 如有必要，请单击“**查看和接受授权许可协议**”按钮来接受 EULA。

3. 选择您要批准或拒绝的更新。

4. 单击“**批准**”批准所选更新或单击“**拒绝**”拒绝所选更新。

   默认值是 *未定义*。

   您分配了*已批准*状态的更新被放置在安装队列。

   您分配了*已拒绝*状态的更新被从先前将其安装的设备上卸载（如果可能）。而且，它们将来也不会被安装到其他设备。

Kaspersky 应用程序的一些更新无法被卸载。如果您为其设置了“*已拒绝*”状态，Kaspersky Security Center Linux 将不会从先前安装到的设备上卸载这些更新。然而，这些更新将来也不会被安装到其他设备。

如果您为第三方软件更新设置了*已拒绝*状态，这些更新将不会安装在计划将其安装但并未将其安装的设备上。更新将保持在已将其安装的设备上。如果您必须删除更新，您可以在本地手动删除它们。

# 自动安装 Kaspersky Endpoint Security for Windows 的更新

您可以在客户端设备上配置 Kaspersky Endpoint Security for Windows 自动更新数据库和软件模块。

*要在设备上配置下载和自动安装 Kaspersky Endpoint Security for Windows 更新：*

1. 在主菜单中，转到“**任务**”。
2. 单击“**添加**”按钮。
   “新任务向导”启动。遵照向导的说明。
3. 对于 Kaspersky Endpoint Security for Windows 应用程序，选择**更新**作为任务子类型。
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. 选择任务范围。
6. 指定管理组、设备分类或应用程序任务的设备。
7. 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。
8. 单击“**创建**”按钮。
   任务被创建并显示在任务列表。
9. 点击创建的任务的名称以打开任务属性窗口。
10. 在任务属性窗口的“**应用程序设置**”选项卡上，以本地或移动模式定义更新任务设置：
    - **本地模式**: 连接在设备和管理服务器之间建立。
    - **移动模式**：Kaspersky Security Center Linux 和设备之间不会建立特定的连接（比如，当设备未连接到互联网时）。
11. 启用您要使用的更新源以更新 Kaspersky Endpoint Security for Windows 的数据库和应用程序模块。如果需要，使用“**上移**”和“**下移**”按钮更改列表中的更新源位置。如果启用了多个更新源，Kaspersky Endpoint Security for Windows 会尝试从列表顶部开始依次进行连接，并通过从第一个可用的更新源处获取更新包来执行更新任务。
12. 启用**安装批准的应用程序模块更新**选项，在更新应用程序数据库同时下载和安装软件模块。
    如果启用该选项，Kaspersky Endpoint Security for Windows 在运行更新任务时，通知用户有可用的软件模块更新并将软件模块更新包含在更新包中。Kaspersky Endpoint Security for Windows 仅安装您设置为*已批准*状态的更新；这些更新将通过应用程序界面或通过 Kaspersky Security Center Linux 在本地安装。
    您也可以启用**自动安装关键应用程序模块更新**选项。如果软件模块有任何更新，Kaspersky Endpoint Security for Windows 将自动安装状态为“*关键*”的更新；其余的更新会在您批准后安装。
    如果软件模块更新需要审查并接受授权许可协议和隐私策略，程序将在用户接受用户授权许可协议和隐私策略的条款后安装更新。
13. 选择**复制更新到文件夹**复选框，程序将已下载的更新保存到指定的文件夹。

14. 计划任务。为确保及时更新，建议您选择“**当新更新下载至存储库时**”选项。

15. 点击“**保存**”。

**更新**任务正在运行时，程序发送请求到 Kaspersky 更新服务器。

一些更新需要安装最新版本的管理插件。

# 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。

# 通过分发点下载更新

Kaspersky Security Center Linux 允许分发点从管理服务器、Kaspersky 服务器或本地网络文件夹接收更新。

*要为分发点配置更新下载：*

1. 在主菜单中，单击管理服务器名称。

   管理服务器属性窗口将打开。

2. 在“**常规**”选项卡上，选择“**分发点**”区域。

3. 单击将用于将更新传送到组中的客户端设备的分发点的名称。

4. 在分发点属性窗口中选择“**更新源**”区域。

5. 为分发点选择更新源：

   - **更新源**

     选择分发点的更新源：

     - 要允许分发点从管理服务器接收更新，请选择“**从管理服务器检索**”。
     - 要允许分发点使用任务接收更新，请选择“**使用更新下载任务**”，然后指定“*将更新下载至分发点存储库*”任务：
       - 如果设备上已存在此类任务，请在列表中选择该任务。
       - 如果设备上尚不存在此类任务，请单击“**创建任务**”链接创建任务。“新任务向导”启动。遵照向导的说明操作。

   - **下载差异文件**

     该选项启用下载 diff 文件功能。

     默认情况下已启用该选项。

分发点将从指定的更新源接收更新。

# 更新离线设备上的 Kaspersky 数据库和软件模块

更新受管理设备上的 Kaspersky 数据库和软件模块对于保持设备对病毒和其他威胁的防护是非常重要的任务。管理员通常通过使用管理服务器存储库来配置定期更新。

当您需要在未连接到管理服务器（主或从）、分发点或互联网的设备（或设备组）上更新数据库和软件模块时，您必须使用其他更新源，例如 FTP 服务器或本地文件夹。此种情况下，您必须使用大容量存储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：/var/opt/kaspersky/klnagent_srv/1093/.working/share_srv/Updates/.

   或者，您可以配置 Kaspersky Security Center Linux 定期复制更新到您选择的文件夹。为此，请使用“*将更新下载至管理服务器存储库*”任务的属性中的“**复制下载的更新到附加文件夹**”选项。如果您指定闪存驱动器或外部硬盘驱动器上的文件夹作为该选项的目标文件夹，该大容量存储设备将总是包含更新的最新版本。
3. 在离线设备上，配置 Kaspersky Endpoint Security 以从本地文件夹或共享文件夹接收更新，例如 FTP 服务器或共享文件夹。

   说明：

   - Kaspersky Endpoint Security for Linux 帮助
   - Kaspersky Endpoint Security for Windows 帮助
4. 从可移动驱动器复制更新到您想用作更新源的本地文件夹或共享资源。
5. 在需要安装更新的离线设备上，启动 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Windows 的*更新*任务，具体取决于离线设备的操作系统。

更新任务完成后，设备上的 Kaspersky 数据库和软件模块为最新。

# 监控、报告和审计

本节介绍 Kaspersky Security Center Linux 的监控和报告功能。这些功能给您一个基础架构、保护状态和统计信息的总览。

在 Kaspersky Security Center Linux 部署之后或操作过程中，您可以配置监控和报告功能以适应您的需要。

# 方案：监控和报告

本节提供在 Kaspersky Security Center Linux 中配置监控和报告功能的方案。

先决条件

在部署 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 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

### 仪表板

仪表板通过对信息进行图形显示来允许您监控您组织网络的安全趋势。

### 报告

报告功能允许您获取您组织网络的详细安全数字信息、保存该信息到文件、通过邮件发送它和打印它。

### 事件分类

事件分类提供了从管理服务器数据库中选择的指定事件集合的屏幕视图。这些事件集根据以下类别进行分组：

- 按重要级别—**严重事件**、**功能失败**、**警告**和**信息事件**
- 按时间—**最近事件**
- 按类型—**用户请求**和**审计事件**

您可以基于 Kaspersky Security Center Web Console 界面上可以配置的设置创建和查看用户定义的事件分类。

### 通知

通知提醒您事件并帮助您通过执行推荐操作或您认为适当的操作来加速您对这些事件的响应。

# 智能培训模式中的规则触发

该部分提供了客户端设备上的 Kaspersky Endpoint Security for Windows 中的自适应异常控制规则执行的检测信息。

规则检测客户端设备上的异常行为并可能阻止它。如果规则在智能培训模式下工作，就会检测异常行为，并向管理服务器发送关于每次此类情况的报告。您可以通过以下路径来查看有关检测到的异常行为的报告：**存储库** → **智能培训状态下的规则触发器**。您可以确认检测为正确或添加它们为排除，因此该行为类型不再被认为是异常。

检测信息存储在管理服务器的事件日志中（与其他事件一起）和自适应异常控制报告中。

关于自适应异常控制、规则以及它们的模式和状态的更多信息，请参阅 Kaspersky Endpoint Security for Windows 帮助。

# 查看并确认使用自适应异常控制规则执行的检测

*要查看使用自适应异常控制规则执行的检测列表：*

1. 在主菜单中，转到**存储库 → 智能培训状态下的规则触发器**。

   列表显示使用自适应异常控制规则执行的检测的以下信息：

   - **管理组**

     设备所属管理组的名称。

   - **虚拟管理服务器**

     管理设备的虚拟管理服务器。

   - **设备名称**

     应用规则的客户端设备名称。

   - **名称**

     应用的规则名称。

   - **状态**

     **正在排除**—如果管理员处理该条目并添加其到排除规则列表。该状态保持到下一次客户端设备与管理服务器同步时，同步之后，该条目从列表消失。

     **正在确认**—如果管理员处理该条目并确认。该状态保持到下一次客户端设备与管理服务器同步时，同步之后，该条目从列表消失。

     空—如果管理员不处理该条目。

   - **检测数量**

     一个启发式规则中的检测数量，一个进程和一个客户端设备。该数量由 Kaspersky Endpoint Security 计算。

   - **用户名**

     运行进程的生成检测的客户端设备用户名称。

   - **源进程路径**

     源进程路径，例如，执行操作的进程路径（更多信息请参阅 Kaspersky Endpoint Security 帮助）。

   - **源进程哈希**

     源进程文件的 SHA256 哈希（更多信息请参阅 Kaspersky Endpoint Security 帮助）。

   - **源对象路径**

     启动进程的对象路径（更多信息请参阅 Kaspersky Endpoint Security 帮助）。

   - **源对象哈希**

     源文件的 SHA256 哈希（更多信息请参阅 Kaspersky Endpoint Security 帮助）。

- **目标进程路径**

  目标进程的路径（更多信息请参阅 Kaspersky Endpoint Security 帮助）。

- **目标进程哈希**

  目标文件的 SHA256 哈希（更多信息请参阅 Kaspersky Endpoint Security 帮助）。

- **目标对象路径**

  目标对象的路径（更多信息请参阅 Kaspersky Endpoint Security 帮助）。

- **目标对象哈希**

  目标文件的 SHA256 哈希（更多信息请参阅 Kaspersky Endpoint Security 帮助）。

- **已处理**

  异常被检测的日期。

*要查看检测的属性：*

1. 在主菜单中，转到**存储库 → 智能培训状态下的规则触发器**。
2. 执行以下操作之一：
   - 在**名称**列中，单击带有您要查看的检测名称的链接。
   - 在检测列表中，选中想要查看的检测旁边的复选框，然后单击“**属性**”按钮。

   所选检测的属性窗口将打开，显示有关它的信息。

您可以从自适应异常控制规则的检测列表或所选检测的属性窗口中确认任何检测。

*确认检测：*

- 在检测列表中选择一项或者多项检测，然后单击“**确认**”按钮。
- 打开所选检测的属性窗口，然后单击“**确认**”按钮。

检测状态被更改为“**正在确认**”。客户端设备与管理服务器下次同步后，该检测将从检测列表中消失。

您的确认将被计入规则使用的统计数据中。有关详细信息，请参阅 Kaspersky Endpoint Security for Windows 帮助。

# 从自适应异常控制规则添加排除

“添加到自适应异常控制排除项”向导允许您从 Kaspersky Endpoint Security 的自适应异常控制规则添加排除项。

*要通过向导添加自适应异常控制规则的排除项：*

1. 通过下列其中一种方式启动向导：
   - 在主菜单中，转到**存储库→智能培训状态下的规则触发器**，选择一个或多个检测，然后单击**排除**按钮。

您可以一次添加 1000 个排除项。

在将检测添加到排除项之前，您可以通过单击检测名称或“**属性**”按钮来查看检测的属性。在打开的检测属性窗口中，您还可以单击“**排除**”按钮。

- 在主菜单中，转到“**监控**”→“**事件分类**”，单击包含所需事件分类的链接，选中要排除的检测旁边的复选框，然后单击“**从自适应异常控制中排除**”按钮。

“添加到自适应异常控制排除项”向导启动。使用“**下一步**”按钮继续向导操作。

2. 选择您要添加排除项的策略和配置文件。

   继承的策略无法被更新。如果您没有修改策略的权限，该策略将不会更新。

3. 单击**完成**关闭向导。

检测状态被更改为“**正在排除**”。客户端设备与管理服务器下次同步后，检测将从检测列表中消失。已配置并应用“自适应异常控制”规则的排除。

# 仪表板和小部件

本部分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。

# 使用仪表板

控制板通过对信息进行图形显示来允许您监控您组织网络的安全趋势。

在 Kaspersky Security Center Web Console 的“**监控**”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 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**

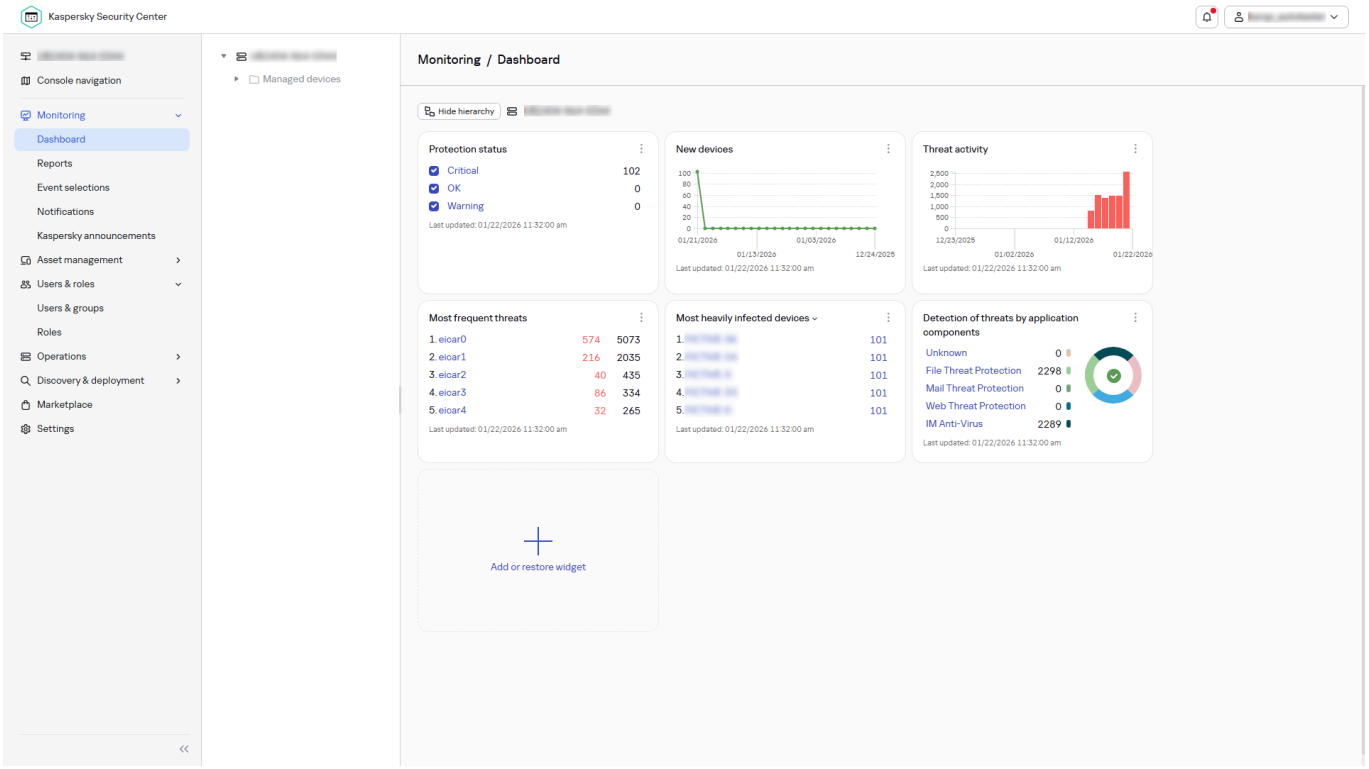
一些部件具有带链接的文本信息。您可以通过点击链接查看详细信息。

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。

# 添加小部件到仪表板

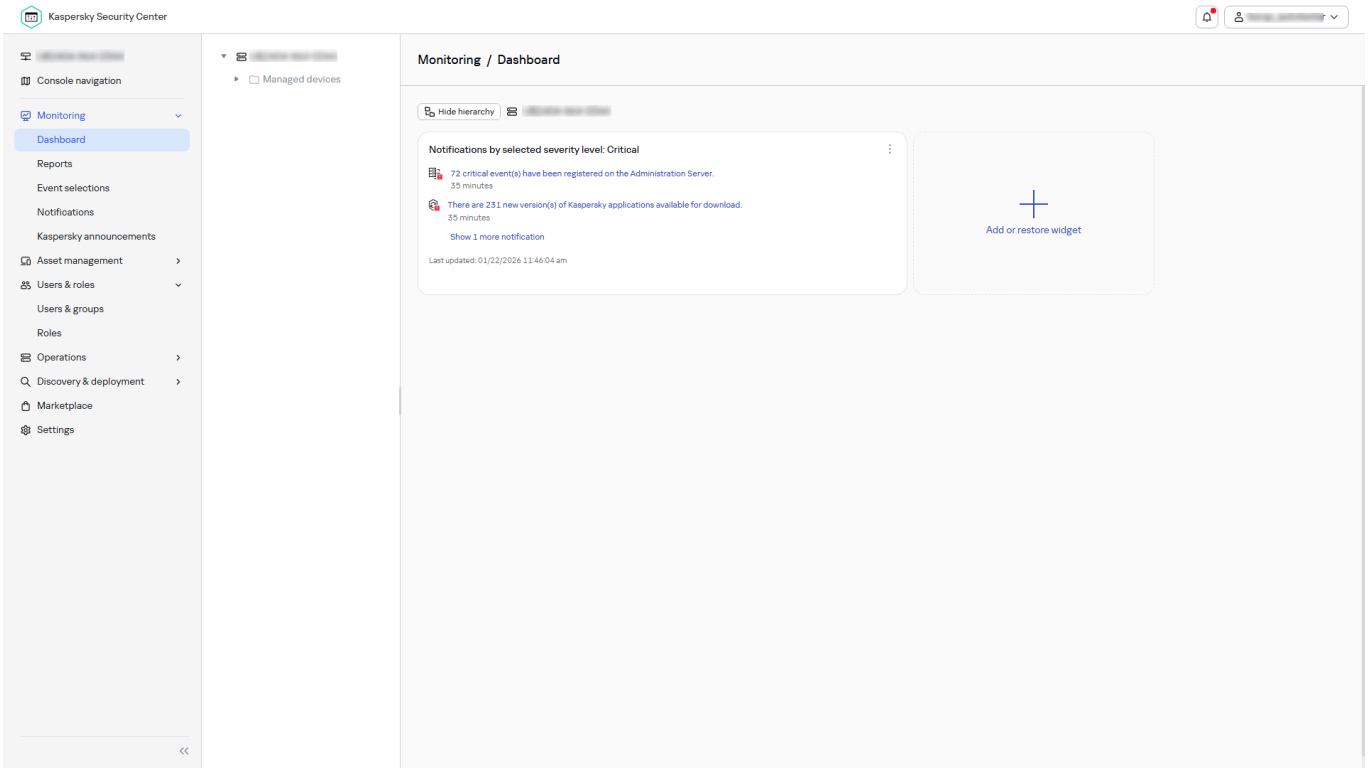
*要添加小部件到仪表板：*

1. 在主菜单中，转到“**监控 → 控制板**”。




带有小部件的仪表板

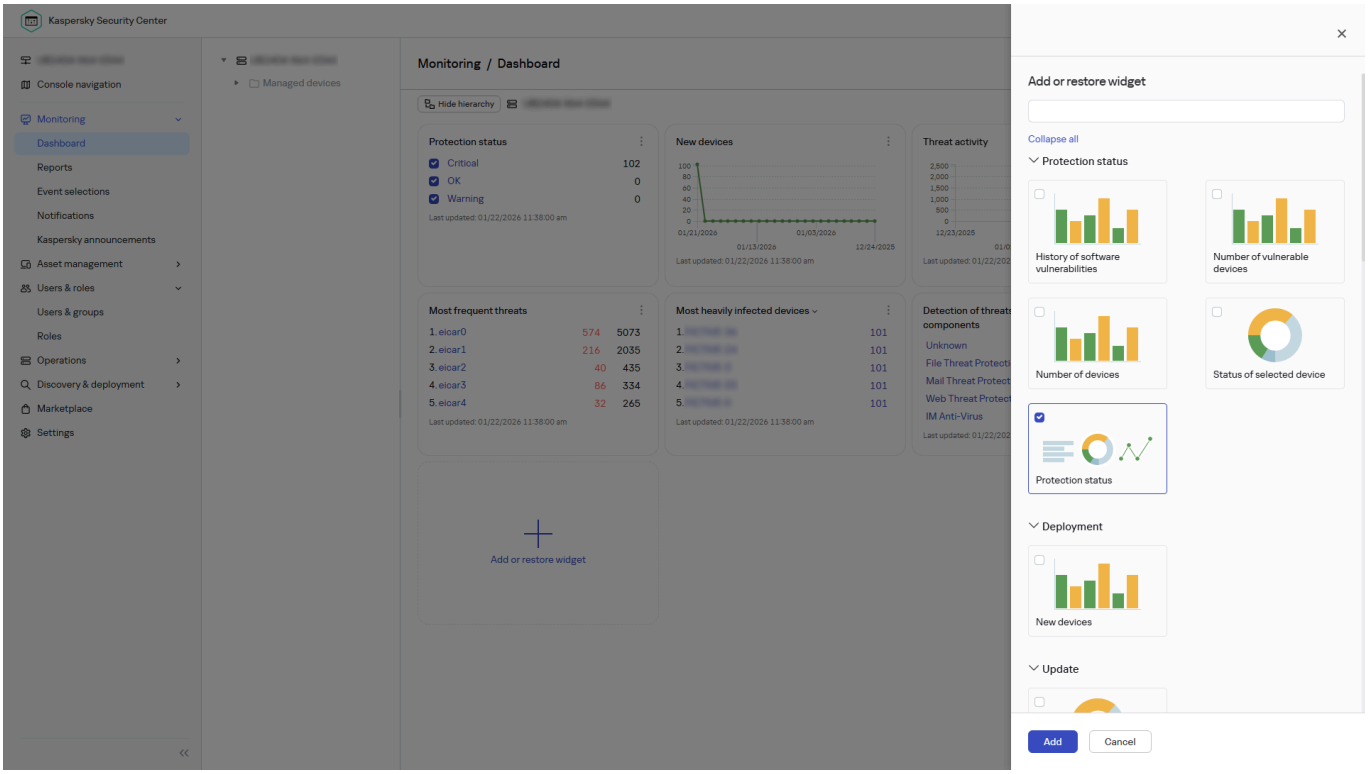
2. 单击“**添加或还原小部件**”按钮。




添加小部件

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 (>)。




选择小部件类型

4. 单击“**添加**”按钮。

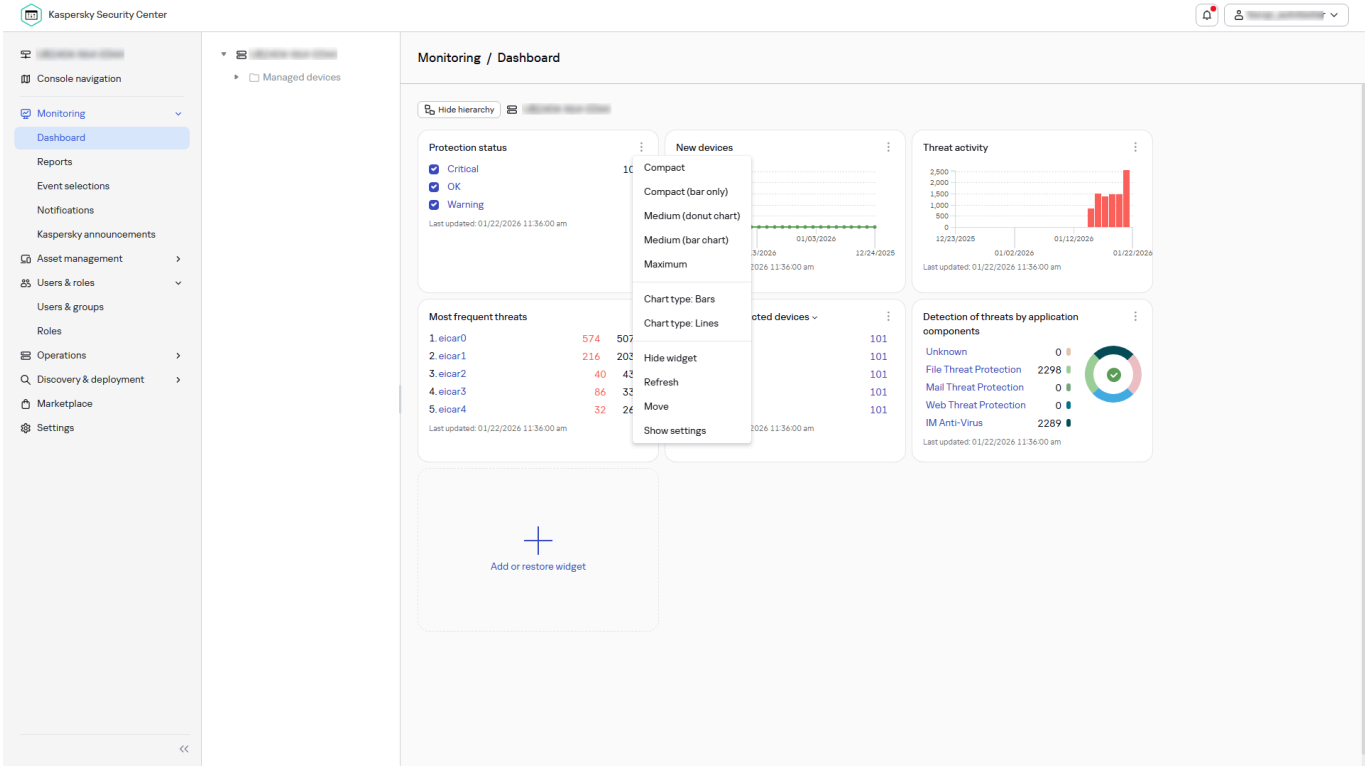
所选的小部件被添加到仪表板结尾。

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**”→“**控制板**”。
2. 点击您要隐藏的小部件旁边的设置图标（⚙）。




小部件菜单

3. 选择**隐藏小部件**。
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**” → “**控制板**”。
2. 单击您要移动的小部件旁边的设置图标（⚙）。
3. 选择**移动**。
4. 单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**” → “**控制板**”。
2. 单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 → 控制板**”。
2. 单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：

- **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。
- **如果指定了以下设置，则设置为"严重"**和**如果指定了以下设置，则设置为"警告"**（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**" → "**控制板**"。
2. 点击您要移动的工具旁边的设置图标（⚙）。
3. 选择**刷新**。

小部件上的数据得到刷新。

# 关于仅仪表板模式

您可以为不管理网络但希望在 Kaspersky Security Center Linux 中查看网络保护统计信息的员工（例如高层管理人员）配置"仅仪表板模式"。当用户启用此模式后，只会向用户显示带有一组预定义小部件的仪表板。因此，用户可以监视小部件中指定的统计信息，例如，所有受管理设备的保护状态、最近检测到的威胁数量或网络中最常见的威胁列表。

当用户在仅仪表板模式下工作时，将应用以下限制：

- 主菜单不向用户显示，因此用户无法更改网络保护设置。
- 用户不能对小部件执行任何操作，例如，添加或隐藏小部件。因此，您需要将用户需要的所有小部件都放在仪表板上并进行配置，例如，设置对象计数规则或指定时间间隔。

您不能为自己分配仅仪表板模式。如果要在此模式下工作，请联系系统管理员、受管理服务提供商 (MSP) 或在"**常规功能：用户权限**"功能区域中拥有"**修改对象 ACL**"权限的用户。

# 配置仅仪表板模式

在开始配置仅仪表板模式之前，确保满足以下先决条件：

- 您在“**常规功能：用户权限**”功能区域中拥有“**修改对象 ACL**”权限。如果您没有此权限，则用于配置模式的选项卡将缺失。
- 您在“**常规功能：基本功能**”功能区域中拥有“**读取**”权限。

如果您的网络中安排了管理服务器层级，若要配置仅仪表板模式，请转到在**用户和角色 → 用户和组** 区域中**用户**选项卡上提供了用户账户的服务器。可以是主服务器或物理从属服务器。无法在虚拟服务器上调整模式。

*要配置仅仪表板模式：*

1. 在主菜单中，转至**用户和角色 → 用户和组**，然后选择**用户**选项卡。
2. 单击要使用小部件调整仪表板的用户账户名。
3. 在打开的账户设置窗口中，选择“**仪表板**”选项卡。

   在打开的选项卡上，您和用户将看到相同的仪表板。
4. 如果启用了“**在仅仪表板模式下显示控制台**”选项，则对切换按钮进行切换以将其禁用。

   启用此选项后，您也无法更改仪表板。禁用该选项后，您可以管理小部件。
5. 配置仪表板外观。“**仪表板**”选项卡上准备的小部件级供具有可自定义账户的用户使用。用户不能更改小部件的任何设置或大小，也不能从仪表板添加或删除任何小部件。因此，请为用户调整好，以便用户可以查看网络保护统计信息。为此，在“**仪表板**”选项卡上，可以对小部件执行与在“**监控**”→“**控制板**”区域中相同的操作：
   - 向仪表板添加新的小部件。
   - 隐藏用户不需要的小部件。
   - 移动小部件到特定文件夹。
   - 更改小部件的大小或外观。
   - 更改小部件设置。
6. 对切换按钮进行切换以启用“**在仅仪表板模式下显示控制台**”选项。

   之后，只有仪表板可供用户使用。用户可以监视统计信息，但不能更改网络保护设置和仪表板外观。由于为您显示的仪表板与为用户显示的仪表板相同，您也无法更改仪表板。

   如果禁用该选项，则会为用户显示主菜单，因此用户可以在 Kaspersky Security Center Linux 中执行各种操作，包括更改安全设置和小部件。
7. 完成配置仅仪表板模式后，单击“**保存**”按钮。只有这样，准备好的仪表板才会显示给用户。
8. 如果用户想要查看支持的卡巴斯基应用程序的统计信息并需要访问权限来执行此操作，请为用户配置权限。之后，卡巴斯基应用程序数据将在这些应用程序的小部件中显示给用户。

现在用户可以在自定义账户下登录 Kaspersky Security Center Linux 并在仅仪表板模式下监视网络保护统计信息。

# 管理和防护报告

本部分介绍如何使用报告、管理自定义报告模板、使用报告模板生成新报告以及创建报告交付任务。

# 使用报告

报告功能允许您获取您组织网络的详细安全数字信息、保存该信息到文件、通过邮件发送它和打印它。

在 Kaspersky Security Center Web Console 的“**监控**”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。

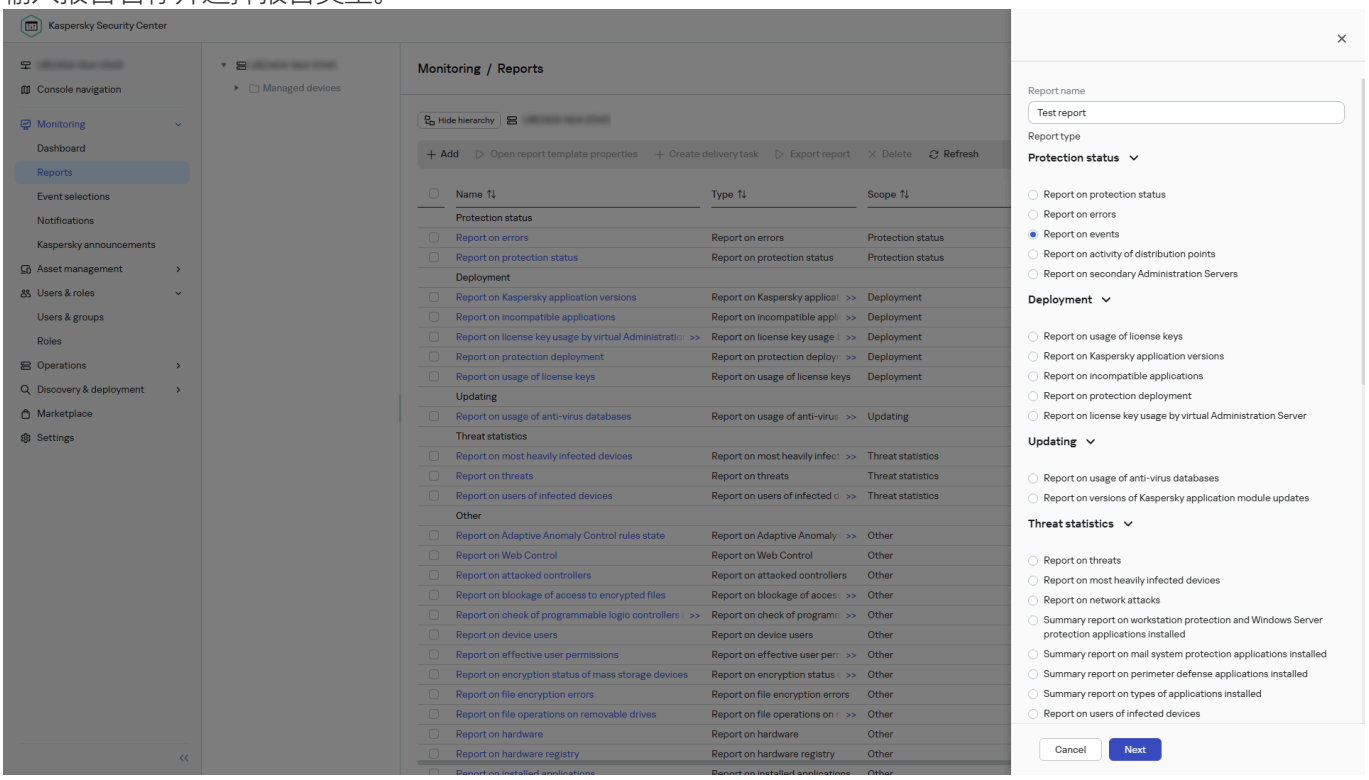
您可以基于现有模板创建报告、导出报告到文件和创建报告传送任务。

# 创建报告模板

*要创建报告模板：*

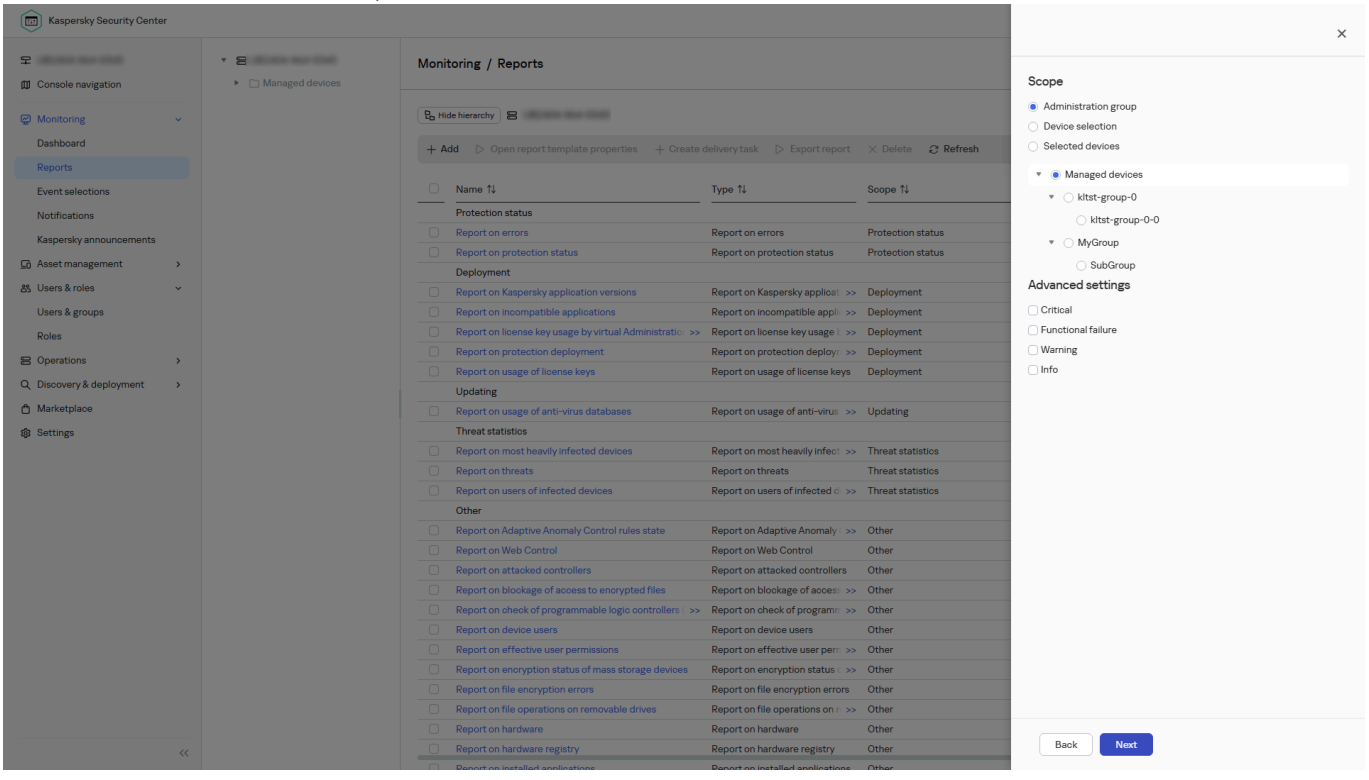
1. 在主菜单中，转到“**监控**”→“**报告**”。
2. 单击**添加**。
   程序将启动“新报告模板向导”。使用“**下一步**”按钮继续向导操作。

3. 输入报告名称并选择报告类型。




指定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）。

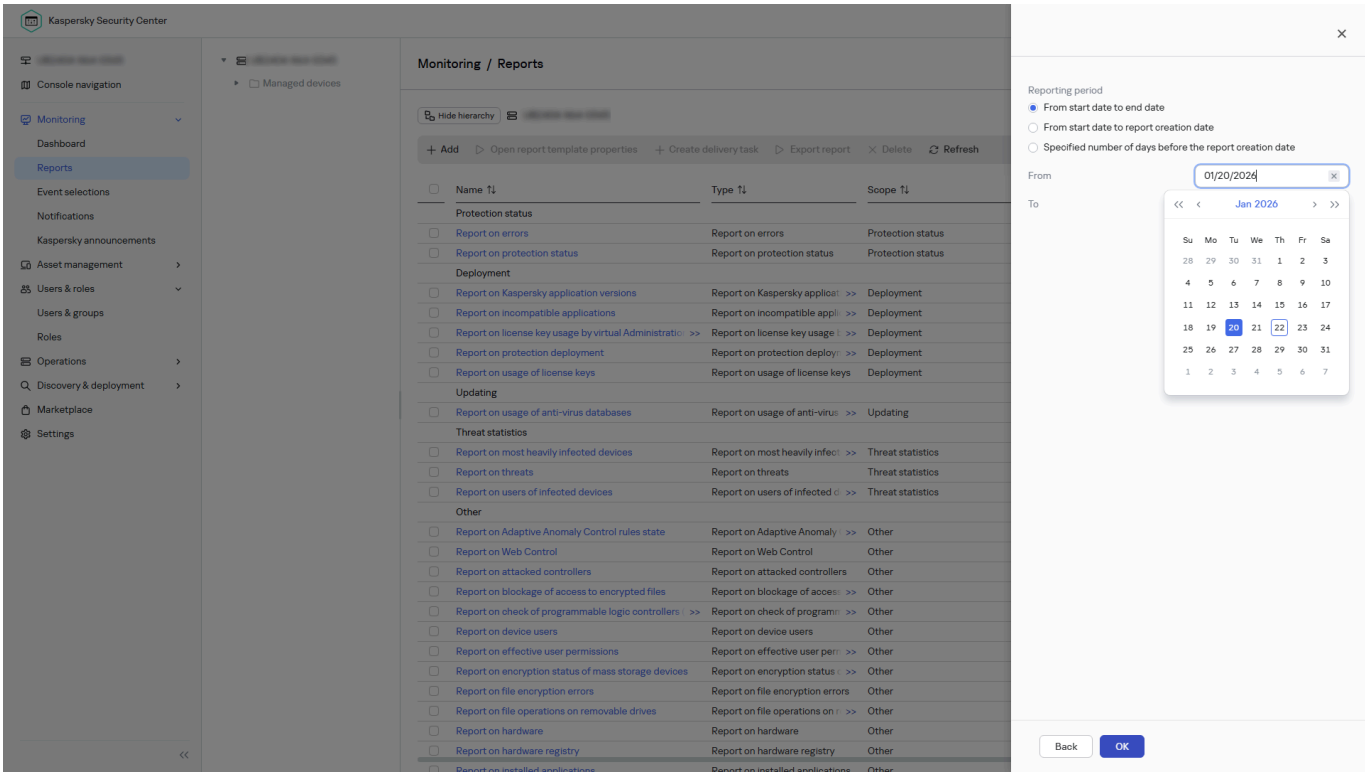



指定报告范围

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。



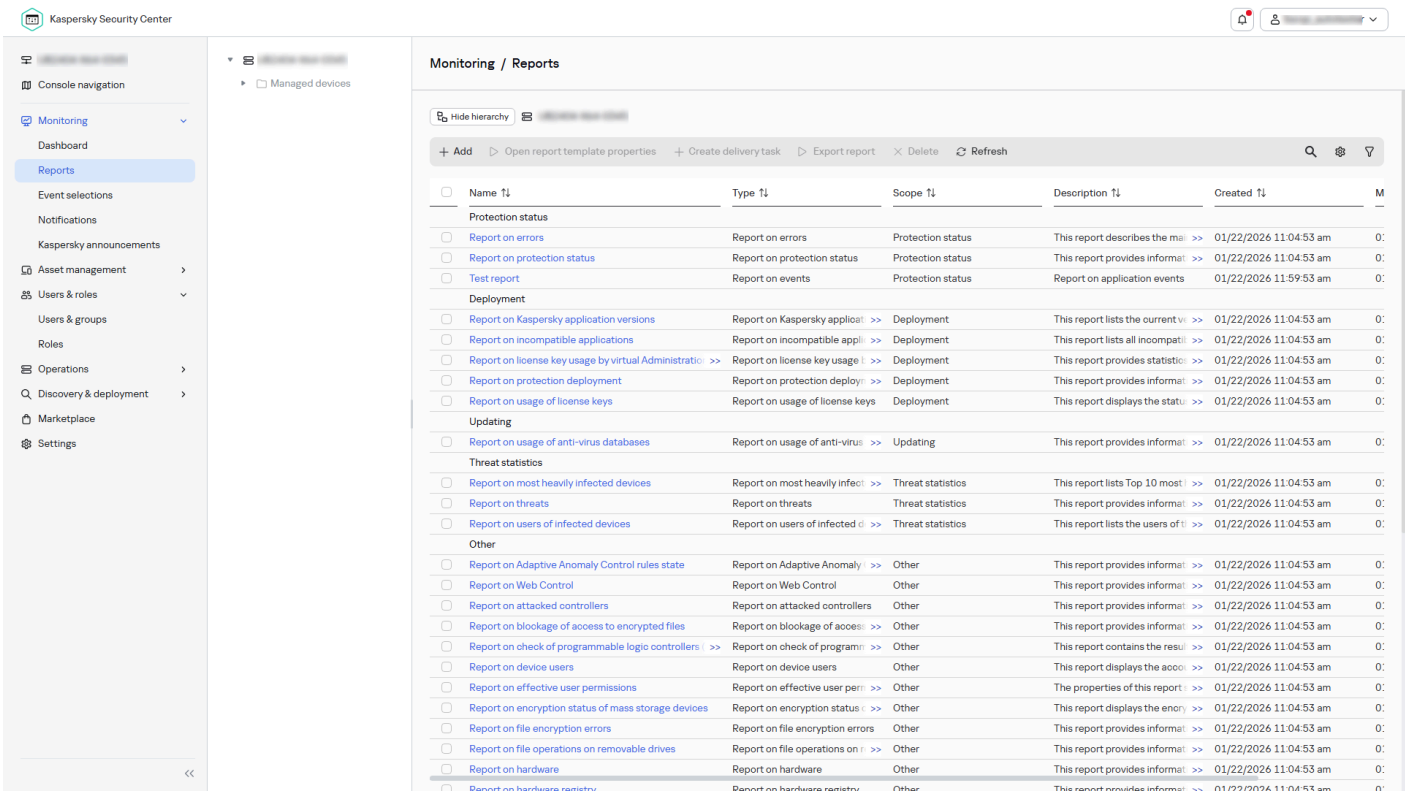

指定报告期间

6. 单击“**确定**”关闭向导。

7. 执行以下操作之一：

- 单击“**保存和运行**”按钮以保存新报告模板并基于其运行报告。
  报告模板被保存。报告被生成。
- 单击“**保存**”按钮保存新报告模板。
  报告模板被保存。

您可以使用新模板来生成和查看报告。




报告列表

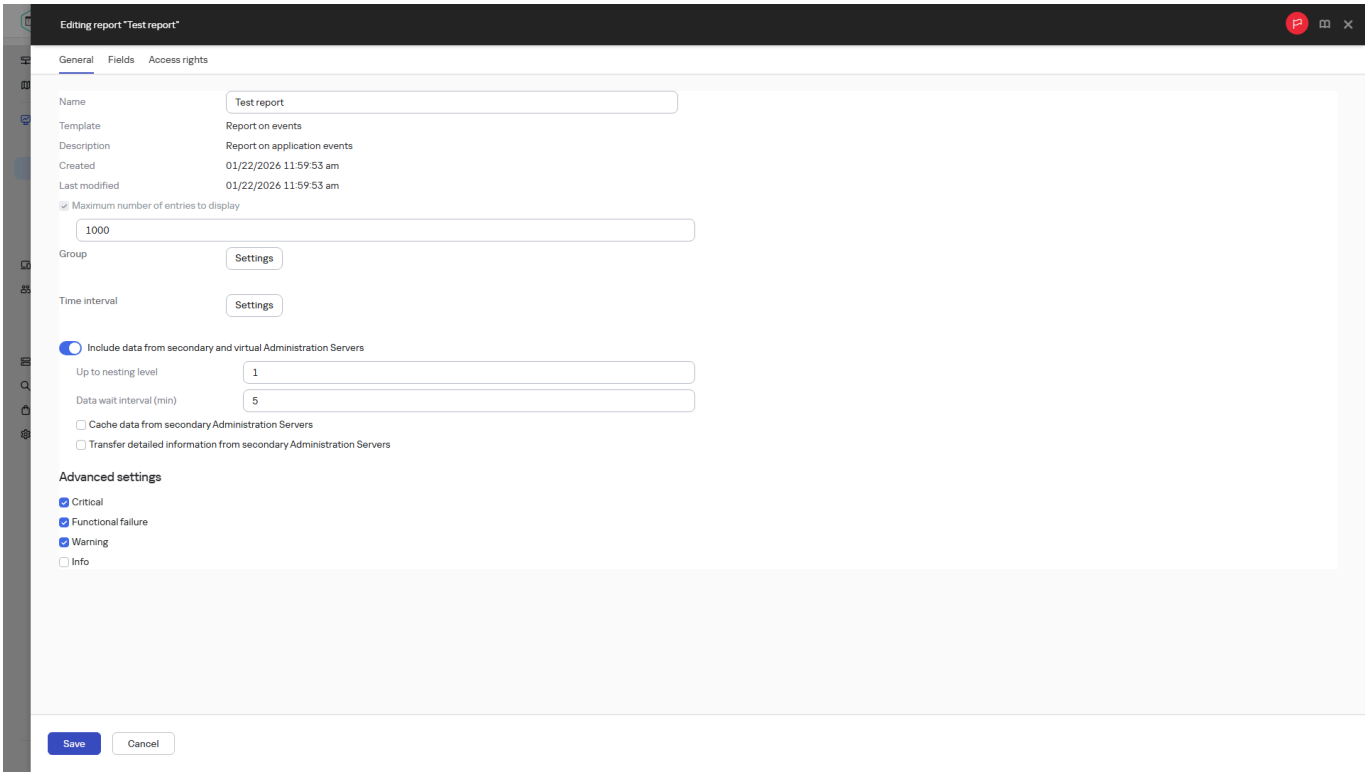
# 查看和编辑报告模板属性

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**” → “**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。




报告模板属性

4. 编辑报告模板属性：

- "**常规**"选项卡：
  - 报告模板名称
  - **显示条目的最大数量**

    如果启用该选项，显示在表格中的带有详细报告数据的条目数量不超过指定值。请注意，此选项不会影响将报告导出到文件时可包含在报告中的最大事件数。

    报告条目首先根据报告模板属性的**字段** → **详细信息字段**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“**详细信息字段**”区域中的条件来定义转换的筛选器，这些条件通过逻辑或运算进行应用。

  将报告转换为支持复杂筛选条件的格式将使该报告与 Kaspersky Security Center 的早期版本（11 及更早版本）不兼容。此外，转换后的报告将不包含运行此类不兼容版本的从属管理服务器的任何数据。

5. 单击“**保存**”保存设置。

6. 关闭**编辑报告<Report name>**窗口。

更新的报告模板显示在报告模板列表。

# 导出报告到文件

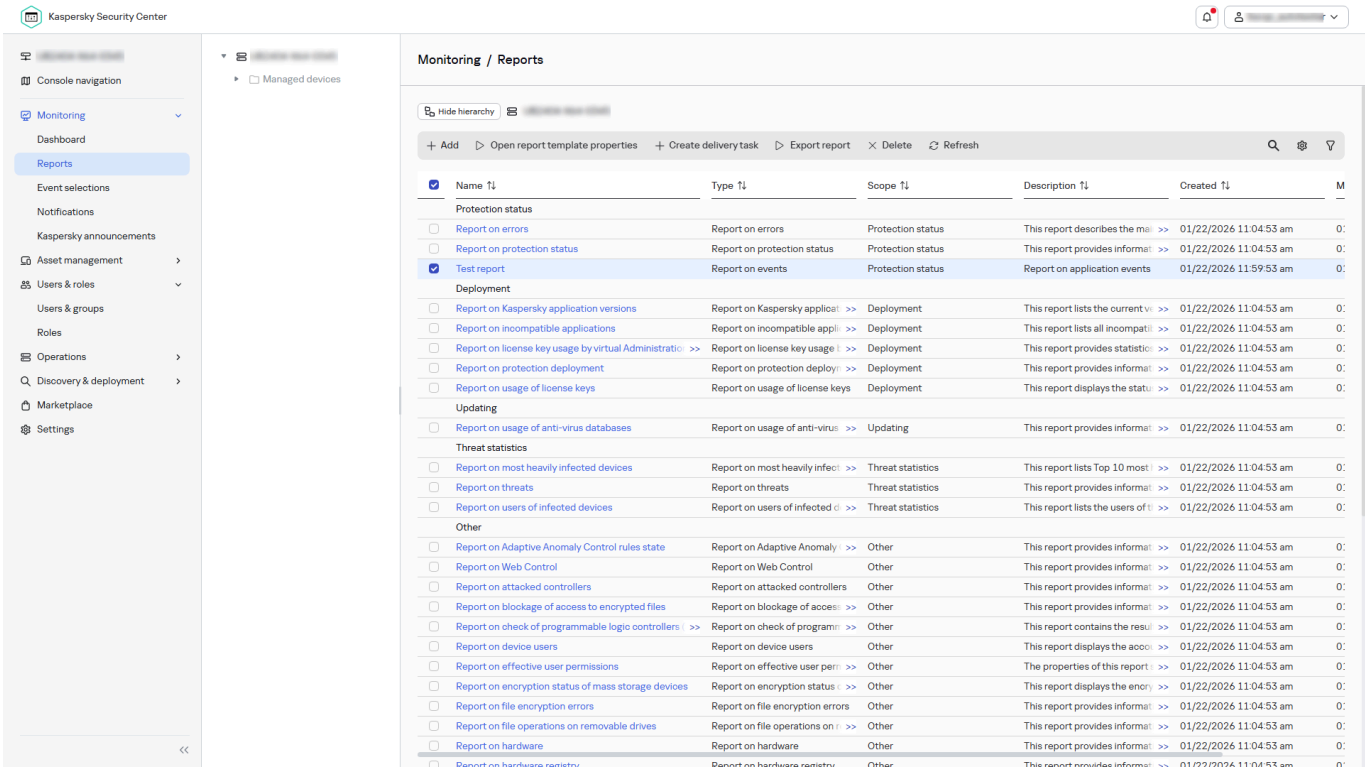
您可以将一份或多份报告保存为 XML、HTML 或 PDF。Kaspersky Security Center Linux 允许您同时将最多 10 个报告导出为指定格式的文件。

*要导出报告到文件：*

1. 在主菜单中，转到“**监控**” → “**报告**”。

2. 选择您要导出的报告。

如果您选择超过 10 个报告，“**导出报告**”按钮将被禁用。




报告列表

3. 单击“**导出报告**”按钮。

4. 在打开的窗口中，指定以下导出参数：

- **文件名**。

  如果您选择导出一份报告，请指定报告文件名。

  如果您选择多个报告，报告文件名将与所选报告模板的名称一致。

- **最大条目数**。

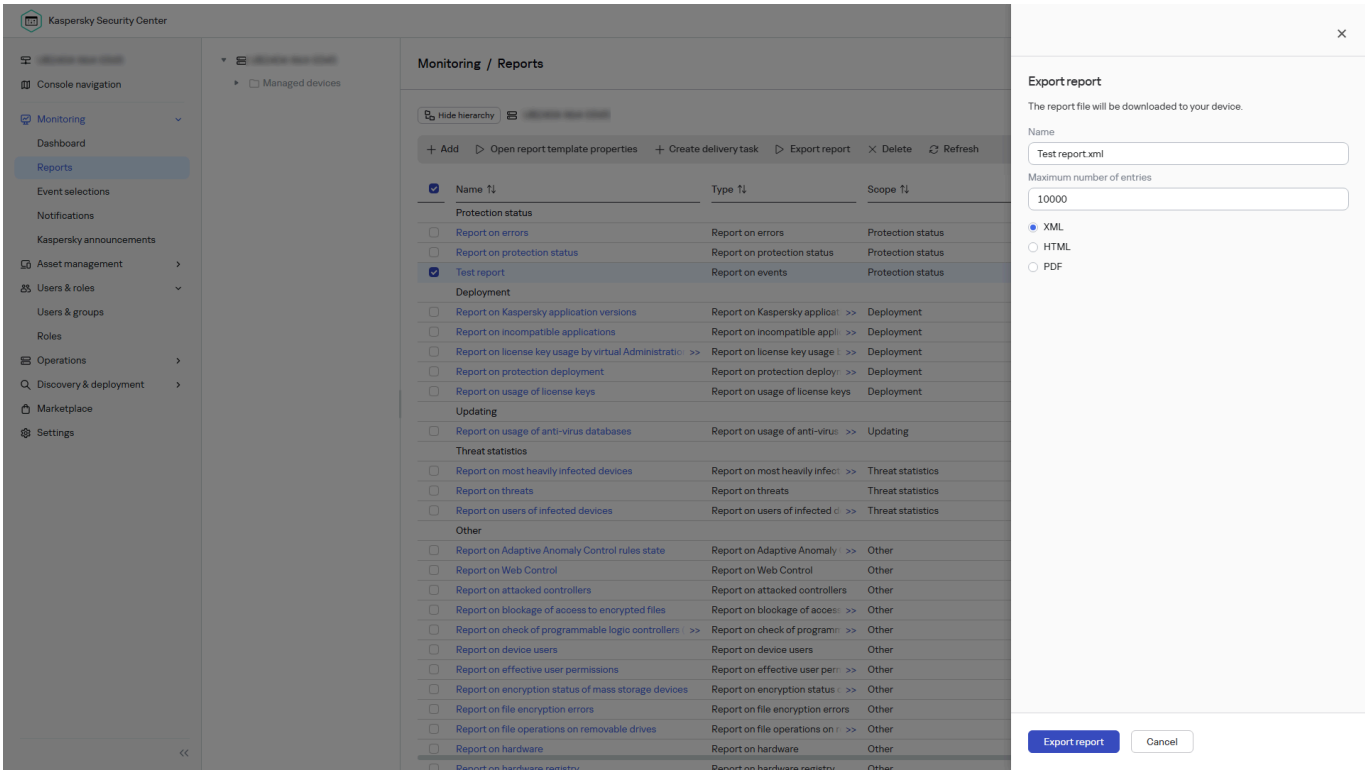
  指定报告文件中包含的最大条目数。默认值是 10,000。

  您可以导出包含无限数量条目的报告。请注意，如果您的报告包含大量条目，则生成和导出报告所需的时间会增加。

- **文件格式**。

  选择报告文件类型：XML、HTML 或 PDF。如果导出多个报告，所有选定的报告都会以指定格式保存为单独文件。

  将报告转换为 PDF 需要 wkhtmltopdf 工具。选择 PDF 选项后，管理服务器会检查设备上是否安装了 wkhtmltopdf 工具。如果未安装该工具，应用程序将显示一条消息，提示必须在管理服务器设备上安装该工具。手动安装该工具，然后继续下一步。




指定报告导出设置

5. 单击“**导出报告**”按钮。

报告以指定格式保存到文件。

# 生成和浏览报告

*要创建和查看报告，请执行以下操作：*

1. 在主菜单中，转到“**监控**” → “**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：

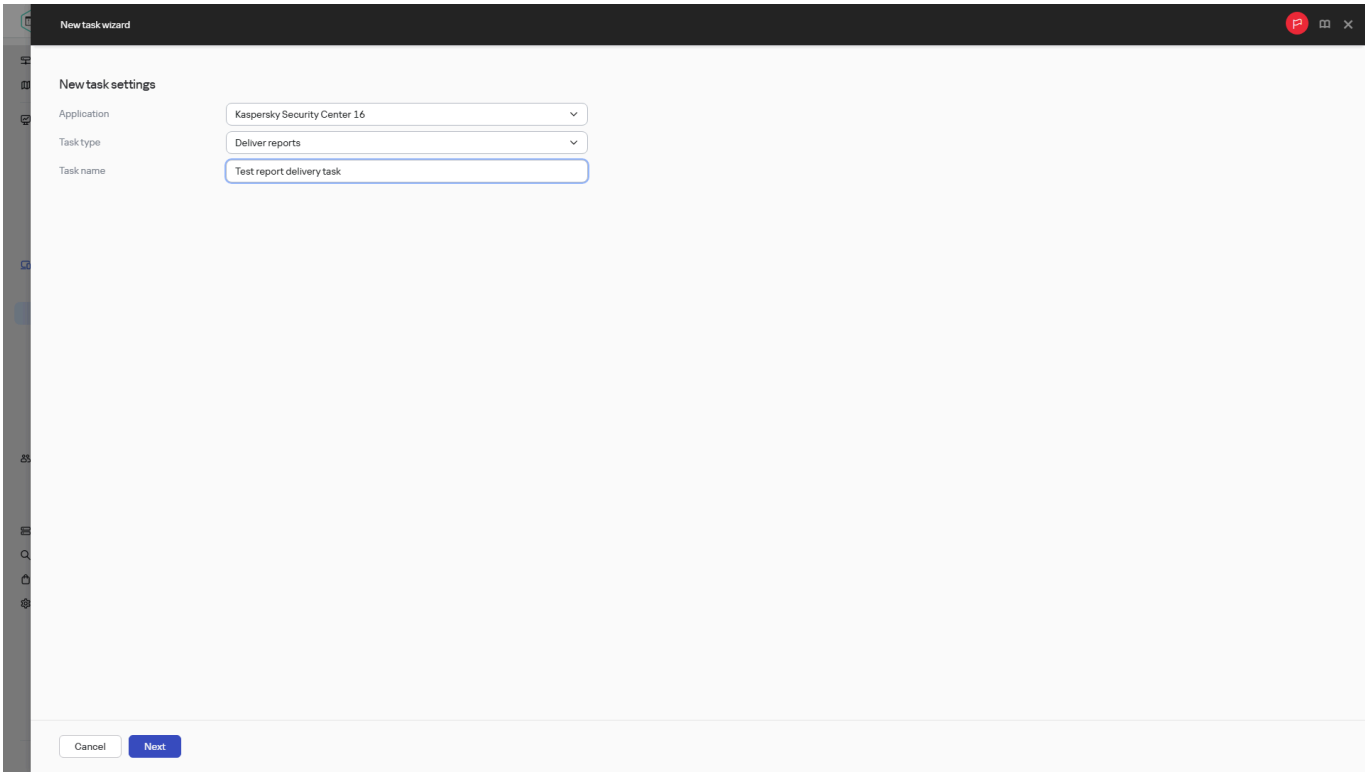
- 在“**概要**”选项卡上：
  - 报告名称和类型、简要描述和报告时间段，以及为哪个设备组生成该报告的相关信息。
  - 图表显示最有代表性的报告数据。
  - 带有计算好的报告指示器的加固表格。
- 在“**详细信息**”选项卡上，显示一个包含详细报告数据的表格。

# 创建报告发送任务

您可以创建传送所选报告的任务。

*要创建报告传送任务：*

1. 在主菜单中，转到“**监控**” → “**报告**”。
2. 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“**创建传送任务**”按钮。
   “新任务向导”启动。使用“**下一步**”按钮继续向导操作。
4. 在向导的“**新任务设置**”步骤中，输入任务名称。
   默认名称为“**传送报告”。**如果已存在同名任务，则添加序列号 (<N>) 到任务名称中。




创建报告发送任务

5. 在向导的“**报告配置**”步骤中，指定以下设置：

   a. 要使用任务传送的报告模板。

   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。

      您最多可以指定 20 个电子邮件地址。要分隔电子邮件地址，请按 **Enter** 键。您还可以粘贴以逗号分隔的电子邮件地址列表，然后按 **Enter** 键。

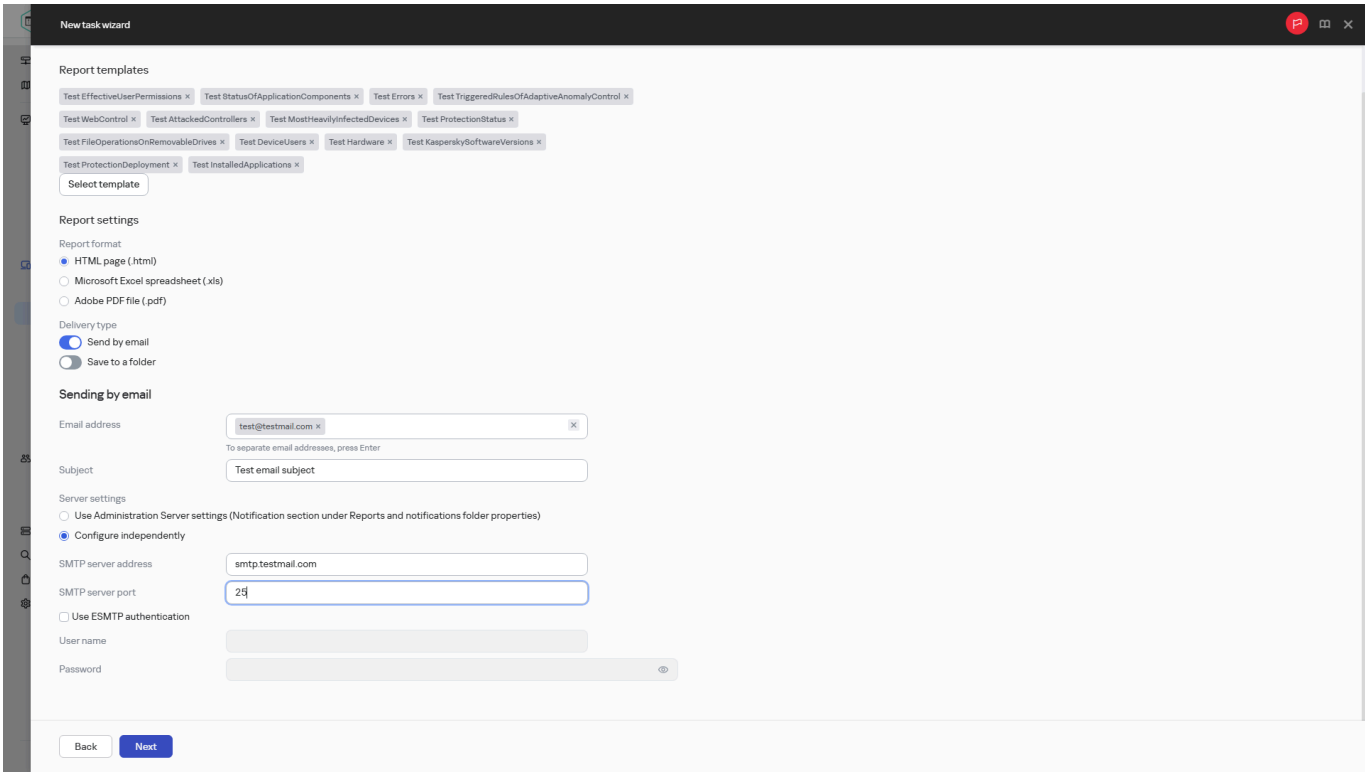
   d. 是否将报告保存到文件夹中，以及相应的设置。

      启用 **保存到文件夹**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。




指定任务设置

6. 在向导的“**配置任务计划**”步骤中，选择任务启动计划。

有以下任务计划选项可用：

- **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 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。

- **在指定的日期**

  任务定期运行，在指定月日的指定时间。

  默认情况下，开始时间为18:00，且未选择任何日期。

  > 请注意，您选择的是当月的星期几，而不是具体的日期，也不是具体的周数（例如，当月的第一周或第二周）。例如，如果您将光标设置在第一行的**周二**单元格中，这意味着任务将在每月的**第一周**星期二运行。

  您可以选择一周中的多个日期。

- **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**

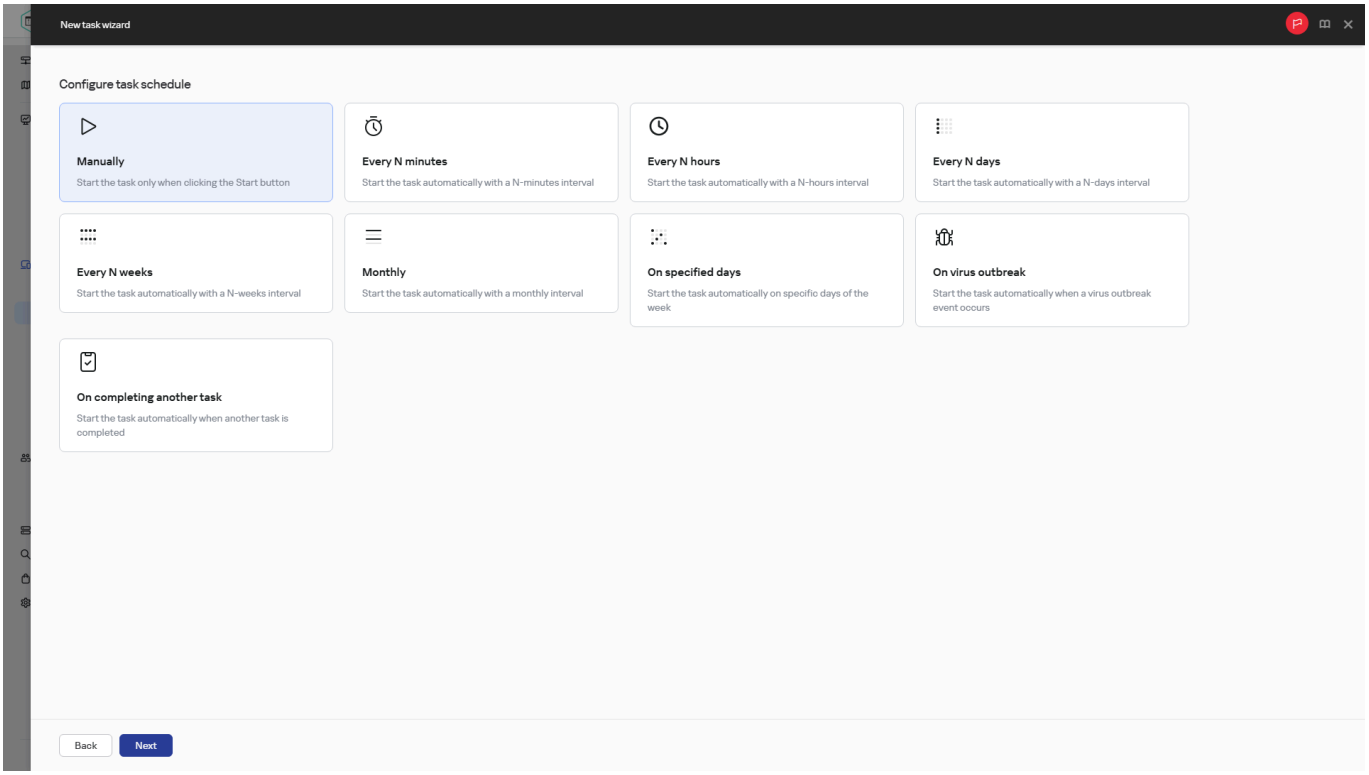
  当前任务在其他任务完成后启动。仅当两个任务被分配给同一设备时，此选项才可用。例如，您可能想使用“***Turn on the device***”选项运行开启设备任务，在它完成后，运行*病毒扫描*任务作为触发任务。

  您必须从表中选择触发任务以及该任务必须完成的状态（**成功完成**或**失败**）。

  如有必要，您可以按如下方式搜索、排序和过滤表中的任务：

  - 在搜索栏中输入任务名称，即可根据名称搜索任务。
  - 单击排序图标可按名称对任务进行排序。

    默认情况下，任务按字母顺序升序排列。
  - 单击过滤器图标，在打开的窗口中按组过滤任务，然后单击**应用**按钮。




选择任务启动计划

7. 在向导的此步骤中，配置其他任务计划设置：

- 在“**任务计划**”部分中，检查或重新配置先前选择的计划并设置时间间隔、月份或星期中的日期，设置病毒爆发条件或完成另一项任务作为启动任务的触发条件。如果选择了适用的计划，还可以在此部分指定开始时间。

- 在“**附加设置**”部分，指定以下设置：

  - **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卡巴斯基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。

  - **使用任务启动自动随机延迟间隔**

    如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

    如果该选项被禁用，任务根据计划在客户端设备上启动。

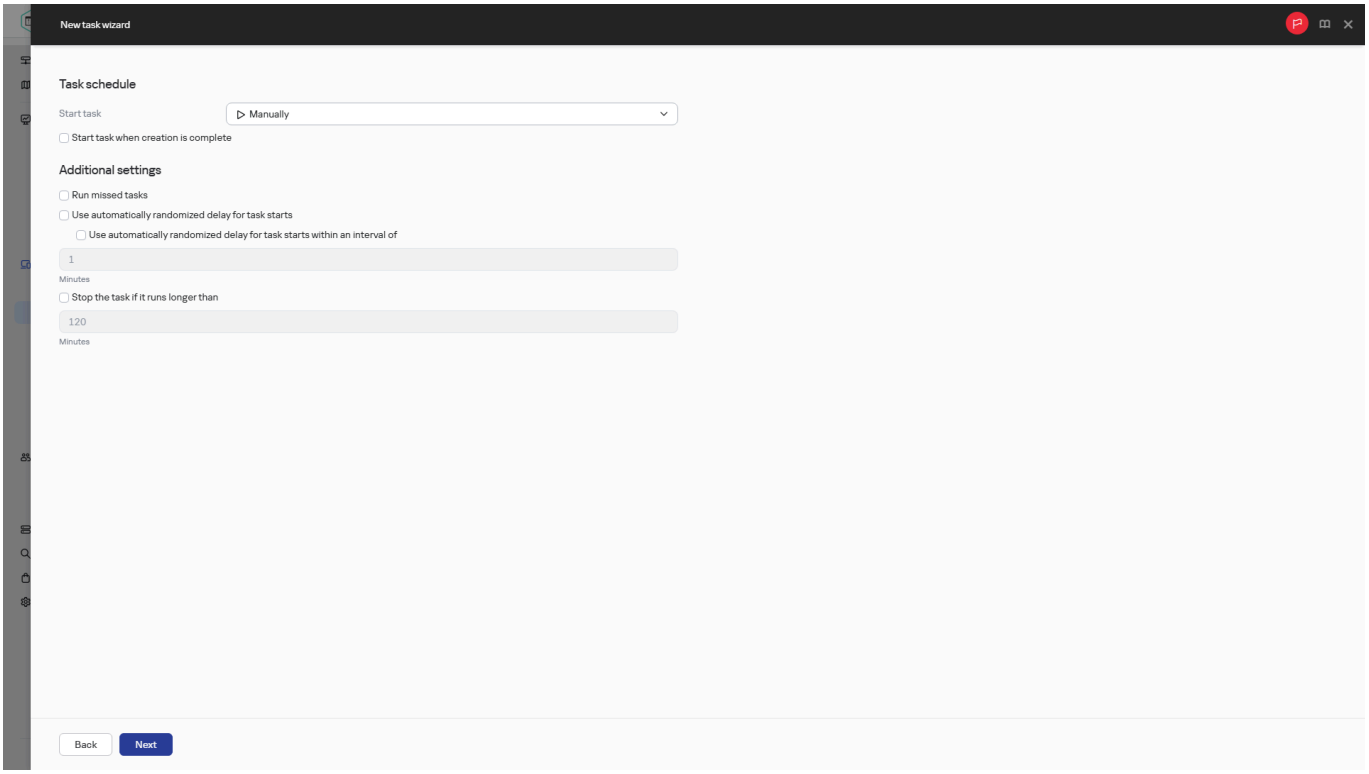
    默认情况下已禁用该选项。默认时间间隔为一分钟。

  - **如果任务运行超过该时间则停止**

    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。

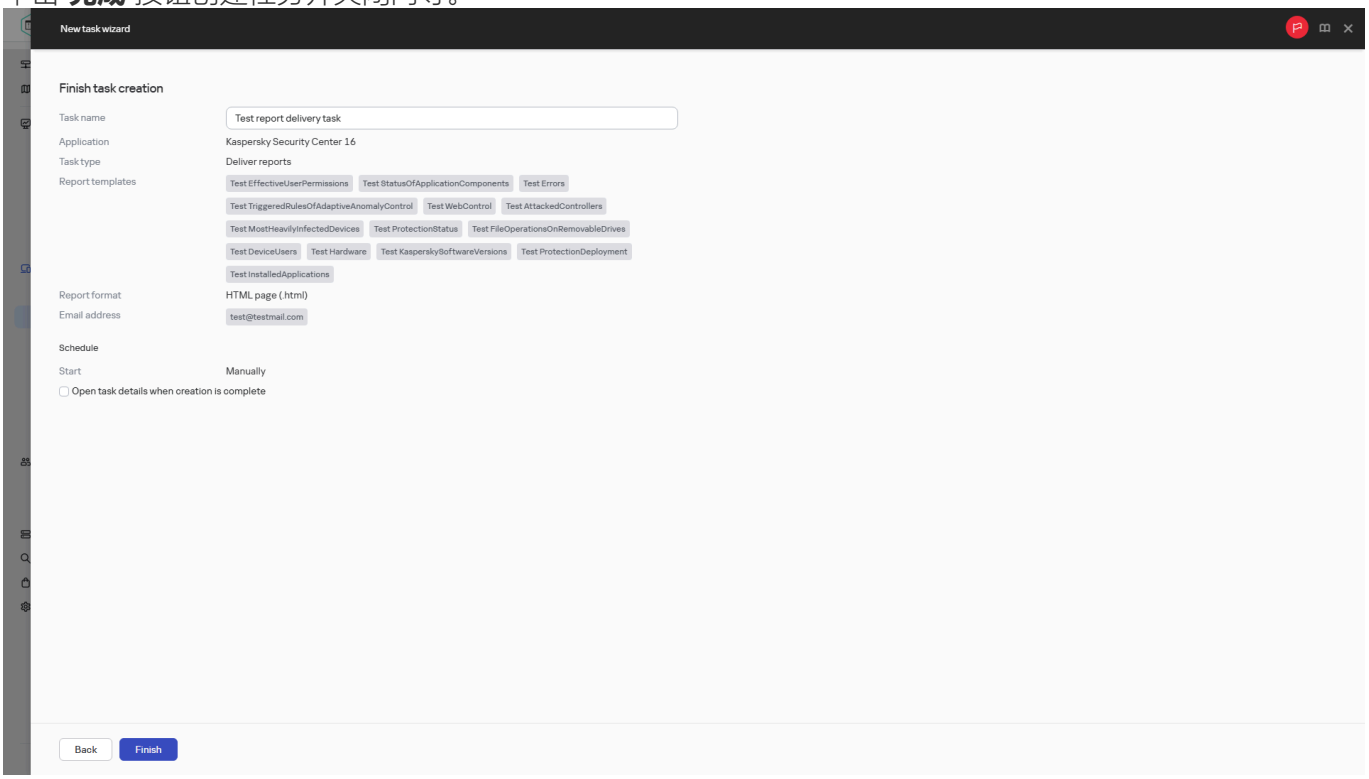



指定任务计划设置

8. 在向导的“**选择账户以运行任务**”步骤中，指定用于运行任务的用户账户的凭据。

9. 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**”步骤中启用“**创建完成时打开任务详情**”选项。

10. 单击“**完成**”按钮创建任务并关闭向导。




完成任务创建

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，任务设置窗口会打开。

# 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**”→“**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。

# 防护等级指示器

防护等级指示器显示有关您的管理服务器和分发点防护情况的最新信息。这使您可以跟踪强化指南的实施情况。该指示器显示在**监控→控制板** 中，无法隐藏或移动到云控制台菜单的其他部分。单击该指示器，您可以转到强化中心，并查看管理服务器和分发点的防护参数状态。要增强基础设施的安全性，您必须解决指示的问题（如果有）。

该指示器可以具有以下状态之一：

- 防护已配置。
- 防护已部分配置。
- 防护未配置。

## 如何查看防护等级的详细信息

总体指示器状态由防护参数的状态决定。

要查看参数，请单击该指示器。

在打开的**强化中心**窗口中，参数按受防护对象分组：管理服务器和分发点。

每个防护参数都会根据您的访问权限显示为以下状态之一：

- ：没有要解决的问题，或者您没有所需的访问权限。
- ⚠ 或 ：有要解决的问题。

以下参数仅针对管理服务器显示：

- 备份已配置
- 管理服务器维护已配置
- TLS加密已启用

以下参数同时针对管理服务器和分发点显示：

- 安全应用程序已安装
- 政策已应用
- 病毒数据库更新已配置

**管理服务器的功能：**

- 所有防护参数仅针对物理管理服务器计算，不适用于虚拟服务器。
  如果您有由多个管理服务器组成的层次结构，则会分别为每个物理服务器计算防护等级指标。
- **已安装的安全应用程序**、**已应用的政策**、**已配置**的**病毒数据库更新**参数是为安装了管理服务器的设备计算的。
- 部署 Kaspersky Security Center Linux 故障转移集群时，将为每个节点计算 **安全应用程序已安装**、**策略已应用**、**反病毒数据库更新已配置** 参数。只有在节点变为活动状态后，才会将其纳入指标状态计算。

### 指标器状态的计算方式

指标器状态按表中所述计算。

| 指标器状态 | 条件 |
| --- | --- |
| 防护已配置。 | 所有防护参数均处于 状态。 |
| 防护已部分配置。 | **已配置的病毒数据库更新** 参数处于 状态，而所有其他参数均处于 状态。 |
| 防护未配置。 | 如果以下防护参数中至少有一个处于 状态。 |

# 安全应用程序已安装

安全应用程序可保护您的设备免受各种类型的威胁，包括网络攻击、钓鱼攻击和诈骗攻击。

如果满足以下任一条件，则该参数显示为 状态：

- 您没有这些设备的访问权限。
- 您在 **常规功能→基本功能** 功能区域中拥有**读取** 权限，同时设备上安装了网络代理程序和安全应用程序。

> 根据您的访问权限可供您访问的所有设备都必须满足该条件，但以下设备除外：已安装不需要任何反病毒保护的应用程序的设备（例如，受保护的操作系统）、未安装网络代理且设备相关信息出现在管理服务器上的时间不到24小时的设备，以及上次连接到管理服务器是在7天或更久以前的离线设备。

如果满足以下至少一个条件，则该参数会以 状态显示。

您必须单击**查看设备**按钮，然后对显示的设备执行表中所述的操作。

| 条件 | 解决方案 |
| --- | --- |
| 设备上未安装网络代理程序 | 安装网络代理。<br>对于管理服务器设备，安装网络代理程序的最简单方法是使用独立安装包。 |
| 该设备包含在**未分配的设备**群组中 | 将该设备移动到"受管理设备"群组或其子群组 |
| 未找到安全应用程序，或者已安装的安全应用程序的实时保护未运行 | 安装安全应用程序。该应用程序会将有关防护状态的数据传输到管理服务器。<br>您可以在设备设置中查看设备的保护状态：**常规部分→设备状态**。<br>在管理服务器设备上，必须安装Kaspersky Endpoint Security for Linux。 |

# 政策已应用

政策是一组应用于 管理群组 及其子群组的安全应用程序设置。

如果满足以下任一条件，则该参数显示为 状态：

- 您没有这些设备的访问权限。
- 您在 **常规功能→基本功能** 功能区域中拥有**读取**权限，同时您的设备上已安装安全应用程序，并且该安全应用程序的活动政策已应用到这些设备。

> 根据您的访问权限可供您访问的所有设备都必须满足该条件，但以下设备除外：已安装不需要任何反病毒保护的应用程序的设备（例如，受保护的操作系统）、未安装网络代理且设备相关信息出现在管理服务器上的时间不到24小时的设备，以及上次连接到管理服务器是在7天或更久以前的离线设备。

如果满足以下至少一个条件，则该参数会以 状态显示。

您必须单击**查看设备**按钮，然后对显示的设备执行表中所述的操作。

| 条件 | 解决方案 |
| --- | --- |
| 设备上未安装安全应用程序。 | 请确保该设备未包含在**安全应用程序已安装**防护参数的选择范围内。 |
| 该设备未应用任何政策。 | 请确保已为该设备所属的管理群组创建政策。<br>如果未创建，请创建并激活该政策。<br>如果已创建，请确保：<br>• 创建的政策处于活动状态。如果未处于活动状态，请激活该政策。<br>• 政策的分发状态为**已成功应用**。<br>如果状态为**已应用但有错误**，则必须在安全应用程序端修复该问题。 |

# 病毒数据库更新已配置

由于病毒数据库可以保护您的设备免受威胁，因此您必须定期及时更新设备上的数据库。

如果满足以下任一条件，则该参数显示为 ✅ 状态：

- 您没有这些设备的访问权限。
- 您在常规功能→基本功能功能区域中拥有读取权限，并且设备上的病毒数据库已更新。

> 根据您的访问权限可供您访问的所有设备都必须满足该条件，但以下设备除外：已安装不需要任何反病毒保护的应用程序的设备（例如，受保护的操作系统）、未安装网络代理且设备相关信息出现在管理服务器上的时间不到24小时的设备，以及上次连接到管理服务器是在7天或更久以前的离线设备。

如果设备上的病毒数据库上次更新时间超过3天，则该参数将显示为 ⚠️ 状态。

如果设备上的病毒数据库上次更新时间超过7天，则该参数将显示为 ❌ 状态。

*要解决这些问题：*

1. 单击该参数旁边的“查看设备”按钮。
2. 对于显示的设备，请执行以下操作：
   a. 确保网络代理程序与管理服务器之间已建立连接。
   如果未建立连接，请参阅以下文章：
   排查Kaspersky Endpoint Security for Linux病毒数据库更新问题
   从Kaspersky Security Center存储库更新反病毒数据库时出现问题
   b. 确保您正在检查其反病毒数据库的卡巴斯基应用程序未停止。
   如果应用程序已停止，请启动它。
   c. 在设备上，查看更新后出现的错误。

# 备份已配置

有关管理服务器数据备份的建议，请参阅管理服务器数据的备份复制和恢复。

如果满足以下任一条件，则该参数显示为 状态：

- 您没有使用管理服务器数据备份任务所需的访问权限。
- 您在**常规功能→在管理服务器上的操作**功能区域中拥有**读取、写入**和**执行**权限，并且已配置备份且会定期执行备份。

如果满足以下至少一个条件，则该参数会以 状态显示。

| 条件 | 解决方案 |
| --- | --- |
| 未创建管理服务器数据备份任务。 | 创建该任务。 |
| 未配置管理服务器数据备份任务所需的计划设置。 | 在管理服务器维护任务中，指定**启动任务**设置，而不是**在检测到病毒爆发时**和**手动**。 |

# 管理服务器维护已配置

管理服务器维护用于释放管理服务器文件夹中的空间，并尽可能减小数据库大小。这有助于加快请求处理速度，并提高系统的整体稳定性。

如果满足以下任一条件，则该参数显示为 状态：

- 您没有操作管理服务器维护任务的访问权限。
- 您在 **常规功能→在管理服务器上的操作** 功能区域中拥有**读取、写入**和**执行** 权限，并且已配置管理服务器维护并定期执行。

> 必须在管理服务器级别设置这些权限。

如果满足以下至少一个条件，则该参数会以 状态显示。

| 条件 | 解决方案 |
| --- | --- |
| 未创建管理服务器维护任务。 | 创建该任务。 |
| 没有为管理服务器维护任务配置必要的计划设置。 | 在管理服务器维护任务中，指定**启动任务**设置，而不是**在检测到病毒爆发时**和**手动**。 |

# TLS加密已启用

您必须确保仅允许使用TLS协议的1.2和1.3版本。允许使用旧版本会导致严重的数据安全风险，并使系统容易受到攻击。

如果仅允许使用TLS协议的1.2和1.3版本，则该参数显示为 状态。

如果允许使用早于1.2的过时TLS版本，则该参数显示为 状态。

要解决此问题，您必须将 SrvUseStrictSslSettings 标志设置为4或5值。

# 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卡巴斯基应用程序中。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。
- 受管理卡巴斯基应用程序特定事件。每个受管理卡巴斯基应用程序都拥有自己的事件集。

### 按来源分组的事件

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。

按重要性级别分组的事件

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。卡巴斯基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 |
|---|---|---|---|---|
| **移动设备的管理服务器证书已过期** | 6129 | KLSRV_EV_SRV_CERT_EXPIRED_DN | 当移动设备和 UEFI 设备的管理服务器证书过期时，会发生此类事件。<br>您需要更新过期的证书。 | 180 天 |
| **审计：导出到 SIEM 失败** | 5130 | KLAUD_EV_SIEM_EXPORT_ERROR | 当由于与 SIEM 系统的连接错误而将事件导出到 SIEM 系统失败时，会发生此类事件。 | 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 |
| **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 Linux 每天检查一次授权许可到期日期是否临近。此类型的事件在授权许可到期之前 30 天、15 天、5 天 和 1 天发布。该天数无法被更改。如果管理服务器在授权许可到期日之前的指定日期被关闭，则事件直到第二天才发布。<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 |
| **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 |

| 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 |
|---|---|---|---|---|
| **受限制功能模式** | 4130 | KLSRV_EV_LICENSE_SRV_LIMITED_MODE | 当 Kaspersky Security Center Linux 开始以基本功能运行，且没有"漏洞和补丁管理"和"移动设备管理"功能时，会发生此类事件。<br>以下是事件发生的原因和正确响应：<br>• 授权许可期限已过期。提供授权许可以使用 Kaspersky Security Center Linux 的完整功能模式（添加有效的激活码或密钥文件到管理服务器）。<br>• 管理服务器管理比授权许可限制更多的设备。从管理服务器的管理组移动设备到其他管理服务器的管理组（如果其他管理服务器的授权许可限制允许）。 | 180 天 |
| **MDM 证书已到期** | 4132 | KLSRV_CERTIFICATE_EXPIRED | 当移动设备上的客户端移动证书过期时，就会发生此类事件。 | 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 |
| **卡巴斯基应用程序模块更新已撤销** | 4142 | KLSRV_SEAMLESS_UPDATE_REVOKED | 如果无缝更新被 Kaspersky 技术专家撤销（这些更新显示"*已撤销*"状态），例如它们必须更新到新版本，则会发生该类型事件。该事件涉及 Kaspersky Security Center Linux 补丁，但不涉及受管理 Kaspersky 应用程序的模块。事件提供无缝更新未被安装的原因。 | 180 天 |
| **病毒爆发** | • 26 (对于文件威胁防护)<br>• 27 (对于邮件威胁防护)<br>• 28 (对于防火墙) | GNRL_EV_VIRUS_OUTBREAK | 当短时间内在若干受管理设备上检测到的恶意对象数量超过阈值时，该类型的事件发生。<br>您可以通过以下方式响应事件：<br>• 您可以在管理服务器属性中配置阈值。<br>• 您还可以创建将被激活的更严格策略，或者创建将在发生此事件时运行的任务。 | |

## 管理服务器功能失败事件

该表显示具有"**功能失败**"重要性级别的 Kaspersky Security Center 管理服务器事件。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。对于管理服务器，您还可以在管理服务器属性中查看和配置事件列表。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

管理服务器功能失败事件

| 事件类型显示名称 | 事件类型 ID | 事件类型 | 描述 | 默认存储期限 |
|---|---|---|---|---|
| **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/或密码是否已更改。<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 |
| **轮询云段失败** | 4143 | KLSRV_KLCLOUD_SCAN_ERROR | 当管理服务器无法在云环境中轮询网段时，将发生此类事件。读取事件描述中的详细信息，并相应做出响应。 | 未存储 |

| 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 |
|---|---|---|---|---|
| **已授权应用程序组之一的安装已超过限制** | 4126 | KLSRV_INVLICPROD_EXCEDED | 管理服务器定期生成该类型的事件（每小时）。如果您在 Kaspersky Security Center Linux 中管理第三方应用程序的授权许可密钥，并且安装数量超过了第三方应用程序授权许可密钥所设置的限制，则会发生该类型事件。<br>您可以通过以下方式响应事件：<br>• 查看受管理设备列表。从未使用第三方应用程序的设备上删除该应用程序。<br>• 为更多设备使用第三方授权许可。<br>您可以使用已授权应用程序组的功能管理第三方应用程序的授权许可密钥。这是一组由满足您所设标准的第三方应用程序组成的授权应用程序群组。 | 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 |
| **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>• 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 策略的设置。<br>在 DBMS 选项处查看信息。 | 180 天 |
| **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 |
| **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 DBMS 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。 | 180 天 |

## 管理服务器警告事件

下表显示了具有“**警告**”重要级别的 Kaspersky Security Center 管理服务器事件。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。对于管理服务器，您还可以在管理服务器属性中查看和配置事件列表。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

| 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 |
|---|---|---|---|---|
| **移动设备的管理服务器证书即将过期** | 6128 | KLSRV_EV_SRV_CERT_EXPIRES_SOON | 当移动设备和 UEFI 设备的管理服务器证书过期时，会发生此类事件。<br>您需要更新过期的证书。 | 90 天 |
| **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 |
| **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 |
| **审计：到 SIEM 服务器的连接测试失败** | 5120 | KLAUD_EV_SIEM_TEST_FAILED | 当 SIEM 服务器的自动连接测试失败时，会发生此类事件。 | 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 |
| **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 |
| **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 |
| **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 |
| **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 |
| **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 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 Web Console 自动将设备自动从组中删除。 | 90 天 |

| 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 |
|---|---|---|---|---|
| **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 |
| **将文件下载到设备失败** | 4165 | KLSRV_FILE_DOWNLOAD_FAILED | 此类事件会在以下情况下发生：<br>• 您尝试将文件下载到企业容器，但企业容器尚未创建。<br>• 设备空间不足。<br>• 从服务器下载文件信息失败。<br>• 文件内容无法从服务器下载。<br>• 无法在设备上创建该文件夹。<br>• 个人设备上缺少文件访问权限。<br>• 企业容器中缺少文件访问权限。 | 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。<br>如果您自己找不到问题的解决方案，建议与 Kaspersky 技术支持联系。 | 90 天 |
| **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 |
| **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 |
| **硬盘几乎已满** | 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 |
| **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 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）。<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 |

| 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** | 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 |
| **已授权应用程序组之一的安装即将达到限制** | 4128 | KLSRV_INVLICPROD_EXPIRED_SOON | 当已授权应用程序组中包含的第三方应用程序的授权许可密钥之一即将过期时，就会发生此类事件。这样一来，其中某一组的安装限额将被调低。<br>您可以通过以下方式响应事件：<br>• 如果某些受管理设备上未使用第三方应用程序，请从这些设备中删除该应用程序。<br>• 如果您预计第三方应用程序安装数量将在不久的将来超过允许的最大值，请考虑预先获取更多设备的第三方授权许可。<br>您可以使用已授权应用程序组的功能管理第三方应用程序的授权许可密钥。 | 90 天 |
| **已注册卡巴斯基应用程序模块的新更新** | 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 |
| **管理服务器数据库空间不足** | 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>• 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 |
| **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

下表显示了具有“**信息**”重要级别的 Kaspersky Security Center 管理服务器事件。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。对于管理服务器，您还可以在管理服务器属性中查看和配置事件列表。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

| 事件类型显示名称 | 事件类型 ID | 事件类型 | 描述 | 默认存储期限 |
|---|---|---|---|---|
| **移动设备的管理服务器证书正在更新中** | 6127 | KLSRV_EV_SRV_CERT_RENEWED | 当管理服务器证书已续费时会发生该事件。 | 30 天 |
| **审计：命令已发送到设备** | 4170 | KLAUD_EV_COMMAND_SENT | 当用户向移动设备发送命令时，会发生此类事件。 | 30 天 |
| **审计：到管理服务器的连接已终止** | 4151 | KLAUD_EV_SERVERDISCONNECT | | 30 天 |
| **审计：到管理服务器的连接已建立** | 4147 | KLAUD_EV_SERVERCONNECT | 当用户使用 Kaspersky Security Center Web Console 连接到管理服务器时，此类事件会发生。这些事件包括安装 Kaspersky Security Center Web Console 服务器的设备的 IP 地址。 | 30 天 |
| **审计：加密密钥已导入/导出** | 5100 | KLAUD_EV_DPEKEYSEXPORT | 例如，在迁移期间发生此类事件。 | 30 天 |
| **审计：组设置已修改** | 4149 | KLAUD_EV_ADMGROUP_CHANGED | 当安全组已被编辑时，会发生此类事件。 | 30 天 |
| **审计：对象已修改** | 4148 | KLAUD_EV_OBJECTMODIFY | 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>• 包<br>• 任务<br>• 策略<br>• 服务器<br>• 虚拟服务器 | 30 天 |
| **审计：对象属性已被修改** | 4152 | KLAUD_EV_OBJECTPROPMODIFIED | 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 | 30 天 |
| **审计：对象状态已更改** | 4150 | KLAUD_EV_TASK_STATE_CHANGED | 例如，当任务以错误失败时会发生该事件。 | 30 天 |
| **审计：到 SIEM 服务器的连接测试成功** | 5110 | KLAUD_EV_SIEM_TEST_SUCCESS | 当 SIEM 服务器的测试连接成功时，会发生此事件。 | 30 天 |
| **审计：用户权限已被修改** | 4153 | KLAUD_EV_OBJECTACLMODIFIED | 该事件在用户权限被修改了时发生。 | 30 天 |
| **到主管理服务器的连接已建立** | 4117 | KLSRV_EV_MASTER_SRV_CONNECTED | | 30 天 |
| **到从属管理服务器的连接已建立** | 4115 | KLSRV_EV_SLAVE_SRV_CONNECTED | 有关详细信息，请参阅下文：创建管理服务器层级：添加从属管理服务器。 | 30 天 |
| **数据库已更新** | 4144 | KLSRV_UPD_BASES_UPDATED | 当"**将更新下载至管理服务器存储库**"任务完成数据库更新时，会发生此类事件。 | 30 天 |
| **设备已被自动添加到组** | 4101 | KLSRV_EVENT_HOSTS_NEW_REDIRECTED | 当设备根据设备移动规则被分配到某个组时，会发生此类事件。 | 30 天 |
| **设备已被根据规则自动移动** | 1074 | KLSRV_HOST_MOVED_WITH_RULE_EX | 当设备根据设备移动规则被移动到某个管理组时，会发生此类事件。 | 30 天 |

| 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 |
|---|---|---|---|---|
| **设备已从组中删除：长时间在网络中不活动** | 4104 | KLSRV_INVISIBLE_HOSTS_REMOVED | 当设备因处于非活动状态而被自动从组中删除时，会发生此类事件。 | 30 天 |
| **此移动设备上的 FCM 实例 ID 已被更改** | 4137 | KLSRV_GCM_DEVICE_REGID_CHANGED | 当设备上的 Firebase Cloud Messaging 令牌发生变化时，会发生此类事件。<br>有关 FCM 令牌轮换的信息，请参阅 Firebase 服务文档。 | 30 天 |
| **文件已从管理服务器删除** | 4163 | KLSRV_FILE_REMOVED | 当文件已被从管理服务器删除时，该事件会发生。 | 30 天 |
| **文件已下载到设备** | 4164 | KLSRV_FILE_DOWNLOADED | 该事件在以下情况下发生：<br>• 文件已在会话中下载到设备。<br>• 文件已从管理服务器下载。 | 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 |
| **文件已上传到管理服务器** | 4162 | KLSRV_FILE_UPLOADED | 当文件已被上传到管理服务器时，该事件会发生。 | 30 天 |
| **已授权应用程序组之一的安装即将超过限制(已经使用 90% 以上)** | 4127 | KLSRV_INVLICPROD_FILLED | 当已授权应用程序组中包含的第三方应用程序安装数量达到授权许可密钥属性中指定的最大允许值的 90% 时，将发生此类事件。<br>您可以通过以下方式响应事件：<br>• 如果某些受管理设备上未使用第三方应用程序，请从这些设备中删除该应用程序。<br>• 如果您预计第三方应用程序安装数量将在不久的将来超过允许的最大值，请考虑预先获取更多设备的第三方授权许可。<br>您可以使用已授权应用程序组的功能管理第三方应用程序的授权许可密钥。 | 30 天 |
| **已检测到新设备** | 4100 | KLSRV_EVENT_HOSTS_NEW_DETECTED | 当发现新的联网设备时，就会发生此类事件。 | 30 天 |
| **授权许可密钥的 90% 已经使用** | 4097 | KLSRV_EV_LICENSE_CHECK_90 | 当管理服务器检测到安装在客户端设备上的 Kaspersky 应用程序快超过授权许可限制，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构成该授权许可覆盖的单元总数的 90%，则该类型的事件发生。<br>即使超出许可限制，客户端设备仍受到保护。<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。 | 30 天 |
| **移动设备的备用管理服务器证书已创建** | 6126 | KLSRV_EV_SRV_CERT_RESERVE_CREATED | 当管理服务器证书已创建时会发生该事件。 | 30 天 |
| **更新已被成功复制到指定文件夹** | 4122 | KLSRV_UPD_REPL_OK | 当“**将更新下载至管理服务器存储库**”任务完成将文件复制到指定文件夹时，会发生此类事件。 | 30 天 |

“**备用证书已创建**”和“**证书续费**”这两类事件，仅当对移动设备和 UEFI 设备的管理服务器证书执行相应操作时，才会由管理服务器自动发布，并显示在管理控制台中。

# 网络代理事件

该部分包含管网络代理相关事件信息。

## 网络代理功能失败事件

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

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

网络代理功能失败事件

| 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 |
|---|---|---|---|---|
| **安装根证书失败** | 7728 | KLNAG_EV_ROOT_CERT_INSTALL_ERR | 事件包含证书安装错误的描述。 | 30 天 |
| **安装第三方软件更新失败** | 7697 | KLNAG_EV_3P_PATCH_INSTALL_ERROR | 如果正在使用“漏洞和补丁管理”功能且未成功更新第三方软件，会发生此类事件。<br>检查到第三方软件的链接是否合法。阅读事件描述。 | 30 天 |
| **安装 Windows Update 更新失败** | 7717 | KLNAG_EV_WUA_INSTALL_ERROR | 如果 Windows 更新未成功，则该类型的事件发生。<br>阅读事件描述。在 Microsoft 知识库中查找错误。如果您无法自己解决问题，请联系 Microsoft 技术支持。 | 30 天 |
| **移除根证书失败** | 7730 | KLNAG_EV_ROOT_CERT_REMOVE_ERR | 事件包含证书删除错误的描述。 | 30 天 |
| **将 sudoers 文件恢复为参考值失败** | 7726 | KLNAG_EV_SUDOER_RESTORED_ERR | 事件包含 sudoers 文件替换错误的描述。 | 30 天 |
| **更新安装错误** | 7702 | KLNAG_EV_PATCH_INSTALL_ERROR | 如果 Kaspersky Security Center Linux 组件自动更新和补丁未成功，会发生此类事件。事件不包含受管理 Kaspersky 应用程序的更新。<br>阅读事件描述。管理服务器上的 Windows 问题可能是该事件的原因。如果描述提到 Windows 配置的任何问题，解决该问题。 | 30 天 |
| **用户管理：错误** | 7723 | KLNAG_EV_USR_MNG_ERR | 一般警告事件。 | 30 天 |

## 网络代理警告事件

下表显示具有“**警告**”严重级别的网络代理事件。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

网络代理警告事件

| 事件类型显示名称 | 事件类型 ID | 事件类型 | 描述 | 默认存储期限 |
|---|---|---|---|---|
| **KSN 代理已启动。检查 KSN 可用性失败** | 7718 | KSNPROXY_STARTED_CON_CHK_FAILED | 当所配置的 KSN 代理连接的测试连接失败时，会发生此类事件。 | 30 天 |
| **发生了安全问题** | 549 | GNRL_EV_APP_INCIDENT_OCCURED | 在设备上发现事故时，就会发生此类事件。例如，当设备磁盘空间不足时会发生此类事件。 | 30 天 |
| **发现 sudoers 文件与参考值不匹配** | 7724 | KLNAG_EV_SUDOER_DIFFERENT | 当 sudoers 文件和参考文件不匹配时，就会发生此类事件。 | 30 天 |
| **第三方软件更新安装已延时** | 7698 | KLNAG_EV_3P_PATCH_INSTALL_SLIPPED | 例如，当第三方更新安装的 EULA 被拒绝时，会发生此类事件。 | 30 天 |
| **第三方软件更新安装已完成但存在警告** | 7696 | KLNAG_EV_3P_PATCH_INSTALL_WARNING | 下载跟踪文件并查看 KLRI_PATCH_RES_DESC 字段值以了解详细信息。 | 30 天 |

| 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 |
|---|---|---|---|---|
| **用户管理：警告** | 7722 | KLNAG_EV_USR_MNG_WRN | 一般警告事件。 | 30 天 |
| **在安装软件模块更新期间返回了警告** | 7701 | KLNAG_EV_PATCH_INSTALL_WARNING | 下载跟踪文件并查看 KLRI_PATCH_RES_DESC 字段值以了解详细信息。 | 30 天 |

## 网络代理信息事件

下表显示具有“**信息**”严重级别的网络代理事件。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

网络代理信息事件

| 事件类型显示名称 | 事件类型 ID | 事件类型 | 默认存储期限 |
|---|---|---|---|
| **应用程序已安装** | 7703 | KLNAG_EV_INV_APP_INSTALLED | 30 天 |
| **应用程序已卸载** | 7704 | KLNAG_EV_INV_APP_UNINSTALLED | 30 天 |
| **已收到 Web 服务器 HTTPS 端口的证书** | — | WEB_SERVER_CERTIFICATE_RENEWED | 30 天 |
| **设备已被授权** | 7711 | KLNAG_EV_NAC_HOST_AUTHORIZED | 30 天 |
| **已检测到新设备** | 7710 | KLNAG_EV_NAC_DEVICE_DISCOVERED | 30 天 |
| **设备已被删除** | 7709 | KLNAG_EV_DEVICE_REMOVE | 30 天 |
| **软件模块更新安装已启动** | 7700 | KLNAG_EV_PATCH_INSTALL_STARTING | 30 天 |
| **KSN 代理已启动。KSN 可用性检查已成功完成** | 7719 | KSNPROXY_STARTED_CON_CHK_OK | 30 天 |
| **KSN 代理已停止** | 7720 | KSNPROXY_STOPPED | 30 天 |
| **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 |
| **根证书已安装** | 7727 | KLNAG_EV_ROOT_CERT_INSTALLED | 30 天 |
| **根证书已删除** | 7729 | KLNAG_EV_ROOT_CERT_REMOVED | 30 天 |
| **Sudoers 文件成功恢复为参考值** | 7725 | KLNAG_EV_SUDOER_RESTORED | 30 天 |
| **已安装第三方应用程序** | 7707 | KLNAG_EV_INV_CMPTR_APP_INSTALLED | 30 天 |
| **第三方软件更新已成功安装** | 7694 | KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY | 30 天 |
| **第三方软件更新安装已开始** | 7695 | KLNAG_EV_3P_PATCH_INSTALL_STARTING | 30 天 |
| **软件模块更新已成功安装** | 7699 | KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY | 30 天 |
| **用户管理：信息** | 7721 | KLNAG_EV_USR_MNG_INF | 30 天 |
| **已在主机上启动 Web 服务器** | — | WEB_SERVER_STARTED | 30 天 |
| **已在主机上停止 Web 服务器** | — | WEB_SERVER_STOPPED | 30 天 |
| **Windows 桌面共享：应用程序已启动** | 7714 | KLUSRLOG_EV_PROCESS_LAUNCHED | 30 天 |
| **Windows 桌面共享：文件已修改** | 7713 | KLUSRLOG_EV_FILE_MODIFIED | 30 天 |
| **Windows 桌面共享：文件已读取** | 7712 | KLUSRLOG_EV_FILE_READ | 30 天 |
| **Windows 桌面共享：已启动** | 7715 | KLUSRLOG_EV_WDS_BEGIN | 30 天 |
| **Windows 桌面共享：已停止** | 7716 | KLUSRLOG_EV_WDS_END | 30 天 |

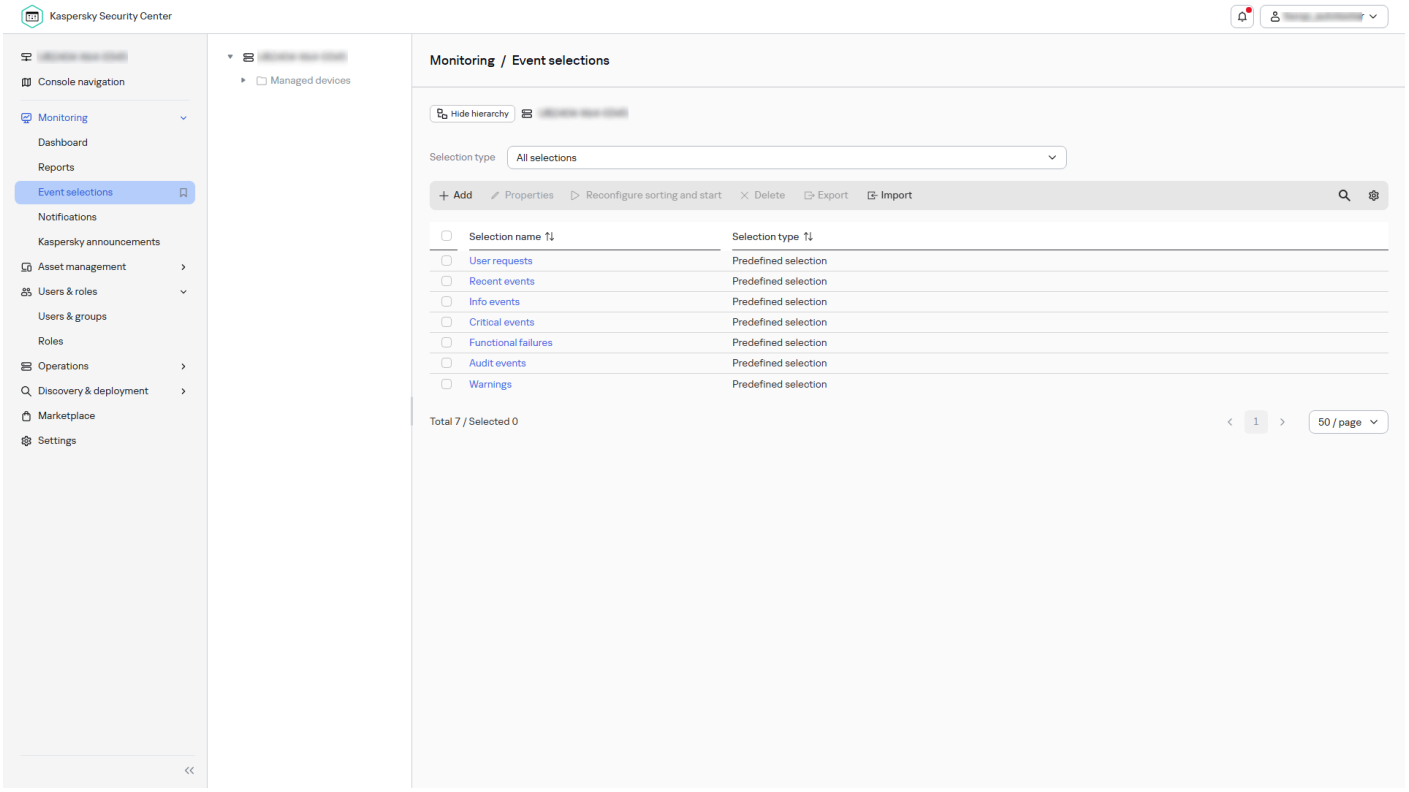
# 使用事件分类

事件分类提供了从管理服务器数据库中选择的指定事件集合的屏幕视图。这些事件集根据以下类别进行分组：

- 按重要级别—**严重事件**、**功能失败**、**警告**和**信息事件**
- 按时间—**最近事件**
- 按类型—**用户请求**和**审计事件**

您可以基于 Kaspersky Security Center Web Console 界面上可以配置的设置创建和查看用户定义的事件分类。

在 Kaspersky Security Center Web Console 的“**监控**”区域中单击“**事件分类**”可使用事件分类。




事件分类列表

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**
  - **信息事件**
- **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。

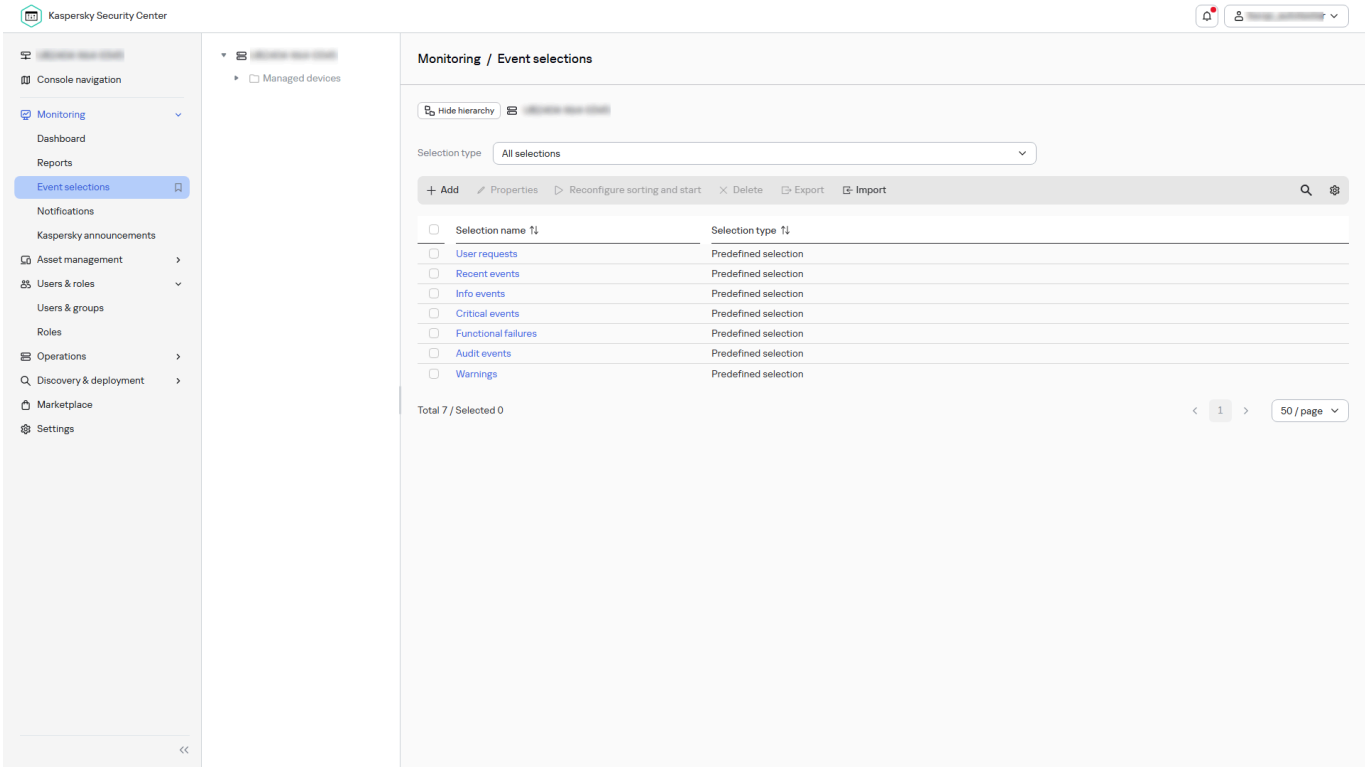
您可以执行以下操作：

- 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：*

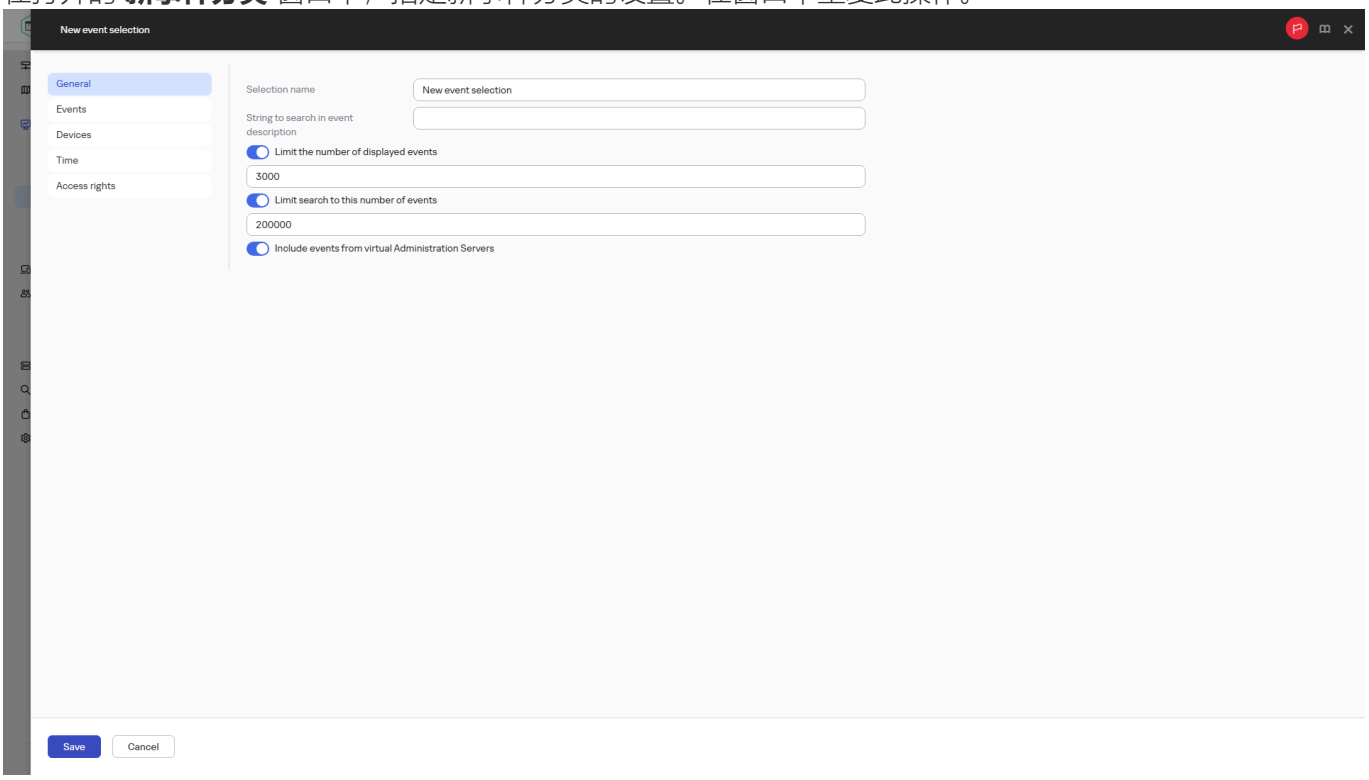
1. 在主菜单中，转到“**监控**”→“**事件分类**”。




事件分类列表

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。




创建新的事件分类

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。

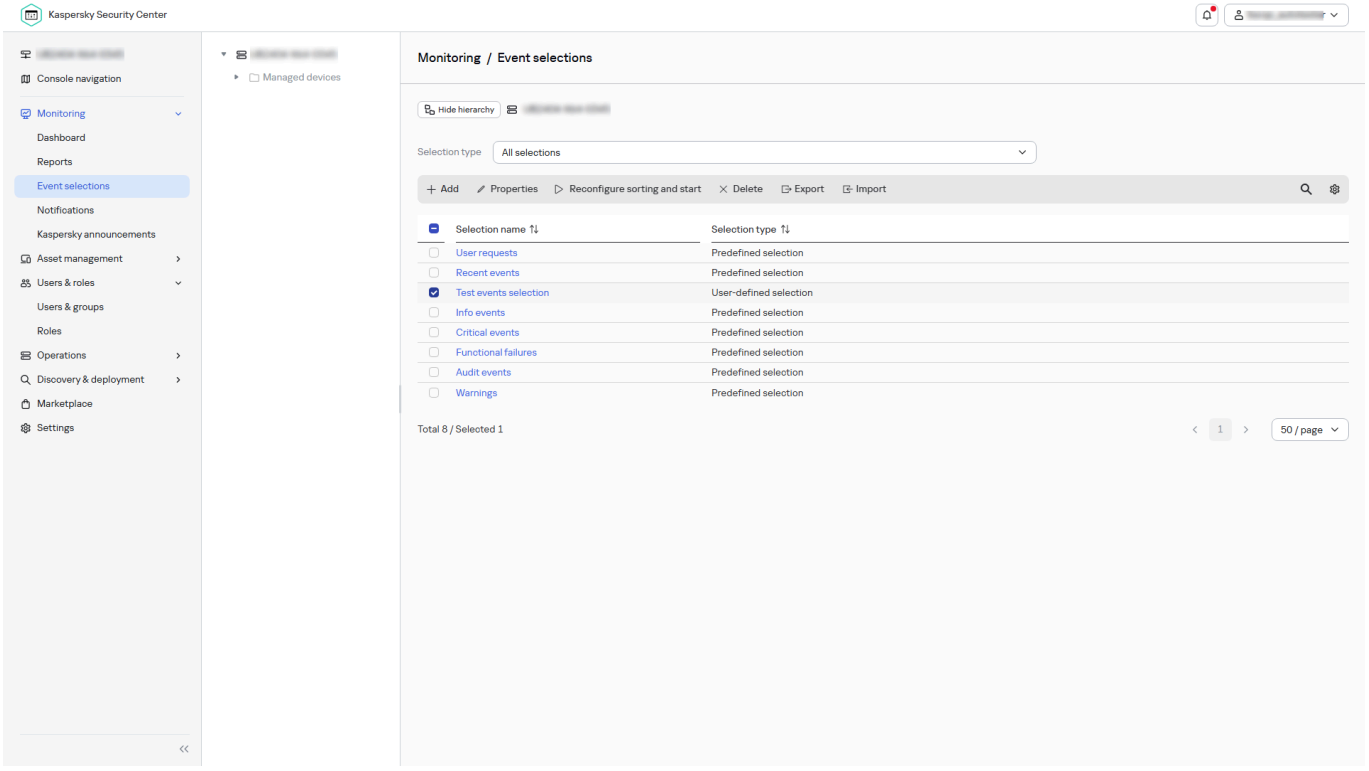
6. 单击“**保存**”确认事件分类创建。

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**”→ “**事件分类**”。
2. 选中您要编辑的事件分类旁边的复选框。




事件分类列表

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**。

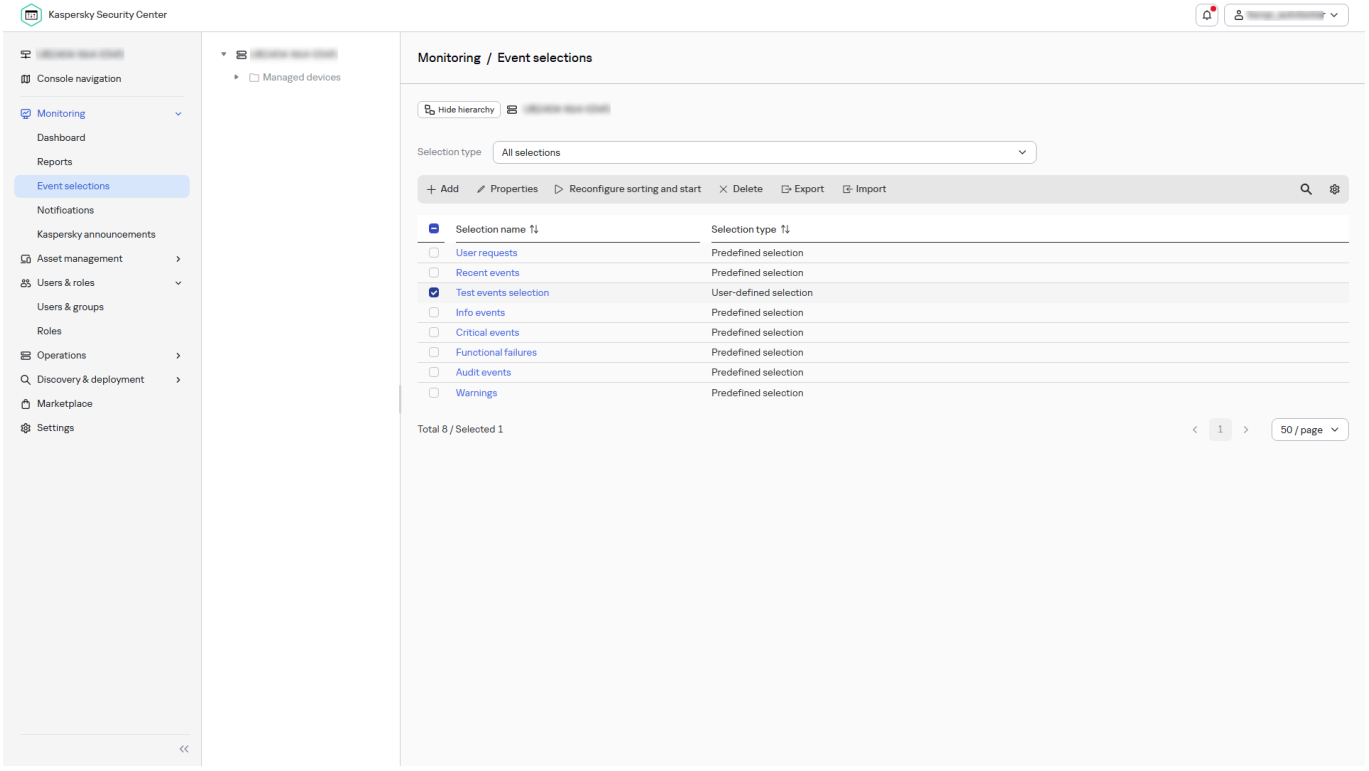
   对于用户定义分类，您可以编辑所有属性。
5. 单击“**保存**”保存设置。

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**”→ “**事件分类**”。
2. 选择您要启动的事件分类旁边的复选框。



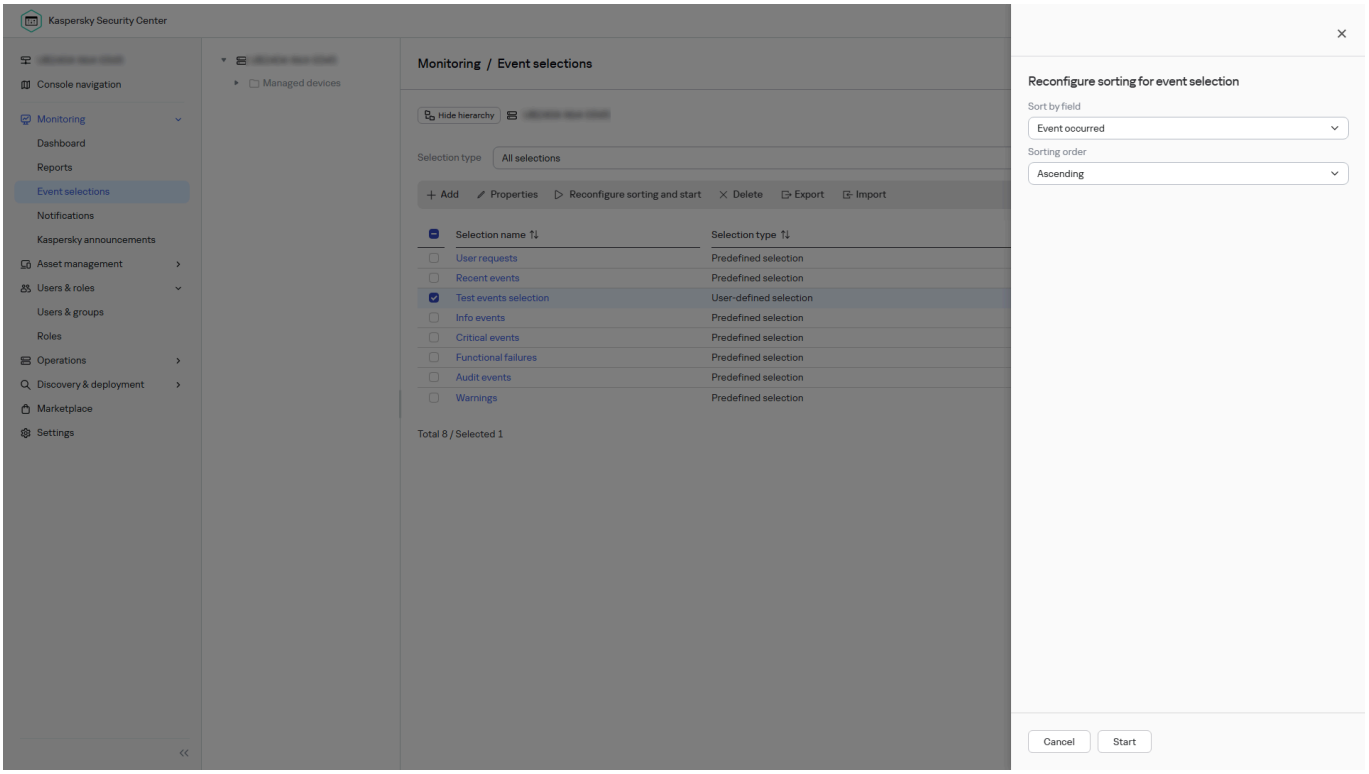

事件分类列表

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。

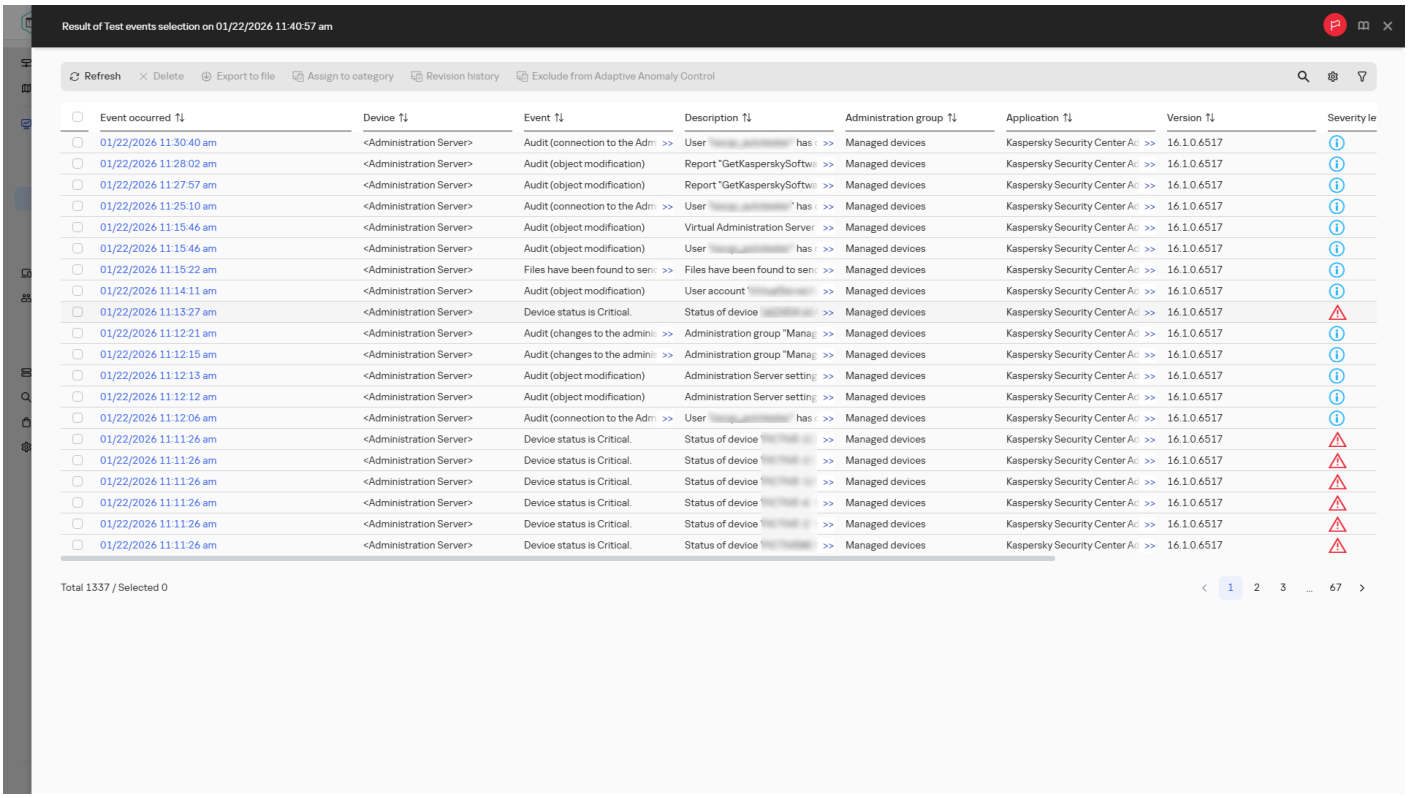



指定事件分类的排序设置

  a. 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。




事件分类结果

# 导出事件分类

Kaspersky Security Center Linux 允许您将事件分类及其设置保存到 KLO 文件。您可以使用此 KLO 文件将保存的事件分类导入到 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux。

请注意，您只能导出用户定义的事件分类。Kaspersky Security Center Linux 默认集中的事件分类（预定义分类）无法保存到文件。

*要导出事件分类：*

1. 在主菜单中，转到“**监控**”→“**事件分类**”。
2. 选中您要导出的事件分类旁边的复选框。

   您不能同时导出多个事件分类。如果您选择了多个分类，**导出**按钮将被禁用。
3. 单击“**导出**”按钮。
4. 在打开的“**另存为**”窗口中，指定事件分类文件名和路径，然后单击**保存**按钮。

   仅当您使用 Google Chrome、Microsoft Edge 或 Opera 时，才会显示“**另存为**”窗口。如果您使用其他浏览器，则事件分类文件会自动保存在“**下载**”文件夹。

# 导入事件分类

Kaspersky Security Center Linux 允许您从 KLO 文件导入事件分类。KLO 文件包含导出的事件分类及其设置。

*要导入事件分类：*

1. 在主菜单中，转到**监控→ 事件分类**。
2. 单击“**导入**”按钮，然后选择要导入的事件分类文件。
3. 在打开的窗口中，指定 KLO 文件的路径，然后单击“**打开**”按钮。请注意，您仅可选择一个事件分类文件。
   事件分类处理开始。

出现包含导入结果的通知。如果事件分类导入成功，您可以单击**查看导入详细信息**链接来查看事件分类属性。

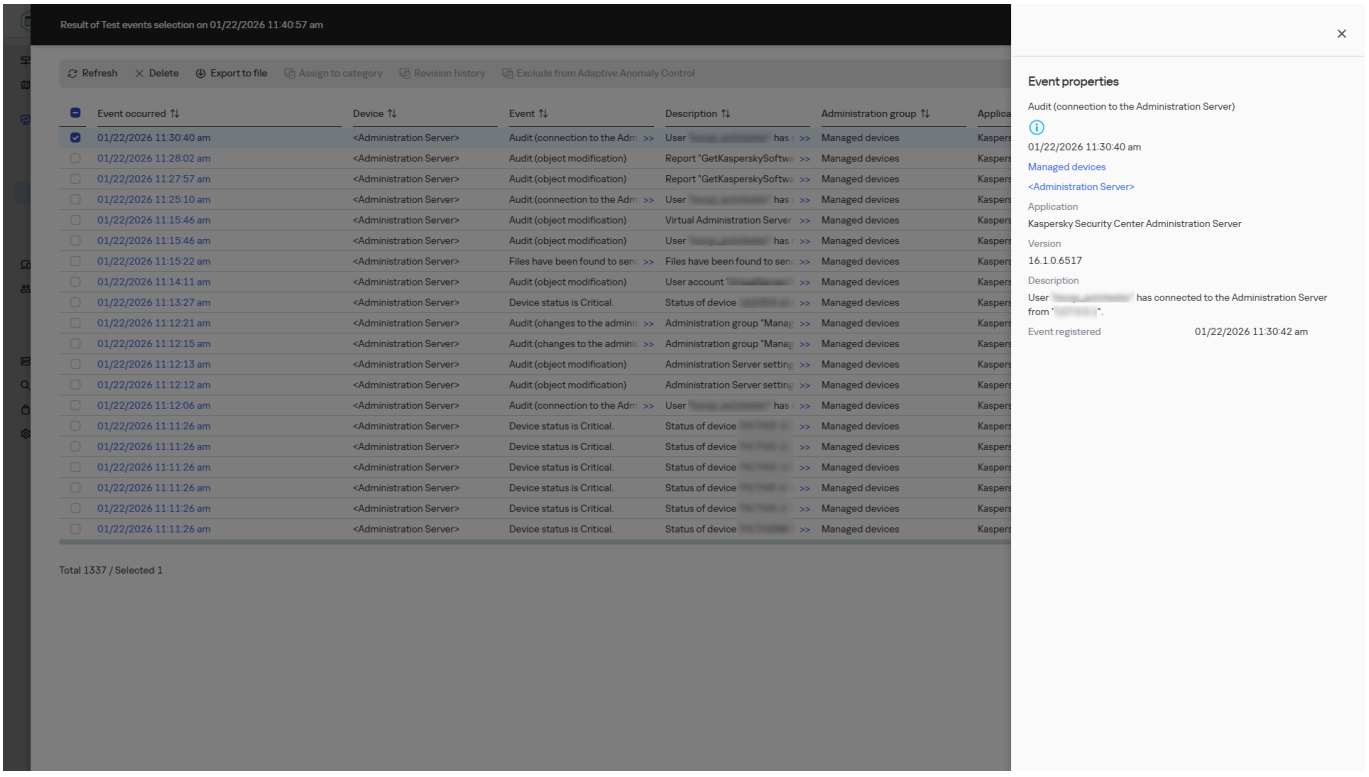
成功导入后，事件分类会显示在分类列表中。事件分类的设置也会被导入。

如果新导入的事件分类与现有事件分类有相同的名称，则导入的分类在名称后会附加一个 **(<下一个序列号>)** 索引，例如：**(1)**、**(2)**。

# 查看事件详情

*要查看事件详情：*

1. 启动事件分类。
2. 单击所需事件的时间。
   “**事件属性**”窗口打开。




“事件属性”窗口

3. 在显示的窗口中，您可以做以下：

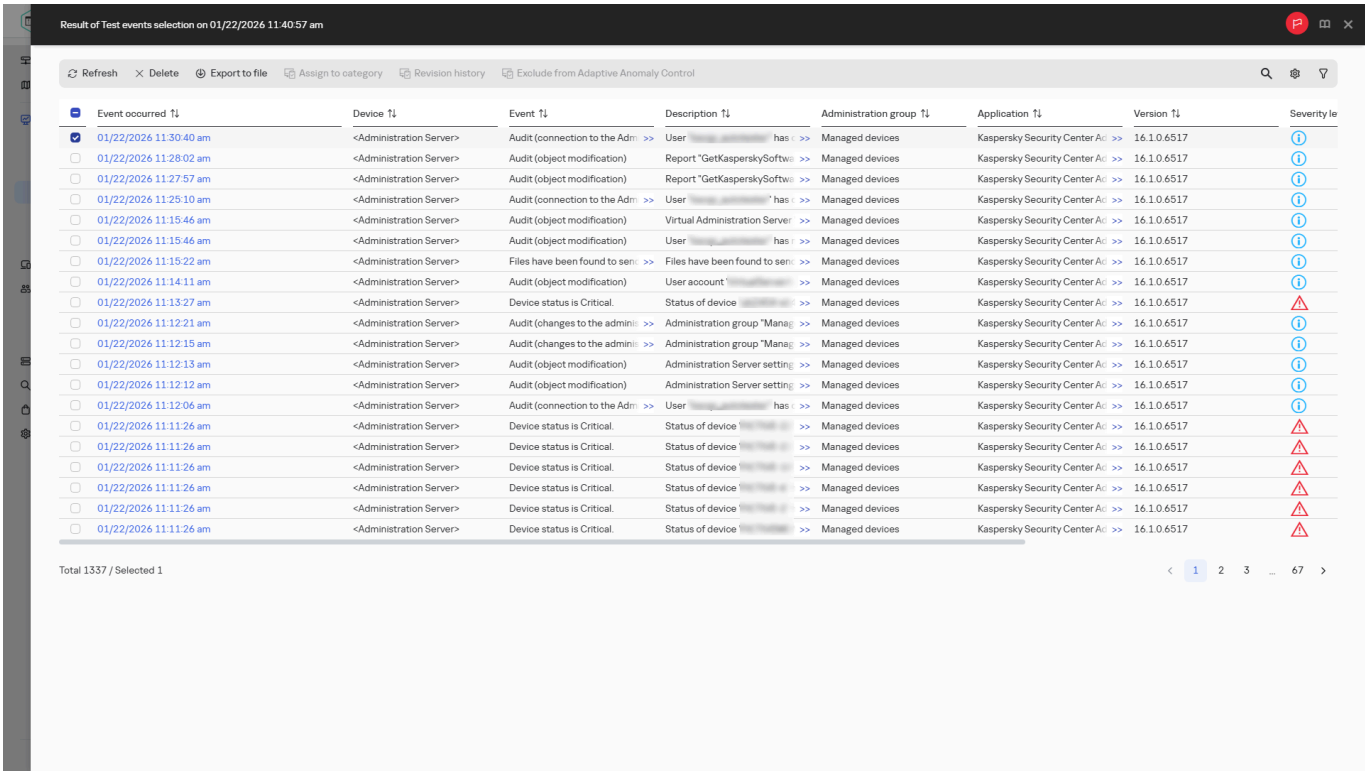
- 查看关于所选事件的信息
- 转到发生事件的设备
- 转到包含发生事件的设备的管理组
- 对于任务相关事件，转到任务属性

# 导出事件到文件

Kaspersky Security Center Linux 可让您将事件分类中的事件保存到 TXT 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。
   您还可以选择多个事件或整个事件分类。




事件分类结果

3. 单击“**导出到文件**”按钮。

所选事件被导出到 TXT 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

*要从事件分类中删除事件：*

1. 启动事件分类。
2. 选择事件：
   - 如果要删除一个或多个事件，请选中其旁边的复选框。
   - 若要删除当前页面上的所有事件，请选中事件列表上方的复选框，然后单击**在当前页面上全选**选项。
   - 如果要删除选定区域中的所有事件，请选中事件列表上方的复选框，然后单击**全部选择**选项。
3. 单击"**删除**"按钮。
4. 在打开的窗口中，单击**删除**。

*若要从设备事件列表中删除事件：*

1. 打开设备列表。
   - 对于受管理设备：**资产管理→资产(设备)**。
   - 对于未分配的设备：**资产管理→未分配的设备**。
2. 在设备列表中，单击所需设备名称的链接，然后前往**事件**选项卡。
3. 选择事件：
   - 如果要删除一个或多个事件，请选中其旁边的复选框。
   - 若要删除当前页面上的所有事件，请选中事件列表上方的复选框，然后单击**在当前页面上全选**选项。
   - 如果要删除选定区域中的所有事件，请选中事件列表上方的复选框，然后单击**全部选择**选项。

4. 单击**删除**，然后确认操作。

5. 在打开的窗口中，单击**删除**。

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**” → “**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卡巴斯基应用程序策略或在管理服务器属性（仅对于管理服务器事件）中禁用相应设置。这将降低数据库中的事件类型数量。

事件的存储期限越长，数据库达到最大值速度越快。但是，事件的存储期限越长，执行监控和报告任务的时间就越长。

*要为管理服务器中的事件设置存储期限：*

1. 在主菜单中，转到“ **资产管理**” → “**策略**“。

2. 单击所需策略的名称。

   您可以选择受管理卡巴斯基应用程序、网络代理或管理服务器的策略。对于管理服务器，您还可以通过单击管理服务器名称来配置事件的存储期限。

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。如果需要，您可以移动到**功能失败**、**警告**或**信息**部分。

4. 在右侧面板中的事件类型列表中，单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)**”切换开关按钮。

5. 在该开关按钮下面的编辑框中，输入存储事件的天数。

6. 如果您不希望在管理服务器数据库中存储事件，请禁用“**存储在管理服务器数据库上(天)**”选项。

   如果您在管理服务器属性窗口中配置管理服务器事件，并且在 Kaspersky Security Center 管理服务器策略中锁定了事件设置，则无法重新定义事件的存储期限值。

7. 单击**确定**，然后在右侧窗格关闭后，单击**保存**按钮。

   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

本部分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. 在主菜单中，单击管理服务器名称。

   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. 在主菜单中，单击管理服务器名称。
   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. 单击“**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，应用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**部分查看分配给事件的类型和严重级别。在**事件配置**部分，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**部分，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。

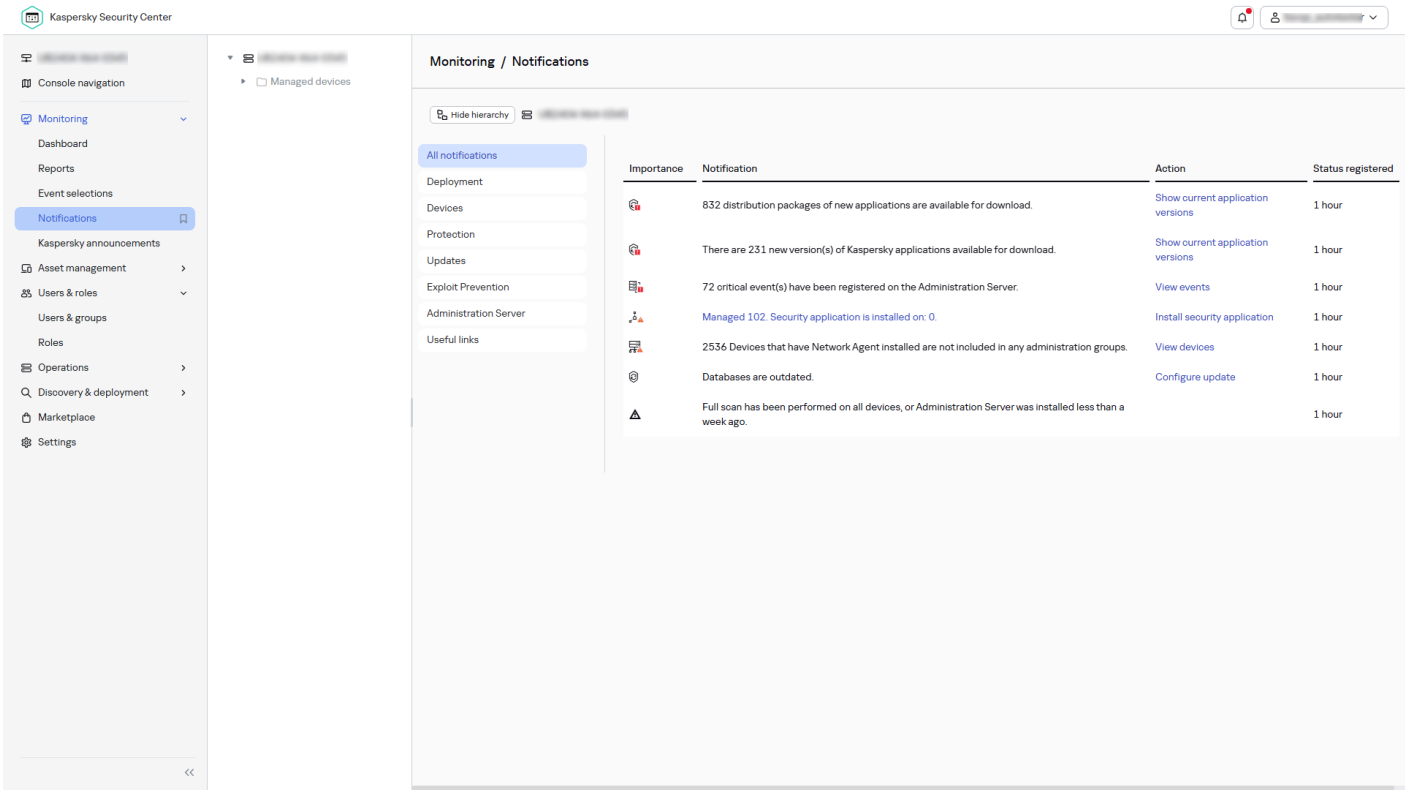
当管理服务器删除旧事件后，它无法保存新事件到数据库。在此时间段内，拒绝事件的信息被写入操作系统日志。新事件被列队，然后在删除操作后被保存到数据库。默认情况下，事件队列限制为 20,000 个事件。您可以通过编辑 KLEVP_MAX_POSTPONED_CNT 标记值来自定义队列限制。

# 通知和设备状态

本部分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。




通知列表

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:

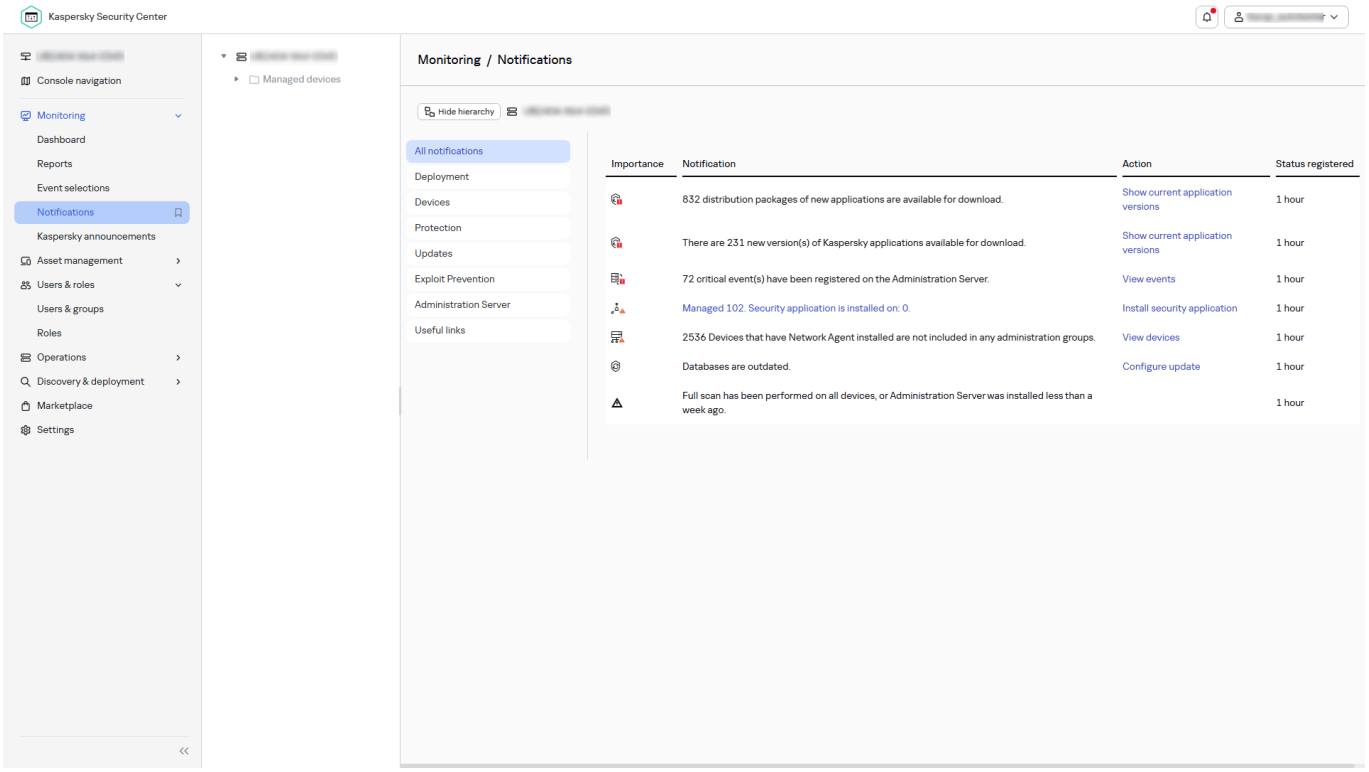
- 在“**监控**”→“**通知**”区域中。这里，您可以查看预定义类别的通知。
- 您可以打开单独的窗口。此种情况下，您可以标记通知为已查看。
- 在“**监控**”→“**控制板**”区域上的“**所选严重级别的通知**”小组件中。在小组件中，可以仅查看处于“*严重*”和“*警告*”重要级别的事件通知。

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**”→ “**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。




通知列表

2. 在左侧面板，选择类别之一：

   - **部署**
   - **设备**
   - **保护**
   - **更新**（包括有关可下载的卡巴斯基应用程序的通知、有关已下载的反病毒数据库更新的通知，以及有关网络代理更新后需要重新启动的设备（如果有）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）

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，通知单击该链接，您可以转到存储库并安装安全应用程序到设备，或查看设备列表或事件列表。您为通知执行推荐操作之后，该通知被分配*已查看*状态。
- **注册的状态**。这包含从通知被注册到管理服务器到现在为止过去的天数或小时数。

*要在单独的窗口中按重要级别查看屏幕通知：*

1. 在 Kaspersky Security Center Web Console 的右上角，点击旗帜图标()。

   如果旗帜图标具有红点，表示有未查看的通知。

   列出通知的窗口被打开。默认情况下，将选择“**所有通知**”选项卡，并且通知按重要级别分组：“*严重*”、“*警告*”和“*信息*”。

2. 选择“**系统**”选项卡。

   将显示“*严重*”() 和“*警告*”() 重要级别通知的列表。通知列表包含以下：

   - 颜色标记。严重通知标记为红色。警告通知标记为黄色。
   - 指示通知主题的图标：部署 ()、保护 ()、更新 ()、设备管理 ()、漏洞利用防御 ()、管理服务器 ()。
   - 通知描述。
   - 旗帜图标。旗帜图标是灰色的，如果通知被分配了*未查看*状态。当您选择灰色旗帜图标并分配*已查看*状态到通知时，图标更改颜色到白色。
   - 推荐操作的链接。单击该链接后执行推荐操作时，通知的状态为*已查看*。
   - 从通知被注册到管理服务器到现在为止过去的天数。

3. 选择“**更多**”选项卡。

   将显示“*信息*”重要级别通知的列表。

   该列表的组织与“**系统**”选项卡上的列表相同（请参见上面说明）。仅有的不同是没有颜色标记。

您可以通过注册在管理服务器上的日期间隔来筛选通知。使用“**显示过滤器**”复选框来管理筛选器。

*要在部件上查看屏幕通知：*

1. 在“**控制板**”区域中，选择“**添加或还原小部件**”。

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。

   您可以单击小组件上的“**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**”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）。例如，如果某个受管理设备因满足“*数据库已过期*”条件而被分配“*严重*”状态，之后又为设备设置了可见性标志，则该设备被分配“*正常*”状态。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，恶意软件扫描任务，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。 |
| 恶意软件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。 |

| 条件 | 条件描述 | 可用值 |
| --- | --- | --- |
| 需要重启后的时间 | 设备在网络上可见，但应用程序要求重启的时间已超过指定时间间隔。 | 超过 0 分钟。 |
| 重启原因 | 设备在网络上可见，但由于所选原因之一，应用程序需要重新启动设备。 | • 未知原因<br>• 应用程序在重启前不会运行<br>• 需要重启以完成更新；应用程序正在运行<br>• 需要重启以启动更新<br>• 需要重启以完成扫描或清除<br>• 需要重启以完成远程安装/卸载<br>• 即将完成磁盘的数据加密 |
| 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。 |
| 检测到软件漏洞 | 设备在网络中可见且网络代理已安装到设备，但“*查找漏洞和所需更新*”任务在设备应用程序中检测到指定严重级别的漏洞。 | • 严重。<br>• 高。<br>• 中。<br>• 如果漏洞无法被修复则忽略。<br>• 如果为安装分配了更新则忽略。 |
| 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。 |

| 条件 | 条件描述 | 可用值 |
| --- | --- | --- |
| Windows Update 更新检查已长时间未执行 | 设备在网络中可见，但"*寻找漏洞和所需更新*"任务在指定时间段内未运行。 | 超过 1 天。 |
| 无效的加密状态 | 网络代理已安装到设备，但设备加密结果等于指定值。 | • 由于用户拒绝未遵从策略(仅对外部设备)。<br>• 由于错误未遵从策略。<br>• 应用策略时需要重启。<br>• 未指定加密策略。<br>• 不支持。<br>• 当应用策略时。 |
| 移动设备设置不遵从策略 | 移动设备设置不同于 Kaspersky Endpoint Security for Android 策略中指定的设置。 | • 开关按钮被关闭。<br>• 开关按钮被开启。 |
| 检测到未处理的安全问题 | 设备上发现了一些未处理的安全问题。安全问题可以通过安装在客户端设备上的受管卡巴斯基应用程序自动创建，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。<br>无论 Kaspersky Security Center Linux 设置如何，受管理设备的状态都可能由受管理应用程序定义。当此状态返回一个由 Kaspersky Security Center Linux 定义的状态后，管理服务器将为受管理设备分配一个最终状态。该状态选自以下两者中最为严重的一项：受管理应用程序返回的状态和管理服务器分配的状态。受管理应用程序定义的状态会附带由受管理应用程序传输的描述。您可以在受管理设备列表的"**状态描述**"列中查看这些描述。 | • 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。<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**"，则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。

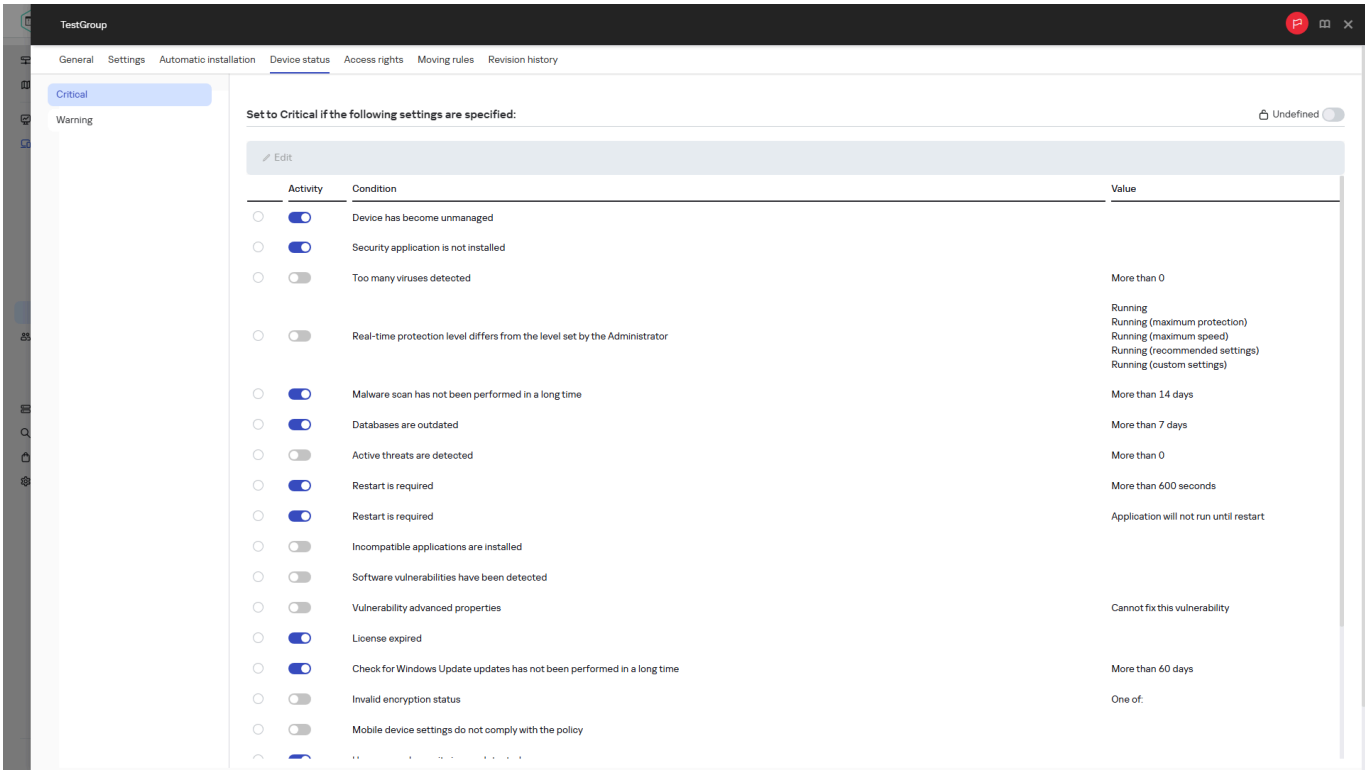
# 配置设备状态切换

您可以更改条件以将*严重*或*警告*状态分配给设备。

*要启用更改设备状态到严重：*

1. 在主菜单中，转到“**资产管理**”→“**组层级**”。
2. 通过以下方式之一，转到要更改设备状态的管理组的属性：
   - 单击管理组的名称。
   - 单击页面顶部的“**显示层级**”按钮。在打开的导航窗格中，将鼠标光标悬停在所需组的名称上，然后单击设置图标（⚙）。

   管理组属性窗口将开启。
3. 在属性窗口中，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“**如果指定了以下设置，则设置为“严重”**”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“**资产管理**” → “**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“**如果指定了以下设置，则设置为“警告”**”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. 在主菜单中，单击管理服务器名称。
   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。

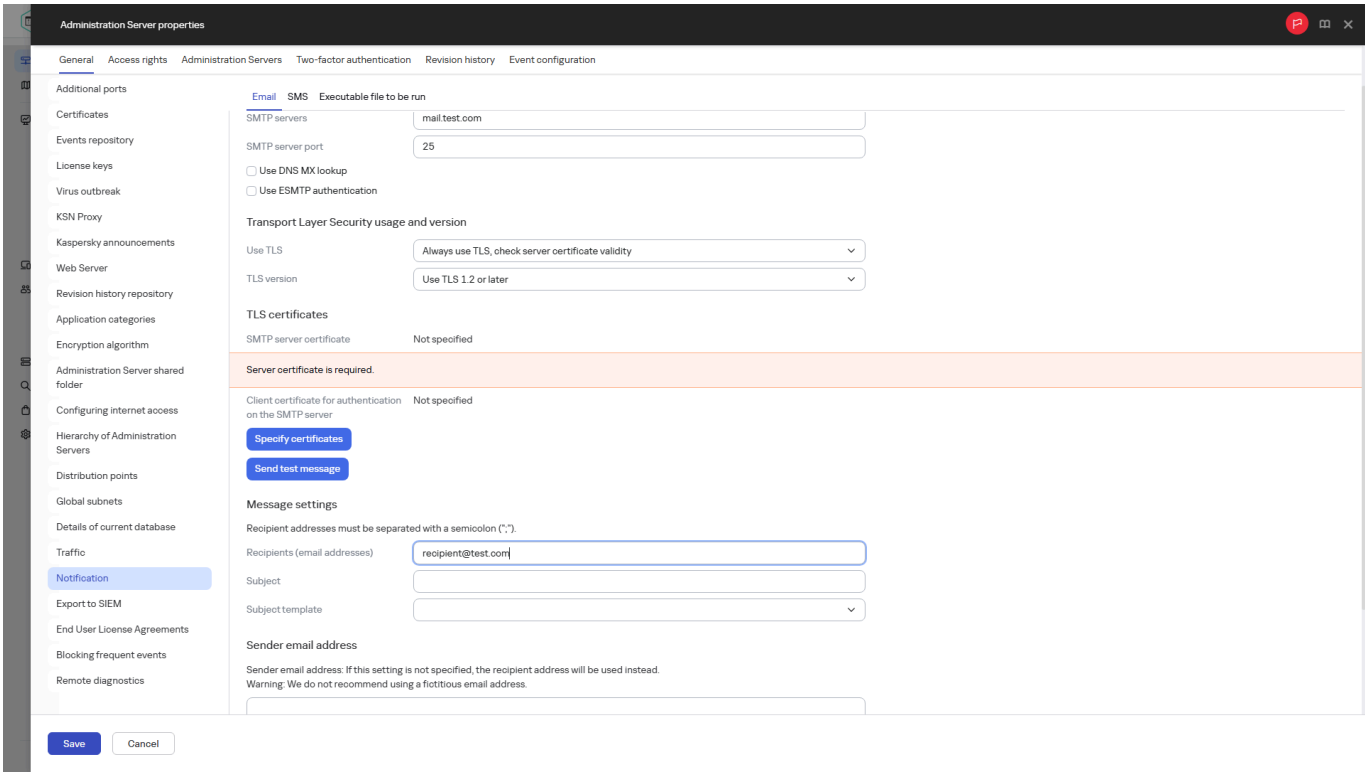
单击“**配置通知限制数**”链接可指定应用程序在指定时间段可以发送的最大通知数量。

- **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情的占位符。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。




选择通知方法

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，应用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**” → “**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环境变量（请见下表）。

用于描述事件的环境变量

| 环境变量 | 环境变量说明 |
| --- | --- |
| $SEVERITY | 事件严重级别。可能值：<br>• **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。 |

| 环境变量 | 环境变量说明 |
| --- | --- |
| $KL_PRODUCT | 应用程序名称。 |
| $KL_VERSION | 应用程序版本号。 |
| $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$COMPUTER 环境变量的另一个可执行文件（例如，script2.bat）。当发生事件时，将在管理员的设备上运行 script1.bat 文件，而该文件随后运行具有$COMPUTER 环境变量的 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

本部分介绍如何使用、配置和禁用卡巴斯基公告。

## 关于 Kaspersky 公告

“Kaspersky 公告”区域（**监控 → Kaspersky announcements**）提供与您的 Kaspersky Security Center Linux 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 Linux 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 Linux 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卡巴斯基应用程序保持最新并具有完整功能。公告可能包括有关卡巴斯基应用程序的关键更新、已发现漏洞的修复以及修复卡巴斯基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 Linux 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

  营销公告包括您的卡巴斯基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 Linux 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 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**” → “**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**”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** → **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。

Kaspersky 包括两种类型的信息：与安全相关的公告和营销公告。您可以单独禁用每种类型的公告。

*要禁用与安全相关的公告：*

1. 在主菜单中，单击管理服务器名称。
   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。

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，才会收到营销公告。您可以通过禁用 KSN 来禁用此类型的公告。

*要禁用营销公告：*

1. 在主菜单中，单击管理服务器名称。

   管理服务器属性窗口将打开。

2. 在“**常规**”选项卡上，选择“**KSN 代理设置**”区域。

3. 禁用**使用卡巴斯基安全网络已启用**选项。

4. 单击“**保存**”按钮。

   营销公告已禁用。

# 查看有关威胁检测的信息

您可以启用或禁用显示有关警报的信息。

使用 Kaspersky Extended Detection and Response Optimum 许可证或 Kaspersky Next XDR Optimum 许可证激活管理服务器后，Kaspersky Security Center Web Console 会自动在主菜单的“**监控**”区域中显示“**警报**”子区域。

*要启用或禁用在主菜单中显示“**警报**”区域：*

1. 在主菜单中，转到“**设置**” → “**界面选项**”。

2. 启用或禁用“**显示 EDR 警告**”选项。

3. 点击**保存**。

启用“**显示 EDR 警告**”选项后，控制台会在主菜单的“**监控**”区域中显示“**警报**”子区域。在“**警报**”子区域中，可以查看有关端点设备上的威胁检测的信息。

您还可以添加小部件来显示有关警报的信息。

为了在警报卡中正确显示有关检测到的威胁的详细信息，您必须安装Kaspersky Endpoint Agent 插件以及兼容版本的Kaspersky Endpoint Security 插件（Kaspersky Endpoint Security for Linux 12.1 或更高版本、 Kaspersky Endpoint Security for Mac 12.1 或更高版本、或 Kaspersky Endpoint Security for Windows 12.6 或更高版本）。

使用**筛选器**菜单按日期和字段值筛选警报。

**对象类型**字段包含以下值：

- 未知
- 钓鱼链接
- 病毒
- 木马
- 恶意工具
- 后门程序
- 蠕虫
- 其他应用程序
- 广告软件
- 色情软件
- 危险打包程序
- 危险行为

**自动响应**字段包含以下值：

- 检测到恶意对象
- 对象已删除
- 对象已清除
- 对象清除失败
- 对象已移动到隔离
- 检测到密码保护的存档
- 检测到的病毒

# 用于响应警报的集成

如果您拥有 Kaspersky Next XDR Optimum 授权许可，则可以配置与以下解决方案的集成以响应威胁：

- Kaspersky Automated Security Awareness Platform
- Kaspersky Threat Intelligence Portal Sandbox
- 活动目录

如果您已在 Kaspersky Next XDR Optimum 授权许可下激活管理服务器，则可以使用这些集成。
要执行响应操作，您必须将 Kaspersky Next XDR Optimum 授权许可密钥部署到您的受管理应用程序。
在试用授权许可下使用 Kaspersky Next XDR Optimum 时，您必须先添加从属物理管理服务器，在试用授权许可下激活此从属管理服务器，然后将授权许可密钥部署到由此管理服务器管理的设备上。

如果您使用的是 Kaspersky Next EDR Optimum 授权许可，则无需激活在 Kaspersky Next XDR Optimum 授权许可下安装在受管理设备上的应用程序。您仅需对新设备（如有）执行此操作。

由于 Kaspersky Next XDR Optimum 授权许可支持多租户，因此您可以将授权许可密钥集中分发到受管理的应用程序上。不支持将授权许可自动分发到从属和虚拟管理服务器。

要配置集成，您必须具有**常规功能：应用程序集成**功能区域的**读取**和**写入**权限。

## 配置与 Active Directory 的集成以执行响应操作

与 Active Directory 集成使您能够对受到警报影响或涉及警报的 Active Directory 用户执行响应操作。

要配置与 Active Directory 的集成以响应警报，您必须使用 Kaspersky Security Center Linux 管理服务器 15.4 或更高版本。

与 Active Directory 集成以响应警报，以及在配置域控制器轮询时指定的 Active Directory 域控制器（域控制器的地址和用户凭证）扫描设置是两种不同设置。由于您需要确保要为其执行响应操作的用户拥有 Active Directory 账户，因此您必须配置这两个集成：用于扫描和用于响应。顺序不重要。

集成设置不会被继承，并且仅适用于您在其上配置这些设置的管理服务器（物理或虚拟）。

*要配置与 Active Directory 的集成以响应警报：*

1. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口打开，**常规**选项卡被选中。
2. 执行以下操作之一：
   - 选择**分发点**部分，单击所需分发点的名称，然后在打开的属性窗口中选择**Active Directory**部分。
   - 选择“**Active Directory 响应**”部分。
3. 在右侧窗格中，启用**Active Directory 整合**切换开关。

稍后，如果想关闭集成，您只能通过禁用**Active Directory 整合**切换开关对所有连接执行此操作。您无法关闭单独连接的集成。相反，您可以删除该连接。

> 当您启用或禁用“**Active Directory 整合**”切换开关时，该设置将应用于“**Active Directory 响应**”和“**分发点**”部分。

4. 通过单击“**添加**”按钮，创建与 Active Directory 域控制器的连接。

5. 在打开的窗口中，指定连接的以下参数：

   - **域控制器地址**

     计算机名称，例如：`server.mycompany.com`。

     您可以指定多个地址。您指定地址的所有域控制器必须属于同一个域。

   - **Active Directory 域名**

     DNS 完全限定域名，例如：`mycompany.com`

     另外，您可以指定 SAM 或 NetBIOS 名称，例如：`mycompany`

     使用小写字母。如果为管理服务器或分发点创建多个连接，请为每个连接指定不同名称。

     > 要执行响应操作，您在此字段中指定的 Active Directory 域名必须与警报中指定的 Active Directory 域名匹配。

   - **登录名**

     具有管理员权限的 Active Directory 账户的登录名，响应操作在该账户下执行。

   - **密码**

     具有管理员权限的 Active Directory 账户的密码，响应操作在该账户下执行。

6. 如果要检查连接状态，请单击“**检查连接**”按钮。

   如果连接成功建立，则显示“**已连接**”状态。否则，状态为“**失败**”，并显示一条错误消息，其中包含您未能连接的域控制器。

> 您必须考虑连接 Active Directory 的方式：**从Linux 设备还是从 Windows 设备**。

从 Linux 设备连接

默认情况下，从 Linux 设备连接并验证域控制器时，逻辑如下：

1. 管理服务器或分发点尝试通过 LDAPS 连接到域控制器。

   执行严格验证 LDAP 服务器证书。

2. 将域控制器证书的公共部分放入系统证书存储库以验证证书。

   使用与操作系统相关的系统证书颁发机构 (CA) 路径来访问证书链。

例如：

- /etc/ssl/certs/ca-certificates.crt — 基于 Debian 的操作系统 (Debian、Ubuntu、Astra) 的路径。
- /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem — CentOS 或 Red Hat 的路径。

3. 如果 LDAPS 连接失败，则会发生错误，不会使用其他连接协议。

> 如果出现 LDAPS 问题，您可以联系卡巴斯基技术支持。

如果您不想将证书安装到系统证书存储库中，可以使用 KLNAG_LDAP_SSL_CACERT 标志来设置域控制器证书的路径。为此，请运行以下命令：

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "</path/to/domain-controller/cert>"
```

其中`</path/to/domain-controller/cert>`是域控制器证书公共部分的路径。

例如，如果路径是`"/var/opt/kaspersky/ldap_cert.crt"`，则命令为`klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "/var/opt/kaspersky/ldap_cert.crt"`

从 Windows 设备连接

从 Windows 设备连接并验证域控制器时，连接设置由域定义。

您只需确保：

- LDAPS 已启用并且设备上的端口 636 可用。
- 您允许通过防火墙或代理服务器连接到域控制器。

7. 单击“**保存**”按钮。

窗口关闭，连接显示在连接表中。

在连接表中，您可以执行以下操作：

- 编辑连接参数。
  为此，请单击所需连接的**域控制器地址**参数的链接。在打开的窗口中，更改所需设置，然后单击“**保存**”按钮。
  您只能编辑**登录名** 和**密码** 参数。
- 删除连接。
  为此，请选中要删除的连接旁边的复选框，单击工具栏中的“**移除**”按钮，然后确认删除连接。

# 配置与 Kaspersky Automated Security Awareness Platform 的集成

与Kaspersky Automated Security Awareness Platform（以下也称为 KASAP）集成使您能够分配 KASAP 学习课程给与警报相关的用户。

集成设置不会被继承，并且仅适用于您在其上配置这些设置的管理服务器（物理或虚拟）。

在 Kaspersky Security Center Web Console 中配置集成之前，您必须在 KASAP 中创建授权令牌并获取 API 请求的 URL。

*要配置与 Kaspersky Automated Security Awareness Platform 的集成：*

1. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口打开，**常规**选项卡被选中。
2. 选择“**KASAP**”部分。
3. 在右侧窗格中，启用**KASAP 整合**切换开关。
4. 指定用于连接 KASAP 的设置：
   - **API 令牌**— 您创建的用于访问 KASAP Open API 的令牌。
   - **网址** — 创建 API令牌时获取的 API 请求的 URL。
   - **使用代理服务器**— 可在连接到 KASAP 时启用代理服务器的切换开关。
     默认情况下已禁用切换开关。
5. 如有必要，请单击**检查连接**按钮来验证您指定的设置。
   连接状态已显示。
6. 单击“**保存**”按钮。

已配置与 Kaspersky Automated Security Awareness Platform 的集成。

保存 KASAP 集成设置后，您可以单击**查看组**按钮查看 KASAP 学习组列表。

如果需要，当组列表显示时，您可以通过单击**刷新组**按钮来更新它。

打开列表后，您将无法隐藏它。如果禁用**KASAP 整合**切换开关，则不会显示 KASAP 组列表。

# 配置与 Kaspersky Threat Intelligence Portal Sandbox 的集成

与Kaspersky Threat Intelligence Portal（以下也称为Kaspersky TIP）集成可让您使用**Kaspersky Sandbox隔离**隔离区的文件。

集成设置不会被继承，并且仅适用于您在其上配置这些设置的管理服务器（物理或虚拟）。

在配置集成之前，您必须获取 Kaspersky TIP 上 API 请求的授权令牌。

*要配置与 Kaspersky TIP Sandbox 的集成：*

1. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口打开，**常规**选项卡被选中。
2. 选择 **Kaspersky TIP**。
3. 在右侧窗格中，启用**整合**切换开关。
   与 Kaspersky TIP 的连接设置将显示。

   如果在配置并保存集成设置后禁用**整合** 拨动开关，则设置不会被删除，但您将无法执行响应操作。
4. 单击**添加令牌**按钮，在打开的窗口中，指定您之前在 Kaspersky TIP 上获取的令牌，然后单击**添加** 按钮。
   窗口关闭，API 令牌已添加。
5. 如果您想在连接到 Kaspersky TIP 时使用代理服务器，请启用**使用代理服务器**切换开关。
   默认情况下已禁用切换开关。
6. 单击“**保存**”按钮。

已配置与 Kaspersky TIP Sandbox 的集成。

现在，您可以将文件从 **隔离** 部分发送到 Kaspersky TIP Kaspersky Sandbox进行威胁分析。文件大小上限为 100 MB。

由于 Kaspersky Next XDR Optimum 授权许可支持多租户，因此放置在**隔离区隔离** 由租户划分。如果管理员使用专用的 TIP 账户和与每个租户相关的 API 令牌，则这种租户级别的分离也适用于将文件发送到 Kaspersky TIP Sandbox 并查看结果时。但是，由于隔离列表不根据服务器层次结构显示对象，因此无法集中管理所有租户的**隔离**部分。

# 按属性分组警报

警报聚合有助于识别可能与同一事故相关的警报，从而简化调查过程。

要启用警报聚合功能，您必须执行以下操作：

- 在主菜单中启用**警报**子部分。
- 在 Kaspersky Next XDR Optimum 授权许可下激活管理服务器，然后将 Kaspersky Next XDR Optimum 授权许可密钥部署到您的受管理应用程序。

  在测试模式下使用试用版授权许可的 Kaspersky Next XDR Optimum 功能时，您必须首先添加从属物理管理服务器，然后在此授权许可下激活该服务器。

如果您使用的是 Kaspersky Next EDR Optimum 授权许可，则无需激活在 Kaspersky Next XDR Optimum 授权许可下安装在受管理设备上的应用程序。您仅需对新设备（如有）执行此操作。
由于 Kaspersky Next XDR Optimum 授权许可支持多租户，因此您可以将授权许可密钥集中分发到受管理的应用程序上。不支持将授权许可自动分发到从属和虚拟管理服务器。

您可以按设备名称、账户或哈希名称（SHA256）聚合警报。

仅当属性不为空时，警报才会根据该属性聚合。

如果警报至少共享一个属性，并且在组中任何其他警报的 24 小时内发生，则这些警报会聚合在一起。

*要按属性聚合警报：*

1. 在主菜单中，转到**监控 → 警报**。
2. 执行以下操作之一：
   - 启用 **警报聚合** 切换开关，然后选择一个或多个属性来聚合警报：
     - **设备名称**
     - **账户**
     - **文件哈希**哈希名称 （SHA256）

     默认情况下选择**设备名称** 和 **账户**属性。
   - 单击设置图标（⚙）。在打开的**表格设置**窗格中，转到 **分组** 选项卡。选择 **聚合组 ID** 并单击 **应用**。

   启用聚合后，警报将按**事件时间**从最新到最旧进行排序。不支持其他排序选项。选择不同的选项组将禁用聚合。

   该表显示按属性聚合的警报。未聚合的警报显示在表格底部。

聚合后，每个警报仅被分配给一个组。

# Cloud Discovery

通过 Kaspersky Security Center Linux，您可以监控运行 Windows 的受管理设备上云服务的使用情况，并阻止对您认为不需要的云服务进行的访问。Cloud Discovery 跟踪用户通过浏览器和桌面应用程序访问这些服务的尝试。它还会对用户尝试通过未加密的连接（例如，使用 HTTP 协议）来访问云服务的活动进行跟踪。此功能可帮助您检测并阻止影子 IT 对云服务的使用。

仅当您在Kaspersky Next EDR Optimum 或 Kaspersky Next XDR Expert 授权许可下激活 Kaspersky Security Center Linux 时，才可以使用阻止功能。

仅当您使用 Kaspersky Endpoint Security 11.2 for Windows 或更高版本时，才可以使用阻止功能。该安全应用程序的较早版本仅允许您监控云服务的使用情况。

您可以启用 Cloud Discovery 功能，并选择要启用该功能的安全策略或配置文件。您也可以在每个安全策略或配置文件中单独启用或禁用该功能。对于您不想让用户访问的云服务，您可以阻止对这些云服务的访问。

为了能够阻止对不需要的云服务进行的访问，请确保满足以下先决条件：

- 您使用的是 Kaspersky Endpoint Security 11.2 for Windows 或更高版本。该安全应用程序的较早版本仅允许您监控云服务的使用情况。
- 您已购买某一级别的 Kaspersky Next 授权许可，因此您可以阻止对不需要的云服务进行的访问。有关详细信息，请参阅 Kaspersky Next 帮助。

Cloud Discovery 小部件和 Cloud Discovery 报告会显示有关成功和被阻止的云服务访问尝试的信息。该小部件还会显示每项云服务的风险级别。Kaspersky Security Center Linux 从所有仅受安全策略或配置文件保护的受管理设备（已启用相关功能）中，获取有关云服务使用情况的信息。

# 使用小部件启用 Cloud Discovery

Cloud Discovery 功能允许您从所有受安全策略保护的受管理设备（已启用相关功能）中，获取有关云服务使用情况的信息。您只能对 Kaspersky Endpoint Security for Windows 策略启用或禁用 Cloud Discovery。

可通过两种方式来启用 Cloud Discovery 功能：

- 使用 Cloud Discovery 小部件。
- 在 Kaspersky Endpoint Security for Windows 策略属性中。

  有关如何在 Kaspersky Endpoint Security for Windows 策略属性中启用 Cloud Discovery 功能的详细信息，请参阅 Kaspersky Endpoint Security for Windows 帮助中的 Cloud Discovery 部分。

请注意，您只能在 Kaspersky Endpoint Security for Windows 策略参数中禁用 Cloud Discovery 功能。

为了启用 Cloud Discovery，您必须在“**常规功能：基本功能**”功能区域中具有**写入**权限。

*要使用 Cloud Discovery 小部件启用 Cloud Discovery 功能，请执行以下操作：*

1. 转到 Kaspersky Security Center Linux。
2. 在主菜单中，转到“**监控**”→“**控制板**”。
3. 在 **Cloud Discovery** 小部件上，单击“**启用**”按钮。

   如果您安装了 Kaspersky Endpoint Security for Windows 版本 12.4，请在 Kaspersky Endpoint Security for Windows 策略属性中启用 Cloud Discovery 功能。有关详细信息，请参阅 Cloud Discovery 部分。

   如果您的 Kaspersky Endpoint Security for Windows 版本低于 12.4，请将 Kaspersky Endpoint Security for Windows 插件更新至版本 12.5。

4. 在打开的“**启用 Cloud Discovery**”窗口中，选择要启用该功能的安全策略，然后单击“**启用**”按钮。
   以下策略设置将自动启用：**将脚本注入到 Web 流量以与网页进行交互**、**Web 会话监控**和**加密连接扫描**。

Cloud Discovery 功能会启用，小部件会被添加到仪表板。

# 将 Cloud Discovery 小部件添加到仪表板

您可以将 **Cloud Discovery** 小部件添加到仪表板，以监控受管理设备上云服务的使用情况。

如要将 Cloud Discovery 小部件添加到仪表板，您必须在“**常规功能：基本功能**”功能区域中具有**写入**权限。

*要将 Cloud Discovery 小部件添加到仪表板，请执行以下操作：*

1. 转到 Kaspersky Security Center Linux。
2. 在主菜单中，转到“**监控**”→“**控制板**”。
3. 单击“**添加或还原小部件**”按钮。
4. 在可用小部件列表中，单击“**其他**”类别旁边的箭头图标 (>)。
5. 选择 **Cloud Discovery** 小部件，然后单击“**添加**”按钮。
   如果 Cloud Discovery 功能被禁用，请按照“使用小部件启用 Cloud Discovery”部分中的说明进行操作。

所选的小部件会添加到仪表板的末端。

# 查看有关云服务使用情况的信息

您可以查看 **Cloud Discovery** 小部件，其中会显示有关云服务访问尝试的信息。该小部件还会显示每项云服务的风险级别。Kaspersky Security Center Linux 从所有仅受安全配置文件保护的受管理设备（已启用相关功能）中，获取有关云服务使用情况的信息。

在查看之前，请确保：

- Cloud Discovery 小部件已添加到仪表板。
- Cloud Discovery 功能已启用。
- 您在“**常规功能：基本功能**”功能区域中具有**读取**权限。

*要查看 Cloud Discovery 小部件，请执行以下操作：*

1. 转到 Kaspersky Security Center Linux。
2. 在主菜单中，转到“**监控**”→“**控制板**”。
   **Cloud Discovery** 小部件会显示在仪表板上。
3. 在 **Cloud Discovery** 小部件的左侧，选择云服务类别。
   小部件右侧的表格会显示在所选类别中用户最常尝试访问的最多五项服务。成功和被阻止的尝试均会计入尝试。
4. 在小部件的右侧，选择特定服务。
   下方的表格会显示最常尝试访问该服务的最多十台设备。在此表中，您可以生成两种类型的报告：成功访问尝试报告和被阻止访问尝试报告。
   此外，您还可以在此表中阻止特定设备访问云服务。

小部件会显示所请求的信息。

在显示的小部件中，您可以执行以下操作：

- 继续转到“**监控**”→“**报告**”部分以查看 Cloud Discovery 报告。
- 阻止或允许访问所选的云服务。

仅当您在Kaspersky Next EDR Optimum 或 Kaspersky Next XDR Expert 授权许可下激活 Kaspersky Security Center Linux 时，才可以使用阻止功能。

仅当您使用 Kaspersky Endpoint Security 11.2 for Windows 或更高版本时，才可以使用阻止功能。该安全应用程序的较早版本仅允许您监控云服务的使用情况。

# 云服务的风险级别

对于每项云服务，Cloud Discovery 都会为您提供风险级别。风险级别可帮助您确定不符合组织安全要求的服务。例如，在决定是否阻止对特定服务的访问时，您可能需要考虑风险级别。

免责声明：风险级别是一个估计指数，并不能说明云服务的质量或服务制造商的任何信息。风险级别只是卡巴斯基专家的建议。

云服务的风险级别显示在 Cloud Discovery 小部件和所有受监控云服务的列表中。

# 阻止对不需要的云服务进行的访问

您可以阻止用户访问您不希望他们访问的云服务。您也可以允许对之前被阻止的云服务的访问。

您在决定是否阻止对特定服务的访问时，除其他考虑因素外，还可能需要考虑风险级别。

您可以在安全策略或配置文件中阻止或允许对云服务的访问。

可通过两种方法来阻止对不需要的云服务进行的访问：

- 使用 Cloud Discovery 小部件。
  在这种情况下，您可以逐个阻止对服务的访问。
- 在 Kaspersky Endpoint Security for Windows 策略属性中。
  在这种情况下，您可以逐个阻止对服务的访问，也可以一次性阻止整个类别。
  有关如何在 Kaspersky Endpoint Security for Windows 策略属性中启用 Cloud Discovery 功能的详细信息，请参阅 Kaspersky Endpoint Security for Windows 帮助中的 Cloud Discovery 部分。

*要使用小部件阻止或允许对云服务的访问，请执行以下操作：*

1. 打开 Cloud Discovery 小部件，然后选择所需的云服务。
2. 在**使用该服务的前 10 台设备**面板中，找到要用于阻止或允许该服务的安全策略或配置文件。
3. 在所需行的“**策略或配置文件中的访问状态**”列中，执行以下任一操作：
   - 要阻止该服务，请在下拉列表中选择“**已阻止**”。
   - 要允许该服务，请在下拉列表中选择“**已允许**”。
4. 单击“**保存**”按钮。

安全策略或配置文件将会阻止或允许对所选服务的访问。

# 导出事件到 SIEM 系统

本部分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 允许通过以下方法之一配置将事件导出到 SIEM 系统：导出到任何使用 Syslog 格式的 SIEM 系统；导出到使用 LEEF 和 CEF 格式的 Kaspersky SIEM、QRadar、Splunk、ArcSight SIEM 系统；或直接从 Kaspersky Security Center 数据库将事件导出到 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、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。

## 从 Kaspersky Security Center Linux 发送事件的方法

有三种方法从 Kaspersky Security Center Linux 发送事件到外部系统：

- 通过 Syslog 协议发送事件到任意 SIEM 系统

  使用 Syslog 协议，您可以转发发生在 Kaspersky Security Center 管理服务器上和受管理设备上安装的 Kaspersky 应用程序中的任意事件。Syslog 协议是标准消息记录协议。您可以用它将事件导出到任何 SIEM 系统。

  为此，您需要标记希望中继到 SIEM 系统的事件。您可以在 Kaspersky Security Center Web Console 中标记事件。只有标记的事件才会被中继到 SIEM 系统。如果您没有标记任何内容，则不会中继任何事件。

- 通过 CEF 和 LEEF 协议将事件发送到 Kaspersky SIEM、QRadar、Splunk 和 ArcSight 系统

  您可以使用 CEF 和 LEEF 协议导出常规事件。当通过 CEF 和 LEEF 协议导出事件时，您不必能够选择指定事件以导出。相反，所有常规事件都被导出。要将 Kaspersky Security Center Linux 事件转换为 CEF 和 LEEF 格式的事件，您需要使用siem_conversion_rules.xml 文件。该文件包含 Kaspersky Security Center Linux 事件属性列表以及 CEF 和 LEEF 格式的事件的相应属性。此外，siem_conversion_rules.xml 文件包含用于生成与事件对应的消息的规则。该文件包含在 Kaspersky Security Center Linux 分发包中。

  不同于 Syslog 协议，CEF 和 LEEF 协议不通用。CEF 和 LEEF 适用于相应的 SIEM 系统（Kaspersky SIEM、QRadar、Splunk 和 ArcSight）。因此，当您选择通过这些协议导出事件时，您使用 SIEM 系统所需解析器。

- 直接从 Kaspersky Security Center Linux 数据库到 SIEM 系统

  以该方法导出事件可以用于通过使用 SQL 查询直接从数据库公共视图接收事件。查询结果被保存到 XML 文件，可以用于外部系统的输入数据。仅仅公共视图中的事件可以被直接从数据库中导出。

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**

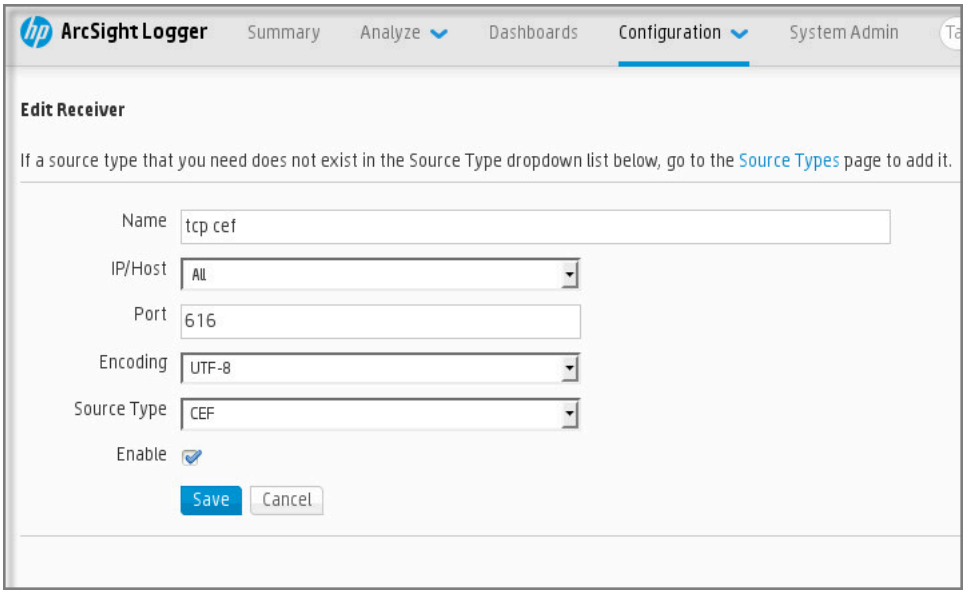
  指定用于连接到 Kaspersky Security Center Linux 的端口号。该端口必须与您在配置 SIEM 系统期间在 Kaspersky Security Center Linux 中指定的端口相同。

- **数据格式**

  指定Syslog、CEF或LEEF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。

# 关于使用 CEF 和 LEEF 格式导出事件

您可以使用 CEF 和 LEEF 格式将常规事件、策略更改事件以及由卡巴斯基应用程序传输到管理服务器的事件导出到 SIEM 系统。导出事件集是预定义的，您无法选择要导出的事件。在将事件发送到 SIEM 系统（Kaspersky SIEM、QRadar、ArcSight 或 Splunk）之前，需要使用 siem_conversion_rules.xml 文件中指定的规则，将 Kaspersky Security Center Linux 事件转换为 CEF 和 LEEF 格式的事件。

基于使用的 SIEM 系统选择导出格式。下表显示了 SIEM 系统和对应的导出格式。

导出事件到 SIEM 系统的格式

| SIEM 系统 | 导出格式 |
|---|---|
| Kaspersky SIEM | CEF |
| ArcSight | CEF |
| Splunk | CEF |
| QRadar | LEEF |

- LEEF (Log Event Extended Format) - 用于 IBM®Security QRadar SIEM 的自定义事件格式。QRadar 可以集成、识别和处理 LEEF 事件。LEEF 事件必须使用 UTF-8 字符编码。您可以在 IBM Knowledge Center 查看 LEEF 协议的详情。

- CEF (通用事件格式)—开放式日志管理标准，涉及来自不同的网络设备和应用程序的安全信息的协同工作。CEF 允许您使用通用日志格式，因此数据可以被简易整合以用企业管理系统分析。CEF 事件必须使用 UTF-8 字符编码。

自动导出意味着 Kaspersky Security Center Linux 发送常规事件到 SIEM 系统。事件自动导出在您启用后立即开始。该部分详细解释了如何启用自动事件导出。

# 将事件转换为 CEF 或 LEEF 格式

在将事件发送到 SIEM 系统（Kaspersky SIEM、QRadar、ArcSight 或 Splunk）之前，需要使用 siem_conversion_rules.xml 文件中指定的规则，将 Kaspersky Security Center Linux 事件转换为 CEF 和 LEEF 格式的事件。该文件包含在 Kaspersky Security Center Linux 分发包中。

siem_conversion_rules.xml 文件包含将事件转换为 CEF 和 LEEF 格式的预定义解释规则。如果想使用额外的事件解释规则，您可以手动将它们添加到文件中。

siem_conversion_rules.xml 文件包含以下部分：

- `<product name="SP_QRADAR" vendor="IBM">`

  本节包含以LEEF格式生成事件的规则，这些规则可以导出到QRadar SIEM系统。

- `<product name="SP_ARCSIGHT" vendor="HP">`.

  本节包含以CEF格式生成事件的规则，这些事件可以导出到ArcSight或Splunk SIEM系统。

- `<product name="Kaspersky SIEM" vendor="Kaspersky">`。

  本节包含以CEF格式生成事件的规则，这些事件可以导出到KUMA。

每个部分都有`<common>`子部分，Kaspersky Security Center Linux 事件属性以及 LEEF 格式事件的相应属性位于其中。这些通用属性用于所有可以导出的事件类型。

此外，每个部分都有`<event>`子部分。每个`<event>`子部分包含添加到`<common>`部分中列出的属性中的其他属性。

您可以手动将新的事件生成规则添加到 siem_conversion_rules.xml 文件中。

*要添加新的事件生成规则：*

1. 将`<event>`子部分新增到`<product name="SP_QRADAR" vendor="IBM">`、`<product name="SP_QRADAR" vendor="IBM">`或`<product name="Kaspersky SIEM" vendor="Kaspersky">`部分，然后根据需要指定其他事件属性。

2. 如果事件仅由通用属性组成，`<event>`子部分将为空。

siem_conversion_rules.xml

```
<conversion_rules>
    <product name="SP_QRADAR" vendor="IBM">
        <common> <!-- Common Kaspersky Security Center Linux event attributes and corresponding LEEF event
attributes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="EVC_EV_DISP_HOST_NAME" type="AT_STRING" limit="255"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND"> <!-- Generation rule for the GNRL_EV_VIRUS_FOUND event with additional
attributes -->
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="EVC_EV_SHA256" type="AT_STRING" limit="255"/>
            </param>
            ...
        </event>
...
```

```
</product>
    <product name="SP_ARCSIGHT" vendor="HP">
        <common> <!-- Common Kaspersky Security Center Linux event attributes and corresponding LEEF event
attributes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="dhost" type="AT_STRING" limit="1023"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND">
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="cs4" type="AT_STRING" limit="255"/>
                <attr name="cs4Label" type="AT_STRING" val="SHA256"/>
            </param>
            ...
</product>
    <product name="Kaspersky SIEM" vendor="Kaspersky">
        <common> <!-- Common Kaspersky Security Center Linux event attributes and corresponding LEEF event
attributes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="dhost" type="AT_STRING" limit="1023"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND">
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="cs4" type="AT_STRING" limit="255"/>
                <attr name="cs4Label" type="AT_STRING" val="SHA256"/>
            </param>
            ...
</product>
</conversion_rules>
```

# 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。

对于策略更改事件，您只能启用或禁用将所有此类事件导出到 SIEM 系统。

## 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“**资产管理**”→“**策略**”。
2. 单击您要为其标记事件的应用程序的策略。

   政策设置窗口打开。

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“**资产管理**” → “**资产(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. 在主菜单中，执行以下操作之一：
   - 单击管理服务器名称。
   - 转到“**资产管理**”→“**策略**”，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卡巴斯基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。

在将事件发送到 SIEM 系统（Kaspersky SIEM、QRadar、ArcSight 或 Splunk）之前，需要使用 siem_conversion_rules.xml 文件中指定的规则，将 Kaspersky Security Center 事件转换为 CEF 和 LEEF 格式的事件。

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

1. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**导出到 SIEM**”区域。
3. 单击“**设置**”链接。
   “**导出设置**”区域将打开。
4. 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 Linux 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 Linux 进行身份验证。因此，您将使用 Kaspersky Security Center Linux 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 Linux 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 Linux 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。

- **数据格式**

  您可以根据 SIEM 系统的要求选择 Kaspersky SIEM、IBM QRadar SIEM、 ArcSight、 Splunk 或系统日志格式。

  如果选择系统日志数据格式，则必须指定**最大消息大小，字节**

  指定 SIEM 系统消息的最大大小。每个事件被一条消息转发。如果消息的精确长度超过指定值，消息被截断且数据可能丢失。默认大小是 2048 字节。仅当在“**协议**”字段中选择了系统日志格式后，该字段才可用。

5. 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。
6. 启用**导出事件到 SIEM**选项。
7. 要将策略更改事件发送到SIEM，请启用**将策略更改的扩展事件导出到 SIEM**选项。系统会为每个已更改的政策设置向SIEM发送一个单独的事件。
8. 要检查 SIEM 系统连接是否已配置，请单击**检查连接**按钮。
   与 SIEM 系统的连接已建立，测试事件已发送。将显示连接状态。
9. 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或策略更改事件导出到 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。

# 监控策略和策略配置文件的更改

当策略设置发生变更时，会生成策略变更事件，然后您可以将其导出到 SIEM 系统，以监控策略变更并生成警报。只能通过 SIEM 系统访问策略变更事件。

策略变更事件生成后不会存储在管理服务器数据库中，也无法在 Kaspersky Security Center Web Console 的 **监控 → 事件分类** 区域查看。您也无法在 **事件配置** 选项卡上为这些事件指定通知设置和存储设置。

创建策略时，会为每个策略设置生成策略变更事件。更改策略时，会为策略中每个已更改的设置生成策略变更事件。删除策略会生成一个事件。例如，创建 Kaspersky Security Center 策略会生成大约 1000 个事件，而创建 Kaspersky Endpoint Security 策略会生成超过 7000 个事件。

## 生成策略变更事件的条件

在以下情况下会创建策略变更事件：

- 以下应用程序策略的创建、修改或删除：
  - Kaspersky Security Center 网络代理
  - Kaspersky Security Center 管理服务器
  - Kaspersky Endpoint Security for Windows 14.1
  - Kaspersky Endpoint Security for Linux 12.5
  - Kaspersky Endpoint Security for Linux 12.4
  - Kaspersky Endpoint Security for Mac 12.2.1
- 已在管理服务器属性中启用 **将策略更改的扩展事件导出到 SIEM** 选项。
- 通过 Kaspersky Security Center Web Console 界面手动修改策略

在以下情况下不会创建策略变更事件：

- 修改常规策略设置。
- 修改从父策略继承的策略设置。
- 通过 Kaspersky Security Center OpenAPI 修改策略设置。
- 直接在应用程序中修改 Kaspersky 应用程序设置。

## 策略变更事件字段

下表显示了一组策略变更事件字段。这些字段的表示形式取决于输出事件格式（例如 Syslog、CEF 或 LEEF）。有关确切的字段名称和事件模板，请参阅 siem_conversion_rules.xml 文件。事件参数仅以英语提供。

| 事件字段 | 数据类型 | 描述 |
| --- | --- | --- |
| eventType | 字符串 | 事件类型。允许为特定类型的事件创建关联规则。<br>可能的值：“Policy created”、“Policy modified”、“Policy deleted”。 |
| srvName | 字符串 | 管理服务器名称。 |
| eventTime | datetime | 事件的日期和时间（UTC）。 |
| eventGroupID | int | 修改的事件组 ID。 |
| objectID | int | 对象的内部 ID。 |

| | | |
|---|---|---|
| objectName | 字符串 | 策略显示名称。 |
| objectGroup | 字符串 | 包含该策略的管理组的完整路径和名称。 |
| user | 字符串 | 作出该修改的用户的名称。 |
| operation | 字符串 | 参数修改类型。<br>可能的值：“Added”、“Removed”、“Changed”。 |
| path | 字符串 | 参数路径。包含末级参数的父节点的路径。该路径基于策略的节和小节的名称创建。该路径结构与网络代理策略设置、常规策略设置和比较策略修订中所述的路径结构相同。 |
| parameter | 字符串 | 末级参数的名称。 |
| oldValue | 字符串 | 末级参数的旧值。 |
| newValue | 字符串 | 末级参数的新值。 |

# 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。使用安装的 Kaspersky Security Center Linux 版本中包含的 klsql2 实用程序版本。

*要使用 klsql2 实用程序：*

1. 转到安装管理服务器的目录。默认安装路径为/opt/kaspersky/ksc64/sbin。
2. 在此目录中，创建一个扩展名为 .sql 的空白文件。
3. 在任意文本编辑器中打开创建的 .sql 文件。
4. 在 .sql 文件中，键入所需的 SQL 查询，然后保存该文件。

5. 在安装了管理服务器的设备上，在命令行，输入以下命令以从 .sql 文件执行 SQL 查询并保存结果到 result.xml 文件：
   ```
   sudo ./klsql2 -i src.sql -u <用户名> -p <密码> -o result.xml
   ```
   其中 < username > 和 < password > 是有权访问数据库的用户账户的凭据。

6. 如果需要，输入有权访问数据库的用户账户的登录名和密码。

7. 打开新创建的 result.xml 文件以查看 SQL 查询结果。

您可以编辑 .sql 文件并创建到公共视图的任意 SQL 查询。然后，从命令行，执行您的查询并保存结果到文件。

## klsql2 实用工具中的 SQL 查询例子

该部分显示 SQL 查询的例子，通过 klsql2 实用工具执行。

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顺序显示事件。首先显示最近的事件。

PostgreSQL 示例：

```
SELECT
  /* 事件标识 */
  "e"."nId",

  /* 事件发生的时间 */
  "e"."tmRiseTime",

  /* 事件类型的内部名称 */
  "e"."strEventType",

  /* 事件的显示名称 */
  "e"."wstrEventTypeDisplayName",

  /* 事件的显示描述 */
  "e"."wstrDescription",

  /* 事件的显示描述 */
  "e"."wstrGroupName",

  /* 发生事件的设备的显示名称 */
  "h"."wstrDisplayName",
  (
    CAST(("h"."nIp" / 16777216 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST(("h"."nIp" / 65536 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST(("h"."nIp" / 256 )& 255 ) AS VARCHAR(4))  || '.'  ||

    /* 发生事件的设备的 IP 地址 */
    CAST(("h"."nIp" )& 255 ) AS VARCHAR(4))
  )  AS "strIp"
FROM "v_akpub_ev_event"  AS "e"
  INNER JOIN  "v_akpub_host"  AS "h" ON "h"."nId" = "e"."nHostId"
WHERE "e"."tmRiseTime" >= NOW() AT TIME ZONE 'utc'  + make_interval(days => CAST(-7  AS INT))
ORDER BY "e"."tmRiseTime" DESC ;
```

MySQL 或 MariaDB 示例：

```
SELECT

  /* 事件标识 */
  `e`.`nId`,

  /* 事件发生的时间 */
  `e`.`tmRiseTime`,

  /* 事件类型的内部名称 */
  `e`.`strEventType`,

  /* 事件的显示名称 */
  `e`.`wstrEventTypeDisplayName`,

  /* 事件的显示描述 */
  `e`.`wstrDescription`,

  /* 设备组名称 */
  `e`.`wstrGroupName`,

  /* 发生事件的设备的显示名称 */
  `h`.`wstrDisplayName`,
  CONCAT(
    LEFT(CAST(((`h`.`nIp`  DIV  1677721) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  65536) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  256) & 255) AS CHAR), 4), '.',

    /* 发生事件的设备的 IP 地址 */
    LEFT(CAST(((`h`.`nIp`) & 255) AS CHAR), 4)
  )  AS `strIp`
FROM `v_akpub_ev_event`  AS `e`
  INNER JOIN  `v_akpub_host`  AS `h` ON `h`.`nId` = `e`.`nHostId`
WHERE `e`.`tmRiseTime` >= ADDDATE( UTC_TIMESTAMP( ) , INTERVAL -7  DAY)
ORDER BY `e`.`tmRiseTime` DESC ;
```

## 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. 在主菜单中，单击管理服务器名称。

   管理服务器属性窗口将打开。

2. 在“**常规**”选项卡上，选择“**当前数据库详情**”区域。

数据库名称在“**数据库名称**”字段中指定。使用数据库名称在您的 SQL 查询中定位数据库。

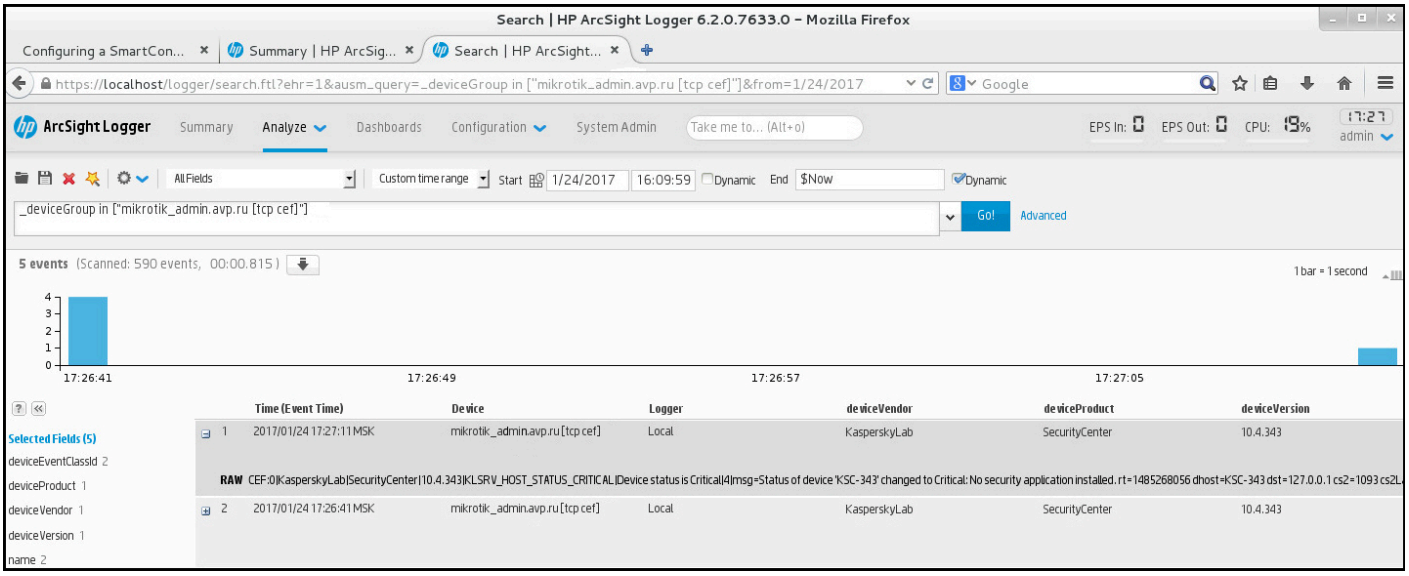
# 查看导出结果

您可以控制事件导出过程的成功完成。为此，检查带有导出事件的邮件是否被您的 SIEM 系统接收。

如果从 Kaspersky Security Center Linux 发送的事件被接收并被您的 SIEM 系统正确解析，两端的配置被正确完成。否则，检查您在 Kaspersky Security Center Linux 中指定的设置是否与您的 SIEM 系统中的设置一致。

下图显示导出到 ArcSight 的事件。例如，第一个事件是严重的管理服务器事件：“*设备状态为严重*”。

导出事件在您 SIEM 系统中的显示随您使用的 SIEM 系统而不同。




事件例子

# 管理对象修订

该区域包含了对象修订管理的信息。Kaspersky Security Center Linux 允许跟踪对象修改。您每次保存更改到对象时，*修订*被创建。每个修订都有一个数字。

支持修订管理的对象包括：

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

您可以对对象修订采取以下操作：

- 查看选定的修订（仅适用于策略）
- 回滚对对象所做的更改到所选的修订
- 将修订保存为 JSON 文件（仅适用于策略）

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。
- **用户设备 IP 地址** — 从其修改对象的设备的 IP 地址。
- **Web Console IP 地址** — 修改对象的 Kaspersky Security Center Web Console 的 IP 地址。
- **操作** — 对于对象执行的操作。
- **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。

# 查看并保存策略修订

通过 Kaspersky Security Center Linux，您可以查看在特定时期内对策略所做的修改，并且将有关这些修改的信息保存在文件中。

如果相应的管理 Web 插件支持此功能，则可以查看和保存策略修订。

*要查看策略修订：*

1. 在主菜单中，转到“**资产管理**”→“**策略**”。
2. 单击要查看修订的策略，然后转到“**修订历史**”部分。
3. 在策略修订列表中，单击要查看的修订编号。

   如果修订大小超过 10 MB，您将无法使用 Kaspersky Security Center Web Console 进行查看。系统将提示您将所选的修订保存到 JSON 文件。

   如果修订大小不超过 10 MB，则会显示 HTML 格式的报告，其中包含所选策略修订的设置。由于报告显示在弹出窗口中，请确保您的浏览器允许弹出窗口。

对于 Kaspersky Endpoint Security for Windows和 Kaspersky Endpoint Security for Mac 的策略，报告将不包含策略配置文件信息。

*要将策略修订保存到 JSON 文件，*

在策略修订列表中，选择要保存的修订，然后单击“**保存到文件**”。

修订会保存到 JSON 文件中。

如有必要，您可以比较政策修订版本。此选项适用于管理服务器、网络代理、 Kaspersky Endpoint Security for Windows （从 14.0 Web 插件版本开始）以及 Kaspersky Endpoint Security for Mac（从 12.2.1 Patch A Web 插件版本开始）的策略。

# 比较策略修订

您可以将政策的历史版本与其当前版本进行比较，比较列表中选定的不同版本，或者将一个政策的版本与另一个政策的版本进行比较。这些选项适用于管理服务器、网络代理、 Kaspersky Endpoint Security for Windows （从 14.0 Web 插件版本开始）以及 Kaspersky Endpoint Security for Mac（从 12.2.1 Patch A Web 插件版本开始）的策略。

*要查看策略修订：*

1. 在主菜单中，转到“**资产管理 → 策略**”。
2. 点击要比较其版本的政策。
   策略设置窗口打开。
3. 转到**修订历史**选项卡，然后选中要比较的版本旁边的复选框。
4. 在工具栏中，单击**比较**按钮，然后从下拉列表中选择以下选项之一：
   - **与当前版本**，如果您想将在步骤 3 中选择的版本与同一策略的上次保存版本进行比较。
   - **选择版本**，如果您想比较步骤3中选中的两个复选框。

     复选框的选择顺序不会影响比较结果。默认情况下，系统会将所选的较早版本与最新版本进行比较。例如，如果您选中版本5和版本1旁边的复选框，则会将版本1与版本5进行比较。报告将包含版本 1 相对于版本 5 新增、删除或更改的设置信息。
   - **与其他政策的版本比较**，如果您想比较两个不同政策的版本。
     在打开的右侧窗格中，执行以下操作：
     a. 在**应用程序名称**字段中，选择要比较的策略：网络代理或管理服务器。
     b. 在**政策名称**字段中，指定要将其版本与在步骤3中选择的政策进行比较的政策名称。
        政策版本列表随即显示。
     c. 选择所需的修订版，然后单击**比较**按钮。

版本对比报告以HTML格式显示在浏览器的新选项卡中。

如果比较结果超过10MB，则会显示相应的对话框。您可以单击**保存到文件**按钮将报告保存为文件，或取消操作。

报告将以您的 Kaspersky Security Center Web Console 的界面语言显示。您可以点击报告某些部分旁边的向下箭头图标（  ）展开这些部分，或者点击向上箭头（  ）图标折叠该部分。

报告包含以下信息：

- 卡巴斯基徽标。
- 报告名称。
- 报告创建的时间和日期。
- 政策名称、管理服务器以及包含该政策（或多个政策）的管理群组，这些政策的修订版本将被进行比较。
- "**另存为 HTML**"按钮。点击该按钮，报告将保存到您的电脑上。
- **摘要**部分显示有关比较版本的常规信息：政策名称、版本号、版本保存的时间和日期、保存版本的用户以及版本描述。

  对于继承的政策，不会显示用户信息。

- 比较各版本之间的差异。差异在以下部分中显示：
  - **被添加设置**
  - **删除的设置**
  - **更改设置**
  - **仅适用于对象1的设置**（如果您比较了两项不同政策的版本）
  - **仅适用于对象2的设置**（如果您比较了两个不同政策的版本）

  如果某个部分没有数据，则不会显示该部分。

对于 Kaspersky Endpoint Security for Windows和 Kaspersky Endpoint Security for Mac 的策略，修订比较报告将不包含策略配置文件信息。

# 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。

# 活动威胁

客户端设备上检测到的有关未处理的文件的信息将存储在“**存储库**”部分的“**活动威胁**”子部分中。

延迟处理和清除在请求时和指定事件发生时被安全应用程序执行。您可以配置推迟的情况处理。

## 清除未处理文件

*要开始清除未处理文件：*

1. 在主菜单中，转到**存储库** → **活动威胁**。

2. 执行以下操作之一：

   - 选择您要解毒的文件旁边的复选框。
   - 单击您要解毒的文件的名称。

3. 单击**清除**按钮开始文件解毒。

然后程序将尝试对选定文件进行解毒。

如果文件被清除，安装在客户端设备上的安全应用程序将其恢复到原始文件夹。该文件的相关记录将会从“**活动威胁**”部分的列表中删除。如果文件无法被清除，安全应用程序将其从设备删除。该文件的相关记录将会从“**活动威胁**”部分的列表中删除。

文件清除和删除功能可能会有所不同，具体取决于安装的安全应用程序、其版本和设置。

## 下载未处理文件

Kaspersky Security Center Linux 允许您下载客户端设备上发现的未处理文件的副本。这指的是由应用程序处理或删除的文件。这些文件将被下载到安装了 Kaspersky Security Center Linux 的设备上的指定文件夹中。

如果文件在杀毒期间被删除或修改，并且其副本存储在托管设备上的Kaspersky Endpoint Security for Linux 存储中，您可以下载文件副本。

*要下载未处理文件的副本，请执行以下操作：*

1. 在主菜单中，转到**存储库** → **活动威胁**。
2. 执行以下操作之一：
   - 选择您要下载的文件旁边的复选框。
   - 单击您要下载的文件的名称。
3. 单击**下载**按钮开始下载。

安装在发现未处理文件的客户端设备上的安全应用程序会下载一份该文件的副本至指定文件夹。

# 从“活动威胁”部分中删除文件

*要从**活动威胁**部分中删除文件，请执行以下操作：*

1. 在主菜单中，转到**存储库** → **活动威胁**。
2. 执行以下操作之一：
   - 选择您要删除的文件旁边的复选框。
   - 单击您要删除的文件的名称。
3. 单击**删除**按钮删除文件。
4. 在打开的窗口中，单击“**删除**”按钮。

这样，将该文件放入客户端设备存储库的安全应用程序将从存储库中删除该文件。该等文件的相关记录将会从“**活动威胁**”部分的列表中删除。

# 对象删除

本部分提供有关删除对象的信息。

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

*要删除对象：*

1. 打开 Kaspersky Security Center Web Console 的所需部分，然后选择对象。
2. 在工具栏上，单击“**删除**”按钮。
3. 在打开的窗口中，单击“**确定**”以确认您的选择。

   所选对象被删除。

当您删除对象时，其信息保留在数据库。已删除对象的信息的存储期限与对象修订的存储期限一致（推荐期限是 90 天）。您仅在权限的**已删除对象**区域具有**修改**权限时才能更改存储期限。

## 关于删除客户端设备

当您从管理组中删除受管理设备时，应用程序会将设备移至未分配的设备组。删除设备后，已安装的卡巴斯基应用程序——网络代理和安全应用程序（例如 Kaspersky Endpoint Security）——将保留在设备上。

Kaspersky Security Center Linux 根据以下规则处理未分配设备组中的设备：

- 如果您配置了设备移动规则，并且设备符合移动规则的条件，则该设备会根据规则被自动移动到管理组。
- 设备会被存储在未分配的设备组中，并根据设备保留规则自动从组中删除。

  设备保留规则不会影响具有一个或多个使用完整磁盘加密进行加密的驱动器的设备。此类设备不会被自动删除——您只能手动删除它们。如果您需要删除带有加密驱动器的设备，请先解密驱动器，然后再删除该设备。

  > 当您删除带有加密驱动器的设备时，解密驱动器所需的数据也会被删除。如果在删除此类设备（从“**未分配的设备**”或“**受管理设备**”组）时打开的确认窗口中选中“**我了解风险并想要删除选定的设备**”复选框，则表示您知晓数据随后会被删除。

  要解密驱动器，必须满足以下条件：

  - 设备被重新连接到管理服务器以恢复解密驱动器所需的数据。
  - 设备用户记住解密密码。
  - 用于加密驱动器的安全应用程序（例如 Kaspersky Endpoint Security for Windows）仍安装在设备上。

  如果驱动器由卡巴斯基磁盘加密技术加密，您还可以尝试使用 FDERT Restore Utility 恢复数据。

> 在 VDI 中，如果您的设备包含加密驱动器，则删除该设备后，加密驱动器上的信息也会被删除。

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 Linux 会在网络轮询期间发现该设备并将其添加回未分配的设备组。因此，最好仅当设备对管理服务器不可见时再手动删除设备。

# 从隔离区和文件备份中下载和删除文件

本节提供有关如何从 Kaspersky Security Center Web Console 的隔离区和文件备份中下载和删除文件的信息。

## 从隔离区和文件备份区下载文件

只有满足以下两个条件之一，您才能下载隔离区和文件备份区中的文件：在设备的设置中启用了“**不断开与管理服务器的连接**”选项，或者正在使用连接网关。否则，下载无法进行。

*要将隔离区或文件备份中的文件的副本保存到硬盘驱动器，请执行以下操作：*

1. 执行以下操作之一：
   - 如果要从隔离区保存文件副本，请在主菜单中转到**操作 → 存储库 → 隔离**。
   - 如果要从备份区保存文件副本，请在主菜单中转到**操作 → 存储库 → 文件备份**。
2. 在打开的窗口中，选择要下载的文件并单击 **下载**。

   下载开始。已放置在客户端设备上隔离区中的文件的副本将被保存到指定的文件夹中。

## 关于从隔离区、文件备份区或活动威胁存储库中删除对象

当客户端设备上安装的卡巴斯基安全应用程序将对象放置到隔离、备份或活动威胁存储库时，它们会将添加对象的信息发送到 Kaspersky Security Center Linux 中的**隔离**、**文件备份**或者**活动威胁**区域。打开其中一个区域时，可以删除所需的对象。

对于“**文件备份**”或“**活动威胁**”区域，从列表中选择一个对象，然后单击“**移除**”按钮。

对于“ **隔离**”区域，您可以执行以下操作之一：

- 选中要移除的对象名称旁边的复选框，然后在工具栏中单击“**删除**”按钮。
- 单击要移除的对象名称，然后在打开的详细信息窗口中，在工具栏中单击“**删除**”按钮。

  此时，对象将被删除，屏幕上将显示相应的通知，并且详细信息窗口将关闭。

Kaspersky Security Center Linux 会从列表中移除选定对象，或从存储库中删除选定对象。要执行的操作由将选定对象放置到存储库的卡巴斯基应用程序定义。卡巴斯基应用程序在“**条目添加者**”字段中予以指定。

有关要执行的操作的详细信息，请参阅卡巴斯基应用程序的文档。

# 通过 SNMP 管理应用程序

本节介绍如何在 Linux 中使用简单网络管理协议 (SNMP) 从管理服务器获取信息。

SNMP 是一种用于管理网络设备的协议。

为了通过 SNMP 工作， Kaspersky Security Center Linux 使用操作系统中包含的 snmpd 服务和 SNMP 代理来监控管理服务器的性能，并通过 OID 将数据发送到侧向应用。Kaspersky Security Center Linux 可以以统计信息或 SNMP 陷阱的形式发送此信息，SNMP 陷阱是关于应用程序事件的通知。

通过 SNMP，您可以访问以下关于应用程序的信息：

- 常规信息
- 自安装了应用程序以来的 Kaspersky Security Center Linux 统计信息
- 关于 Kaspersky Security Center Linux 事件的信息

已授予只读权限。

有关 SNMP 陷阱和通过 SNMP 发送的统计信息的信息存储在 adminkit.mib 文件中。默认情况下，adminkit.mib 文件位于 /opt/kaspersky/ksc64/share/snmp/ 文件夹中。

每个集群节点上的本地 snmpd 服务充当 SNMP 服务器，接收统计信息。不支持与外部 SNMP 服务器交互。SNMP 陷阱可以通过在每个集群节点上使用本地 snmptrapd 服务来接收，或者可以被重定向到外部服务器。

对于通过 SNMP 进行的操作，请在每个集群节点的操作系统中预先配置 snmpd 服务。

# 在操作系统中配置 snmpd 服务

配置之前，请确保您的操作系统中已安装 snmpd 服务。

创建用于访问数据的用户账户

创建账户之前，请运行以下命令停止 snmpd 服务：

```
bash
sudo systemctl stop snmpd
```

为了使用身份验证和加密通过 SNMPv3 确保数据访问的安全性，您需要使用以下信息在 snmpd 服务端创建用户账户：

- 用户名（区分大小写）
- 身份验证算法（MD5 或 SHA，推荐 SHA）
- 身份验证密码
- 加密算法（仅支持 AES）
- 加密密码

您可以通过以下方式创建用户账户：

- 如果操作系统中提供了 net-snmp-create-v3-user 实用程序，则使用该实用程序。
- 通过向 snmpd 服务的配置文件中添加相应指令进行手动操作。

*要使用 net-snmp-create-v3-user 实用程序创建用户账户，请运行以下命令：*

```
net-snmp-create-v3-user -ro -a <身份验证算法> -x <加密算法> <用户名>
```

身份验证和加密密码将以交互方式提示。

例如：

```
net-snmp-create-v3-user -ro -a SHA -x AES MonitoringUser
```

*要手动创建用户账户：*

1. 要创建 /var/lib/snmp/snmpd.conf 配置文件，请运行以下命令：

   ```
   touch /var/lib/snmp/snmpd.conf
   ```

2. 在配置文件中添加下列行：

   ```
   createUser <用户名> <身份验证算法> "<身份验证密码>" <加密算法> "<加密密码>"
   ```

   例如：

   ```
   createUser MonitoringUser SHA "MonitoringAuthSecret" AES "MonitoringPrivSecret"
   ```

创建用于接收 SNMP 陷阱的用户账户

需要通过 SNMPv3 接收经过身份验证和加密的 SNMP 陷阱，需要在监控系统端的相应服务（通常是 snmptrapd 服务）的上下文中创建一个账户。

账户必须包含以下信息：

- 用户名
- 身份验证算法
- 身份验证密码
- 加密算法
- 加密密码

出于安全考虑，请使用不同的用户账户分别访问数据和接收 SNMP 陷阱。

有关创建用于接收 SNMP 陷阱的用户账户的说明，请参阅监控系统的文档。

## 配置 snmpd 服务

snmpd 服务的配置存储在 `/etc/snmp/snmpd.conf` 文件中。您可以将必要的信息添加到现有配置文件中，也可以创建一个新的配置文件，并按给定顺序添加下列行。

如果您选择创建新的配置文件，请确保只有超级用户有访问权限。如果未设置所需的访问权限，请按指定顺序运行以下命令来配置这些权限：

```
chown root:root /etc/snmp/snmpd.conf
[[chmod 600 /etc/snmp/snmpd.conf
```

*要配置 snmpd 服务：*

1. 在配置文件中，指定 snmpd 服务监听传入请求的协议、网络接口地址和端口号。

   - 如果要监听所有网络接口上的请求，请将以下行添加到配置文件中：

     ```
     agentAddress udp:161
     ```

   - 如果只想监听本地网络接口上的请求（例如，如果监控系统安装程序在同一台机器上），请将以下行添加到配置文件：

     ```
     agentAddress udp:127.0.0.1:161
     ```

2. 配置 Kaspersky Security Center Linux 与 snmpd 服务之间的交互。您可以使用 UNIX 套接字或 TCP 套接字。

- 如果使用 UNIX 套接字：

  a. 指定 UNIX 套接字的路径和权限。为此，请在配置文件中添加下列行：

  ```
  master agentx
  agentXSocket unix:/var/run/agentx-master.socket
  agentXPerms 770 770 kluser klusers
  ```

  b. 将 klusers 组添加为 {'KLSRV_UNATT_KLSVCUSER'} 账户的补充组。

- 如果使用 TCP 套接字，请指定 TCP 套接字的端口和地址。为此，请在配置文件中添加下列行：

```
master agentx
agentXSocket tcp:127.0.0.1:705,tcp6:[::1]:705
```

3. 将最小响应超时时间设置为至少 30 秒。为此，请在配置文件中添加下列行：

```
agentxTimeout 30
```

4. 如有必要，您可以提供配置了 SNMP 的服务器的描述、系统位置以及管理员的联系地址。为此，请在配置文件中添加下列行：

```
sysDescr <server description>
sysLocation <server location>
sysContact <contact address of the administrator>
sysServices 72
```

5. 指定您希望通过 SNMP 协议向监控系统提供的 OID 树范围。为此，请在配置文件中添加下列行：

```
view monitoring included .1.3.6.1.4.1.23668.1093.1
view systemonly included .1.3.6.1.4.1.23668.1093.1
```

6. 如有必要，您还可以指定包含 snmpd 服务存储的操作系统信息的 OID 树的范围。此范围将对您的监控系统可用。

操作系统信息包括 CPU 和 RAM 使用情况、磁盘分区可用空间、网络接口负载、已安装软件列表、已打开的网络连接列表以及正在运行的进程列表等。部分信息可能属于机密信息。

- 如果您只想允许访问常规系统信息以及 RAM、CPU 和磁盘设备的使用情况信息，请将以下行添加到配置文件中：

```
# SNMPv2-MIB - Basic system information
view monitoring included .1.3.6.1.2.1.1
# HOST-RESOURCES-MIB - CPU, Memory, Filesystems
view monitoring included .1.3.6.1.2.1.25.1
view monitoring included .1.3.6.1.2.1.25.2
view monitoring included .1.3.6.1.2.1.25.3
view monitoring included .1.3.6.1.2.1.25.5
# UCD-SNMP-MIB - Memory and CPU usage
view monitoring included .1.3.6.1.4.1.2021.4
view monitoring included .1.3.6.1.4.1.2021.10
view monitoring included .1.3.6.1.4.1.2021.11
# UCD-SNMP-DISKIO-MIB - Block devices I/O statistics
view monitoring included .1.3.6.1.4.1.2021.13
# IF-MIB - Network interfaces I/O statistics
view monitoring included .1.3.6.1.2.1.2
view monitoring included .1.3.6.1.2.1.31
```

- 如果您想要允许访问所有系统信息，请将以下行添加到配置文件中：

```
view monitoring included .1
```

7. 为创建的用户账户指定访问模式和信息范围。为此，请在配置文件中添加下列行：

```
rouser <user name> priv -V monitoring
```

8. 要发送 SNMP 陷阱，请指定监控系统的 IP 地址和接收陷阱的用户凭证。为此，请在配置文件中添加下列行：

```
trapsess -Ci -v3 -t0.1 -r1 -l authPriv -u <用于接收陷阱的用户名> -a <身份验证算法> -A "<用于接收陷阱的用户密码>" -x
<加密算法> -X "<加密密码>" udp:<IP 地址>:162
```

snmpd 服务已配置。

要与多个监控系统集成，请为每个系统创建一个单独的用户账户，指定每个用户账户的可用信息范围（“view”和“rouser”指令），并配置 SNMP 陷阱的发送（“trapsess”指令）。

使用新配置启动 snmpd 服务

*应用新配置：*

1. 重新启动 snmpd 服务。

```
systemctl restart snmpd
```

2. 检查 snmpd 服务的状态：

```
systemctl status snmpd
```

状态必须是`running`。

3. 允许该服务在操作系统启动时自动启动：

```
systemctl enable snmpd
```

4. 如果您在操作系统或网络设备中使用防火墙，请添加规则以允许 SNMP 数据包通过。

snmpd 服务正在运行。

如果在配置 snmpd 服务时 klcssnmp 服务正在运行，则也需要重新启动 klcssnmp 服务。

检查 snmpd 服务的运行状况

要测试 snmpd 服务，请在 Kaspersky Security Center Linux 中配置 SNMP 的使用，并使用 snmpwalk 实用程序请求 SNMP 数据。

*要获取 Kaspersky Security Center Linux 提供的 SNMP 数据范围，*

运行以下命令：

```
snmpwalk -v3 -l authPriv -u <user name> -a <authentication algorithm> -A "<authentication password>" -x
<encryption algorithm> -X "<encryption password>" <IP address> .1.3.6.1.4.1.23668.1093.1
```

例如：

```
snmpwalk -v3 -l authPriv -u MonitoringUser -a SHA -A "MonitoringAuthSecret" -x AES -X "MonitoringPrivSecret"
127.0.0.1 .1.3.6.1.4.1.23668.1093.1
```

# 启用和禁用 SNMP 通知

Kaspersky Security Center Linux 以 SNMP 陷阱的形式发送有关管理服务器事件的通知。

默认情况下，Kaspersky Security Center Linux事件的 SNMP 通知被禁用。

*启用或禁用 Kaspersky Security Center Linux 事件的 SNMP 通知：*

1. 在主菜单中，单击管理服务器名称。
**管理服务器属性**窗口将打开。

2. 在属性窗口的**事件配置**选项卡上，单击要接收 SNMP 通知的事件类型。

3. 在打开的窗格中，启用或禁用**通过 SNMP 通知**切换开关。
   仅当启用**通过 SNMP 发送统计信息**选项时，此选项才可用。

根据您的选择，可以启用或禁用 Kaspersky Security Center Linux 事件的 SNMP 通知。

# 在 Kaspersky Security Center Linux 中启用和禁用 SNMP

默认情况下，已启用通过 SNMP 发送统计信息。要发送 SNMP 陷阱，请配置 snmpd 服务。

*启用或禁用通过 SNMP 发送统计信息：*

1. 在主菜单中，单击管理服务器名称。
   **管理服务器属性**窗口将打开。
2. 在**常规**选项卡上，选择**SNMP**区域。
3. 启用或禁用**通过 SNMP 发送统计信息**开关。
4. 单击“**保存**”。

根据您的选择，可以启用或者禁用通过 SNMP 发送统计信息。

# SNMP 的对象标识符的值

下表给出了用于将有关管理服务器性能的信息传输到第三方应用程序的对象标识符（也称为 OID）的值和说明。

用于 SNMP 的对象标识符的值和说明

| 对象标识符的值 | 数值数据类型 | OID | 描述 |
|---|---|---|---|
| deploymentStatus | INTEGER { ok(0), info(1), warning(2), critical(3) } | .1.3.6.1.4.1.23668.1093.1.1.1 | 部署状态。状态可以是以下之一：<br>• **信息**。授权许可不再对 N 个设备有效。<br>• **警告**。以下之一：<br>总共包含 N 台设备的管理服务器组中有 M 台设备安装了 Kaspersky 应用程序 (N > M)。<br>N 台设备上的授权许可 L 将在 M 天后到期。<br>N 台设备上的应用程序安装任务 T 已成功完成，M 台设备需要重新启动。<br>• **严重**。N 台设备的授权许可已过期。<br>• **正常**。以上都不是。 |
| noAntivirusSoftware | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.1.2.1 | deploymentStatus 显示管理服务器组包含了太多未安装受管理应用程序的设备。<br>如果发现几台设备未安装受管理应用程序，值等于 1，否则等于 0。 |
| remoteInstallTaskFailed | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.1.2.2 | deploymentStatus 显示某些设备上的远程安装任务失败。可以通过 hostsRemoteInstallFailed 获取这些设备的数量。 |
| licenceExpiring | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.1.2.3 | deploymentStatus 显示某些设备的授权许可在 7 天后到期。可以通过 hostsLicenseExpiring 获取这些设备的数量。 |
| licenceExpired | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.1.2.4 | deploymentStatus 显示某些设备的授权许可已过期。您可以通过 hostsLicenseExpired 获得这些设备的数量。 |
| hostsInGroups | Counter32 | .1.3.6.1.4.1.23668.1093.1.1.3 | 管理服务器组中的设备数。 |

| 对象标识符的值 | 数值数据类型 | OID | 描述 |
| --- | --- | --- | --- |
| hostsWithAntivirus | Counter32 | .1.3.6.1.4.1.23668.1093.1.1.4 | 安装了受管理应用程序的管理服务器组中的设备数。 |
| hostsRemoteInstallFailed | Counter32 | .1.3.6.1.4.1.23668.1093.1.1.5 | 远程安装任务失败的设备数。 |
| licenceExpiringSerial | OCTET STRING | .1.3.6.1.4.1.23668.1093.1.1.6 | 少于 7 天内过期的授权许可密钥的 ID。 |
| licenceExpiredSerial | OCTET STRING | .1.3.6.1.4.1.23668.1093.1.1.7 | 授权许可密钥已过期的 ID。 |
| licenceExpiringDays | Unsigned32 | .1.3.6.1.4.1.23668.1093.1.1.8 | 授权许可到期前的天数。对于此参数，如果距离到期日期还剩不到 7 天，则认为授权许可期限已到期。<br>如果距离到期日期还剩 7 天以上，则该值为 0。 |
| hostsLicenceExpiring | Counter32 | .1.3.6.1.4.1.23668.1093.1.1.9 | 授权许可在不到 7 天内过期的设备数。 |
| hostsLicenceExpired | Counter32 | .1.3.6.1.4.1.23668.1093.1.1.10 | 授权许可已到期的设备数。 |
| updatesStatus | INTEGER { ok(0), info(1), warning(2), critical(3) } | .1.3.6.1.4.1.23668.1093.1.2.1 | 反病毒库更新的当前状态。状态可以是以下之一：<br>• **信息**。管理服务器或设备上的反病毒库已超过 1 天未更新，应用程序安装后不到 1 天。<br>• **警告**。管理服务器或设备上的反病毒库已超过 3 天没有更新。该值可以在组设置中更改。<br>• **严重**。管理服务器或设备上的反病毒库已超过 7 天没有更新。该值可以在组设置中更改。<br>• **正常**。以上都不是。 |
| serverNotUpdated | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.2.2.1 | 管理服务器长时间未更新。被认为是长时间的时间量在 updatesStatus 中指定。 |
| notUpdatedHosts | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.2.2.2 | 某些设备很长时间没有更新（对于**严重**，默认为 7 天或更长时间，对于**警告**为 3 天）。您可以通过 hostsNotUpdated 获得这些设备的数量。 |
| lastServerUpdateTime | Hex-STRING | .1.3.6.1.4.1.23668.1093.1.2.3 | 管理服务器上次更新反病毒库的时间。 |
| hostsNotUpdated | Counter32 | .1.3.6.1.4.1.23668.1093.1.2.4 | 包含长期未更新的防病毒库的设备数量（默认情况下，对于**严重**为 7 天或更长时间，对于**警告**为 3 天）。如果有设备处于**严重**更新状态，则仅计算这些设备。您可以通过 updatesStatus 获取更新状态。 |
| protectionStatus | INTEGER { ok(0), warning(2), critical(3) } | .1.3.6.1.4.1.23668.1093.1.3.1 | 实时保护的状态。以下之一：<br>• **警告**。以下之一：<br>在属于管理服务器组的设备上检测到安全漏洞。<br>加密错误使某些设备更改了保护状态。<br>长时间未执行全盘扫描。<br>• **严重**。反病毒保护在管理服务器组中的某些设备上不起作用。<br>• **正常**。以上都不是。 |
| antivirusNotRunning | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.3.2.1 | 某些设备上未运行安全应用程序。您可以通过 hostsAntivirusNotRunning 获得这些设备的数量。 |
| realtimeNotRunning | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.3.2.2 | 某些设备上未运行实时保护。您可以通过 hostsRealtimeNotRunning 获取这些设备的数量。 |
| psRealtimeLevelChanged | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.3.2.3 | 运行时保护级别与管理员在管理组中 N 台计算机上设置的级别不同。 |
| notCuredFound | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.3.2.4 | 某些设备包含未解毒对象。您可以通过 hostsNotCuredObject 获得这些设备的数量。 |
| tooManyThreats | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.3.2.5 | 某些设备上发现威胁。您可以通过 hostsTooManyThreats 获得这些设备的数量。 |
| virusOutbreak | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.3.2.6 | 系统的病毒爆发状态。<br>如果在一定时间内发现一定数量的病毒，则该值等于 1，否则等于 0。通过使用“病毒攻击”设置，在管理服务器上指定病毒数量和时间量。 |
| psVulnerabilitiesFound | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.3.2.7 | 检测到漏洞。 |

| 对象标识符的值 | 数值数据类型 | OID | 描述 |
| --- | --- | --- | --- |
| psEncryptionFaultsFound | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.3.2.8 | 检测到导致设备保护状态发生变化的加密错误。 |
| psVulnerableHostsFound | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.3.2.9 | 某些设备上检测到漏洞。 |
| psNotScannedLately | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.3.2.10 | 检测到长时间未进行全盘扫描的设备。 |
| psNagentsNotRunningUntilReboot | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.3.2.11 | 检测到网络代理仅在重启后才启动的设备。 |
| hostsAntivirusNotRunning | Counter32 | .1.3.6.1.4.1.23668.1093.1.3.3 | 安全应用程序未运行的设备数。 |
| hostsRealtimeNotRunning | Counter32 | .1.3.6.1.4.1.23668.1093.1.3.4 | 未运行实时保护的设备数。 |
| hostsRealtimeLevelChanged | Counter32 | .1.3.6.1.4.1.23668.1093.1.3.5 | 实时保护级别不可接受的设备数。 |
| hostsNotCuredObject | Counter32 | .1.3.6.1.4.1.23668.1093.1.3.6 | 包含未消除对象的设备数。 |
| hostsTooManyThreats | Counter32 | .1.3.6.1.4.1.23668.1093.1.3.7 | 包含威胁的设备数。 |
| fullscanStatus | INTEGER { ok(0), info(1), warning(2), critical(3) } | .1.3.6.1.4.1.23668.1093.1.4.1 | 防病毒全盘扫描状态为以下之一：<br>• **信息**。自安装应用程序以来，经过的时间不到 7 天。<br>• **警告**。自安装应用程序以来，超过 7 天未执行反病毒全盘扫描。<br>• **严重**。自安装应用程序以来，超过 14 天未执行反病毒全盘扫描。<br>• **正常**。以上都不是。 |
| notScannedLately | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.4.2.1 | 某些设备一定时间内未进行扫描。您可以通过 hostsNotScannedLately 获得这些设备的数量。时间量在 fullScanStatus 中 指定。 |
| hostsNotScannedLately | Counter32 | .1.3.6.1.4.1.23668.1093.1.4.3 | 一定时间内未扫描的设备数。时间量在 fullScanStatus 中 指定。 |
| logicalNetworkStatus | INTEGER { ok(0), warning(1), critical(2) } | .1.3.6.1.4.1.23668.1093.1.5.1 | 管理服务器逻辑网络的状态。以下之一：<br>• **警告**。如果存在无法访问的处于警告状态的设备，或者存在不属于任何管理服务器组的设备。<br>• **严重**。如果管理服务器已失去某些设备的控制权，或者存在无法访问的处于严重状态的设备。<br>• **正常**。以上都不是。 |
| notConnectedLongTime | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.5.2.1 | 某些设备很长时间未连接到管理服务器（**警告**状态的设备为 7 天或更长，而**严重**状态的设备为 4 天）。您可以通过 hostsNotConnectedLongTime 获得这些设备的数量。 |
| controlLost | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.5.2.2 | 管理服务器已失去某些设备的控制权。您可以通过 hostsControlLost 获得这些设备的数量。 |
| hostsFound | Counter32 | .1.3.6.1.4.1.23668.1093.1.5.3 | 管理服务器发现的不属于任何管理服务器组的设备数。 |
| groupsCount | Counter32 | .1.3.6.1.4.1.23668.1093.1.5.4 | 管理服务器上的组数量。 |
| hostsNotConnectedLongTime | Counter32 | .1.3.6.1.4.1.23668.1093.1.5.5 | 长时间未连接到管理服务器的设备数。被认为是长时间的时间量在 notConnectedLongTime 中指定。 |
| hostsControlLost | Counter32 | .1.3.6.1.4.1.23668.1093.1.5.6 | 不受管理服务器控制的设备数。 |

| 对象标识符的值 | 数值数据类型 | OID | 描述 |
| --- | --- | --- | --- |
| eventsStatus | INTEGER { ok(0), info(1), warning(2), critical(3) } | .1.3.6.1.4.1.23668.1093.1.6.1 | 事件子系统状态为以下之一：<br>• **警告**。以下之一：<br>管理服务器组的设备长时间未搜索 Windows 更新。<br>有些设备的状态出现问题。<br>• **严重**。以下之一：<br>至少一台设备上存在“严重”事件。<br>至少一台设备上存在“错误”事件。<br>至少一台设备上存在任务未成功完成的事件。<br>管理服务器组的设备长时间未搜索 Windows 更新。<br>有些设备的状态出现问题。<br>• **信息。**以下之一：<br>所有设备上次进行病毒全盘扫描至今不足一周。<br>远程安装任务已完成，无需重启任何设备。<br>上次管理服务器更新至今不足一周。<br>管理服务器长时间未更新，但目前正在进行更新。<br>• **正常**。以上都不是。 |
| criticalEventOccured | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.6.2.1 | eventsStatus 显示管理服务器上存在一些严重事件。您可以通过 criticalEventsCount 获得这些事件的数量。<br>如果任何设备上存在至少一个严重事件，则该值等于 1，否则等于 0。 |
| criticalEventsCount | Counter32 | .1.3.6.1.4.1.23668.1093.1.6.3 | 管理服务器上的严重事件数。 |

# 在 Kaspersky Next XDR Optimum 授权许可下使用 Kaspersky Security Center Linux

如果您购买了 Kaspersky Next XDR Optimum 授权许可作为 EPP 应用程序授权许可和 Kaspersky Security Center Linux 授权许可的一部分，则在执行初始设置后，您将能够使用 Kaspersky Next XDR Optimum 功能。

如果您在设备上安装并激活卡巴斯基应用程序后，单独购买了 Kaspersky Next XDR Optimum 授权许可作为之前购买的授权许可的扩展，则必须使用新的激活码或密钥文件在设备上重新激活 Kaspersky Security Center Linux，具体取决于您购买 Kaspersky Next XDR Optimum 授权许可的方式。之后，您可以执行初始设置。

此外，您还可以在测试模式下使用 Kaspersky Next XDR Optimum 的功能。为此，您必须首先添加一个从属物理管理服务器，然后在 Kaspersky Next XDR Optimum 试用授权许可下激活此服务器。在试用授权许可的期限内，Kaspersky Next XDR Optimum 功能将在从属服务器上可用。

在您在 Kaspersky Next XDR Optimum 授权许可下激活管理服务器并将授权许可密钥部署到相关管理服务器管理的设备上之后，您可以执行以下操作：

- 通过使用与Kaspersky Automated Security Awareness Platform、Kaspersky Threat Intelligence Portal Sandbox 和Active Directory进行集成来响应威胁。
- 按属性对警报进行分组。

有关 Kaspersky Next XDR Optimum 授权许可启用的功能的更多信息，请参阅Kaspersky Endpoint Detection and Response Optimum 帮助。

# 用于响应警报的集成

如果您拥有 Kaspersky Next XDR Optimum 授权许可，则可以配置与以下解决方案的集成以响应威胁：

- Kaspersky Automated Security Awareness Platform
- Kaspersky Threat Intelligence Portal Sandbox
- 活动目录

如果您已在 Kaspersky Next XDR Optimum 授权许可下激活管理服务器，则可以使用这些集成。
要执行响应操作，您必须将 Kaspersky Next XDR Optimum 授权许可密钥部署到您的受管理应用程序。
在试用授权许可下使用 Kaspersky Next XDR Optimum 时，您必须先添加从属物理管理服务器，在试用授权许可下激活此从属管理服务器，然后将授权许可密钥部署到由此管理服务器管理的设备上。

如果您使用的是 Kaspersky Next EDR Optimum 授权许可，则无需激活在 Kaspersky Next XDR Optimum 授权许可下安装在受管理设备上的应用程序。您仅需对新设备（如有）执行此操作。

由于 Kaspersky Next XDR Optimum 授权许可支持多租户，因此您可以将授权许可密钥集中分发到受管理的应用程序上。不支持将授权许可自动分发到从属和虚拟管理服务器。

要配置集成，您必须具有**常规功能：应用程序集成**功能区域的**读取**和**写入**权限。

# 配置与 Active Directory 的集成以执行响应操作

与 Active Directory 集成使您能够对受到警报影响或涉及警报的 Active Directory 用户执行响应操作。

要配置与 Active Directory 的集成以响应警报，您必须使用 Kaspersky Security Center Linux 管理服务器 15.4 或更高版本。

与 Active Directory 集成以响应警报，以及在配置域控制器轮询时指定的 Active Directory 域控制器（域控制器的地址和用户凭证）扫描设置是两种不同设置。由于您需要确保要为其执行响应操作的用户拥有 Active Directory 账户，因此您必须配置这两个集成：用于扫描和用于响应。顺序不重要。

集成设置不会被继承，并且仅适用于您在其上配置这些设置的管理服务器（物理或虚拟）。

*要配置与 Active Directory 的集成以响应警报：*

1. 在主菜单中，单击管理服务器名称。

   管理服务器属性窗口打开，**常规**选项卡被选中。

2. 执行以下操作之一：

   - 选择**分发点**部分，单击所需分发点的名称，然后在打开的属性窗口中选择**Active Directory**部分。
   - 选择“**Active Directory 响应**”部分。

3. 在右侧窗格中，启用**Active Directory 整合**切换开关。

   稍后，如果想关闭集成，您只能通过禁用**Active Directory 整合**切换开关对所有连接执行此操作。您无法关闭单独连接的集成。相反，您可以删除该连接。

   > 当您启用或禁用“**Active Directory 整合**”切换开关时，该设置将应用于“**Active Directory 响应**”和“**分发点**”部分。

4. 通过单击“**添加**”按钮，创建与 Active Directory 域控制器的连接。

5. 在打开的窗口中，指定连接的以下参数：

   - **域控制器地址**

     计算机名称，例如：`server.mycompany.com`。

     您可以指定多个地址。您指定地址的所有域控制器必须属于同一个域。

   - **Active Directory 域名**

     DNS 完全限定域名，例如：`mycompany.com`

     另外，您可以指定 SAM 或 NetBIOS 名称，例如：`mycompany`

     使用小写字母。如果为管理服务器或分发点创建多个连接，请为每个连接指定不同名称。

     > 要执行响应操作，您在此字段中指定的 Active Directory 域名必须与警报中指定的 Active Directory 域名匹配。

- **登录名**

  具有管理员权限的 Active Directory 账户的登录名，响应操作在该账户下执行。

- **密码**

  具有管理员权限的 Active Directory 账户的密码，响应操作在该账户下执行。

6. 如果要检查连接状态，请单击“**检查连接**”按钮。

   如果连接成功建立，则显示“**已连接**”状态。否则，状态为“**失败**”，并显示一条错误消息，其中包含您未能连接的域控制器。

> 您必须考虑连接 Active Directory 的方式：**从Linux 设备还是从 Windows 设备**。

从 Linux 设备连接

默认情况下，从 Linux 设备连接并验证域控制器时，逻辑如下：

1. 管理服务器或分发点尝试通过 LDAPS 连接到域控制器。

   执行严格验证 LDAP 服务器证书。

2. 将域控制器证书的公共部分放入系统证书存储库以验证证书。

   使用与操作系统相关的系统证书颁发机构 (CA) 路径来访问证书链。

   例如：

   - /etc/ssl/certs/ca-certificates.crt — 基于 Debian 的操作系统 (Debian、Ubuntu、Astra) 的路径。
   - /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem — CentOS 或 Red Hat 的路径。

3. 如果 LDAPS 连接失败，则会发生错误，不会使用其他连接协议。

> 如果出现 LDAPS 问题，您可以联系卡巴斯基技术支持。

如果您不想将证书安装到系统证书存储库中，可以使用 KLNAG_LDAP_SSL_CACERT 标志来设置域控制器证书的路径。为此，请运行以下命令：

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "</path/to/domain-controller/cert>"
```

其中`</path/to/domain-controller/cert>`是域控制器证书公共部分的路径。

例如，如果路径是`"/var/opt/kaspersky/ldap_cert.crt"`，则命令为`klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "/var/opt/kaspersky/ldap_cert.crt"`

从 Windows 设备连接

从 Windows 设备连接并验证域控制器时，连接设置由域定义。

您只需确保：

- LDAPS 已启用并且设备上的端口 636 可用。
- 您允许通过防火墙或代理服务器连接到域控制器。

7. 单击“**保存**”按钮。

窗口关闭，连接显示在连接表中。

在连接表中，您可以执行以下操作：

- 编辑连接参数。
  为此，请单击所需连接的**域控制器地址**参数的链接。在打开的窗口中，更改所需设置，然后单击“**保存**”按钮。
  您只能编辑**登录名** 和**密码** 参数。
- 删除连接。
  为此，请选中要删除的连接旁边的复选框，单击工具栏中的“**移除**”按钮，然后确认删除连接。

# 配置与 Kaspersky Automated Security Awareness Platform 的集成

与Kaspersky Automated Security Awareness Platform（以下也称为 KASAP）集成使您能够分配 KASAP 学习课程给与警报相关的用户。

集成设置不会被继承，并且仅适用于您在其上配置这些设置的管理服务器（物理或虚拟）。

在 Kaspersky Security Center Web Console 中配置集成之前，您必须在 KASAP 中创建授权令牌并获取 API 请求的 URL。

*要配置与 Kaspersky Automated Security Awareness Platform 的集成：*

1. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口打开，**常规**选项卡被选中。
2. 选择“**KASAP**”部分。
3. 在右侧窗格中，启用**KASAP 整合**切换开关。
4. 指定用于连接 KASAP 的设置：
   - **API 令牌**— 您创建的用于访问 KASAP Open API 的令牌。
   - **网址** — 创建 API令牌时获取的 API 请求的 URL。
   - **使用代理服务器**— 可在连接到 KASAP 时启用代理服务器的切换开关。
     默认情况下已禁用切换开关。

5. 如有必要，请单击**检查连接**按钮来验证您指定的设置。
   连接状态已显示。

6. 单击“**保存**”按钮。

已配置与 Kaspersky Automated Security Awareness Platform 的集成。

保存 KASAP 集成设置后，您可以单击**查看组**按钮查看 KASAP 学习组列表。

如果需要，当组列表显示时，您可以通过单击**刷新组**按钮来更新它。

> 打开列表后，您将无法隐藏它。如果禁用**KASAP 整合**切换开关，则不会显示 KASAP 组列表。

# 配置与 Kaspersky Threat Intelligence Portal Sandbox 的集成

与Kaspersky Threat Intelligence Portal（以下也称为Kaspersky TIP）集成可让您使用**Kaspersky Sandbox隔离**隔离区的文件。

集成设置不会被继承，并且仅适用于您在其上配置这些设置的管理服务器（物理或虚拟）。

> 在配置集成之前，您必须获取 Kaspersky TIP 上 API 请求的授权令牌。

*要配置与 Kaspersky TIP Sandbox 的集成：*

1. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口打开，**常规**选项卡被选中。

2. 选择 **Kaspersky TIP**。

3. 在右侧窗格中，启用**整合**切换开关。
   与 Kaspersky TIP 的连接设置将显示。

   > 如果在配置并保存集成设置后禁用**整合** 拨动开关，则设置不会被删除，但您将无法执行响应操作。

4. 单击**添加令牌**按钮，在打开的窗口中，指定您之前在 Kaspersky TIP 上获取的令牌，然后单击**添加** 按钮。
   窗口关闭，API 令牌已添加。

5. 如果您想在连接到 Kaspersky TIP 时使用代理服务器，请启用**使用代理服务器**切换开关。
   默认情况下已禁用切换开关。

6. 单击“**保存**”按钮。

已配置与 Kaspersky TIP Sandbox 的集成。

现在，您可以将文件从 **隔离** 部分发送到 Kaspersky TIP Kaspersky Sandbox进行威胁分析。文件大小上限为 100 MB。

由于 Kaspersky Next XDR Optimum 授权许可支持多租户，因此放置在**隔离区隔离** 由租户划分。如果管理员使用专用的 TIP 账户和与每个租户相关的 API 令牌，则这种租户级别的分离也适用于将文件发送到 Kaspersky TIP Sandbox 并查看结果时。但是，由于隔离列表不根据服务器层次结构显示对象，因此无法集中管理所有租户的**隔离**部分。

# 按属性分组警报

警报聚合有助于识别可能与同一事故相关的警报，从而简化调查过程。

要启用警报聚合功能，您必须执行以下操作：

- 在主菜单中启用**警报**子部分。
- 在 Kaspersky Next XDR Optimum 授权许可下激活管理服务器，然后将 Kaspersky Next XDR Optimum 授权许可密钥部署到您的受管理应用程序。

  在测试模式下使用试用版授权许可的 Kaspersky Next XDR Optimum 功能时，您必须首先添加从属物理管理服务器，然后在此授权许可下激活该服务器。

如果您使用的是 Kaspersky Next EDR Optimum 授权许可，则无需激活在 Kaspersky Next XDR Optimum 授权许可下安装在受管理设备上的应用程序。您仅需对新设备（如有）执行此操作。
由于 Kaspersky Next XDR Optimum 授权许可支持多租户，因此您可以将授权许可密钥集中分发到受管理的应用程序上。不支持将授权许可自动分发到从属和虚拟管理服务器。

您可以按设备名称、账户或哈希名称（SHA256）聚合警报。

> 仅当属性不为空时，警报才会根据该属性聚合。

如果警报至少共享一个属性，并且在组中任何其他警报的 24 小时内发生，则这些警报会聚合在一起。

*要按属性聚合警报：*

1. 在主菜单中，转到**监控 → 警报**。
2. 执行以下操作之一：
   - 启用 **警报聚合** 切换开关，然后选择一个或多个属性来聚合警报：
     - **设备名称**
     - **账户**
     - **文件哈希**哈希名称 （SHA256）

     默认情况下选择**设备名称** 和 **账户**属性。
   - 单击设置图标（⚙）。在打开的**表格设置**窗格中，转到 **分组** 选项卡。选择 **聚合组 ID** 并单击 **应用**。

启用聚合后，警报将按**事件时间**从最新到最旧进行排序。不支持其他排序选项。选择不同的选项组将禁用聚合。

该表显示按属性聚合的警报。未聚合的警报显示在表格底部。

聚合后，每个警报仅被分配给一个组。

# Kaspersky Security Center 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 Web Console 访问其他 Kaspersky 应用程序，例如 Kaspersky Managed Detection and Response。此部分还介绍了如何配置导出到 SIEM 系统。

## 建立后台连接

要配置 Kaspersky Security Center Linux 与其他卡巴斯基应用程序或解决方案（例如 Kaspersky Managed Detection and Response（也称为 MDR））之间的交互，必须在 Kaspersky Security Center Web Console 与管理服务器之间建立后台连接。仅当您的账户在“**常规功能：用户权限**”功能区域中拥有“修改对象 ACL”权限时，才能建立此连接。

您只能配置 Kaspersky Managed Detection and Response 与基于 Windows 的 Kaspersky Security Center 版本之间的交互。

*要建立后台连接：*

1. 在主菜单中，转到“**设置** → **整合**”。
2. 选择**Web Console 代理服务器设置**选项卡。
3. 在**整合**区域，将用于建立后台连接的切换按钮切换到位置：**用于整合的后台连接 已启用**。
4. 在打开的“**启用后台连接**”区域中，单击“**确定**”按钮。

即在 Kaspersky Security Center Web Console 与管理服务器之间建立后台连接。管理服务器会为后台连接创建一个账户，该账户用作服务账户以维护 Kaspersky Security Center Linux 与其他 Kaspersky 应用程序或解决方案之间的交互。该服务账户的名称包含 NWCSvcUser 前缀。出于安全原因，管理服务器每 30 天自动更改一次服务账户的密码。您不能手动删除服务账户。当禁用跨服务连接时，管理服务器会自动删除此账户。管理服务器为每个 Kaspersky Security Center Web Console 和管理控制台都创建一个服务账户，并将所有服务账户分配到名称为 ServiceNwcGroup 的安全组。在 Kaspersky Security Center Linux 安装过程中，管理服务器会自动创建此安全组。您不能手动删除此安全组。

## 配置代理服务器连接

*要为 Kaspersky Security Center Web Console 和 Web 插件配置代理服务器连接：*

1. 在主菜单中，转到“**设置** → **整合**”。
2. 选择**Web Console 代理服务器设置**选项卡。
3. 启用**使用代理服务器**选项。

4. 指定代理服务器连接设置：

- **代理服务器地址**
- **端口号**
- **代理服务器身份验证**
- **用户名**（如果启用**代理服务器身份验证**选项则需要）
- **密码**（如果启用**代理服务器身份验证**选项则需要）

5. 单击**保存**以保存代理服务器连接设置。

如果您有多层管理服务器，代理服务器连接设置不会被传输到用于管理从属管理服务器的 Web Console。您必须为每个 Kaspersky Security Center Web Console 单独配置代理服务器连接。

# 客户端设备的远程诊断

您可以使用远程诊断在 Windows 和 Linux客户端设备上远程执行以下操作：

- 启用和禁用跟踪、更改跟踪等级、下载跟踪文件
- 下载系统信息和应用程序设置
- 下载事件日志
- 为应用程序创建内存转储文件
- 开始诊断并下载诊断报告
- 开始、停止和重新启动应用程序

您可以使用从客户端设备下载的事件日志和诊断报告以自行定位问题。此外，如果您联系 Kaspersky 技术支持，一名技术支持专家可能让您从客户端设备下载跟踪文件、转储文件、事件日志和诊断报告以便让 Kaspersky 进一步分析。

# 打开远程诊断窗口

要对 Windows 和 Linux 客户端设备执行远程诊断，首先必须打开远程诊断窗口。

*要打开远程诊断窗口：*

1. 要选择要为其打开远程诊断窗口的设备，请执行以下操作之一：
   - 如果该设备属于管理组，请在主菜单中转到**资产管理 → 资产(设备)**。
   - 如果该设备属于未分配的设备群组，请在主菜单中，前往**资产管理 → 未分配的设备**。
2. 单击所需设备的名称。
3. 在打开的设备属性窗口中，选择“**高级**”选项卡。
4. 在“**高级**”选项卡上，单击“**远程诊断**”。
   这将打开客户端设备的“**远程诊断**”窗口。如果管理服务器和客户端设备之间未建立连接，则会显示错误消息。

或者，如果需要立即获取有关基于 Linux 的客户端设备的所有诊断信息，您可以在此设备上运行 collect.sh 脚本。

# 启用和禁用应用程序跟踪

您可以启用和禁用应用程序跟踪，包括 Xperf 跟踪。

## 启用和禁用跟踪

*要在远程设备上启用或禁用跟踪：*

1. 打开客户端设备的远程诊断窗口。
2. 在远程诊断窗口中，选择**卡巴斯基应用程序**选项卡。
   “**应用程序管理**”区域会显示设备上安装的卡巴斯基应用程序列表。
3. 在应用程序列表中，选择您要启用或禁用跟踪的应用程序。
   远程诊断选项列表将打开。
4. 如果要启用跟踪：
   a. 在列表的“**跟踪**”区域中，单击“**启用跟踪**”。
   b. 在打开的“**修改跟踪级别**”窗口中，我们建议您保留设置的默认值。当需要时，技术支持专家将指导您配置过程。下列设置可用：
      - **跟踪级别**

        跟踪级别定义跟踪文件包含的详情数据量。
      - **基于循环的跟踪**

        应用程序覆盖跟踪信息以防止跟踪文件过量增长。指定用于存储跟踪信息的文件最大数量，以及每个文件的最大大小。如果写入了最大数量的最大大小的跟踪文件，最旧的文件被删除以便新跟踪文件可以被写入。

        此设置仅适用于 Kaspersky Endpoint Security。
   c. 单击“**保存**”。

   将为所选应用程序启用跟踪。某些情况下，要启用跟踪，必须重新启动安全应用程序及其任务。

   > 在 Linux 客户端设备上，网络代理组件更新程序的跟踪由网络代理设置管理。因此，在运行 Linux 的客户端设备上，此组件的“**启用跟踪**”和“**修改跟踪级别**”选项被禁用。

5. 如果要禁用对所选应用程序的跟踪，请单击“**禁用跟踪**”按钮。
   对所选应用程序的跟踪即被禁用。

## 启用 Xperf 跟踪

对于 Kaspersky Endpoint Security，技术支持专家可能要求您对系统性能信息启用 Xperf 跟踪。

*要启用和配置 Xperf 跟踪或禁用它：*

1. 打开客户端设备的远程诊断窗口。
2. 在远程诊断窗口中，选择**卡巴斯基应用程序**选项卡。

   **应用程序管理**区域会显示设备上安装的卡巴斯基应用程序列表。
3. 在应用程序列表中，选择“Kaspersky Endpoint Security for Windows”。

   Kaspersky Endpoint Security for Windows 的远程诊断选项列表将显示。
4. 在“**Xpref 跟踪**”区域中，单击“**启用 Xperf 跟踪**”。

   如果已经启用 Xperf 跟踪，将显示“**禁用 Xperf 跟踪**”按钮。如果您想要禁用 Kaspersky Endpoint Security for Windows的 Xperf 跟踪，请单击此按钮。
5. 在打开的“**更改 Xperf 跟踪级别**”窗口中，根据技术支持专家的请求，执行以下操作：

   a. 选择以下跟踪级别之一：

   - **轻度级别**

     该类型的跟踪文件包含系统最少量信息。

     默认情况下已选定该选项。

   - **深度级别**

     相比于*轻度*类型的跟踪文件，该类型的跟踪文件包含更多详细信息，且可能在*轻度*类型跟踪文件不足以评估性能时被技术支持专家要求。*深度*跟踪文件包含关于系统的硬件、操作系统、应用程序的启动和结束进程列表、用于性能评估的事件和来自 Windows System Assessment 工具的事件的技术信息。

   b. 选择以下 Xperf 跟踪类型之一：

   - **基本类型**

     跟踪信息在 Kaspersky Endpoint Security 应用程序运行期间被接收。

     默认情况下已选定该选项。

   - **重启时类型**

     跟踪信息在操作系统从受管理设备上启动时接收。该跟踪类型在影响系统性能的问题发生时，在设备被开启后和 Kaspersky Endpoint Security 启动之前有效。

   您可能被要求启用“**循环文件大小(MB)**”选项以防止跟踪文件的过量增长。然后指定跟踪文件的最大大小。当文件达到最大大小时，最旧的跟踪信息被新信息覆盖。

   c. 定义循环文件大小。

   d. 点击“**保存**”。

   将启用并配置 Xperf 跟踪。
6. 如果您想要禁用 Kaspersky Endpoint Security for Windows的 Xperf 跟踪，请单击“**Xpref 跟踪**”区域中的“**禁用 Xperf 跟踪**”。

   Xperf 跟踪即被禁用。

# 下载应用程序的跟踪文件

*要下载应用程序的跟踪文件：*

1. 打开客户端设备的远程诊断窗口。
2. 在远程诊断窗口中，选择**卡巴斯基应用程序**选项卡。
   **应用程序管理**区域会显示设备上安装的卡巴斯基应用程序列表。
3. 在应用程序列表中，选择要为其下载跟踪文件的应用程序。
4. 在“**跟踪**”区域，单击“**跟踪文件**”按钮。
   这将打开“**设备跟踪日志**”窗口，其中显示了跟踪文件列表。
5. 在跟踪文件列表中，选择要下载的文件。
6. 执行以下操作之一：
   - 单击“**下载**”下载所选文件。您可以选择一个或多个文件进行下载。
   - 下载所选文件的一部分：
     a. 单击“**下载一部分**”。
        您无法同时下载多个文件的部分内容。如果您选择多个跟踪文件，**下载一部分**按钮将被禁用。
     b. 在打开的窗口中，根据需要指定名称和要下载的文件部分。
        对于 Linux 设备，无法编辑文件部分名称。
     c. 单击“**下载**”。

所选文件或其一部分将下载到您指定的位置。

# 删除跟踪文件

您可以删除不再需要的跟踪文件。

*要删除跟踪文件：*

1. 打开客户端设备的远程诊断窗口。
2. 在打开的远程诊断窗口中，选择“**事件日志**”选项卡。
3. 在“**跟踪文件**”区域中，单击“**Windows Update 日志**”或“**远程安装日志**”，具体取决于要删除哪些跟踪文件。

   **Windows Update 日志**链接仅适用于基于 Windows 的客户端设备。

   这将打开“**设备跟踪日志**”窗口，其中显示了跟踪文件列表。

4. 在跟踪文件列表中，选择一个或多个要删除的文件。
5. 单击“**删除**”按钮。

所选跟踪文件即被删除。

# 下载应用程序设置

*要从客户端设备下载应用程序设置：*

1. 打开客户端设备的远程诊断窗口。
2. 在远程诊断窗口中，选择**卡巴斯基应用程序**选项卡。
3. 在“**应用程序设置**”区域中，单击“**下载**”按钮下载有关客户端设备上安装的应用程序的设置的信息。

包含信息的 ZIP 存档将被下载到指定位置。

# 从客户端设备下载系统信息

*要从客户端设备下载系统信息：*

1. 打开客户端设备的远程诊断窗口。
2. 在远程诊断窗口中，选择**系统信息**选项卡。
3. 单击“**下载**”按钮可下载有关客户端设备的系统信息。
   如果您获取有关 Linux 设备的系统信息，紧急终止应用程序的转储文件将被添加到结果文件中。

   该压缩文件可能包含明文形式的敏感数据（例如，密钥和密码）。建议您在将压缩文件发送给卡巴斯基技术支持之前，检查压缩文件中的文件并移除此类数据。

包含信息的文件将被下载到指定位置。

# 下载事件日志

*要从远程设备下载事件日志：*

1. 打开客户端设备的远程诊断窗口。
2. 在远程诊断窗口的“**事件日志**”选项卡上，单击“**所有设备日志**”。
3. 在“**所有设备日志**”窗口中，选择一个或多个相关日志。

4. 执行以下操作之一：

- 单击“**下载整个文件**”下载所选日志。
- 下载所选日志的一部分：

  a. 单击“**下载一部分**”。
  您无法同时下载多个日志的部分内容。如果您选择了多个事件日志，**下载一部分**按钮将被禁用。

  b. 在打开的窗口中，根据需要指定名称和要下载的文件部分。
  对于 Linux 设备，无法编辑日志部分名称。

  c. 单击“**下载**”。

所选事件日志或其一部分将被下载到指定的位置。

# 启动、停止和重新启动应用程序

您可以启动、停止和重新启动客户端设备上的应用程序。

*若要启动、停止和重新启动应用程序，请执行以下操作：*

1. 打开客户端设备的远程诊断窗口。
2. 在远程诊断窗口中，选择**卡巴斯基应用程序**选项卡。
**应用程序管理**区域会显示设备上安装的卡巴斯基应用程序列表。
3. 在应用程序列表中，选择要启动、停止或重新启动的应用程序。
4. 单击以下按钮之一来选择操作：

- **停止应用程序**
  仅当应用程序当前正在运行时，此按钮才可用。
- **重启应用程序**
  仅当应用程序当前正在运行时，此按钮才可用。
- **启动应用程序**
  仅当应用程序当前未运行时，此按钮才可用。

根据您选择的操作，客户端设备上将启动、停止或重新启动所需应用程序。

如果重新启动网络代理，将显示一条消息，指示设备与管理服务器的当前连接将丢失。

# 运行 Kaspersky Security Center Linux 网络代理的远程诊断并下载结果

*要在远程设备上启动 Kaspersky Security Center Linux 网络代理的诊断并下载结果：*

1. 打开客户端设备的远程诊断窗口。
2. 在远程诊断窗口中，选择**卡巴斯基应用程序**选项卡。
   **应用程序管理**区域会显示设备上安装的卡巴斯基应用程序列表。
3. 在应用程序列表中，选择**Kaspersky Security Center Linux 网络代理**。
   远程诊断选项列表将打开。
4. 在“**诊断报告**”部分中，单击“**运行诊断**”按钮。
   这将启动远程诊断过程并生成诊断报告。诊断过程完成后，“**下载诊断报告**”按钮变为可用。
5. 单击“**下载诊断报告**”按钮下载报告。

报告将被下载到指定位置。

# 在客户端设备上运行应用程序

如果 Kaspersky 支持专家要求，您可能需要在客户端设备上运行应用程序。您不必在该设备上安装应用程序。

如果想在客户端设备上运行自定义脚本，您可以使用`KLACDT_SAVE_SETTING`环境变量来确定保存执行结果的路径。例如：

- 对于基于 Windows 的设备：
  ```
  @echo some result > %KLACDT_SAVE_SETTING%\res.log
  ```
- 对于基于 Linux 的设备：
  ```
  [[echo some result > $KLACDT_SAVE_SETTING/res.log
  ```

*要在客户端设备上运行应用程序：*

1. 打开客户端设备的远程诊断窗口。
2. 在远程诊断窗口中，选择**运行远程应用程序**选项卡。
3. 在**对象类型**字段中，选择要上传的对象类型：
   - 选择**文件**来上传可执行文件。
   - 选择**文件夹**以上传包含要在客户端设备上运行的应用程序的文件夹。
     如果选择此对象类型，则会出现**要运行的可执行文件的名称**字段。在此字段中，指定文件夹中可执行文件的名称。您还可以指定文件的相对路径。

- 选择**存档**上传包含要在客户端设备上运行的应用程序的 ZIP 存档。

  如果选择此对象类型，则会出现**要运行的可执行文件的名称**字段。在此字段中，指定文件夹中可执行文件的名称。您还可以指定文件的相对路径。

  > ZIP 存档必须包含实用程序文件夹。此文件夹包含要在远程设备上运行的可执行文件。

4. 通过在系统窗口中选择对象或将其拖到上传字段来上传对象。
5. 如果需要，在**命令行参数**字段中指定运行可执行文件时要传递的命令行参数。
6. 单击**上传和运行**按钮以在客户端设备上运行选定的应用程序。
7. 应用程序执行成功完成后，单击**下载应用程序执行结果**按钮下载执行结果。

> 应用程序执行结果将保存，直到您运行新的诊断或关闭窗口为止。

使用该应用程序对客户端设备进行远程诊断已完成。

# 在基于 Linux 的客户端设备上运行远程诊断

Kaspersky Security Center Linux 允许您从客户端设备下载基本诊断信息。或者，您可以使用卡巴斯基的 collect.sh 脚本获取有关基于Linux 的设备的诊断信息。该脚本在需要诊断的 Linux 客户端设备上运行，然后生成一个文件，其中包含诊断信息、该设备的系统信息、应用程序的跟踪文件、设备日志以及被紧急终止的应用程序的转储文件。

> 我们建议您使用 collect.sh 脚本一次性获取有关 Linux 客户端设备的所有诊断信息。如果通过 Kaspersky Security Center Linux 远程下载诊断信息，您将需要浏览远程诊断界面的所有部分。此外，可能无法完全获得 Linux 设备的诊断信息。

> 如果您需要将生成的包含诊断信息的文件发送给卡巴斯基技术支持，请在发送文件之前删除所有机密信息。

*要使用 collect.sh 脚本从 Linux 客户端设备下载诊断信息：*

1. 下载 collect.sh 脚本，它在collect.tar.gz 存档中。
2. 将下载的压缩包复制到需要诊断的 Linux 客户端设备上。
3. 运行以下命令解压 collect.tar.gz 存档：

   ```
   # tar -xzf collect.tar.gz
   ```

4. 执行以下命令指定脚本执行权限：

   ```
   # chmod +x collect.sh
   ```

5. 使用具有管理员权限的账户运行 collect.sh 脚本：

   ```
   # ./collect.sh
   ```

一个包含诊断信息的文件将生成并被保存到 /tmp/$HOST_NAME-collect.tar.gz 文件夹中。

# 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。

# 使用应用程序控制来管理可执行文件

您可以使用“应用程序控制”组件来允许或阻止可执行文件在用户设备上启动。“应用程序控制”组件支持基于 Windows 和基于 Linux 的操作系统。

对于基于 Linux 的操作系统，从 Kaspersky Endpoint Security 11.2 for Linux 开始，均提供应用程序控制组件。

## 先决条件

- Kaspersky Security Center Linux 已部署在您的组织中。
- Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Windows 的策略已创建并处于活动状态。策略中启用了“应用程序控制”组件。

## 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。

   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. **为组织中使用的可执行文件创建类别**

   分析受管理设备上存储的可执行文件列表。根据分析，为可执行文件创建类别。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可执行文件集。如果不同的安全组在工作中使用不同的可执行文件集，则可以为每个安全组创建单独的类别。

   其设置与任何应用程序控制规则都不匹配的可执行文件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可执行文件外的所有可执行文件，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可执行文件外的所有可执行文件，则使用该模式。

应用程序控制规则是通过可执行文件的类别来实施的。在 Kaspersky Security Center Linux 中，有三种类型的可执行文件类别：

- 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、文件路径。
- 包含来自所选设备的可执行文件的类别。您指定自动包含在该类别中的可执行文件所属的设备。
- 包含来自所选文件夹的可执行文件的类别。您指定自动包含在该类别中的可执行文件所来自的文件夹。

3. **在 Kaspersky Endpoint Security 策略中配置“应用程序控制”**

   使用您在上一阶段创建的类别，在 Kaspersky Endpoint Security for Linux 策略中配置应用程序控制组件。

   操作说明：在 Kaspersky Endpoint Security for Windows 策略中配置“应用程序控制”

4. **在测试模式下开启“应用程序控制”组件**

   为确保应用程序控制规则不会阻止用户工作所需的可执行文件，建议在创建新规则后启用应用程序控制规则测试并分析其操作。启用测试后，Kaspersky Endpoint Security for Windows 将不会阻止被应用程序控制规则禁止启动的可执行文件，而是将有关其启动的通知发送到管理服务器。

   测试应用程序控制规则时，建议执行以下操作：

   - 确定测试周期。测试周期从几天到两个月不等。
   - 检查由测试“应用程序控制”操作生成的事件。

   Kaspersky Security Center Web Console 操作说明：在 Kaspersky Endpoint Security for Windows 策略中配置“应用程序控制”组件。遵循此说明并在配置过程中启用“**测试模式**”选项。

5. **更改应用程序控制组件的设置**

   如有必要，请更改“应用程序控制”设置。根据测试结果，您可以将与应用程序控制组件事件相关的可执行文件添加到含有手动添加内容的类别中。

   操作说明：Kaspersky Security Center Web Console：添加事件相关的可执行文件到应用程序类别

6. **在操作模式下应用“应用程序控制”的规则**

   测试应用程序控制规则并完成类别的配置后，您可以在操作模式下应用这些应用程序控制规则。

   Kaspersky Security Center Web Console 操作说明：在 Kaspersky Endpoint Security for Windows 策略中配置“应用程序控制”组件。遵循此说明并在配置过程中禁用“**测试模式**”选项。

7. **验证“应用程序控制”配置**

   确保已完成以下操作：

   - 为可执行文件创建类别。
   - 已使用类别来配置应用程序控制。
   - 已在操作模式下应用“应用程序控制”的规则。

## 结果

方案完成后，可执行文件在受管理设备上的启动受到控制。用户只能运行组织中允许的可执行文件，而不能运行组织中禁止的可执行文件。

有关“应用程序控制”的详细信息，请参阅 Kaspersky Endpoint Security for Linux 帮助和 Kaspersky Endpoint Security for Windows 帮助。

# 获取并查看客户端设备上存储的可执行文件列表

您可以通过以下方式之一获取存储在客户端设备上的可执行文件列表：

- 在 Kaspersky Endpoint Security 策略中启用应用程序启动通知。
- 创建清查任务。

## 在 Kaspersky Endpoint Security 策略中启用应用程序启动通知

*要启用有关应用程序启动的通知：*

1. 打开 Kaspersky Endpoint Security 策略设置，然后转到**常规设置** → **报告和存储**。
2. 在**到管理服务器的数据传输**设置组中，选择**关于启动的应用程序**复选框，保存更改。

当用户尝试启动可执行文件时，关于这些文件的信息将被添加到客户端设备上的可执行文件列表中。Kaspersky Endpoint Security 会将该信息发送到网络代理，然后网络代理将其发送到管理服务器。

## 创建清查任务

对于 Kaspersky Endpoint Security for Linux，清查可执行文件的功能在 11.2 之前的版本中不可用。

您可以在获取已安装应用程序相关信息的同时减少数据库的负载。为了节省数据库空间，在安装了一组标准软件的参考设备上运行清单任务。建议设备数量为 1-3。

*要在客户端设备上为可执行文件创建清查任务：*

1. 在主菜单中，转到“**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“**新任务设置**”页面上的“**应用程序**”下拉列表中，选择 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Windows，具体取决于客户端设备的操作系统。

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 帮助 和 Kaspersky Endpoint Security for Windows 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。

清查过程中可检测以下格式的可执行文件（具体取决于您在清单任务属性中选择的选项）：MZ、COM、PE、NE、SYS、CMD、BAT、PS1、JS、VBS、REG、MSI、CPL、DLL、JAR 和 HTML。

查看受管理设备上存储的可执行文件列表

*要查看客户端设备上存储的可执行文件列表：*

在主菜单中，前往**软件管理→第三方应用程序→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。

如有必要，您可以将受管理设备的可执行文件发送到 Kaspersky Security Center Web Console 在其中打开的设备。

*要发送可执行文件：*

1. 在主菜单中，前往**软件管理→第三方应用程序→可执行文件**。

2. 单击要发送的可执行文件的链接。

3. 在打开的窗口中，转到**设备**部分，然后选中要从其发送可执行文件的受管理设备的复选框。

在发送可执行文件之前，请确保受管理设备与管理服务器有直接连接，方法是选择**不断开与管理服务器的连接** 复选框。

4. 单击“**发送**”按钮。

所选可执行文件将下载以进一步发送到您的 Kaspersky Security Center Web Console 在其中打开的设备。

# 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. 在主菜单中，前往**软件管理→第三方应用程序→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**按钮进行向导。

3. 在“**选择策略创建方法**”步骤中，指定应用程序类别名称并选择“**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，执行以下操作：

   a. 选择用于创建类别的规则类型：

   - **从 KL 类别**

     如果选中此选项，您可以指定卡巴斯基应用程序类别作为添加应用程序到用户类别的条件。来自指定 Kaspersky 类别的应用程序将被添加到用户应用程序类别。

   - **从存储库选择证书**

     如果选中此选项，则可以指定来自存储库的证书。类别条件仅匹配由指定证书签名的可执行文件。

     如果您创建并启动了清查任务并在 Kaspersky Endpoint Security 策略中勾选了“**关于已启动的应用程序**”复选框，则会将证书添加到存储库中。您可以执行以下两项操作。

     > 证书信息只能从 PE 格式（.exe、.dll、.sys）的可执行文件中提取。

   - **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。从注册表中选择一个应用程序后，窗口将打开，其中的参数将使用您选择的应用程序的元数据进行填充：

       - 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。

请注意，仅阻止满足指定参数的可执行文件的启动，而不阻止您选择的应用程序的启动。如果选定的应用程序元数据与启动应用程序时启动的可执行文件的元数据相匹配，那么您可以继续下一步。否则，您必须手动更改值以匹配可执行文件的元数据。

- **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。有关由哈希函数计算的哈希值的信息存储在管理服务器数据库中。

  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“**SHA256**”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。类别条件仅匹配具有相同元数据的可执行文件。

  **证书**

  如果选中此选项，则可以指定来自存储库的证书。类别条件仅匹配由指定证书签名的可执行文件。

  如果您创建并启动了清查任务并在 Kaspersky Endpoint Security 策略中勾选了“**关于已启动的应用程序**”复选框，则会将证书添加到存储库中。您可以执行以下两项操作。

- **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。

> 如果您想使用这些标准，必须在上传文件或存档文件夹后手动指定**元数据**和**证书**标准。

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。

> 如果您想使用这些标准，必须在上传文件或存档文件夹后手动指定**元数据**和**证书**标准。

b. 如有必要，请在**描述**字段中添加注释。符号数量不能超过 1000 个。

之后，您可以通过打开**应用程序类别属性条件**条件选项卡，然后在**条件标准**列中，单击要编辑或删除评论的条件链接来编辑或删除评论。

> 选择**从 KL 类别**规则类型时，您可以为基于此规则类型创建的所有条件添加一条注释。您可以单独编辑或删除每个条件的注释。

所选条件将添加到条件列表中。

您可以为要创建的应用程序类别添加所需的任意数量的标准。

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。

   如有必要，您可以在**描述**字段中添加注释。符号数量不能超过 1000 个。

   之后，您可以通过打开**应用程序类别属性排除项**排除项选项卡，然后在**条件标准**列中，单击要编辑或删除评论的条件链接来编辑或删除评论。

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。

向导结束后，应用程序类别将被创建并显示在应用程序类别列表中。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 和 Kaspersky Endpoint Security for Windows 帮助 。

# 创建包括选定设备中的可执行文件的应用程序类别

您可以将选定设备中的可执行文件用作要允许或阻止的可执行文件的模板。基于选定设备中的可执行文件，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。

请确保满足以下先决条件：

- 应用程序控制组件已在 Kaspersky Endpoint Security 策略中启用。
- 已获取存储在受管理设备上的可执行文件列表。

*要创建包括选定设备中的可执行文件的应用程序类别：*

1. 在主菜单中，前往**软件管理 → 第三方应用程序 → 应用程序类别**。
   显示包含可执行文件类别列表的页面。
2. 单击“**添加**”按钮。
   新类别向导启动。使用**下一步**按钮进行向导。
3. 在**选择策略创建方法**步骤，指定类别名称并选择**包含所选设备上可执行文件的类别。这些可执行文件被自动处理，它们的度量数据被添加到类别中**选项。
4. 单击**添加**。
5. 在打开的窗口中，选择一个或多个设备，其可执行文件将用于创建应用程序类别。
6. 指定下列设置：

   - **哈希值计算算法**

     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。有关由哈希函数计算的哈希值的信息存储在管理服务器数据库中。

     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“**SHA256**”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。

     “**为该类别中的文件计算 SHA256(在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更新版本中支持)**”复选框被默认选中。

     **为该类别中的文件计算 MD5(在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 更早版本中支持)**复选框被默认清空。

   - **与管理服务器存储库同步数据**

     如果您希望该管理服务器定期检查指定文件夹中的更改，则选择此选项。

     默认情况下已禁用该选项。

如果启用此选项，请指定检查指定文件夹中的更改的周期（以小时为单位）。默认情况下，扫描间隔为 24 小时。

- **文件类型**

  在此区域中，可以指定用于创建应用程序类别的文件类型。

  **所有文件**。创建类别时会考虑所有文件。默认情况下已选定该选项。

  **仅应用程序类别之外的文件**。创建类别时仅考虑应用程序类别之外的文件。

- **文件夹**

  在此区域中，可以指定选定设备中的哪些文件夹包含用于创建应用程序类别的文件。

  **所有文件夹**。创建类别时会考虑所有文件夹。默认情况下已选定该选项。

  **指定文件夹**。创建类别时仅考虑指定文件夹。如果选择此选项，则必须指定文件夹的路径。

向导完成后，会创建可执行文件类别。它显示在类别列表中。配置应用程序控制时，可以使用已创建的类别。

# 创建包括选定文件夹中的可执行文件的应用程序类别

您可以将选定文件夹中的可执行文件用作要在组织中允许或阻止的可执行文件的标准。在选定文件夹中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。

*要创建包括选定文件夹中的可执行文件的类别：*

1. 在主菜单中，前往**软件管理→ 第三方应用程序→ 应用程序类别**。

   显示含有类别列表的页面。

2. 单击“**添加**”按钮。

   新类别向导启动。使用**下一步**按钮进行向导。

3. 在“**选择策略创建方法**”步骤中，指定类型名称并选择“**包含指定文件夹内可执行文件的类别。复制到指定文件夹的应用程序可执行文件被自动处理，它们的度量数据被添加到类别中**”选项。

4. 指定将用于创建该类别的可执行文件所在的文件夹。

5. 定义下列设置：

   - **包含动态链接库 (DLL) 到该类别**

     应用程序类别包含动态链接库(DLL 格式的文件)，应用程序控制组件记录系统中运行的此类库的操作。包含 DLL 文件到类别可能降低 Kaspersky Security Center 的性能。

     默认情况下已清除该选框。

   - **包含脚本数据到该类别**

     应用程序类别包含脚本数据，脚本不被 Web 威胁防护阻止。包含脚本数据到类别可能降低 Kaspersky Security Center 的性能。

     默认情况下已清除该选框。

- **哈希值计算算法**：**为该类别中的文件计算 SHA256(在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更新版本中支持) / 为该类别中的文件计算 MD5(在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 更早版本中支持)**

  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。有关由哈希函数计算的哈希值的信息存储在管理服务器数据库中。

  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“**SHA256**”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。

  “**为该类别中的文件计算 SHA256(在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更新版本中支持)**”复选框被默认选中。

  **为该类别中的文件计算 MD5(在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 更早版本中支持)**复选框被默认清空。

- **强制扫描文件夹以查找更改**

  如果启用此选项，应用程序会定期检查“类别内容添加”文件夹的任何变化。您可以在该选框旁的输入字段中指定检查频率（小时）。默认情况下，强制检查的时间间隔为 24 小时。

  如果禁用此选项，应用程序不会强制检查文件夹。如果文件被修改、添加或删除，服务器会尝试访问这些文件。

  默认情况下已禁用该选项。

向导完成后，会创建可执行文件类别。它显示在类别列表中。您可以在“应用程序控制”配置中使用该类别。

有关“应用程序控制”的详细信息，请参阅 Kaspersky Endpoint Security for Linux 帮助和 Kaspersky Endpoint Security for Windows 帮助。

# 查看应用程序类别列表

您可以查看已配置的可执行文件类别列表以及每个类别的设置。

*要查看应用程序类别列表，*

在主菜单中，前往**软件管理 → 第三方应用程序 → 应用程序类别**。

显示含有类别列表的页面。

*要查看应用程序类别的属性，*

单击该类别的名称。

显示该类别的属性窗口。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 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. 在主菜单中，转到“**监控**” → “**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 SHA256 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 SHA256 (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 帮助和 Kaspersky Endpoint Security for Windows 帮助。

# 在 Kaspersky Endpoint Security for Windows 策略中配置“应用程序控制”

创建“应用程序控制”类别后，可以在 Kaspersky Endpoint Security for Windows 策略中使用它们配置“应用程序控制”。

*在 Kaspersky Endpoint Security for Windows 策略中配置"应用程序控制":*

1. 在主菜单中，转到"**资产管理**"→"**策略**"。

   将显示含有策略列表的页面。

2. 单击 **Kaspersky Endpoint Security for Windows** 策略。

   策略设置窗口打开。

3. 转到"**应用程序设置**"→"**安全控制**"→"**应用程序控制**"。

   将显示带"应用程序控制"设置的"**应用程序控制**"窗口。

4. "**应用程序控制**"选项默认启用。开启切换按钮**应用程序控制已禁用**以禁用该选项。

5. 在"**应用程序控制设置**"区块设置中，启用操作模式以应用"应用程序控制"规则并允许 Kaspersky Endpoint Security for Windows 阻止应用程序启动。

   如果要测试应用程序控制规则，请在"**应用程序控制设置**"区域启用测试模式。在测试模式中，Kaspersky Endpoint Security for Windows 不会阻止应用程序启动，但会在报告中记录有关所触发规则的信息。单击**查看报告**链接可查看此信息。

6. 如果您希望 Kaspersky Endpoint Security for Windows 在用户启动应用程序时监控 DLL 模块的加载，请启用"**控制 DLL 模块加载**"选项。

   有关模块和加载了模块的应用程序的信息将保存到报告中。

   Kaspersky Endpoint Security for Windows 仅监控在选择"**控制 DLL 模块加载**"选项后加载的 DLL 模块和驱动程序。如果您希望 Kaspersky Endpoint Security for Windows 监控所有 DLL 模块和驱动程序，包括在启动 Kaspersky Endpoint Security for Windows 之前加载的 DLL 模块和驱动程序，请在选择"**控制 DLL 模块加载**"选项后重新启动设备。

7. （可选）在"**消息模板**"块中，更改当应用程序被阻止启动时显示的消息模板以及发送给您的电子邮件模板。

8. 在"**应用程序控制模式**"区块设置中，选择"**拒绝列表**"或"**允许列表**"模式。

   默认情况下，选择"**拒绝列表**"模式。

9. 单击"**规则列表设置**"链接。

   将打开"**拒绝列表和允许列表**"窗口，您可以在其中添加应用程序类别。默认情况下，如果选择"**拒绝列表**"模式则选定"**拒绝列表**"选项卡，如果选择"**允许列表**"模式则选定"**允许列表**"选项卡。

10. 在"**拒绝列表和允许列表**"窗口中，单击"**添加**"按钮。

    "**应用程序控制规则**"窗口将开启。

11. 单击"**请选择类别**"链接。

    将打开"**应用程序类别**"窗口。

12. 添加您先前创建的应用程序类别。

    可以单击"**编辑**"按钮来编辑已创建类别的设置。

    可以单击"**添加**"按钮来创建新类别。

    可以单击"**删除**"按钮以从列表中删除类别。

13. 完成应用程序类别列表后，单击"**确定**"按钮。

    "**应用程序类别**"窗口关闭。

14. 在"**应用程序控制规则**"窗口的"**主题及其权限**"区域中，创建要应用"应用程序控制"规则的用户和用户组列表。

15. 单击“**确定**”按钮以保存设置并关闭“**应用程序控制规则**”窗口。

16. 单击“**确定**”按钮以保存设置并关闭“**拒绝列表和允许列表**”窗口。

17. 单击“**确定**”按钮以保存设置并关闭“**应用程序控制**”窗口。

18. 关闭含有 Kaspersky Endpoint Security for Windows 策略设置的窗口。

“应用程序控制”已配置。策略传播到客户端设备后，可执行文件的启动将受到管理。

有关“应用程序控制”的详细信息，请参阅 Kaspersky Endpoint Security for Linux 帮助和 Kaspersky Endpoint Security for Windows 帮助。

# 获取并查看客户端设备上安装的应用程序列表

Kaspersky Security Center Linux 清查在运行 Linux 和 Windows 操作系统的受管理客户端设备上安装的所有软件。

网络代理编辑安装在设备上的应用程序列表，并把该列表传给管理服务器。网络代理更新应用程序列表大约需要 10-15 分钟。

对于基于 Windows 的客户端设备，网络代理从 Windows 注册表接收有关已安装应用程序的大部分信息。对于基于 Linux 的客户端设备，包管理器向网络代理提供有关已安装应用程序的信息。

*要查看受管理设备上安装的应用程序列表：*

1. 在主菜单中，转到“**操作**”→“**第三方应用程序**”→“**应用程序注册表**”。

   该页面显示一个表格，其中包含安装在受管理设备上的应用程序。选择应用程序以查看其属性，例如，供应商名称、版本号、可执行文件列表、安装了该应用程序的设备列表。

2. 您可以按如下方式对包含已安装应用程序的表中的数据进行分组和筛选：

   - 单击表格右上角的“设置”图标（ ）。

     在调用的“**列设置**”菜单中，选择要在表中显示的列。要查看安装应用程序的客户端设备的操作系统类型，请选择“**OS 类型**”列。

   - 单击表格右上角的过滤器图标（ ），然后在调用的菜单中指定并应用过滤条件。

     显示筛选出的已安装应用程序表。

*要查看特定受管理设备上安装的应用程序列表，*

在主菜单中，转到“**资产管理**”→“**资产(设备)**”→“**<设备名称>**”→“**高级**”→“**应用程序注册表**”。在此菜单中，您可以将应用程序列表导出到 CSV 文件或 TXT 文件。

有关“应用程序控制”的详细信息，请参阅 Kaspersky Endpoint Security for Linux 帮助和 Kaspersky Security for Windows 帮助。

# 关于第三方应用程序

Kaspersky Security Center Linux 可以帮助您更新安装在客户端设备上的第三方软件，并修复第三方软件的漏洞。Kaspersky Security Center Linux 只能将第三方软件从当前版本更新到最新版本。

第三方软件列表可以更改，并动态更新。您可以通过在 Kaspersky Security Center Web Console 中查看可用更新列表来检查是否可以使用 Kaspersky Security Center Linux 更新第三方软件（安装在用户设备上）。

以下概述的步骤仅用于查看可通过 Kaspersky Security Center Linux 更新的第三方软件列表。按照以下步骤访问相关信息，无需启动任何任务。

*要查看可以使用 Kaspersky Security Center Linux 更新的第三方软件列表：*

1. 在主菜单中，转到“**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. 在向导的“**新任务设置**”步骤中，指定以下设置：
   a. 在“**应用程序**”下拉列表中，选择**Kaspersky Security Center Linux**。
   b. 在“**任务类型**”字段中，选择“**安装所需更新并修复漏洞**”。
4. 在向导的“**任务范围**”步骤中，选择“**受管理设备**”选项。
5. 在向导的“**指定更新安装规则**”步骤中，点击“**添加**”按钮。
   规则创建向导开始。使用“**下一步**”按钮继续向导操作。
6. 在向导的“**选择规则类型**”步骤中，选择“**第三方更新的规则**”选项。
7. 在向导的**常规条件**步骤中，选择**安装所有更新 (除了拒绝的)**选项，然后单击**下一步**。

第三方软件列表将显示。

# 安装第三方软件更新

Kaspersky Security Center Linux 允许您管理安装在受管理设备上的第三方软件的更新，并通过安装所需的更新来修复此类软件中的漏洞。

Kaspersky Security Center Linux 通过“*查找漏洞和所需更新*”任务搜索更新。完成此任务后，管理服务器会收到检测到的漏洞列表，以及在任务属性中指定的设备上安装的第三方软件的所需更新。查看可用更新的信息后，您可以将这些更新安装到设备上。

Kaspersky Security Center Linux 通过删除先前版本的应用程序并安装新版本来更新某些应用程序。

在受管理设备上更新第三方应用程序或修复第三方应用程序中的漏洞时，可能需要用户交互。例如，如果第三方应用程序当前处于打开状态，则用户可能会被提示将其关闭。

出于安全原因，卡巴斯基技术会自动扫描您使用漏洞和补丁管理功能安装的任何第三方软件更新，以查找恶意软件。这些技术用于自动文件检查，包括病毒扫描、静态分析、动态分析、沙盒环境中的行为分析和机器学习。

卡巴斯基专家不会对可以使用漏洞和补丁管理功能安装的第三方软件更新进行手动分析。此外，卡巴斯基专家不会在此类更新中搜索漏洞（已知或未知）或未记录的功能，也不会对上面段落中指定的更新以外的更新进行其他类型的分析。

将第三方软件更新的元数据下载到存储库后，可以使用"*安装所需更新并修复漏洞*"任务在客户端设备上安装更新。

仅当您具有"漏洞和补丁管理"功能的授权许可时，才能创建"*安装所需更新并修复漏洞*"任务。

完成此任务后，更新将自动安装在受管理设备上。新更新的元数据下载到管理服务器存储库后，Kaspersky Security Center Linux 会检查更新是否满足更新规则中指定的条件。符合条件的所有新更新都将在任务下次运行时自动下载并安装。

# 方案：更新第三方软件

本节提供了更新客户端设备上安装的第三方软件的方案。第三方软件包括其他软件供应商的应用程序。

## 先决条件

管理服务器必须连接到互联网才能安装第三方软件更新。

## 阶段

更新第三方软件分阶段进行：

1. **搜索所需更新**

   要查找受管理设备所需的第三方软件更新，请运行"*查找漏洞和所需更新*"任务。完成此任务后，Kaspersky Security Center Linux 会收到检测到的漏洞列表，以及在任务属性中指定设备上安装的第三方软件的所需更新。

   "*查找漏洞和所需更新*"任务由管理服务器快速启动向导自动创建。如果未运行向导，请立即创建"*查找漏洞和所需更新*"任务或运行快速启动向导。

   您只能为 Windows 设备创建"*查找漏洞和所需更新*"任务。您无法为运行其他操作系统的设备创建此任务。

2. **查看发现的更新列表**

   查看有关可用的第三方软件更新的信息并决定要安装哪些更新。要查看有关每个更新的详细信息，请单击列表中的更新名称。对于列表中的每个更新，您还可以查看客户端设备上更新安装的统计信息。

3. **配置更新安装**

   Kaspersky Security Center Linux 收到第三方软件更新列表后，您可以通过创建"*安装所需更新并修复漏洞*"任务，将这些更新安装到客户端设备上。

您只能为 Windows 设备创建“*安装所需更新并修复漏洞*”任务。您无法为运行其他操作系统的设备创建此任务。

“*安装所需更新并修复漏洞*”任务用于安装 Microsoft 应用程序的更新，包括 Windows Update 服务提供的更新以及其他供应商软件的更新。注意：仅当您具有“漏洞和补丁管理”功能的授权许可时，才能创建“*安装所需更新并修复漏洞*”任务。

要安装某些软件更新，您必须接受最终用户授权许可协议 (EULA) 才能安装软件。如果您拒绝 EULA，则不会安装该软件更新。

您可以按计划启动更新安装任务。指定任务计划时，请确保更新安装任务在“*查找漏洞和所需更新*”任务完成后启动。

**4 安排任务**

为确保漏洞列表始终是最新的，请安排“*查找漏洞和所需更新*”任务以不时自动运行该任务。默认情况下，“*查找漏洞和所需更新*”任务设置为手动启动。

如果您创建了“*安装所需更新并修复漏洞*”任务，则可以安排其与“*查找漏洞和所需更新*”任务相同或更少的频率运行。

计划任务时，请确保更新安装任务在“*查找漏洞和所需更新*”任务完成后启动。

**5 批准和拒绝第三方软件更新（可选）**

如果已创建“*安装所需更新并修复漏洞*”任务，则可以在任务属性窗口中指定安装更新的规则。

对于每条规则，都可以根据更新状态定义要安装的更新：*未定义*、*已批准* 或 *已拒绝*。例如，您可能想为服务器创建一个特定任务，并为该任务设置一条规则，以仅允许安装状态为“*已批准*”的更新。之后，手动为要安装的更新设置“*已批准*”状态。在这种情况下，状态为“*未定义*”或“*已拒绝*”的更新将不会安装到任务中指定的服务器上。

使用“*已批准*”状态来管理更新安装对于少量更新来说非常有效。要安装多个更新，请使用可以在“*安装所需更新并修复漏洞*”任务中配置的规则。我们建议仅为那些不符合规则中指定条件的特定更新设置“*已批准*”状态。如果您手动批准大量更新，管理服务器的性能会下降，这可能会导致管理服务器过载。

默认情况下，下载的软件更新具有“*未定义*”状态。您可以在“**软件更新**”列表（“**操作**”→“**补丁管理**”→“**软件更新**”）中将状态更改为“*已批准*”或“*已拒绝*”。

有关更多详细信息，请参阅有关批准和拒绝第三方软件更新的说明。

**6 运行更新安装任务**

创建“*安装所需更新并修复漏洞*”任务。启动此任务后，更新将下载并安装到受管理设备上。任务完成后，请确保它在任务列表中具有“*成功完成*”状态。

**7 创建更新安装结果报告（可选）**

要查看有关更新安装的详细统计信息，请创建“第三方软件更新安装结果报告”。

## 结果

如果已创建并配置了“*安装所需更新并修复漏洞*”任务，则更新将自动安装到受管理设备上。新更新下载到管理服务器存储库后，Kaspersky Security Center Linux 会检查更新是否满足更新规则中指定的条件。符合条件的所有新更新都将在任务下次运行时自动安装。

# 第三方软件更新安装选项

您可以通过创建并运行“*安装所需更新并修复漏洞*”任务在受管理设备上安装第三方软件更新和来自 Windows Update 的更新。仅当您具有“漏洞和补丁管理”功能的授权许可时，才能创建“*安装所需更新并修复漏洞*”任务。您可以使用此任务来安装其他供应商软件的更新。

在受管理设备上更新第三方应用程序或修复第三方应用程序中的漏洞时，可能需要用户交互。例如，如果第三方应用程序当前处于打开状态，则用户可能会被提示将其关闭。

作为一种选择，您可以创建任务以通过以下方式安装所需的更新：

- 通过打开更新列表并指定要安装的更新。

  结果，创建了安装所选更新的新任务。作为一个选项，您可以将选定更新添加到现有任务。

- 通过运行更新安装向导。

  更新安装向导仅在漏洞和补丁管理授权许可下可用。

  该向导简化了更新安装任务的创建和配置，并允许您消除包含要安装的相同更新的冗余任务创建。

## 使用更新列表安装第三方软件更新

*要使用更新列表安装第三方软件更新：*

1. 使用以下路径之一打开更新列表：

   - **软件管理→补丁管理→软件更新**。
   - **资产管理 → 资产(设备)** → <设备名称> → **高级 → 可用更新**。
   - **软件管理→第三方应用程序→应用程序注册表**→<应用程序名称>→**可用更新**。

   此时将显示可用更新列表。

2. 选中要下载的更新旁边的复选框。

3. 单击“**安装更新**”按钮。如果此按钮不可见，请单击省略号按钮，然后从下拉列表中选择“**安装更新**”。

   要安装某些软件更新，您必须接受最终用户授权许可协议 (EULA)。如果您拒绝 EULA，则不会安装该软件更新。

4. 您可以选择以下选项之一：

   - **新任务**

     “新任务向导”启动。如果您拥有漏洞和补丁管理授权许可，则会预先选择“*安装所需更新并修复漏洞*”任务。按照向导的步骤完成任务创建。

- **安装更新(添加规则到指定任务)**

  选择要向其中添加选定更新的任务。如果您拥有漏洞和补丁管理授权许可，请选择“*安装所需更新并修复漏洞*”任务。安装所选更新的新规则将自动添加到所选任务中。所选更新将添加到任务属性中。

  任务属性窗口打开。单击“**保存**”按钮以保存更改。

如果您选择了创建新任务，则会创建新任务并将其显示在**任务**处的任务列表中。如果您选择了将更新添加到现有任务中，更新将保存在任务属性中。

要安装第三方软件更新，您必须启动“*安装所需更新并修复漏洞*”任务。您可以通过单击任务列表中的“**开始**”按钮或在启动的任务的属性中指定计划设置来启动此任务。指定任务计划时，请确保更新安装任务在“*查找漏洞和所需更新*”任务完成后启动。

使用更新安装向导安装第三方软件更新

更新安装向导功能仅在“漏洞和补丁管理授权许可”下可用。

*要使用更新安装向导来创建安装第三方软件更新的任务，请执行以下操作：*

1. 在主菜单中，前往**软件管理→补丁管理→ 软件更新**。

   可用更新列表被显示。

2. 选中要安装的更新旁边的复选框。

3. 单击**运行更新安装向导**按钮。

   更新安装向导开始。“**选择更新安装任务**”页面显示以下类型的所有现有任务的列表：

   - *安装所需更新并修复漏洞*
   - *修复漏洞*

4. 如果您希望向导仅显示安装所选更新的那些任务，则启用“**仅显示安装该更新的任务**”选项。

5. 选择您要执行的操作：

   - 要启动现有任务，请选中“*安装所需更新并修复漏洞*”任务旁边的复选框，然后单击“**开始**”按钮。

     该任务将在后台模式下完成。不需要进一步操作。

   - 要将新规则添加到现有任务：

     a. 选中任务名称旁边的复选框，然后单击“**添加规则**”按钮。

     如果选择多个任务，“**添加规则**”按钮将被禁用。

     您无法为“*修复漏洞*”任务添加规则。如果您选择“*修复漏洞*”任务，则会出现以下通知：“*要安装更新，请使用“安装所需更新并修复漏洞”任务。*”

b. 在向导的“**创建更新安装规则**”步骤中，配置新规则：

- **该重要级别的更新的安装规则**

  有时候，软件更新可能损害用户的软件体验。此种情况下，您可能决定仅安装软件操作的关键更新并跳过其他更新。

  如果启用该选项，更新仅修复 Kaspersky 设置的严重级别等于或高于所选更新的严重性级别（**中度**、**高危**或**严重**）的漏洞。严重级别低于选定值的漏洞不被修复。

  如果禁用该选项，更新修复所有漏洞，无论它们的严重级别是什么。

  默认情况下已禁用该选项。

  如果所选更新的重要级别为“*未知*”，则不会显示此规则。

- **根据 MSRC 的该重要级别的更新的安装规则**

  有时候，软件更新可能损害用户的软件体验。此种情况下，您可能决定仅安装软件操作的关键更新并跳过其他更新。

  如果启用该选项（仅可用于 Windows Update 更新），更新仅修复 Microsoft Security Response Center (MSRC) 设置的严重级别等于或高于列表中选定的值（**低**、**中度**、**高危**或**严重**）的漏洞。严重级别低于选定值的漏洞不被修复。

  如果禁用该选项，更新修复所有漏洞，无论它们的严重级别是什么。

  默认情况下已禁用该选项。

  仅针对 Microsoft 软件更新显示此规则。如果所选更新的重要级别为“*未知*”，则不会显示规则。

- **该供应商的更新的安装规则**

  此选项仅适用于第三方应用程序的更新。Kaspersky Security Center Linux 仅安装与所选更新由同一供应商制作的应用程序相关的更新。未安装拒绝更新和其他供应商提供的应用程序更新。

  默认情况下已禁用该选项。

  仅针对第三方软件更新显示此规则。

- **类型是 的更新的安装规则**

- **所选应用程序的更新的安装规则**

  仅针对第三方软件更新显示此规则。

- **所选更新的安装规则**

- **批准所选更新**

  所选更新将被批准安装。如果一些应用的更新安装规则仅允许安装批准的更新，启用该选项。

  默认情况下已禁用该选项。

- **自动安装所选更新安装所需的所有先前应用程序更新**

  如果在安装所选更新需要时，您同意安装临时应用程序版本，保持该选项被启用。

  如果禁用该选项，仅选定的应用程序版本被安装。如果您想直截了当地更新应用程序，而不尝试安装增量版本，请禁用该选项。如果安装所选更新不能不安装先前版本的应用程序，应用程序更新失败。

  例如，您在设备上安装了应用程序的版本 3，您想更新它到版本 5，但是该应用程序的版本 5 仅可以在版本 4 之上安装。如果启用该选项，软件先安装版本 4，然后安装版本 5。如果禁用该选项，软件更新应用程序失败。

默认情况下已启用该选项。

c. 单击“**添加**”按钮。

任务属性窗口打开。新规则已添加到任务属性中。您可以查看或修改规则或其他任务设置。单击“**保存**”按钮以保存更改。

- 要创建任务：

a. 单击“**新任务**”按钮。

b. 在向导的“**创建更新安装规则**”步骤中，配置新规则：

- **该重要级别的更新的安装规则**

  有时候，软件更新可能损害用户的软件体验。此种情况下，您可能决定仅安装软件操作的关键更新并跳过其他更新。

  如果启用该选项，更新仅修复 Kaspersky 设置的严重级别等于或高于所选更新的严重性级别（**中度**、**高危**或**严重**）的漏洞。严重级别低于选定值的漏洞不被修复。

  如果禁用该选项，更新修复所有漏洞，无论它们的严重级别是什么。

  默认情况下已禁用该选项。

  如果所选更新的重要级别为“*未知*”，则不会显示此规则。

- **根据 MSRC 的该重要级别的更新的安装规则**

  有时候，软件更新可能损害用户的软件体验。此种情况下，您可能决定仅安装软件操作的关键更新并跳过其他更新。

  如果启用该选项（仅可用于 Windows Update 更新），更新仅修复 Microsoft Security Response Center (MSRC) 设置的严重级别等于或高于列表中选定的值（**低**、**中度**、**高危**或**严重**）的漏洞。严重级别低于选定值的漏洞不被修复。

  如果禁用该选项，更新修复所有漏洞，无论它们的严重级别是什么。

  默认情况下已禁用该选项。

  仅针对 Microsoft 软件更新显示此规则。如果所选更新的重要级别为“*未知*”，则不会显示规则。

- **该供应商的更新的安装规则**

  此选项仅适用于第三方应用程序的更新。Kaspersky Security Center Linux 仅安装与所选更新由同一供应商制作的应用程序相关的更新。未安装拒绝更新和其他供应商提供的应用程序更新。

  默认情况下已禁用该选项。

  仅针对第三方软件更新显示此规则。

- **类型是 的更新的安装规则**

- **所选应用程序的更新的安装规则**

  仅针对第三方软件更新显示此规则。

- **所选更新的安装规则**

- **批准所选更新**

  所选更新将被批准安装。如果一些应用的更新安装规则仅允许安装批准的更新，启用该选项。

默认情况下已禁用该选项。

- **自动安装所选更新安装所需的所有先前应用程序更新**

  如果在安装所选更新需要时，您同意安装临时应用程序版本，保持该选项被启用。

  如果禁用该选项，仅选定的应用程序版本被安装。如果您想直截了当地更新应用程序，而不尝试安装增量版本，请禁用该选项。如果安装所选更新不能不安装先前版本的应用程序，应用程序更新失败。

  例如，您在设备上安装了应用程序的版本 3，您想更新它到版本 5，但是该应用程序的版本 5 仅可以在版本 4 之上安装。如果启用该选项，软件先安装版本 4，然后安装版本 5。如果禁用该选项，软件更新应用程序失败。

  默认情况下已启用该选项。

c. 单击“**添加**”按钮。

继续在新任务向导中创建任务。您在更新安装向导中添加的新规则将显示在新任务向导中。完成向导后，“*安装所需更新并修复漏洞*”任务将添加到任务列表中。

# “查找漏洞和所需更新”任务设置

快速启动向导运行时，将自动创建“*查找漏洞和所需更新*”任务。如果未运行向导，可以手动创建该任务。

除了常规任务设置外，您还可以在创建“*查找漏洞和所需更新*”任务或稍后配置已创建任务的属性时指定以下设置：

- **搜索 Microsoft 列出的漏洞和更新**

  搜索漏洞和更新时，Kaspersky Security Center Linux 会使用当前可用的 Microsoft 更新源中有关适用 Microsoft 更新的信息。

  例如，如果您有带有不同 Microsoft 更新和第三方应用程序更新设置的不同任务，您可能想要禁用该选项。

  默认情况下已启用该选项。

  有关 Microsoft Windows 可选更新的信息未发送至管理服务器。

- **连接更新服务器更新数据**

  受管理设备上的“Windows 更新代理”连接到 Microsoft 更新源。以下服务器可以充当 Microsoft 更新源：

  - 在组织网络中部署了 Microsoft Windows Server Update Services (WSUS) 的 Windows 服务器
  - Microsoft 更新服务器

  如果启用该选项，受管理设备上的 Windows 更新代理将连接到 Microsoft 更新源以刷新适用 Microsoft Windows 更新的信息。

  如果禁用此选项，受管理设备上的 Windows 更新代理将使用以前从 Microsoft 更新源所收到的适用 Microsoft Windows 更新的信息。

  到 Microsoft 更新源的连接可能消耗资源。如果在其他任务中或网络代理策略属性中设置了到该更新源的常规连接，则您可能想要在“**软件更新和漏洞**”区域禁用此选项。如果您不想禁用此选项，则为了减少服务器过载，您可以配置任务计划以随机分配任务启动延迟（不超过 360 分钟）。

  默认情况下已启用该选项。

网络代理策略设置的以下选项的组合定义了获取更新的方式：

- 仅当在**查找漏洞和所需更新连接更新服务器更新数据任务的属性中**启用了*连接到更新服务器以更新数据查找漏洞和所需更新*选项，并且在网络代理策略的设置中**Windows Update 搜索模式**选项被设置为**主动**时，受管理设备上的 Windows 更新代理才会连接到更新服务器以获取更新 。

- 如果您在执行*漏洞扫描*任务时不需要网络代理发起与 Microsoft Windows 更新源的连接并下载更新，您可以将**Windows Update 搜索模式**选项设置为**被动**，同时**连接更新服务器更新数据**选项必须保持启用。这使您可以节省资源并使用以前收到的 Windows 更新来扫描漏洞。如果您以不同的方式配置接收 Microsoft Windows 更新，则可以使用被动模式。如果没有以其他方式配置接收 Microsoft Windows 更新，请不要将**Windows Update 搜索模式**选项设置为**被动**，因为在这种情况下，将永远不会收到有关更新的信息。

- 不管“**连接更新服务器更新数据**”选项的状态如何（启用或禁用），如果“**Windows Update 搜索模式**”选项被设置为“**已禁用**”，Kaspersky Security Center Linux 不会请求有关更新的任何信息。

如果您的组织网络中使用了 WSUS 服务器（本地 WSUS 服务器），并且您希望将其与 Kaspersky Security Center 管理服务器一起使用，则必须首先确保 Kaspersky Security Center 管理服务器未用作 WSUS 服务器，然后执行以下操作：

1. 在运行 Windows 的受管理设备上，为 Windows 更新服务指定本地 WSUS 服务器。您可以在 Windows 注册表中手动执行此操作，也可以使用 Windows 组策略执行此操作。

2. 在本地 WSUS 服务器上，指定更新所需的分类以及要分发更新的应用程序。

3. 将您的 WSUS 服务器与上游服务器同步（这可以是 Microsoft WSUS 服务器，也可以是另一个本地上游 WSUS 服务器）。

在设备上运行“*查找漏洞和所需更新*”任务后，网络代理使用 Windows 更新服务发起适用于该设备的 Windows 更新请求。Windows 更新服务从注册表中获取外部 WSUS 服务器的地址，并直接从该外部 WSUS 服务器搜索更新。然后，Windows 更新服务通过网络代理将此列表转发到管理服务器。因此，管理服务器拥有了最新的数据库。

- **搜索卡巴斯基列出的第三方漏洞和更新**

  如果启用该选项，Kaspersky Security Center Linux 会在 Windows 注册表和“**指定文件系统中应用程序高级搜索的路径**”下指定的文件夹中搜索漏洞和第三方应用程序（由非 Kaspersky 和 Microsoft 软件供应商制作的应用程序）所需的更新。支持的第三方应用程序的完整列表由 Kaspersky 管理。

  如果禁用该选项，Kaspersky Security Center Linux 不会查找第三方应用程序的漏洞和所需更新。例如，如果您有带有不同 Microsoft Windows 更新和第三方应用程序更新设置的不同任务，您可能想要禁用该选项。

  默认情况下已启用该选项。

- **指定文件系统中应用程序高级搜索的路径**

  Kaspersky Security Center Linux 在其中搜索需要修复漏洞和安装更新的第三方应用程序的文件夹。您可以使用系统变量。

  指定应用程序安装文件夹。默认下，列表包含大多数应用程序所安装的系统文件夹。

- **启用高级诊断**

  如果启用该功能，即便写入跟踪文件在 Kaspersky Security Center Linux 远程诊断实用程序中对网络代理禁用，网络代理也会写入跟踪文件。跟踪轮流写入两个文件中；两个文件的总大小由“**高级诊断文件的最大大小，MB**”值决定。当两个文件都满时，网络代理再次开始写入它们。带有跟踪的文件存储在 %WINDIR%\Temp 文件夹。这些文件在远程诊断实用程序中可以被访问，您可以在那里下载或删除它们。

如果禁用该功能，网络代理根据 Kaspersky Security Center Linux 远程诊断实用程序中的设置写入跟踪。没有附加跟踪被写入。

当创建任务时，您不必启用高级诊断。例如，如果某个任务在一些设备上失败并且您希望在另一个任务运行期间获取额外信息，您可能希望稍后使用该功能。

默认情况下已禁用该选项。

- **高级诊断文件的最大大小，MB**

  默认值是 100 MB，可用值介于 1 MB 和 2048 MB 之间。当您所发送的高级诊断文件信息不足以定位问题时，您可能被 Kaspersky 技术支持专家要求更改默认值。

关于任务计划的建议

计划“*查找漏洞和所需更新*”任务时，请确保两个选项“**运行错过的任务**”和“**使用任务启动自动随机延迟**”已启用。

默认情况下，“*查找漏洞和所需更新*”任务设置为手动启动。如果组织的工作区规则规定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后运行，即，第二天早晨。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。

# 创建“查找漏洞和所需更新”任务

通过“*查找漏洞和所需更新*”任务，Kaspersky Security Center Linux 会收到检测到的漏洞列表以及受管理设备上安装的第三方软件的所需更新列表。

> 您只能为 Windows 设备创建“*查找漏洞和所需更新*”任务。您无法为运行其他操作系统的设备创建此任务。

快速启动向导运行时，将自动创建“*查找漏洞和所需更新*”任务。如果未运行向导，可以手动创建该任务。

*要创建“查找漏洞和所需更新”任务：*

1. 在主菜单中，转到“**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. 对于 Kaspersky Security Center 应用程序，选择**查找漏洞和所需更新**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. 指定对漏洞和需要更新的应用程序进行扫描的方式：

   - **搜索 Microsoft 列出的漏洞和更新**

     搜索漏洞和更新时，Kaspersky Security Center Linux 会使用当前可用的 Microsoft 更新源中有关适用 Microsoft 更新的信息。

     例如，如果您有带有不同 Microsoft 更新和第三方应用程序更新设置的不同任务，您可能想要禁用该选项。

默认情况下已启用该选项。

有关 Microsoft Windows 可选更新的信息未发送至管理服务器。

- **连接更新服务器更新数据**

  受管理设备上的“Windows 更新代理”连接到 Microsoft 更新源。以下服务器可以充当 Microsoft 更新源：

  - 在组织网络中部署了 Microsoft Windows Server Update Services (WSUS) 的 Windows 服务器
  - Microsoft 更新服务器

  如果启用该选项，受管理设备上的 Windows 更新代理将连接到 Microsoft 更新源以刷新适用 Microsoft Windows 更新的信息。

  如果禁用此选项，受管理设备上的 Windows 更新代理将使用以前从 Microsoft 更新源所收到的适用 Microsoft Windows 更新的信息。

  到 Microsoft 更新源的连接可能消耗资源。如果在其他任务中或网络代理策略属性中设置了到该更新源的常规连接，则您可能想要在“**软件更新和漏洞**”区域禁用此选项。如果您不想禁用此选项，则为了减少服务器过载，您可以配置任务计划以随机分配任务启动延迟（不超过 360 分钟）。

  默认情况下已启用该选项。

  网络代理策略设置的以下选项的组合定义了获取更新的方式：

  - 仅当在**查找漏洞和所需更新连接更新服务器更新数据任务的属性中**启用了*连接到更新服务器以更新数据查找漏洞和所需更新*选项，并且在网络代理策略的设置中**Windows Update 搜索模式**选项被设置为**主动**时，受管理设备上的 Windows 更新代理才会连接到更新服务器以获取更新 。
  - 如果您在执行*漏洞扫描*任务时不需要网络代理发起与 Microsoft Windows 更新源的连接并下载更新，您可以将**Windows Update 搜索模式**选项设置为**被动**，同时**连接更新服务器更新数据**选项必须保持启用。这使您可以节省资源并使用以前收到的 Windows 更新来扫描漏洞。如果您以不同的方式配置接收 Microsoft Windows 更新，则可以使用被动模式。如果没有以其他方式配置接收 Microsoft Windows 更新，请不要将**Windows Update 搜索模式**选项设置为**被动**，因为在这种情况下，将永远不会收到有关更新的信息。
  - 不管“**连接更新服务器更新数据**”选项的状态如何（启用或禁用），如果“**Windows Update 搜索模式**”选项被设置为“**已禁用**”，Kaspersky Security Center Linux 不会请求有关更新的任何信息。

  如果您的组织网络中使用了 WSUS 服务器（本地 WSUS 服务器），并且您希望将其与 Kaspersky Security Center 管理服务器一起使用，则必须首先确保 Kaspersky Security Center 管理服务器未用作 WSUS 服务器，然后执行以下操作：

  1. 在运行 Windows 的受管理设备上，为 Windows 更新服务指定本地 WSUS 服务器。您可以在 Windows 注册表中手动执行此操作，也可以使用 Windows 组策略执行此操作。
  2. 在本地 WSUS 服务器上，指定更新所需的分类以及要分发更新的应用程序。
  3. 将您的 WSUS 服务器与上游服务器同步（这可以是 Microsoft WSUS 服务器，也可以是另一个本地上游 WSUS 服务器）。

  在设备上运行“*查找漏洞和所需更新*”任务后，网络代理使用 Windows 更新服务发起适用于该设备的 Windows 更新请求。Windows 更新服务从注册表中获取外部 WSUS 服务器的地址，并直接从该外部 WSUS 服务器搜索更新。然后，Windows 更新服务通过网络代理将此列表转发到管理服务器。因此，管理服务器拥有了最新的数据库。

- **搜索卡巴斯基列出的第三方漏洞和更新**

  如果启用该选项，Kaspersky Security Center Linux 会在 Windows 注册表和“**指定文件系统中应用程序高级搜索的路径**”下指定的文件夹中搜索漏洞和第三方应用程序（由非 Kaspersky 和 Microsoft 软件供应商制作的应用程序）所需的更新。支持的第三方应用程序的完整列表由 Kaspersky 管理。

  如果禁用该选项，Kaspersky Security Center Linux 不会查找第三方应用程序的漏洞和所需更新。例如，如果您有带有不同 Microsoft Windows 更新和第三方应用程序更新设置的不同任务，您可能想要禁用该选项。

  默认情况下已启用该选项。

您可以在任务属性窗口的“**应用程序设置**”选项卡上创建任务后禁用这些选项。

7. **指定文件系统中应用程序高级搜索的路径**

   Kaspersky Security Center Linux 在其中搜索需要修复漏洞和安装更新的第三方应用程序的文件夹。您可以使用系统变量。

   指定应用程序安装文件夹。默认下，列表包含大多数应用程序所安装的系统文件夹。

   您可以在任务属性窗口的“**应用程序设置**”选项卡上创建任务后更改指定的路径。

8. 如果需要，**启用高级诊断**

   如果启用该功能，即便写入跟踪文件在 Kaspersky Security Center Linux 远程诊断实用程序中对网络代理禁用，网络代理也会写入跟踪文件。跟踪轮流写入两个文件中；两个文件的总大小由“**高级诊断文件的最大大小，MB**”值决定。当两个文件都满时，网络代理再次开始写入它们。带有跟踪的文件存储在 %WINDIR%\Temp 文件夹。这些文件在远程诊断实用程序中可以被访问，您可以在那里下载或删除它们。

   如果禁用该功能，网络代理根据 Kaspersky Security Center Linux 远程诊断实用程序中的设置写入跟踪。没有附加跟踪被写入。

   当创建任务时，您不必启用高级诊断。例如，如果某个任务在一些设备上失败并且您希望在另一个任务运行期间获取额外信息，您可能希望稍后使用该功能。

   默认情况下已禁用该选项。

   您可以在任务属性窗口的“**应用程序设置**”选项卡上创建任务后禁用此选项。

9. 指定“**高级诊断文件的最大大小，MB**”

   默认值是 100 MB，可用值介于 1 MB 和 2048 MB 之间。当您所发送的高级诊断文件信息不足以定位问题时，您可能被 Kaspersky 技术支持专家要求更改默认值。

   如果您在上一步中启用了高级诊断，则必须指定此值。您可以在任务属性窗口的“**应用程序设置**”选项卡上创建任务后更改此值。

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。

    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。

关于任务计划的建议

计划“*查找漏洞和所需更新*”任务时，请确保两个选项“**运行错过的任务**”和“**使用任务启动自动随机延迟**”已启用。

默认情况下，“*查找漏洞和所需更新*”任务设置为手动启动。

您还可以安排“*查找漏洞和所需更新*”任务在特定时间启动。例如，您可以从任务属性窗口的“**每 N 小时**”选项卡上的“**启动任务**”下拉列表中选择“**计划**”计划启动。此时要注意，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后运行。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。您必须根据组织的工作规则为该任务设置最方便的计划。

有关计划启动设置的详细说明，请参阅常规任务设置。

# 查看有关可用的第三方软件更新的信息

您可以查看客户端设备上安装的第三方软件（包括 Microsoft 软件）的可用更新列表。

*要查看客户端设备上安装的第三方应用程序的可用更新列表：*

在主菜单中，前往**软件管理→补丁管理→ 软件更新**。

此时将显示可用更新列表。

您可以指定一个过滤器以查看软件更新列表。单击软件更新列表的“**过滤器**”图标 (  ) 以管理过滤器。您也可以从软件漏洞列表上方的“**预设过滤器**”下拉列表中选择一个预设过滤器。

*要查看更新的属性：*

1. 单击所需软件更新的名称。
2. 更新的属性窗口将打开，其中显示分组到以下选项卡上的信息：

- **常规**

  此选项卡显示所选更新的常规详细信息：

  - 更新批准状态（可以通过在下拉列表中选择新状态来手动更改）
  - 更新的注册日期和时间
  - 更新的创建日期和时间
  - 更新的重要级别
  - 更新限制的安装要求
  - 更新所属的应用程序系列
  - 更新适用的应用程序
  - 更新修订号

- **属性**

  此选项卡显示一组属性，这些属性可用于获取有关所选更新的更多信息。根据更新由 Microsoft 发布还是由第三方供应商发布，该属性组会有所不同。

  该选项卡显示 Microsoft 更新的以下信息：

  - 根据 Microsoft 安全响应中心 (MSRC) 定义的更新重要级别
  - 描述该更新的 Microsoft 知识库文章链接
  - 描述该更新的 Microsoft 安全公告文章链接
  - 更新标识符 (ID)

  该选项卡显示第三方更新的以下信息：

  - 更新是补丁还是完整分发包
  - 更新的本地化语言
  - 更新是自动安装还是手动安装
  - 应用更新后是否撤销更新
  - 更新的下载链接

- **设备**

  此选项卡显示已安装所选更新的设备列表。

- **已修复漏洞**

  此选项卡显示所选更新可以修复的漏洞列表。

- **更新融合**

  此选项卡显示为同一应用程序发布的各种更新之间的可能交叉，即，所选更新是否可以取代其他更新，或者反过来被其他更新取代（仅适用于 Microsoft 更新）。

- **安装该更新的任务**

  此选项卡显示一个任务列表，这些任务的范围包括安装所选更新。该选项卡还允许为更新创建新的远程安装任务。

*要查看更新安装的统计信息：*

1. 选中所需软件更新旁边的复选框。
2. 单击**更新安装状态统计信息**按钮。

将显示更新安装状态图。单击某个状态将打开具有所选状态的设备列表。

您可以查看所选的运行 Windows 的受管理设备上安装的第三方软件（包括 Microsoft 软件）的可用软件更新的信息。

*要查看所选受管理设备上安装的第三方软件的可用更新列表：*

1. 在主菜单中，转到“**资产管理**” → “**资产(设备)**”。

   将显示受管理设备列表。

2. 在受管理设备列表中，单击含有要查看其第三方软件更新的设备的名称的链接。

   将显示所选设备的属性窗口。

3. 在所选设备的属性窗口中，选择“**高级**”选项卡。

4. 在左侧窗格中，选择“**可用更新**”区域。如果只想查看已安装的更新，请启用“**显示已安装的更新**”选项。

将显示所选设备的可用第三方软件更新列表。

# 将可用软件更新列表导出到文件

您可以将第三方软件（包括 Microsoft 软件）的更新列表导出为 CSV 或 TXT 文件。例如，您可以将这些文件发送给信息安全经理或妥善保存以供统计之用。

*要将所有受管理设备上安装的第三方软件的可用更新列表导出到文本文件：*

1. 在主菜单中，转到**操作 → 补丁管理 → 软件更新**。

   此时将显示可用更新列表。

   如果要导出完整的软件更新列表，则仅导出当前页面上显示的更新。

   如果您只想导出特定更新，请选中列表中所需更新旁边的复选框。

2. 根据您需要导出的格式，单击“**导出到 TXT**”或“**导出到 CSV**”按钮。如果这两个按钮都不可见，请单击省略号按钮，然后从下拉列表中选择所需的选项。

包含第三方软件（包括 Microsoft 软件）可用更新列表的文件将下载到您当时正在使用的设备上。

*要将选定受管理设备上安装的第三方软件的可用更新列表导出到文本文件：*

1. 打开选定受管理设备上的可用第三方软件更新列表。

   此时将显示可用更新列表。

   如果要导出完整的软件更新列表，则仅导出当前页面上显示的更新。

   如果您只想导出特定更新，请选中列表中所需更新旁边的复选框。

   如果要只导出已安装的更新，请选中“**显示已安装的更新**”复选框。

2. 根据您需要导出的格式，单击“**导出到 TXT**”或“**导出到 CSV**”按钮。如果这两个按钮都不可见，请单击省略号按钮，然后从下拉列表中选择所需的选项。

包含所选受管理设备上安装的第三方软件（包括 Microsoft 软件）的可用更新列表的文件将下载到您当时正在使用的设备上。

# 批准和拒绝第三方软件更新

配置“*安装所需更新并修复漏洞*”任务时，可以创建一条要求待安装的更新处于特定状态的规则。例如，更新规则可以允许安装以下更新：

- 仅限已批准的更新
- 仅限已批准和未定义的更新
- 所有更新，无论更新状态如何

您可以批准必须安装的更新并拒绝不能安装的更新。

使用“*已批准*”状态来管理更新安装对于少量更新来说非常有效。要安装多个更新，请使用可以在“*安装所需更新并修复漏洞*”任务的属性中配置的规则。我们建议仅为那些不符合规则中指定条件的特定更新设置“*已批准*”状态。当您手动批准大量更新时，管理服务器的性能会下降，这可能会导致管理服务器过载。

*要批准或拒绝一个或几个更新：*

1. 在主菜单中，前往**软件管理→补丁管理→ 软件更新**。

   将显示可用更新列表。

2. 选择您要批准或拒绝的更新。
3. 单击“**批准**”按钮以批准所选更新或单击“**拒绝**”按钮以拒绝所选更新。如果这两个按钮都不可见，请单击省略号按钮，然后从下拉列表中选择所需的选项。

   更新的默认状态为“*未定义*”。

所选更新具有您定义的状态。

作为一个选项，您可以在特定更新的属性中更改批准状态。

*要在其属性中批准或拒绝更新：*

1. 在主菜单中，前往**软件管理→补丁管理→ 软件更新**。

   将显示可用更新列表。

2. 单击要批准或拒绝的更新的名称。

   更新属性窗口打开。

3. 在“**常规**”部分中，在“**更新批准状态**”下拉列表中选择更新状态。您可以选择“*已批准*”、“*已拒绝*”或“*未定义*”状态。
4. 单击“**保存**”按钮以保存更改。

所选更新具有您定义的状态。

如果您为第三方软件更新设置了“*已拒绝*”状态，这些更新将不会安装在计划安装但尚未安装的设备上。更新将保持在已将其安装的设备上。如有必要，您可以手动在本地删除这些更新。

# 创建“安装所需更新并修复漏洞”任务

“*安装所需更新并修复漏洞*”任务仅在漏洞和补丁管理授权许可下可用。

“*安装所需更新并修复漏洞*”任务用于更新和修复在受管理设备上安装的第三方软件存在的漏洞。此任务允许您根据在任务设置中指定的规则安装多个更新并修复多个漏洞。

要使用“*安装所需更新并修复漏洞*”任务安装更新或修复漏洞，可以执行以下任一操作：

- 运行更新安装向导或漏洞修复向导。
- 创建“*安装所需更新并修复漏洞*”任务。
- 向现有的“*安装所需更新并修复漏洞*”任务添加更新安装规则。

*要创建“安装所需更新并修复漏洞”任务：*

1. 在主菜单中，转到“**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 Kaspersky Security Center。
4. 在“**任务类型**”列表中，选择“**安装所需更新并修复漏洞**”任务类型。

   如果未显示任务，请检查您的账户是否有对“**系统管理**：**漏洞和补丁管理**”功能区域的**读取**、**写入**和**执行**权限。如果没有这些访问权限，您无法创建和配置“*安装所需更新并修复漏洞*”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. 在向导的“**指定更新安装规则**”步骤，添加更新安装规则。

   这些规则被应用到客户端设备上的更新安装。如果规则未被指定，任务无可执行。有关按照规则进行操作的信息，请参考更新安装规则。

   这些规则被应用到客户端设备上的更新安装。如果不指定任何规则，则该任务无可执行。
8. 指定下列设置：

   - **在设备重启或关闭时开始安装**

     如果启用该选项，更新在设备被重启或关闭时安装。否则，更新根据计划安装。

     如果安装更新可能影响设备性能则使用该选项。

     默认情况下已禁用该选项。

- **安装所需的常规系统组件**

  如果启用该选项，在安装更新之前，应用程序自动安装所需的所有常规系统组件（先决条件）。例如，这些先决条件可以是操作系统更新。

  如果禁用该选项，您可能必须手动安装先决条件。

  默认情况下已禁用该选项。

- **更新过程中允许安装新应用程序版本**

  如果启用该**选项**，如果更新导致软件应用程序新版本的安装，更新将被允许。

  如果禁用该选项，软件不被升级。您可以稍后手动或通过其他任务安装软件的新版本。例如，如果公司基础架构不被新软件版本支持，或者如果您想要在测试基础架构中检查升级，您可能使用该选项。

  默认情况下已启用该选项。

  > 升级应用程序可能导致安装在客户端设备上的独立应用程序功能异常。

- **下载更新到设备而不安装**

  如果启用该选项，应用程序下载更新到设备但是不自动安装它们。您可以稍后手动安装下载的更新。

  Microsoft 更新被下载到系统 Windows 存储。第三方应用程序更新（由非 Kaspersky 和 Microsoft 软件供应商开发的应用程序）将会下载到"**下载更新到**"字段中指定的文件夹中。

  如果禁用该选项，更新被自动安装到设备。

  默认情况下已禁用该选项。

  - **下载更新到**

    该文件夹用于下载第三方应用程序（由非 Kaspersky 和 Microsoft 软件供应商制作的应用程序）更新。

- **启用高级诊断**

  如果启用该功能，即便写入跟踪文件在 Kaspersky Security Center Linux 远程诊断实用程序中对网络代理禁用，网络代理也会写入跟踪文件。跟踪轮流写入两个文件中；两个文件的总大小由"**高级诊断文件的最大大小，MB**"值决定。当两个文件都满时，网络代理再次开始写入它们。带有跟踪的文件存储在 %WINDIR%\Temp 文件夹。这些文件在远程诊断实用程序中可以被访问，您可以在那里下载或删除它们。

  如果禁用该功能，网络代理根据 Kaspersky Security Center Linux 远程诊断实用程序中的设置写入跟踪。没有附加跟踪被写入。

  当创建任务时，您不必启用高级诊断。例如，如果某个任务在一些设备上失败并且您希望在另一个任务运行期间获取额外信息，您可能希望稍后使用该功能。

  默认情况下已禁用该选项。

  - **高级诊断文件的最大大小，MB**

    默认值是 100 MB，可用值介于 1 MB 和 2048 MB 之间。当您所发送的高级诊断文件信息不足以定位问题时，您可能被 Kaspersky 技术支持专家要求更改默认值。

继续执行向导的下一步。

9. 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。

- **提示用户操作**

  客户端设备屏幕上将显示重启提醒，提示用户手动重启设备。可以为该选项定义一些高级设置：用户消息文本、消息显示频率以及强制重启（不需要用户确认）的时间间隔。该选项适用于用户必须可以选择最方便的时间进行重启的工作站。

  默认情况下已选定该选项。

- **重复提示间隔(分钟)**

  如果启用该选项，应用程序以指定频率提示用户重启操作系统。

  默认情况下已启用该选项。默认时间间隔为 5 分钟。可用值介于 1 和 1 440 分钟之间。

  如果禁用该选项，提示仅显示一次。

- **在该时间后重启(分钟)**

  提示用户之后，应用程序在指定时间间隔后强制操作系统重启。

  默认情况下已启用该选项。默认延时是 30 分钟。可用值介于 1 和 1 440 分钟之间。

- **在该时间后强制关闭阻止会话中的应用程序(分钟)**

  用户设备锁定时，程序以强制模式关闭（指定不活动间隔之后自动锁定，或手动锁定）。

  如果启用此选项，当输入字段中指定的时间间隔结束后，锁定设备上的应用程序将被强制关闭。

  如果禁用此选项，应用程序在锁定的设备上不关闭。

  默认情况下已禁用该选项。

10. 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。

11. 单击“**完成**”按钮。

    新任务向导将创建任务。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。

12. 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。

任务完成后，安装所需的更新并修复漏洞。

如果您的组织网络中使用了 WSUS 服务器（本地 WSUS 服务器），并且您希望将其与 Kaspersky Security Center 管理服务器一起使用，则必须首先确保 Kaspersky Security Center 管理服务器未用作 WSUS 服务器，然后执行以下操作：

a. 在运行 Windows 的受管理设备上，为 Windows 更新服务指定本地 WSUS 服务器。您可以在 Windows 注册表中手动执行此操作，也可以使用 Windows 组策略执行此操作。

b. 在本地 WSUS 服务器上，指定更新所需的分类以及要分发更新的应用程序。

c. 将您的 WSUS 服务器与上游服务器同步（这可以是 Microsoft WSUS 服务器，也可以是另一个本地上游 WSUS 服务器）。

在设备上运行*安装所需更新和修复漏洞*任务后，网络代理使用 Windows 更新服务安装 Windows 更新。Windows 更新服务从注册表中获取外部 WSUS 服务器的地址，并直接从该外部服务器下载更新。

# 添加更新安装规则

此功能仅在“漏洞和补丁管理”授权许可下可用。

使用“*安装所需更新并修复漏洞*”任务安装软件更新或修复软件漏洞时，您必须指定更新安装规则。这些规则决定要安装的更新和要修复的漏洞。

精确设置取决于您是否添加了所有更新、Windows Update 更新、第三方应用程序（由非 Kaspersky 和 Microsoft 软件供应商制作的应用程序）更新的规则。当添加 Windows Update 更新或第三方应用程序更新的规则时，您可以选择特定的应用程序和您要安装更新的应用程序版本。当添加所有更新的规则时，您可以选择您要安装的特定更新和您要通过安装更新进行修复的漏洞。

您可以通过以下方式添加更新安装规则：

- 通过在创建新“*安装所需更新并修复漏洞*”任务时添加规则。
- 通过在现有的“*安装所需更新并修复漏洞*”任务属性窗口的“**应用程序设置**”选项卡中添加规则。
- 通过更新安装向导或漏洞修复向导。

## 添加所有更新的规则

*要添加所有更新的规则：*

1. 单击“**添加**”按钮。

   “规则创建向导”向导启动。使用“**下一步**”按钮继续向导操作。

2. 在向导的“**选择规则类型**”步骤中，选择“**所有更新的规则**”。

3. 在向导的“**常规标准**”步骤中，指定以下设置：

- **要安装的一组更新**

  选择必须在客户端设备上安装的更新：

  - **仅安装批准的更新**。这仅安装批准的更新。
  - **安装所有更新 (除了拒绝的)**。这将安装带有“*已批准*”或“*未定义*”批准状态的更新。
  - **安装所有更新 (包括拒绝的)**。这安装所有更新，无论什么批准状态。警惕选择该选项。例如，如果您想要在测试基础架构中检查一些被拒绝的更新的安装，使用该选项。

- **修复严重级别等于或大于该项的漏洞**

  有时候，软件更新可能损害用户的软件体验。此种情况下，您可能决定仅安装软件操作的关键更新并跳过其他更新。

  如果启用该选项，更新仅修复 Kaspersky 设置的严重级别等于或高于列表中选定的值（**中度**、**高危**或**严重**）的漏洞。严重级别低于选定值的漏洞不被修复。

  如果禁用该选项，更新修复所有漏洞，无论它们的严重级别是什么。

  默认情况下已禁用该选项。

继续执行向导的下一步。

4. 选择要安装的更新：

- **安装所有适用的更新**

  安装符合向导“**常规标准**”步骤中指定条件的所有软件更新。默认选择。

- **仅安装列表中的更新**

  仅安装您从列表中手动选择的软件更新。该列表包含所有可用软件更新。

  例如，您可能想要在以下情况下选择特定更新：要在测试环境中检查它们的安装、要仅更新严重应用程序、或者要仅更新特定应用程序。

  - **自动安装所选更新安装所需的所有先前应用程序更新**

    如果在安装所选更新需要时，您同意安装临时应用程序版本，保持该选项被启用。

    如果禁用该选项，仅选定的应用程序版本被安装。如果您想直截了当地更新应用程序，而不尝试安装增量版本，请禁用该选项。如果安装所选更新不能不安装先前版本的应用程序，应用程序更新失败。

    例如，您在设备上安装了应用程序的版本 3，您想更新它到版本 5，但是该应用程序的版本 5 仅可以在版本 4 之上安装。如果启用该选项，软件先安装版本 4，然后安装版本 5。如果禁用该选项，软件更新应用程序失败。

    默认情况下已启用该选项。

继续执行向导的下一步。

5. 选择通过安装所选更新进行修复的漏洞：

- **修复所有匹配其他标准的漏洞**

  修复符合向导“**常规标准**”步骤中指定条件的所有漏洞。默认选择。

- **仅修复列表中的漏洞**

  仅修复您手动从列表中选择的漏洞。列表包含所有检测到的漏洞。

  例如，您可能想要在以下情况下选择特定漏洞：要在测试环境中检查它们的修复、要仅修复严重应用程序中的漏洞、或者要仅修复特定应用程序中的漏洞。

继续执行向导的下一步。

6. 指定要添加的规则的名称。您可以稍后在所创建任务的属性窗口的"**应用程序设置**"选项卡中更改该名称。

新规则已创建、配置并显示在新任务向导的规则表中。

## 为来自 Windows Update 的更新添加规则

*要为来自 Windows Update 的更新添加新规则：*

1. 单击"**添加**"按钮。

   "规则创建向导"向导启动。使用"**下一步**"按钮继续向导操作。

2. 选择"**Windows 更新的规则**"。

   继续执行向导的下一步。

3. 在向导的"**常规标准**"步骤中，指定以下设置：

   - **要安装的更新集**

     选择必须在客户端设备上安装的更新：

     - **仅安装批准的更新**。这仅安装批准的更新。
     - **安装所有更新 (除了拒绝的)**。这将安装带有"*已批准*"或"*未定义*"批准状态的更新。
     - **安装所有更新 (包括拒绝的)**。这安装所有更新，无论什么批准状态。警惕选择该选项。例如，如果您想要在测试基础架构中检查一些被拒绝的更新的安装，使用该选项。

   - **修复严重级别等于或大于该项的漏洞**

     有时候，软件更新可能损害用户的软件体验。此种情况下，您可能决定仅安装软件操作的关键更新并跳过其他更新。

     如果启用该选项，更新仅修复 Kaspersky 设置的严重级别等于或高于列表中选定的值（**中度**、**高危**或**严重**）的漏洞。严重级别低于选定值的漏洞不被修复。

     如果禁用该选项，更新修复所有漏洞，无论它们的严重级别是什么。

     默认情况下已禁用该选项。

   - **修复 MSRC 严重级别等于或大于该项的漏洞**

     有时候，软件更新可能损害用户的软件体验。此种情况下，您可能决定仅安装软件操作的关键更新并跳过其他更新。

     如果启用该选项，更新仅修复 Microsoft Security Response Center (MSRC) 设置的严重级别等于或高于列表中选定的值（**低**、**中度**、**高危**或**严重**）的漏洞。严重级别低于选定值的漏洞不被修复。

     如果禁用该选项，更新修复所有漏洞，无论它们的严重级别是什么。

     默认情况下已禁用该选项。

4. 在**应用程序**页面，选择您要安装更新的应用程序和应用程序版本。默认情况下选定所有应用程序。

5. 在**更新类别**页面，选择要安装的更新类别。这些类别与 Microsoft Update Catalog 中的类别相同。默认情况下选定所有类别。

6. 在“**名称**”页面，指定您正在添加的规则的名称。您可以稍后在所创建任务的属性窗口的“**设置**”区域更改该名称。

规则创建向导完成操作后，新规则将添加，并显示在新任务向导或任务属性的规则列表中。

## 添加第三方应用程序更新规则

*要添加第三方应用程序更新的新规则：*

1. 单击“**添加**”按钮。

   “规则创建向导”向导启动。使用“**下一步**”按钮继续向导操作。

2. 在向导的“**选择规则类型**”步骤中，选择“**第三方更新的规则**”。

3. 在向导的“**常规标准**”步骤中，指定以下设置：

   - **要安装的更新集**

     选择必须在客户端设备上安装的更新：

     - **仅安装批准的更新**。这仅安装批准的更新。
     - **安装所有更新 (除了拒绝的)**。这将安装带有“*已批准*”或“*未定义*”批准状态的更新。
     - **安装所有更新 (包括拒绝的)**。这安装所有更新，无论什么批准状态。警惕选择该选项。例如，如果您想要在测试基础架构中检查一些被拒绝的更新的安装，使用该选项。

   - **修复严重级别等于或大于该项的漏洞**

     有时候，软件更新可能损害用户的软件体验。此种情况下，您可能决定仅安装软件操作的关键更新并跳过其他更新。

     如果启用该选项，更新仅修复 Kaspersky 设置的严重级别等于或高于列表中选定的值（**中度**、**高危**或**严重**）的漏洞。严重级别低于选定值的漏洞不被修复。

     如果禁用该选项，更新修复所有漏洞，无论它们的严重级别是什么。

     默认情况下已禁用该选项。

   继续执行向导的下一步。

4. 选择您要安装更新的应用程序和应用程序版本。

   默认情况下选定所有应用程序。

   继续执行向导的下一步。

5. 指定要添加的规则的名称。您可以稍后在所创建任务的属性窗口的“**应用程序设置**”选项卡中更改该名称。

新规则已创建、配置并显示在新任务向导的规则表中。

# 任务创建后指定的安装所需更新并修复漏洞任务的设置

创建“*安装所需更新并修复漏洞*”任务后，您可以在任务属性窗口的“**应用程序设置**”选项卡上指定以下设置：

- 在“**测试安装**”部分：
  - **不扫描**。如果您不希望执行更新的测试安装，请选择该选项。
  - **在选定设备上运行扫描**。如果要在所选设备上测试更新安装，请选择该选项。单击“**添加**”按钮，然后选择您需要在其上执行更新安装测试的设备。
  - **在指定组中的设备上运行扫描**。如果要在一组设备上测试更新安装，请选择该选项。在“**指定测试组**”字段中，指定您要在其上执行测试安装的设备组。
  - **在指定百分比的设备上运行扫描**。如果要在一定比例的设备上测试更新安装，请选择该选项。在“**所有目标设备中测试设备的百分比**”字段中，指定您要在其上执行更新测试安装的设备的百分比。

  选择除了“**不扫描**”的任意选项，在“**决定是否继续进行安装所需的时间(小时)**”字段中指定从更新安装测试到开始将更新安装到所有目标设备上必须历经的小时数。
- 在“**要安装的更新**”区域，您可以查看任务安装的更新列表。仅匹配应用的任务设置的更新被显示。

有关任务设置的详细说明，请参阅常规任务设置。

# 自动更新第三方应用程序

某些第三方应用程序可以自动更新。应用程序供应商定义应用程序是否支持自动更新功能。如果受管理设备上安装的第三方应用程序支持自动更新，则可以在应用程序属性中指定自动更新设置。更改自动更新设置后，网络代理会将新设置应用于安装了该应用程序的每个受管理设备。

自动更新设置独立于“漏洞和补丁管理”功能的其他对象和设置。例如，此设置不取决于更新批准状态或更新安装任务，如“*安装所需更新并修复漏洞*”和“*修复漏洞*”。

*要为第三方应用程序配置自动更新设置：*

1. 在主菜单中，前往**软件管理→第三方应用程序→ 应用程序注册表**。
2. 单击要为其更改自动更新设置的应用程序的名称。

   为简化搜索，您可以按“**自动更新状态**”和“**管理自动更新**”列过滤列表。

   应用程序属性窗口打开。
3. 在“**常规**”区域中，为以下功能选择一个值：

   **自动更新状态**。

   您可以选择以下选项之一：
   - **未定义**

     自动更新功能已禁用。Kaspersky Security Center Linux 使用以下任务来安装第三方应用程序更新：“*安装所需更新并修复漏洞*”和“*修复漏洞*”。

- **已允许**

  供应商发布应用程序更新后，此更新将自动安装在受管理设备上。不需要其他操作。

- **已阻止**

  应用程序更新不会自动安装。Kaspersky Security Center Linux 使用以下任务来安装第三方应用程序更新：“*安装所需更新并修复漏洞*”和“*修复漏洞*”。

4. 单击“**保存**”按钮以保存更改。

自动更新设置将应用于所选应用程序。

# 修复第三方软件漏洞

本部分描述了 Kaspersky Security Center Linux 的功能，这些功能与修复受管理设备上所安装软件中的漏洞有关。

# 关于查找和修复软件漏洞

Kaspersky Security Center Linux 会检测并修复运行 Microsoft Windows 操作系统的受管理设备上的软件漏洞。将在操作系统和第三方软件（包括 Microsoft 软件）中检测漏洞。

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。

## 查找软件漏洞

Kaspersky Security Center Linux 会根据已知漏洞数据库中的特征来查找软件漏洞。该数据库由卡巴斯基专家创建并保持更新。数据库包含有关漏洞的信息，例如漏洞描述、漏洞检测日期、漏洞严重级别。您可以在卡巴斯基网站上查看软件漏洞详情。

Kaspersky Security Center Linux 使用“*查找漏洞和所需更新*”任务来查找软件漏洞。

## 修复软件漏洞

Kaspersky Security Center 使用软件供应商发布的软件更新来修复软件漏洞。运行“*将更新下载至管理服务器存储库*”任务后，软件更新的元数据将被下载到管理服务器存储库。该任务旨在下载卡巴斯基和第三方软件更新的元数据。该任务由 Kaspersky Security Center Linux 快速启动向导自动创建。您可以手动创建“*将更新下载至管理服务器存储库*”任务。

修复漏洞的软件更新可以是完整的分发包，也可以是补丁。修复软件漏洞的软件更新称为*修补程序*。*推荐的修补程序*是 Kaspersky 专家建议安装的修补程序。*用户修补程序*是用户手动指定安装的修补程序。要安装用户修补程序，您必须创建一个包含此修补程序的安装包。

如果您没有带漏洞和补丁管理功能的 Kaspersky Security Center Linux 授权许可，则可以使用“*安装所需更新并修复漏洞*”任务。该任务会通过安装建议修复程序来自动修复多个漏洞。对于此任务，您可以手动配置某些规则来修复多个漏洞。

如果您没有带漏洞和补丁管理功能的 Kaspersky Security Center Linux 授权许可，则可以使用“*修复漏洞*”任务。借助此任务，您可以通过安装针对 Microsoft 软件的建议修复程序和针对其他第三方软件的用户修复程序来修复漏洞。

出于安全原因，卡巴斯基技术会自动扫描您使用漏洞和补丁管理功能安装的任何第三方软件更新，以查找恶意软件。这些技术用于自动文件检查，包括病毒扫描、静态分析、动态分析、沙盒环境中的行为分析和机器学习。

卡巴斯基专家不会对可以使用漏洞和补丁管理功能安装的第三方软件更新进行手动分析。此外，卡巴斯基专家不会在此类更新中搜索漏洞（已知或未知）或未记录的功能，也不会对上面段落中指定的更新以外的更新进行其他类型的分析。

在受管理设备上更新第三方应用程序或修复第三方应用程序中的漏洞时，可能需要用户交互。例如，如果第三方应用程序当前处于打开状态，则用户可能会被提示将其关闭。

要修复某些软件漏洞，如果请求接受最终用户授权许可协议 (EULA)，则必须接受 EULA 才能安装软件。如果您拒绝 EULA，则该软件漏洞不会得到修复。

# 方案：查找和修复第三方软件中的漏洞

本节提供了在运行 Windows 的受管理设备上查找和修复漏洞的方案。您可以在操作系统和第三方软件（包括 Microsoft 软件）中查找和修复软件漏洞。

## 先决条件

- Kaspersky Security Center Linux 已部署在您的组织中。
- 您的组织中存在运行 Windows 系统的受管理设备。
- 管理服务器需要连接互联网才能执行以下任务：
  - 针对 Microsoft 软件漏洞生成推荐的修复程序列表。该列表由 Kaspersky 专家创建并定期更新。
  - 修复除 Microsoft 软件以外的第三方软件的漏洞。

## 阶段

查找和修复软件漏洞的过程分为以下几个阶段：

1. **扫描受管理设备上安装的软件中的漏洞**

   要查找受管理设备上安装的软件中的漏洞，请运行“*查找漏洞和所需更新*”任务。完成此任务后，Kaspersky Security Center Linux 会收到检测到的漏洞列表，以及任务属性中指定设备上安装的第三方软件的所需更新。

"*查找漏洞和所需更新*"任务由 Kaspersky Security Center Linux 快速启动向导自动创建。如果您未运行向导，请立即启动向导或手动创建该任务。

> 您只能为 Windows 设备创建"*查找漏洞和所需更新*"任务。您无法为运行其他操作系统的设备创建此任务。

### 2 查看检测到的软件漏洞列表

查看"**软件漏洞**"列表，并确定要修复的漏洞。要查看有关每个漏洞的详细信息，请单击列表中的漏洞名称。对于列表中的每个漏洞，您还可以查看关于受管理设备上的这些漏洞的统计信息。

### 3 配置漏洞修复

检测到软件漏洞后，可以使用"*安装所需更新并修复漏洞*"任务或"*修复漏洞*"任务来修复受管理设备上的这些软件漏洞。

"*安装所需更新并修复漏洞*"任务用于更新和修复在受管理设备上安装的第三方软件（包括 Microsoft 软件）中的漏洞。通过此任务，您可以根据某些规则安装多个更新并修复多个漏洞。请注意，仅当您具有漏洞和补丁管理功能的授权许可时，才能创建此任务。为修复软件漏洞，*安装所需更新并修复漏洞*任务将使用建议的软件更新。

*修复漏洞*任务不需要"漏洞和补丁管理"功能的授权许可选项。要使用此任务，必须手动为任务设置中列出的第三方软件中的漏洞指定用户修复程序。"*修复漏洞*"任务使用针对 Microsoft 软件的建议修复程序和针对第三方软件的用户修复程序。

> 您只能为 Windows 设备创建"*安装所需更新并修复漏洞*"任务和"*修复漏洞*"任务。您无法为运行其他操作系统的设备创建这些任务。

您可以启动漏洞修复向导来自动创建这些任务之一，也可以选择手动操作。

如果已创建并配置了"*安装所需更新并修复漏洞*"任务，则受管理设备上的漏洞会自动修复。已创建的任务启动时，它会将可用软件更新列表与任务设置中指定的规则相关联。所有符合指定规则中条件的软件更新都将下载到管理服务器存储库中，并将进行安装以修复软件漏洞。

如果创建了"*修复漏洞*"任务，则仅修复 Microsoft 软件中的软件漏洞。

### 4 安排任务

安排"*查找漏洞和所需更新*"任务定期自动运行，确保漏洞列表始终是最新版本。建议每周运行一次。

如果您创建了"*安装所需更新并修复漏洞*"任务，则可以安排其与"*查找漏洞和所需更新*"任务相同或更少的频率运行。计划"*修复漏洞*"任务时，请注意，每次启动任务之前，都必须选择 Microsoft 软件的修补程序或为第三方软件指定用户修补程序。

安排任务时，请确保在完成"*查找漏洞和所需更新*"任务之后启动修复漏洞的任务。

### 5 忽略软件漏洞（可选）

您可以忽略所有受管理设备上或仅所选受管理设备上的软件漏洞。

### 6 运行漏洞修复任务

启动*安装所需更新并修复漏洞*任务或*修复漏洞*任务。任务完成后，请确保它在任务列表中具有"*成功完成*"状态。

### 7 创建有关修复软件漏洞的结果报告（可选）

要查看有关已修复漏洞的详细统计信息，请生成漏洞报告。该报告显示有关未修复软件漏洞的信息。报告有助于识别和修复组织中使用的第三方软件（包括 Microsoft 软件）中的漏洞。

### 8 检查关于查找和修复第三方软件中漏洞的配置

确保已完成以下操作：

- 获取并查看了受管理设备上的软件漏洞列表。
- 可以酌情忽略某些软件漏洞。
- 配置任务以修复漏洞。
- 安排查找和修复软件漏洞的任务，使其按顺序启动。
- 检查是否已运行修复软件漏洞的任务。

# 修复第三方软件漏洞

要查找第三方软件漏洞，您可以创建并运行“*查找漏洞和所需更新*”任务并接收软件漏洞列表。获取软件漏洞列表后，可以修复运行 Windows 的受管理设备所存在的漏洞。

您可以通过创建并运行“修复漏洞”任务或“安装所需更新并修复漏洞”任务来修复操作系统和第三方软件（包括 Microsoft 软件）中的软件漏洞。

> 在受管理设备上更新第三方应用程序或修复第三方应用程序中的漏洞时，可能需要用户交互。例如，如果第三方应用程序当前处于打开状态，则用户可能会被提示将其关闭。

作为一种选择，您可以通过以下方式创建任务来修复软件漏洞：

- 通过打开漏洞列表并指定要修复的漏洞。
  结果，创建了修复软件漏洞的新任务。作为一个选项，您可以将选定漏洞添加到现有任务。
- 通过运行漏洞修复向导。

  > 漏洞修复向导仅在漏洞和补丁管理授权许可下可用。

  该向导简化了漏洞修复任务的创建和配置，并允许您消除冗余任务的创建。

## 使用漏洞列表修复软件漏洞

*要使用漏洞列表修复软件漏洞：*

1. 通过执行以下操作之一打开漏洞列表：
   - 在主菜单中，前往**软件管理→补丁管理→软件漏洞**。
   - 在主菜单中，转到“**资产管理**”→“**资产(设备)**”→ <设备名称> →“**高级**”→“**软件漏洞**”。
   - 在主菜单中，前往**软件管理→第三方应用程序→应用程序注册表→**<应用程序名称>**→漏洞**。

   将显示一个表格，其中列出了受管理设备上安装的第三方软件中的漏洞。

2. 在漏洞列表中，选中需要修复的漏洞旁边的复选框，然后单击“**修复漏洞**”按钮。

   如果缺少用于修复所选漏洞之一的推荐软件更新，将显示一条信息消息。

   要修复某些软件漏洞，如果请求接受最终用户授权许可协议 (EULA)，则必须接受 EULA 才能安装软件。如果您拒绝 EULA，则该软件漏洞不会得到修复。

3. 您可以选择以下选项之一：

   - **新任务**

     新任务向导启动。如果您拥有漏洞和补丁管理授权许可，则会预先选择“安装所需更新并修复漏洞”任务。如果您没有授权许可，则会预先选择“修复漏洞”任务。按照向导的步骤完成任务创建。

   - **修复漏洞(添加规则到指定任务)**

     选择要向其中添加选定漏洞的任务。如果您拥有漏洞和补丁管理授权许可，请选择“安装所需更新并修复漏洞”任务。修复选定漏洞的新规则将自动添加到选定任务中。如果您没有授权许可，请选择“修复漏洞”任务。所选漏洞将添加到任务属性中。

     任务属性窗口打开。单击“**保存**”按钮以保存更改。

如果您选择了创建任务，则会创建任务并将其显示在“**任务**”处的任务列表中。如果您选择了将漏洞添加到现有任务中，漏洞将保存在任务属性中。

要修复第三方软件漏洞，请启动“安装所需更新并修复漏洞”任务或“修复漏洞”任务。如果您已创建“修复漏洞”任务，则必须手动指定任务设置中列出的软件更新。

## 使用漏洞修复向导修复软件漏洞

> 漏洞修复向导仅在“漏洞和补丁管理”授权许可下可用。

*要使用漏洞修复向导来修复软件漏洞：*

1. 在主菜单中，前往**软件管理→补丁管理→软件漏洞**。

   将显示一个表格，其中列出了受管理设备上安装的第三方软件中的漏洞。

2. 选中要修复的漏洞旁边的复选框。

3. 单击**运行漏洞修复向导**按钮。

   > 如果选择多个漏洞，该按钮将被禁用。

   漏洞修复向导启动。将显示现有任务列表。此列表可能包含以下类型的任务：

   - 安装所需更新并修复漏洞
   - 修复漏洞

   您无法修改“修复漏洞”任务来安装新更新。要安装新更新，您只能使用“安装所需更新并修复漏洞”任务。

4. 如果您希望向导仅显示那些修复所选漏洞的任务，请启用“**仅显示修复该漏洞的任务**”选项。

5. 执行以下操作之一：

- 要启动任务，请选中任务名称旁边的复选框，然后单击“**开始**”按钮。

  不需要进一步操作。您可以关闭该向导。该任务将在后台模式下完成。

- 向现有的“安装所需更新并修复漏洞”任务添加新规则：

  a. 选中任务名称旁边的复选框，然后单击“**添加规则**”按钮。

  > 如果选择多个任务，“**添加规则**”按钮将被禁用。

  您无法为“修复漏洞”任务添加规则。如果您选择“修复漏洞”任务，会显示以下通知：“要安装更新，请使用“安装所需更新并修复漏洞”任务。”

  b. 在打开的页面上，配置新规则：

  - **修复该严重级别的漏洞的规则**

    有时候，软件更新可能损害用户的软件体验。此种情况下，您可能决定仅安装软件操作的关键更新并跳过其他更新。

    如果启用该选项，更新仅修复 Kaspersky 设置的严重级别等于或高于所选更新的严重性级别（**中度**、**高危**或**严重**）的漏洞。严重级别低于选定值的漏洞不被修复。

    如果禁用该选项，更新修复所有漏洞，无论它们的严重级别是什么。

    默认情况下已禁用该选项。

  - **通过与所选漏洞的建议定义的更新类型相同的更新来修复漏洞的规则**

    仅针对 Microsoft 软件漏洞显示此规则。

  - **修复所选供应商的应用程序中的漏洞的规则**

    仅针对第三方软件漏洞显示此规则。

  - **修复所选应用程序的所有版本中的漏洞的规则**

    仅针对第三方软件漏洞显示此规则。

  - **修复所选漏洞的规则**

  - **批准修复该漏洞的更新**

    所选更新将被批准安装。如果一些应用的更新安装规则仅允许安装批准的更新，启用该选项。

    默认情况下已禁用该选项。

  c. 单击“**添加**”按钮。

  任务属性窗口打开。新规则已添加到任务属性中。您可以查看或修改规则或其他任务设置。单击“**保存**”按钮以保存更改。

- 要创建任务：

  a. 单击“**新任务**”按钮。

  b. 在打开的页面上，配置新规则：

  - **修复该严重级别的漏洞的规则**

    有时候，软件更新可能损害用户的软件体验。此种情况下，您可能决定仅安装软件操作的关键更新并跳过其他更新。

    如果启用该选项，更新仅修复 Kaspersky 设置的严重级别等于或高于所选更新的严重性级别（**中度**、**高危**或**严重**）的漏洞。严重级别低于选定值的漏洞不被修复。

    如果禁用该选项，更新修复所有漏洞，无论它们的严重级别是什么。

    默认情况下已禁用该选项。

  - **通过与所选漏洞的建议定义的更新类型相同的更新来修复漏洞的规则**

    仅针对 Microsoft 软件漏洞显示此规则。

  - **修复所选供应商的应用程序中的漏洞的规则**

    仅针对第三方软件漏洞显示此规则。

  - **修复所选应用程序的所有版本中的漏洞的规则**

    仅针对第三方软件漏洞显示此规则。

  - **修复所选漏洞的规则**

  - **批准修复该漏洞的更新**

    所选更新将被批准安装。如果一些应用的更新安装规则仅允许安装批准的更新，启用该选项。

    默认情况下已禁用该选项。

  c. 单击“**添加**”按钮。

  d. 继续在新任务向导中创建任务。

  您在漏洞修复向导中添加的新规则将显示在新任务向导的“**指定更新安装规则**”步骤中。完成向导后，“安装所需更新并修复漏洞”任务将被添加到任务列表中。

# 创建“修复漏洞”任务

“*修复漏洞*”任务允许您修复受管理设备上的软件漏洞。您可以修复第三方软件（包括 Microsoft 软件）中的软件漏洞。

> 您只能为 Windows 设备创建“*修复漏洞*”任务。您无法为运行其他操作系统的设备创建此任务。

仅当您拥有*漏洞和补丁管理授权许可*时，才可以创建新的“修复漏洞”任务。

要修复新漏洞，您可以将其添加到现有的*修复漏洞*任务中。我们建议您使用"*安装所需更新并修复漏洞*"任务，而不是"*修复漏洞*"任务。"*安装所需更新并修复漏洞*"任务让您能够根据您定义的规则自动安装多个更新和修复多个漏洞。

在受管理设备上更新第三方应用程序或修复第三方应用程序中的漏洞时，可能需要用户交互。例如，如果第三方应用程序当前处于打开状态，则用户可能会被提示将其关闭。

*要创建"修复漏洞"任务：*

1. 在主菜单中，转到"**任务**"。

   或者，您可以在"**任务**"选项卡的设备属性窗口中创建此任务。

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 Kaspersky Security Center。

4. 在"**任务类型**"列表中，选择"**修复漏洞**"任务类型。

5. 在**任务名称**字段中，指定新任务的名称。

   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（*<>-_?:\"|）。

6. 选择要将任务分配到的设备。

   继续执行向导的下一步。

7. 单击"**添加**"按钮。

   漏洞列表打开。

8. 在漏洞列表中，选中需要修复的漏洞旁边的复选框，然后单击"**确定**"按钮。

   Microsoft 软件漏洞通常具有建议的修复程序。无需其他操作。

   对于其他供应商的软件中的漏洞，您首先需要为要修复的每个漏洞指定用户修复程序。然后，您可以将这些漏洞添加至"*修复漏洞*"任务。

   继续执行向导的下一步。

9. 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。

- **提示用户操作**

  客户端设备屏幕上将显示重启提醒，提示用户手动重启设备。可以为该选项定义一些高级设置：用户消息文本、消息显示频率以及强制重启（不需要用户确认）的时间间隔。该选项适用于用户必须可以选择最方便的时间进行重启的工作站。

  默认情况下已选定该选项。

- **重复提示间隔(分钟)**

  如果启用该选项，应用程序以指定频率提示用户重启操作系统。

  默认情况下已启用该选项。默认时间间隔为 5 分钟。可用值介于 1 和 1 440 分钟之间。

  如果禁用该选项，提示仅显示一次。

- **在该时间后重启(分钟)**

  提示用户之后，应用程序在指定时间间隔后强制操作系统重启。

  默认情况下已启用该选项。默认延时是 30 分钟。可用值介于 1 和 1 440 分钟之间。

- **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。

继续执行向导的下一步。

10. 指定账户设置：

    - **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。

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**的任务列表中。

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。

任务完成后，所选漏洞就会被修复。

# 为第三方软件中的漏洞选择用户修补程序

要使用“*修复漏洞*”任务，您必须手动指定软件更新以修复任务设置中列出的第三方软件中的漏洞。“*修复漏洞*”任务使用针对 Microsoft 软件的建议修复程序以及针对其他第三方软件的用户修复程序。

*用户修复程序*是管理员手动指定安装以修复漏洞的软件更新。

*要为第三方软件中的漏洞选择用户修补程序，请执行以下操作：*

1. 在主菜单中，前往**软件管理→补丁管理→软件漏洞**。

   将显示一个表格，其中列出了受管理设备上安装的第三方软件中的漏洞。

2. 在软件漏洞列表中，单击带有要为其指定用户修复的软件漏洞名称的链接。

   所选漏洞的属性窗口将打开。

3. 在左侧窗格中，选择“**用户修复和其他修复**”区域。

   将显示所选软件漏洞的用户修复列表。

4. 单击“**添加**”按钮。

   此时将显示可用安装包的列表。显示的安装包列表对应于**软件管理→安装包**列表。

   如果尚未创建包含针对所选漏洞的用户修复程序的安装包，则可以立即通过单击“**新建**”按钮，然后按照新安装包向导来创建该包。

5. 选择一个或多个安装包，其中包含针对所选漏洞的一个或多个用户修复程序。

6. 单击“**保存**”按钮。

系统会指定包含软件漏洞用户修补程序的安装包。启动“*修复漏洞*”任务时，安装包就会进行安装并修复软件漏洞。

# 查看有关在所有受管理设备上检测到的软件漏洞的信息

在扫描受管理设备上的软件是否存在漏洞之后，您可以查看检测到的软件漏洞列表。如果运行管理服务器层次结构的任务，则可以只针对所选的管理服务器，查看已检测出漏洞的受管理设备列表。

您还可以生成和查看漏洞报告。

*要查看在所有受管理设备上检测到的软件漏洞列表，*

在主菜单中，转到“**操作**” → “**补丁管理**” → “**软件漏洞**”。

将显示在客户端设备上检测到的软件漏洞列表。

*要调整软件漏洞列表，*

单击软件漏洞列表右上角的“**过滤器**”图标 ( )，然后选择所需的过滤器。您也可以从软件漏洞列表上方的“**预设过滤器**”下拉列表中选择一个预设过滤器。

您可以获取列表中任何漏洞的详细信息。

*要获取有关软件漏洞的信息：*

在软件漏洞列表中，单击带有漏洞名称的链接。

软件漏洞的属性窗口打开。

# 查看有关在选定受管理设备上检测到的软件漏洞的信息

您可以查看有关在选定的运行 Windows 的受管理设备上检测到的软件漏洞的信息。

*要查看在选定受管理设备上检测到的软件漏洞列表：*

1. 在主菜单中，转到“**资产管理**”→“**资产(设备)**”。
   将显示受管理设备列表。
2. 在受管理设备列表中，单击含有要查看在其中检测到的软件漏洞的设备的名称的链接。
   将显示所选设备的属性窗口。
3. 在所选设备的属性窗口中，选择“**高级**”选项卡。
4. 在左侧窗格中，选择“**软件漏洞**”区域。

将显示在选定受管理设备上检测到的软件漏洞列表。

*要查看所选软件漏洞的属性，*

在软件漏洞列表中单击带有软件漏洞名称的链接。

将显示所选软件漏洞的属性窗口。

# 查看受管理设备上的漏洞统计信息

您可以查看受管理设备上每个软件漏洞的统计信息。统计信息以图表形式展示。图表将显示具有以下状态的设备数量：

- *忽略：<设备数>*。如果您在漏洞属性中手动设置了忽略漏洞的选项，则分配此状态。
- *已修复：<设备数>*。如果修复漏洞的任务成功完成，则分配此状态。
- *计划修复：<设备数>*。如果已创建修复漏洞的任务但该任务尚未执行，则分配此状态。
- *应用补丁：<设备数>*。如果您手动选择了软件更新以修复漏洞，但此软件更新尚未修复漏洞，则分配此状态。
- *需要修复：<设备数>*。如果漏洞仅在某些受管理设备上得到修复，并且需要在更多托管设备上修复漏洞，则分配此状态。

*要查看受管理设备上的漏洞统计信息，请执行以下操作：*

1. 在主菜单中，转到“**操作**” → “**补丁管理**” → “**软件漏洞**”。
   该页面显示在受管理设备上检测到的应用程序漏洞的列表。
2. 选中所需漏洞旁边的复选框。
3. 单击**设备漏洞统计信息**按钮。

   > 如果选择多个漏洞，“**设备漏洞统计信息**”按钮将被禁用。

将显示漏洞状态图。单击一种状态将打开漏洞处于选定状态的设备列表。

# 将软件漏洞列表导出到文件

您可以将显示的漏洞列表下载为 CSV 或 TXT 文件。您可以将这些文件发送给您的信息安全经理或者保存起来以供统计。

*要将在所有受管理设备上检测到的软件漏洞列表导出到文本文件：*

1. 在主菜单中，转到“**操作**” → “**补丁管理**” → “**软件漏洞**”。
   显示在受管理设备上检测到的应用程序中软件漏洞的列表。
   默认情况下，只导出当前页面显示的漏洞。
   如果您只想导出特定漏洞，请选中这些漏洞旁边的复选框。
2. 根据您需要导出的格式，单击“**导出到 TXT**”或“**导出到 CSV**”按钮。如果这些按钮不可见，请单击省略号按钮，然后从下拉列表中选择所需的选项。

包含软件漏洞列表的文件将下载到您的设备上。

*要查看在选定受管理设备上检测到的软件漏洞列表：*

1. 在主菜单中，转到“**资产管理**”→“**资产(设备)**”。
   将显示受管理设备列表。
2. 在受管理设备列表中，单击含有要查看在其中检测到的软件漏洞的设备的名称的链接。
   将显示所选设备的属性窗口。
3. 在所选设备的属性窗口中，选择“**高级**”选项卡。
4. 在左侧窗格中，选择“**软件漏洞**”区域。

将显示在选定受管理设备上检测到的软件漏洞列表。

默认情况下，只导出当前页面显示的漏洞。

如果您只想导出特定漏洞，请选中这些漏洞旁边的复选框。

1. 根据您需要导出的格式，单击“**导出到 TXT**”或“**导出到 CSV**”按钮。如果这些按钮不可见，请单击省略号按钮，然后从下拉列表中选择所需的选项。

包含软件漏洞列表的文件将下载到您的设备上。

# 忽略软件漏洞

您可以忽略要修复的软件漏洞。忽略软件漏洞的原因可能有如下几点：

- 您认为该软件漏洞对您的组织不严重。
- 您了解该软件漏洞修补程序可能会破坏与需要该漏洞修补程序的软件相关的数据。
- 您可以确定该软件漏洞对组织的网络没有危险，因为您使用其他措施来保护受管理设备。

您可以忽略所有受管理设备上或仅选定受管理设备上的软件漏洞。

*要忽略所有受管理设备上的软件漏洞，请执行以下操作：*

1. 在主菜单中，转到“**操作**” → “**补丁管理**” → “**软件漏洞**”。
   显示在受管理设备上检测到的应用程序中软件漏洞的列表。
2. 在软件漏洞列表中，单击带有要忽略的软件漏洞名称的链接。
   软件漏洞属性窗口将打开。
3. 在“**常规**”选项卡上，启用“**忽略漏洞**”选项。
4. 单击“**保存**”按钮。
   软件漏洞属性窗口将关闭。

在所有受管理设备上都会忽略该软件漏洞。

*要忽略所选受管理设备上的软件漏洞：*

1. 在主菜单中，转到“**资产管理**”→“**资产(设备)**”。
   将显示受管理设备列表。
2. 在受管理设备列表中，单击含有要忽略其中的软件漏洞的设备的名称的链接。
   设备属性窗口打开。
3. 在设备属性窗口中，选择“**高级**”选项卡。
4. 在左侧窗格中，选择“**软件漏洞**”区域。
   将显示在设备上检测到的软件漏洞列表。
5. 在软件漏洞列表中，选择要在选定设备上忽略的漏洞。
   软件漏洞属性窗口将打开。
6. 在软件漏洞属性窗口或“**常规**”选项卡中，启用“**忽略漏洞**”选项。
7. 单击“**保存**”按钮。
   软件漏洞属性窗口将关闭。
8. 关闭设备属性窗口。

选定设备上的软件漏洞将被忽略。

在完成“*修复漏洞*”任务或“*安装所需更新并修复漏洞*”任务后，将无法修复被忽略的软件漏洞。您可以通过使用过滤器从漏洞列表中排除被忽略的软件漏洞。

# 从 Kaspersky 数据库创建第三方应用程序的安装包

Kaspersky Security Center Web Console 允许您使用安装包执行第三方应用程序的远程安装。此类第三方应用程序包含在专用的 Kaspersky 数据库中。首次运行“*将更新下载至管理服务器存储库*”任务时，将自动创建此数据库。

只有拥有漏洞和补丁管理授权许可，您才可以从卡巴斯基数据库创建第三方应用程序的安装包。

*要从 Kaspersky 数据库创建第三方应用程序的安装包，请执行以下操作：*

1. 在主菜单中，转到“**软件管理**” → “**安装包**”。
2. 单击“**添加**”按钮。
   新安装包向导 启动。使用**下一步**按钮进行向导。
3. 选择“**从卡巴斯基数据库中选择一个应用程序来创建安装包**” 选项。

   此选项仅在“漏洞和补丁管理”授权许可下可用。

   继续执行向导的下一步。

4. 选择您要为其创建安装包的应用程序。
   继续执行向导的下一步。

5. 在下拉列表中选择相关的本地化语言，然后单击“下一步”。

   仅当应用程序提供多种语言选项时，才显示此步骤。

6. 如果系统提示您接受安装的授权许可协议，请在向导的“**授权许可协议和隐私策略**”步骤中执行以下操作：

   a. 单击“**显示**”链接即可阅读供应商网站上的授权许可协议或查看授权许可更新。

   b. 选择“**我确认我已完整阅读、理解并接受该最终用户授权许可协议的条款和条件**”复选框。

   c. 单击“**全部接受**”按钮以接受列表中显示的所有授权许可协议和隐私政策。

7. 进入向导的“**新安装包名称**”步骤时，在“**包名称**”字段中，输入安装包的名称，然后单击“**下一步**”。
   新创建的安装包将上传到管理服务器。“新安装包向导”显示一条消息，通知您安装包已成功创建。

8. 单击“**完成**”按钮。

新创建的安装包将出现在安装包列表中。您可以在创建或重新配置“*远程安装应用程序*”任务时选择此安装包。

仅当您拥有漏洞和补丁管理授权许可时，您才可以使用来自卡巴斯基数据库的第三方应用程序安装包来创建和重新配置“*远程安装应用程序*”任务。

# 从 Kaspersky 数据库查看和修改第三方应用程序安装包的设置

如果您先前已经创建 Kaspersky 数据库中列出的任意第三方应用程序安装包，则可以随后查看和修改这些安装包的设置。

从卡巴斯基数据库修改第三方应用程序安装包的设置只能在漏洞和补丁管理授权许可下进行。

*要从 Kaspersky 数据库查看和修改第三方应用程序安装包的设置：*

1. 在主菜单中，前往**软件管理→安装包**。

2. 在打开的安装包列表中，单击相关安装包的名称。
   属性窗口打开。

3. 如有必要，可以修改设置。

4. 单击“**保存**”按钮。

您修改的设置将会保存。

# 从 Kaspersky 数据库设置第三方应用程序的安装包

第三方应用程序安装包的设置在以下选项卡上分组：

默认情况下，下面列出的设置不会全部显示。您可以通过单击“**过滤器**”按钮，然后从列表中选择相关列名称来添加所需的列。

- “**常规**”选项卡：
  - 包含可以手动编辑的安装包名称的输入字段
  - **应用程序**

    为其创建安装包的第三方应用程序的名称。
  - **版本**

    为其创建安装包的第三方应用程序的版本号。
  - **大小**

    第三方安装包的大小 (KB)。
  - **创建日期**

    第三方安装包的创建日期和时间。
  - **路径**

    存储第三方安装包的网络文件夹的路径。
- “**安装进程**”选项卡：
  - **安装所需的常规系统组件**

    如果启用该选项，在安装更新之前，应用程序自动安装所需的所有常规系统组件（先决条件）。例如，这些先决条件可以是操作系统更新。

    如果禁用该选项，您可能必须手动安装先决条件。

    默认情况下已禁用该选项。
  - 显示更新属性并包含以下列的表：
    - **名称**

      更新名称。
    - **描述**

      更新说明。

- **源**

  更新的来源，即由 Microsoft 发布还是由其他第三方开发商发布。

- **类型**

  更新类型，即用于驱动程序还是用于应用程序。

- **类别**

  针对 Microsoft 更新显示的 Windows Server Update Services (WSUS) 类别（关键更新、定义更新、驱动程序、Feature Pack、安全更新、Service Pack、工具、更新汇总、更新或升级）。

- **根据 MSRC 的重要级别**

  Microsoft 安全响应中心 (MSRC) 定义的更新重要级别。

- **重要级别**

  Kaspersky 定义的更新重要级别。

- **补丁重要级别**

  补丁的重要级别（如果用于 Kaspersky 应用程序）。

- **文章**

  知识库中描述更新的文章的标识符 (ID)。

- **公告**

  描述更新的安全公告的 ID。

- **未指定安装(新版本)**

  显示更新是否具有“未分配安装”状态。

- **即将安装**

  显示更新是否具有“待安装”状态。

- **正在安装**

  显示更新是否具有“正在安装”状态。

- **已安装**

  显示更新是否具有“已安装”状态。

- **失败**

  显示更新是否具有“失败”状态。

- **需要重新启动**

  显示更新是否具有“需要重新启动”状态。

- **注册日期**

  显示注册更新的日期和时间。

- **以交互模式安装**

  显示更新是否需要在安装过程中与用户交互。

- **更新批准状态**

  显示更新是否被批准安装。

- **修订**

  显示更新的当前修订号。

- **更新 ID**

  显示更新的 ID。

- **应用程序版本**

  显示应用程序要更新到的版本号。

- **被替代的**

  显示可以替代该更新的其他更新。

- **替代**

  显示该更新可以替代的其他更新。

- **您必须接受授权许可协议的条款**

  显示更新是否需要接受最终用户授权许可协议 (EULA) 的条款。

- **URL 描述**

  显示更新供应商的名称。

- **应用程序系列**

  显示更新所属的应用程序系列的名称。

- **应用程序**

  显示更新所属的应用程序的名称。

- **本地化语言**

  显示更新本地化的语言。

- **未指定安装(新版本)**

  显示更新是否具有“未分配安装（新版本）”状态。

- **需要安装的先决条件**

  显示更新是否具有“需要安装先决条件”状态。

- **下载模式**

  显示更新下载的模式。

- **是一个补丁**

  显示更新是否为补丁。

- **未安装**

  显示更新是否具有“未安装”状态。

- **创建日期**

- “**设置**”选项卡，显示在安装过程中用作命令行参数的安装包设置（名称、描述和值）。如果安装包未提供此类设置，则显示相应的消息。您可以修改这些设置的值。

- “**修订历史**”选项卡，显示安装包版本并包含以下列：

  - **修订** – 安装包的修订号。

  - **时间**– 修改安装包设置的日期和时间。

  - **用户** – 修改安装包设置的用户的名称。

  - **用户设备 IP 地址** – 从其修改对象的设备的 IP 地址。

  - **Web Console IP 地址** – 修改对象的 Kaspersky Security Center Web Console 的 IP 地址。

  - **操作** – 修订内对安装包执行的操作。

  - **描述** – 与安装包设置更改相关的修订描述。

    默认下，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。

# 修复隔离网络中的漏洞

本节介绍要修复已连接到没有互联网访问权限的管理服务器的受管理设备上的第三方软件漏洞所采取的步骤。

## 方案：修复隔离网络中的第三方软件漏洞

您可以在隔离网络中的受管理设备上安装更新和修复已安装的第三方软件的漏洞。此类网络包括管理服务器和连接到它们但没有接入互联网的受管理设备。要修复此类网络中的漏洞，您需要已连接到互联网的管理服务器。通过使用可连接互联网的管理服务器，您可以下载补丁（所需的更新），然后将其传输到隔离的管理服务器上。

> 您可以下载软件供应商发布的第三方软件更新，但无法在隔离的管理服务器上使用 Kaspersky Security Center 下载 Microsoft 软件更新。

要了解在隔离网络中修复漏洞的过程，请参阅此过程的描述和方案。

## 先决条件

在开始之前，请执行以下操作：

1. 分配一台设备用于连接互联网和下载补丁。该设备将被视为具有互联网访问权限的管理服务器。
2. 在以下设备上安装 Install Kaspersky Security Center Linux，版本不能低于 15.1：
   - 分配的设备，将用作具有互联网访问权限的管理服务器
   - 隔离的设备，将用作与互联网隔离的管理服务器（以下称为隔离的管理服务器）
3. 确保每个管理服务器都有足够的磁盘空间用于下载和存储更新和补丁。

## 阶段

在隔离的管理服务器的受管理设备上安装更新和修复第三方软件漏洞分为以下几个阶段：

1. **配置具有互联网访问权限的管理服务器**

   准备具有互联网访问权限的管理服务器以处理对所需第三方软件更新的请求和下载补丁。

2. **配置隔离的管理服务器**

   准备隔离的管理服务器，让它们定期形成所需更新列表并处理通过具有互联网访问权限的管理服务器下载的补丁。配置后，隔离的管理服务器不再尝试从互联网下载补丁。相反，它们通过补丁获取更新。

3. **在隔离的管理服务器上传输补丁和安装更新**

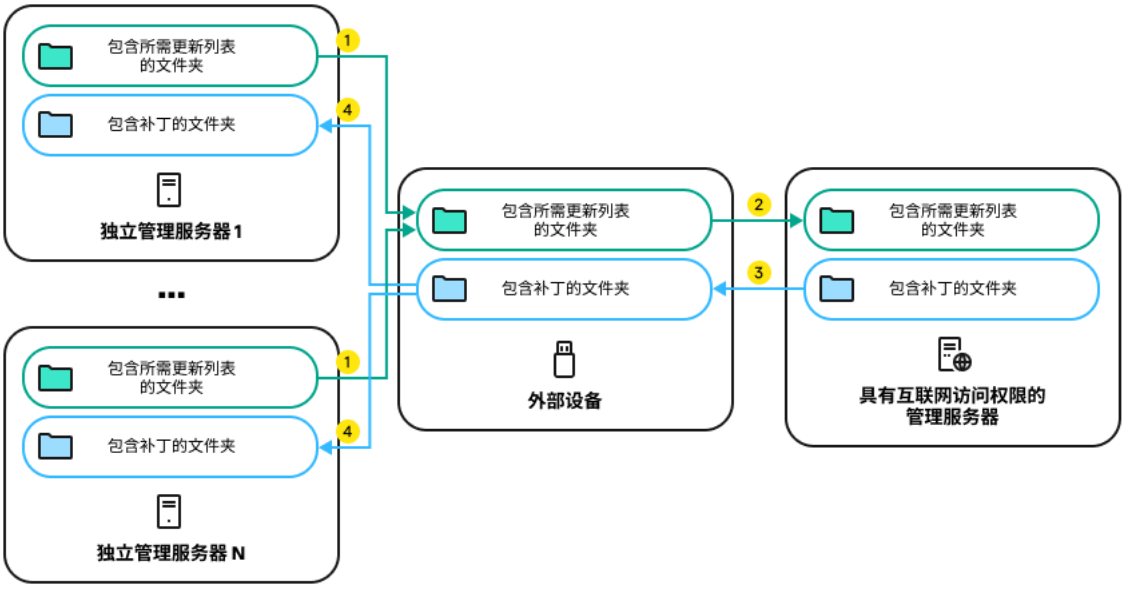
   完成管理服务器配置后，您可以将所需的更新列表和补丁从具有互联网访问权限的管理服务器传输到隔离的管理服务器上。接下来，补丁中的更新将通过“*安装所需更新并修复漏洞*”任务安装到受管理设备上。

## 结果

这样一来，第三方软件更新将传输到隔离的管理服务器并通过Kaspersky Security Center Linux 安装到连接的受管理设备上。只需对管理服务器进行一次配置，之后就可以根据需要随时获取更新，例如每天一次或多次。

# 关于修复隔离网络中的第三方软件漏洞

修复隔离网络中的第三方软件漏洞的过程如下图所示。您可以定期重复此过程。




在具有互联网访问权限的管理服务器和隔离的管理服务器之间传输补丁和所需更新列表的过程

每个与互联网隔离的管理服务器（以下称为隔离的管理服务器）都会生成一个更新列表，其中的更新必须安装在与管理服务器连接的受管理设备上。此更新列表作为一组二进制文件存储在特定文件夹中，每个文件都以包含必要更新的补丁的 ID 命名。因此，列表中的每个文件都对应一个特定的补丁。

通过外部设备将所需更新列表从隔离的管理服务器传输到可访问互联网的指定管理服务器。之后，指定的管理服务器从互联网下载补丁并将其放到指定的文件夹中。

当所有补丁都下载完毕并放到指定文件夹中后，它们将被传输回获取所需更新列表的每个隔离的管理服务器。补丁保存在每个隔离的管理服务器上专门为其创建的文件夹中。

结果，“*安装所需更新并修复漏洞*”任务在隔离的管理服务器的受管理设备上运行补丁并安装更新。

# 配置具有互联网访问权限的管理服务器以修复隔离网络中的漏洞

要准备在隔离网络中修复漏洞并传输补丁，请首先配置具有互联网访问权限的管理服务器，然后配置隔离的管理服务器。

*要配置具有互联网访问权限的管理服务器：*

1. 在安装了管理服务器的磁盘上创建两个文件夹：
   - 所需更新列表的文件夹
   - 补丁文件夹

   您可以根据需要命名这些文件夹。
2. 使用操作系统的标准管理工具为 KLAdmins 组授予对所创建的文件夹的“**修改**”访问权限。

3. 使用 klscflag 实用程序将文件夹的路径写入管理服务器属性。

   运行命令行，然后将当前目录更改为包含 klscflag 实用程序的目录。klscflag 实用程序位于安装管理服务器的目录中。默认安装路径为/opt/kaspersky/ksc64/sbin。

4. 在命令行中执行以下命令：

   - 要设置补丁文件夹的路径：
     `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "<文件夹路径>"`
   - 要设置所需更新列表的文件夹的路径：
     `klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v "<文件夹路径>"`

   示例：`klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "/FolderForPatches"`

5. 如果必要，使用 klscflag 实用程序指定管理服务器检查新补丁请求的频率：
   `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v <以秒为单位的值>`

   默认值是 120 秒。

   示例：`klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v 120`

6. 创建“*查找漏洞和所需更新*”任务以获取有关受管理设备上安装的第三方软件的补丁信息，然后设置任务计划。

7. 创建“*修复漏洞*”任务，指定用于修复漏洞的第三方软件的补丁，并设置任务计划。

   如果您希望该任务在计划中指定的时间之前运行，请手动运行任务。任务启动的顺序很重要。完成“*查找漏洞和所需更新*”任务后必须运行“*修复漏洞*”任务。

8. 重启管理服务器服务。

现在，可访问互联网的管理服务器已准备好下载更新并将更新传输到隔离的管理服务器上。在开始修复漏洞之前，配置隔离的管理服务器。

# 配置隔离的管理服务器以修复隔离网络中的漏洞

完成配置可访问互联网的管理服务器后，准备好网络中的每个隔离的管理服务器，这样您就可以对连接到隔离管理服务器的受管理设备进行漏洞修复和更新安装。

*要配置隔离的管理服务器，请对每个管理服务器执行以下步骤：*

1. 激活漏洞和补丁管理 (VAPM) 功能的授权许可密钥。

2. 在安装了管理服务器的磁盘上创建两个文件夹：

   - 所需更新列表的文件夹
   - 补丁文件夹

   您可以根据需要命名这些文件夹。

3. 使用操作系统的标准管理工具为 KLAdmins 组授予对所创建的文件夹的“**修改**”权限。

4. 使用 klscflag 实用程序将文件夹的路径写入管理服务器属性。

   运行命令行，然后将当前目录更改为包含 klscflag 实用程序的目录。klscflag 实用程序位于安装管理服务器的目录中。默认安装路径为/opt/kaspersky/ksc64/sbin。

5. 在命令行中执行以下命令：

   - 要设置补丁文件夹的路径：
     `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "<文件夹路径>"`
   - 要设置所需更新列表的文件夹的路径：
     `klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v "<文件夹路径>"`

   例如：`klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "/FolderForPatches"`

6. 如果必要，使用 klscflag 实用程序指定隔离的管理服务器检查新补丁的频率：
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v <以秒为单位的值>`

   默认值是 120 秒。

   例如：`klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v 120`

7. 如果必要，使用 klscflag 实用程序计算补丁的 SHA256 哈希：
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_VERIFY_HASH -t d -v 1`

   通过运行此命令，您可以确保补丁在传输到隔离管理服务器期间未被修改，并且您已收到包含所需更新的正确补丁。

   默认情况下，Kaspersky Security Center Linux 不计算补丁的 SHA256 哈希。如果启用此选项，在隔离的管理服务器收到补丁后，Kaspersky Security Center Linux 会计算其哈希，并将获取的值与管理服务器数据库中存储的哈希进行比较。如果计算出的哈希与数据库中的哈希不匹配，则会发生错误，您必须更换不正确的补丁。

8. 创建“*查找漏洞和所需更新*”任务以获取有关受管理设备上安装的第三方软件的补丁信息，然后设置任务计划。

9. 创建“*修复漏洞*”任务，指定用于修复漏洞的第三方软件的补丁，并设置任务计划。

   如果您希望该任务在计划中指定的时间之前运行，请手动运行任务。任务启动的顺序很重要。完成“*查找漏洞和所需更新*”任务后必须运行“*修复漏洞*”任务。

10. 重启管理服务器服务。

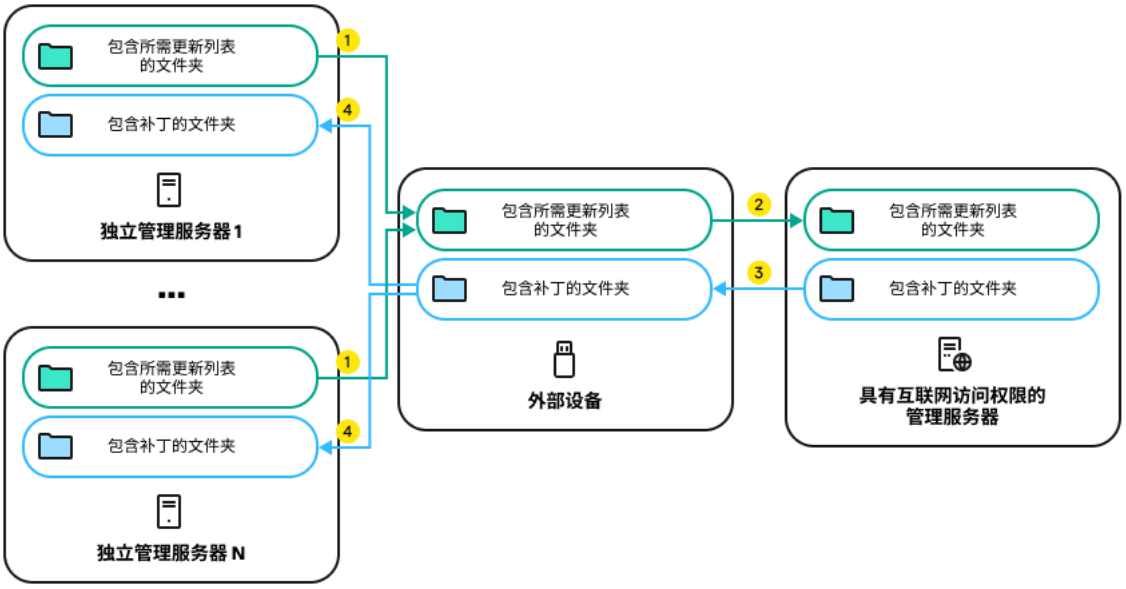
    配置所有管理服务器后，您就可以在隔离网络内传输补丁和所需更新列表，并修复受管理设备上的第三方软件漏洞。

# 在隔离网络中传输补丁和安装更新

完成配置管理服务器后，您可以将包含所需更新的补丁从具有互联网访问权限的管理服务器传输到隔离的管理服务器。您可以根据需要随时传输和安装更新，例如每天一次或多次。

您需要外部设备（如可移动驱动器）才能在管理服务器之间传输补丁和所需更新的列表。因此，请确保外部设备具有足够的磁盘空间用于下载和存储补丁。

传输补丁的过程和所需更新的列表如下图所示：




在具有互联网访问权限的管理服务器和隔离的管理服务器之间传输补丁和所需更新列表的过程

*要在连接到隔离的管理服务器的受管理设备上安装更新和修复漏洞：*

1. 启动"*安装所需更新并修复漏洞*"任务（如果尚未运行）。
2. 将外部设备连接到任一隔离的管理服务器。
3. 在外部设备上创建两个文件夹：一个用于所需更新列表，一个用于补丁。您可以根据自己的喜好为这些文件夹命名。

   如果您之前创建了这些文件夹，请清除。
4. 从每个独立的管理服务器复制所需更新列表，并将此列表粘贴到外部设备上保存所需更新列表的文件夹中。

   因此，您可以将从所有隔离的管理服务器获取的所有列表合并到一个文件夹中。此文件夹包含二进制文件，其中包含所有隔离的管理服务器所需的补丁 ID。
5. 将外部设备连接到具有互联网访问权限的管理服务器。
6. 从外部设备复制所需更新列表，并将此列表粘贴到具有互联网访问权限的管理服务器上保存所需更新列表的文件夹中。

   所有所需补丁都会自动从互联网下载到管理服务器上的补丁文件夹中。这可能需要几个小时的时间。
7. 确保所有所需补丁均已下载。为此，您可以执行以下操作之一：

   - 检查具有互联网访问权限的管理服务器上的补丁文件夹。所需更新列表中指定的所有补丁都应该下载到必需的文件夹中。如果需要的补丁数量较少，这样会更方便。
   - 准备一个特殊的脚本，例如，一个 shell 脚本。如果有大量补丁，将很难自行检查是否已下载所有补丁。在这种情况下，最好将检查自动化。

8. 从具有互联网访问权限的管理服务器复制补丁并粘贴到外部设备上的相应文件夹中。

9. 将补丁传输到每个隔离的管理服务器。将补丁放入它们的特定文件夹。

结果，每个隔离的管理服务器都会创建一个实际的更新列表，这些更新是连接到当前管理服务器的受管理设备所需的。在具有互联网访问权限的管理服务器收到所需更新列表后，管理服务器会从互联网下载补丁。当这些补丁出现在隔离的管理服务器上后，“*安装所需更新并修复漏洞*”任务将处理补丁。这样一来，更新会安装在受管理设备上，第三方软件漏洞会得到修复。

当“*安装所需更新并修复漏洞*”任务运行时，不要重新启动管理服务器设备，也不要运行“*备份管理服务器数据*”任务（它也会导致重新启动）。结果，“*安装所需更新并修复漏洞*”任务被中断，并且更新没有安装。在这种情况下，您必须手动重新启动此任务或等待任务按照配置的计划启动。

# 禁用在隔离网络中传输补丁和安装更新

例如，如果您决定将一台或多台管理服务器从隔离网络中移出，您可以禁用向隔离的管理服务器传输补丁。这样，您可以减少补丁的数量和下载所用的时间。

*要禁用将补丁传输给隔离的管理服务器：*

1. 如果要将所有管理服务器解除隔离，请在可访问互联网的管理服务器的属性中删除用于补丁和所需更新列表的文件夹路径。如果要在隔离网络中保留一些管理服务器，请跳过此步骤。

   运行命令行，然后将当前目录更改为包含 klscflag 实用程序的目录。klscflag 实用程序位于安装管理服务器的目录中。默认安装路径为/opt/kaspersky/ksc64/sbin。

   在命令行中执行以下命令：

   - 要删除补丁文件夹的路径：
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v ""
     ```
   - 要删除所需更新列表的文件夹的路径：
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v ""
     ```

2. 如果删除了文件夹路径，请在可访问互联网的管理服务器上重启服务。

3. 在要从隔离网络中移除的每个隔离管理服务器的属性中，删除用于补丁和所需更新列表的文件夹路径。

   在拥有 root 权限的账户下，在命令行中运行以下命令：

   - 要删除补丁文件夹的路径：
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v ""
     ```
   - 要删除所需更新列表的文件夹的路径：
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v ""
     ```

4. 重启已删除文件夹路径的每个管理服务器的服务。

如果您重新配置了可访问互联网的管理服务器，补丁将不再通过 Kaspersky Security Center Linux 传输。

如果您仅重新配置了特定的管理服务器并将其从隔离网络中移除，它们将不再通过 Kaspersky Security Center Linux 接收补丁。只有仍位于隔离网络内的管理服务器才会继续接收补丁。

如果在将来要开始修复已禁用的隔离管理服务器上的漏洞，您必须再次配置这些管理服务器和具有互联网权限的管理服务器。

# 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 Linux 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，*

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。

KlAkOAPI 包包含一组执行典型操作的示例。您只能在安装了管理服务器和 KlAkOAPI 包的设备上调用 OpenAPI 方法、运行示例和您自己的脚本。包含此包的 KlAkOAPI.tar.gz 存档位于 Kaspersky Security Center Linux 安装文件夹中。

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 |
| 通过连接网关下载网络列表文件到指定主机 | 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 |
| 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 |
| 创建有效用户权限报告 | 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 |
| 启动设备任务 | 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 |
| 为组中的设备注册分发点 | 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 |

| 示例 | 示例目的 | 方案 |
| --- | --- | --- |
| 对所有组进行枚举 | 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<br>• 检索完整的、扩展的组层次结构以及它们的名称和嵌套 | 配置管理服务器 |
| 枚举任务、查询任务统计信息和运行任务 | 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 |
| 创建并运行任务 | 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 |
| 枚举授权许可密钥 | 您可以获得安装在管理服务器受管理设备上的卡巴斯基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 |
| 创建和查找内部用户 | 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 |
| 创建自定义类别 | 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 |
| 使用 SrvView 枚举用户 | 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 |
| 创建内部用户，创建并通过电子邮件发送 Android 安装包 | 您可以使用"SecurityPolicy"类来创建内部用户，创建一个 Android 安装包，并通过电子邮件发送给用户。 | 添加内部用户账户 |

## 通过 OpenAPI 与 Kaspersky Security Center Linux 交互的应用程序

一些应用程序通过 OpenAPI 与 Kaspersky Security Center Linux 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 Linux 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 Linux 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 Web Console 工具发布独立包
- 8060 TCP—HTTPS 端口，用于使用 Kaspersky Security Center 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 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

一些客户公司，例如 MSP，可能运行多个管理服务器。可能不方便管理几个不同的管理服务器，因此可以应用层次结构。在层次结构中，基于 Linux 的管理服务器既可以作为主服务器也可以作为辅助服务器。基于 Linux 的主服务器可以管理基于 Linux 和基于 Windows 的从属服务器。基于 Windows 的主服务器可以管理基于 Linux 的辅助服务器。

两个管理服务器的“主/从”配置提供了以下选项：

- 一个从属管理服务器从主管理服务器继承策略、任务、用户角色和安装包，从而防止了重复设置。
- 主管理服务器上的设备分类可以包含从属管理服务器的设备。
- 主管理服务器的报告可以包含从属管理服务器的数据（包括详细信息）。
- 主管理服务器可以用作从属管理服务器的更新源。

主管理服务器仅接收来自上面列出的选项范围内的非虚拟从属管理服务器的数据。此限制不适用于虚拟管理服务器，虚拟管理服务器与其主管理服务器共享数据库。

管理服务器的层次结构为多租户模式提供支持。此模式允许主管理员独立地集中管理多个客户端。每个客户端组织或办公室都与其他组织或办公室隔离，被称为租户。您可以将多个受管理设备及其相关数据、设置、策略和任务分配给一个租户，并按租户配置用户权限。

安装在主要组织基础设施中的主管理服务器充当主要租户。主管理服务器使从属或虚拟管理服务器（其隔离的租户）能够独立接收和处理自己的事件并使用自己的资源、服务和配置。

拥有多个客户端组织的服务提供商可以向每个客户端组织独立提供 Kaspersky Security Center Linux 功能，包括警报聚合和响应操作。为了实现这点，服务提供商将从属或虚拟管理服务器作为每个客户端组织的租户进行连接。服务提供商使用自己的人员和资源提供服务。

# 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允许您提供客户端通过 Kaspersky Security Center Web Console 的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 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 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 Linux之前，您必须为Kaspersky Security Center Linux 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。 |
| Tantor（参见支持的版本） | 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。<br>Tantor DBMS 仅在 Astra Linux Special Edition RUSB.10015-01（操作更新 1.8）上受支持。 |

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 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。

## 保持空闲连接

我们建议您在连接网关设备上配置以下 keepalive 参数，以提高连接稳定性：

- `net.ipv4.tcp_keepalive_intvl` 指定在发送第一个 keepalive 消息之后多久发送一次。将此参数设置为 `1`
- `net.ipv4.tcp_keepalive_probes` 指定在连接被视为断开之前，可以发送多少条 keepalive 消息而没有收到回复。将此参数设置为 `10`
- `net.ipv4.tcp_keepalive_time` 指定在发送第一个 keepalive 消息之前，在最后一个数据包之后等待多长时间。将此参数设置为 `900`

*配置 keepalive 参数：*

1. 打开 /etc/sysctl.conf 文件。
2. 添加以下参数值：

```
net.ipv4.tcp_keepalive_intvl = 1
net.ipv4.tcp_keepalive_probes = 10
net.ipv4.tcp_keepalive_time = 900
```

3. 运行以下命令以更新 keepalive 参数：

```
sudo sysctl -p /etc/sysctl.conf
```

4. 运行以下命令以确保参数值已应用：

```
sudo sysctl net.ipv4.tcp_keepalive_intvl
sudo sysctl net.ipv4.tcp_keepalive_probes
sudo sysctl net.ipv4.tcp_keepalive_time
```

# 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。

有关移动设备保护的信息，请参阅移动设备管理部分。

在 Microsoft Windows XP 中，网络代理可能错误执行以下操作：直接从卡巴斯基服务器（作为分发点）下载更新并作为 KSN 代理服务器（作为分发点）起作用；检测第三方漏洞（如果漏洞和补丁管理被使用）。

# 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 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**关键威胁防护**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**关键威胁防护 → 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**关键威胁防护 → 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 Kaspersky Security Center Web Console 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*
  - *应用程序启动被禁止*
  - *清除不可能*
  - *最终用户授权许可协议被违反*
  - *无法加载加密模块*
  - *无法同时启动两个任务*
  - *检测到主动威胁. 应开始高级清除*
  - *检测到网络攻击*
  - *未更新所有组件*
  - *激活错误*
  - *启用便携模式错误*
  - *与 Kaspersky Security Center Linux 交互错误*
  - *禁用便携模式错误*
  - *更改应用程序组件时出错*
  - *应用文件加密/解密规则错误*

- *策略无法被应用*
- *禁止已终止*
- *网络活动被阻止*

- 在**功能失败**选项卡上：*无效的任务设置. 设置未应用*
- 在**警告**选项卡上：
  - *自我保护已禁用*
  - *备用密钥不正确*
  - *用户已退出加密策略*
- 在"**信息**"选项卡上：*应用程序启动在测试模式中被禁止*

## 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：

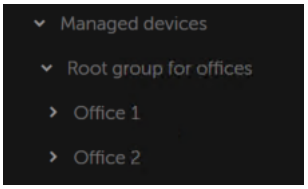
- 构建管理组结构涉及到网络拓扑。管理组结构可能不精确反映网络拓扑。网络各部分之间以及特定管理组相互匹配。您可以使用分发点自动分配或手动分配它们。

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

特定应用程序的任务仅在安装了该应用程序的管理插件时可以被创建。

任务可以在管理服务器和设备上执行。

以下任务在管理服务器上执行：

- 自动分发报告
- 将更新下载至管理服务器存储库
- 备份管理服务器数据
- 数据库维护

以下类型的任务在设备上执行：

- *本地任务* — 在特定设备上执行的任务。

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

- *组任务* — 在特定组的所有设备上执行的任务。

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

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

您可以为每个应用程序创建不管多少个组任务、全局任务或本地任务。

您可以更改任务设置、查看任务进度、复制、导出、导入和删除任务。

仅当为其创建任务的应用程序在运行时，才能在设备上启动任务。

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

不在任务设置中包括私人数据。例如，避免指定域管理员密码。

## 设备移动规则

建议通过*设备移动规则*自动分配设备到管理组。设备移动规则由三个主要部分组成：名称、执行条件（带设备属性的逻辑表达式）和目标管理组。如果设备属性满足规则执行条件，则规则移动设备到目标管理组。

所有设备移动规则都有优先级。管理服务器检查设备属性以查看它们是否满足每条规则的执行条件（升序优先级）。如果设备属性满足某条规则的执行条件，设备被移动到目标组，至此规则处理在该设备上完成。如果设备属性满足多个规则的条件，设备被移动到具有高优先级的规则的目标组。

设备移动规则可以被间接创建。例如，在安装包或远程安装任务的属性中，您可以指定安装网络代理后设备必须被移动到的管理组。而且，设备移动规则可以被 Kaspersky Security Center Linux 管理员明确创建，在“**资产管理**”→“**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 /var/opt/kaspersky/KSC_Backups*。

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：

- 必须为新的管理服务器分配相同的 DNS 名称。

  如果在部署网络代理时，网络代理安装包中设置了静态 IP 地址，则还必须将相同的 IP 地址分配给新的管理服务器。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）。

- 在 IAM 配置文件`var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml`中，将`server_iam.ksc_address`参数设置为与之前使用的管理服务器证书的主题备选名称 (SAN) 中指定的管理服务器地址完全相同。有关详细信息，请参阅以下文章：将管理服务器地址添加到 IAM 服务器配置。

- 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。成功恢复后重新安装 Web Console。

## 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。

### 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。

# 关于将网络代理切换到其他管理服务器

如果更改了下列网络设置，Kaspersky Security Center Linux 允许您将客户端设备网络代理切换至其他管理服务器：

- **DHCP 服务器地址条件** – 网络 Dynamic Host Configuration Protocol (DHCP) 服务器的 IP 地址已更改。

  > **DHCP 服务器地址条件**设置当前不可用。

- **默认连接网关地址条件** – 主要网络网关的地址已更改。
- **DNS 域条件** – 子网的 DNS 后缀已更改。
- **DNS 服务器地址条件** – 网络 DNS 服务器的 IP 地址已更改。
- **WINS 服务器地址条件** – 网络 WINS 服务器的 IP 地址已更改。此设置仅适用于运行 Windows 的设备。
- **名称可解析性条件** – 客户端设备的 DNS 或 NetBIOS 名称已更改。
- **子网条件** – 更改子网地址和掩码。
- **Windows 域可访问性条件** – 更改客户端设备连接到的 Windows 域的状态。此设置仅适用于运行 Windows 的设备。
- **SSL 连接地址可访问性条件** – 客户端设备可以或无法（取决于您选择的选项）与指定服务器建立SSL连接（名称：端口）。您必须使用具有能够处理高负载和频繁的网络代理连接请求的软件的专用服务器。请勿指定管理服务器的端口。对于每个服务器，都可以额外指定一个 SSL 证书。在这种情况下，网络代理除了检查 SSL 连接的功能外，还会验证服务器证书。如果证书不匹配，连接将失败。

网络代理连接至管理服务器的初始设置在安装网络代理时定义。此后，如果创建了将网络代理切换至其他管理服务器的规则，网络代理将以下列方式响应网络设置的更改：

- 如果网络设置符合已创建的规则之一，网络代理将连接至该规则中指定的管理服务器。如果该规则中已经启用漫游切换策略，客户端设备上的应用程序将切换至漫游策略。
- 如果未应用任何规则，网络代理将回滚至安装过程中指定的管理服务器连接默认设置。客户端设备上安装的应用程序将回滚至活动策略。
- 如果无法访问管理服务器，网络代理将使用用户漫游策略。

> 仅当在网络代理策略设置中启用“**当管理服务器不可用时启用漫游模式**”选项时，网络代理才会切换到漫游策略。

网络代理连接至管理服务器的设置保存在连接配置文件中。在连接配置文件中，您可以创建将客户端设备切换至漫游策略的规则，并可对配置文件进行配置，使其仅可用于下载更新。

# 为漫游用户创建连接配置文件

*若要为漫游用户创建网络代理连接至管理服务器的连接配置文件，请执行以下操作：*

1. 如果要为一组受管理设备创建连接配置文件，请打开该组的网络代理策略。为此，请执行以下操作：
   a. 在主菜单中，转到“**资产管理**”→“**策略**“。
   b. 选择要为其创建连接配置文件的管理组：
      - 对于根组，您可以继续进行下一步。
      - 对于子组，单击页面顶部的“**显示层级**”按钮，然后在打开的窗口中单击所需子组的名称。

      所选组的路径显示在页面顶部。如果需要，您可以单击带有管理组名称的链接前往该组。默认情况下，路径中的最后一个链接不活动。您也可以单击“**隐藏层级**”按钮关闭层次结构窗口。
   c. 为受管理设备组添加网络代理策略。如果您已经创建网络代理策略，请单击其名称以打开策略属性。
2. 如果要为特定的受管理设备创建连接配置文件，请执行以下操作：
   a. 在主菜单中，转到“**资产管理**” → “**资产(设备)**”。
   b. 单击受管理设备的名称。
   c. 在打开的受管理设备属性窗口中，转到“**应用程序**”选项卡。
   d. 单击仅应用于选定的受管理设备的网络代理策略的名称。
3. 在打开的属性窗口中，转到“**应用程序设置**”→“**连接**”→“**连接配置文件**”。
4. 在“**管理服务器连接配置文件**”区域中，单击“**添加**”按钮。
   默认下，连接配置文件列表包含<离线模式>和<归属管理服务器>配置文件。您不能编辑或删除配置文件。

<离线模式>配置文件不指定任何服务器以连接。因此，网络代理，当切换到该配置文件时，当客户端设备上的应用程序工作在漫游策略下时不试图连接到任何管理服务器。如果设备与网络断开连接，可以使用 <离线模式> 配置文件。

<归属管理服务器> 配置文件用于指定在网络代理安装过程中选择的管理服务器的连接。当设备在外部网络中运行了一段时间后重新连接到管理服务器时，<归属管理服务器>配置文件被应用。

5. 在打开的“**配置配置文件**”窗口中，配置连接配置文件：

- **配置文件名称**

  在该输入字段中，您可以查看或更改连接配置文件名称。

- **管理服务器地址**

  客户端设备在配置文件激活期间必须连接的管理服务器地址。

- **端口号**

  用于连接的端口号。

- **SSL 端口**

  使用 SSL 协议时的连接端口号。

- **使用 SSL 连接**

  如果启用此选项，则使用 SSL 协议通过安全端口建立连接。

  默认情况下已启用该选项。我们建议您不要禁用此选项，以便您的连接保持安全。

- 如果您要在连接到互联网时使用代理服务器，请选择“**使用代理服务器**”选项。如果选择此选项，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。

  - **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据。

  - **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。

- **连接网关地址**

  通过客户端设备连接管理服务器的网关地址。

- **当管理服务器不可用时启用漫游模式**

  选中此复选框，当管理服务器不可用时，允许客户端设备上安装的应用程序在任何连接尝试中使用处于漫游模式的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。

  默认情况下已清除该选框。

- **仅用来接收更新**

  如果启用此选项，则该配置文件将仅被客户端设备上安装的应用程序用来下载更新。对于其他操作，程序将使用在网络代理安装过程中定义的初始连接设置连接管理服务器。

  默认情况下已启用该选项。

- **与此配置文件中指定的管理服务器设置同步连接设置**

  如果启用此选项，网络代理将使用配置文件属性中指定的设置连接至管理服务器。

  如果禁用此选项，网络代理将使用安装期间已指定的原始设置连接至管理服务器。

  如果禁用“**仅用来接收更新**”选项，则此选项可用。

  默认情况下已禁用该选项。

程序将为漫游用户创建一个用于将网络代理连接至管理服务器的配置文件。当网络代理使用此配置文件连接到管理服务器后，客户端设备上安装的应用程序将使用处于漫游模式的设备的策略或漫游策略。

# 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“**资产管理**” → “**资产(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 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 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 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。

# 层级指南

该部分提供了 Kaspersky Security Center Linux 尺寸信息。

# 关于本指南

Kaspersky Security Center Linux（也称为 Kaspersky Security Center）层级指南专为安装管理 Kaspersky Security Center 的专业人员，以及为使用 Kaspersky Security Center 的企业提供技术支持的人员而设计。

所有建议和计算的前提是，在网络上 Kaspersky Security Center 管理安装了 Kaspersky 软件的设备的保护。

要在不同的操作条件下获取和维持优化运行，您必须考虑网络设备数量、网络拓扑和您需要的 Kaspersky Security Center 功能集。

此指南提供下列信息：

- Kaspersky Security Center 的限制
- Kaspersky Security Center 关键节点的限制（管理服务器和分发点）：
  - 管理服务器和分发点的硬件需求
  - 管理服务器数量和层级限制
  - 计算分发点的数量和配置
- 数据库中的事件记录配置取决于网络设备的数量
- 性能优化的常见最佳实践
- 特定任务的配置旨在优化 Kaspersky Security Center 的性能
- Kaspersky Security Center 管理服务器和每个受保护设备间的流量率(网络负载)

以下情况下建议参考该文档：

- 当在安装 Kaspersky Security Center 前计划资源时
- 当向部署了 Kaspersky Security Center 的网络计划显著更改时
- 从在受限制网段（测试环境）使用 Kaspersky Security Center 切换到在企业网络上全面部署 Kaspersky Security Center 时
- 当对使用的 Kaspersky Security Center 功能集做更改时

# 管理服务器计算

该部分提供了管理服务器设备的软件和硬件需求。也提供了根据组织网络配置计算管理服务器数量和层级的建议。

建议在设备上安装管理服务器和 DBMS 后，在这些设备上安装 Kaspersky Endpoint Security for Linux。有关 Kaspersky Endpoint Security的硬件要求，请参阅Kaspersky Endpoint Security for Linux帮助。

Kaspersky Endpoint Security for Linux 在与 Managed Detection and Response 和 Kaspersky Endpoint Detection and Response Expert（本地部署）集成时产生的负载，不会计入 Kaspersky Security Center Linux 和 Kaspersky Endpoint Security for Linux 同时安装的计算中。

## 管理服务器的硬件资源计算

该部分包含为计划管理服务器的硬件资源提供向导的计算。

## DBMS 和管理服务器的硬件需求

下表提供了测试得出的 DBMS 和管理服务器建议最低硬件要求。对于支持的操作系统和 DBMS 的完整列表，请参考硬件和软件需求列表。

> 您必须在安装了管理服务器的设备上启用交换文件。交换文件的最小大小必须是 RAM 容量的 1.5 倍。

建议在设备上安装管理服务器和 DBMS 后，在这些设备上安装 Kaspersky Endpoint Security for Linux。
对于同时安装，必须至少具备 225 IOPS，并在带有 DBMS 的管理服务器的要求基础上增加 1.5 GB RAM。
有关 Kaspersky Endpoint Security 的硬件要求，请参阅Kaspersky Endpoint Security for Linux 帮助。

### 该网络包括 50,000 台设备

安装了管理服务器的设备的配置

| 硬件 | 参数值 |
|---|---|
| CPU | 8 核（建议 12 核），2500 MHz |
| RAM | 16 GB |
| 磁盘空间 | 300 GB，150 IOPS 或更高 |

安装了 PostgreSQL DBMS 的设备的配置

| 硬件 | 参数值 |
|---|---|
| CPU | 16 核，2500 MHz |
| RAM | 32 GB |
| 磁盘空间 | 300 GB，150 IOPS 或更高 |

故障转移集群的节点配置

| 硬件 | 参数值 |
| --- | --- |
| CPU | 16 核，2500 MHz |
| RAM | 32 GB |
| 磁盘空间 | 500 GB，300 IOPS 或更高 |
| 网络接口控制器 | 1 Gbps |

安装了管理服务器和 PostgreSQL DBMS 的设备的配置

| 硬件 | 参数值 |
| --- | --- |
| CPU | 24 核（建议 28 核），2500 MHz |
| RAM | 48 GB |
| 磁盘空间 | 600 GB，300 IOPS 或更高 |

## 该网络包括 30,000 台设备

安装了管理服务器的设备的配置

| 硬件 | 参数值 |
| --- | --- |
| CPU | 6 核（建议 8 核），2500 MHz |
| RAM | 12 GB |
| 磁盘空间 | 200 GB，150 IOPS 或更高 |

安装了 PostgreSQL DBMS 的设备的配置

| 硬件 | 参数值 |
| --- | --- |
| CPU | 12 核，2500 MHz |
| RAM | 22 GB |
| 磁盘空间 | 250 GB，150 IOPS 或更高 |

故障转移集群的节点配置

| 硬件 | 参数值 |
| --- | --- |
| CPU | 16 核，2500 MHz |
| RAM | 32 GB |
| 磁盘空间 | 500 GB，300 IOPS 或更高 |
| 网络接口控制器 | 1 Gbps |

安装了管理服务器和 PostgreSQL DBMS 的设备的配置

| 硬件 | 参数值 |
| --- | --- |
| CPU | 16 核（建议 20 核），2500 MHz |
| RAM | 34 GB |
| 磁盘空间 | 450 GB，300 IOPS 或更高 |

## 该网络包括 10,000 台设备

安装了管理服务器的设备的配置

| 硬件 | 参数值 |
| --- | --- |
| CPU | 4 核（建议 6 核），2500 MHz |
| RAM | 8 GB |
| 磁盘空间 | 100 GB，150 IOPS 或更高 |

安装了 PostgreSQL DBMS 的设备的配置

| 硬件 | 参数值 |
| --- | --- |
| CPU | 6 核，2500 MHz |
| RAM | 10 GB |
| 磁盘空间 | 200 GB，150 IOPS 或更高 |

故障转移集群的节点配置

| 硬件 | 参数值 |
| --- | --- |
| CPU | 16 核，2500 MHz |
| RAM | 32 GB |
| 磁盘空间 | 500 GB，300 IOPS 或更高 |
| 网络接口控制器 | 1 Gbps |

安装了管理服务器和 PostgreSQL DBMS 的设备的配置

| 硬件 | 参数值 |
| --- | --- |
| CPU | 8 核（建议 14 核），2500 MHz |
| RAM | 18 GB |
| 磁盘空间 | 300 GB，300 IOPS 或更高 |

## 该网络包括 1000 台设备

安装了管理服务器的设备的配置

| 硬件 | 参数值 |
| --- | --- |
| CPU | 2 核，2500 MHz |
| RAM | 6 GB |
| 磁盘空间 | 10 GB，150 IOPS 或更高 |

安装了 PostgreSQL DBMS 的设备的配置

| 硬件 | 参数值 |
| --- | --- |
| CPU | 2 核，2500 MHz |
| RAM | 4 GB |
| 磁盘空间 | 20 GB，150 IOPS 或更高 |

故障转移集群的节点配置

| 硬件 | 参数值 |
| --- | --- |
| CPU | 16 核，2500 MHz |
| RAM | 32 GB |

| 硬件 | 参数值 |
| --- | --- |
| 磁盘空间 | 500 GB，300 IOPS 或更高 |
| 网络接口控制器 | 1 Gbps |

安装了管理服务器和 PostgreSQL DBMS 的设备的配置

| 硬件 | 参数值 |
| --- | --- |
| CPU | 4 核，2500 MHz |
| RAM | 10 GB |
| 磁盘空间 | 30 GB，300 IOPS 或更高 |

测试在以下系统上运行：

- 自动分配分发点在管理服务器上启用，或者分发点根据建议的表格被手动指定。
- PostgreSQL DBMS 不包含除 plpgsql 之外的任何扩展程序。

在安装了 DBMS 的设备上，数据库大约占用 100 GB 的磁盘空间，事务日志大约占用 200 GB 的磁盘空间。

## 数据库空间计算

必须在数据库中保留的大约空间可以使用以下公式计算：

(600 * C + 2.3 * E + 2.5 * A + 1.2 * N * F), KB

其中：

- C 是设备数量。
- E 要存储的事件的数量。
- A 是活动目录对象的总数：
  - 设备账户
  - 用户账户
  - 安全组账户
  - 活动目录组织单元

  如果活动目录扫描被禁用，A 等效于 0。
- N 是端点设备上已清查可执行文件的平均数量。
- F 是端点设备的数量，其中可执行文件已清查。

如果您计划在 Kaspersky Endpoint Security 策略设置中启用通知管理服务器您运行的应用程序，您将需要额外空间(0.03 * C GB)在数据库中存储您运行的应用程序信息。

操作期间，一定的*未占用空间*总是出现在数据库。因此，数据库文件的实际大小通常大约是数据库中被占用空间的两倍。

不推荐明确限制事务日志的大小。建议保留 MAXSIZE 参数的默认值。

## 磁盘空间计算

文件夹 /var/opt/kaspersky/klnagent_srv/ 需要的管理服务器磁盘空间可以使用以下公式估算：

(724 * C + 0.15 * E + 0.17 * A), KB

其中：

- C 是设备数量。
- E 要存储的事件的数量。
- A 是活动目录对象的总数：
  - 设备账户
  - 用户账户
  - 安全组账户
  - 活动目录组织单元

如果活动目录扫描被禁用，A 等效于 0。

# 计算管理服务器的数量和配置

要减少主管理服务器负载，您可以分配另外的管理服务器到每个管理组。每个主管理服务器的从属管理服务器的数量不能超过 500。

我们建议您基于您组织网络的配置来创建管理服务器配置。

# 有关将动态虚拟机连接到 Kaspersky Security Center 的建议

动态虚拟机（也简称为“动态 VM”）比静态虚拟机消耗更多资源。

有关动态虚拟机的更多信息，请参阅对动态虚拟机的支持。

连接新的动态 VM 时，Kaspersky Security Center Linux 在 Kaspersky Security Center Web Console 中为此动态 VM 创建一个记录并将该动态 VM 移至管理组。此后，动态 VM 被添加到管理服务器数据库中。管理服务器与安装在此动态 VM 上的网络代理完全同步。

在组织的网络中，网络代理为每个动态 VM 创建以下网络列表：

- 硬件
- 安装的软件

- 检测到的漏洞
- 应用程序控制组件的事件和可执行文件列表

网络代理将这些网络列表传输到管理服务器。网络列表的大小取决于安装在动态 VM 上的组件，并且可能会影响 Kaspersky Security Center Linux 和数据库管理系统的 (DBMS) 性能。注意，负载可能呈非线性增长。

在用户使用完动态 VM 并将其关闭后，该虚拟机将从虚拟基础架构中删除，且有关该虚拟机的条目也将从管理服务器数据库中删除。

所有这些操作都会消耗大量的 Kaspersky Security Center Linux 和管理服务器数据库资源，并会降低 Kaspersky Security Center Linux 和 DBMS 的性能。建议您最多将 20,000 个动态 VM 连接到 Kaspersky Security Center Linux。

如果连接的动态 VM 执行标准操作（例如，数据库更新）并且消耗不超过 80% 的内存和 75-80% 的可用内核，您可以将超过 20,000 个动态 VM 连接到 Kaspersky Security Center Linux。

更改动态 VM 上的策略设置、软件或操作系统可能减少或增加资源消耗。最优资源消耗占比为 80-95%。

# 分发点和连接网关的计算

该部分提供了用作分发点的设备的硬件需求，以及根据企业网络配置计算分发点和连接网关数量的建议。

## 分发点需求

本文介绍了基于 Windows 和 Linux 的分发点的硬件和软件要求。

如果管理服务器上有任何远程安装任务等待，带有分发点的设备也会请求一定的剩余磁盘空间，这些空间与要安装的安装包大小相当。

如果管理服务器上有一个或多个更新（补丁）安装和漏洞修复任务实例，带有分发点的设备也会请求一定的剩余磁盘空间，相当于两倍的补丁总大小。

如果在分发点直接从卡巴斯基更新服务器接收数据库更新和应用程序软件模块的地方使用此方案，则分发点必须连接到互联网。

不建议将管理服务器分配为分发点，因为这样会增加管理服务器的负荷。

### 基于 Windows 的分发点的硬件要求

**基于 Windows 的分发点的最低硬件要求**

| 客户端设备的数量 | CPU | RAM | RAM，已启用补丁管理 | 磁盘空间 |
|---|---|---|---|---|
| 10,000 | 4 核，2500 MHz | 8 GB | 8 GB | 120 GB |

| | | | | |
|---|---|---|---|---|
| 5000 | 4 核，2500 MHz | 6 GB | 8 GB | 120 GB |
| 1000 | 2 核，2500 MHz | 4 GB | 8 GB | 120 GB |

### 基于 Linux 的分发点的硬件要求

**基于 Linux 的分发点的最低硬件要求**

| 客户端设备的数量 | CPU | RAM | 磁盘空间 |
|---|---|---|---|
| 10,000 | 4 核，2500 MHz | 10 GB | 120 GB |
| 5000 | 4 核，2500 MHz | 8 GB | 120 GB |
| 1000 | 2 核，2500 MHz | 6 GB | 120 GB |

# 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/5000 + 2)，N 是网络设备数量 |

网络中基于网络设备数量被专门分配的包含多个网段的分发点的数量

| 每个网段中的客户端设备的数量 | 分发点数量 |
|---|---|
| 少于 10 | 0（不分配分发点） |
| 10–100 | 1 |
| 大于 100 | 可接受：(N/10,000 + 1)，建议：(N/5,000 + 2)，N 是网络设备数量 |

### 使用标准客户端设备（工作站）作为分发点

如果您计划使用标准客户端设备（就是，工作站）作为分发点，我们建议您按照所示分配分发点（参见下表），以便避免通信渠道和管理服务器过载。

网络中基于网络设备数量作为分发点工作的包含单一网段的工作站的数量

| 网段中的客户端设备的数量 | 分发点数量 |
|---|---|
| 少于 300 | 0（不分配分发点） |
| 大于 300 | (N/300 + 1)，N 是网络设备数量；至少有三台分发点 |

网络中基于网络设备数量作为分发点工作的包含多个网段的工作站的数量

| 每个网段中的客户端设备的数量 | 分发点数量 |
| --- | --- |
| 少于 10 | 0（不分配分发点） |
| 10–30 | 1 |
| 31–300 | 2 |
| 大于 300 | (N/300 + 1)，N 是网络设备数量；至少有三台分发点 |

如果分发点被关闭(或由于某些原因不可用)，其范围内的受管理设备可以访问管理服务器以更新。

# 连接网关数量计算

如果您计划使用连接网关，我们建议您为该功能指定特别的设备。

一个连接网关可以覆盖最多 10,000 台受管理设备。

# 任务和策略事件信息的记录

该部分提供了管理服务器数据库中的事件存储计算，并提供如何最小化事件数量的建议，从而降低管理服务器负载。

默认情况下，每个任务和策略的属性可以用于存储所有任务执行和策略强制执行的相关事件。

然而，如果任务运行过于频繁（例如，每周多于一次）且在大量设备间（例如，多于 10,000 台），事件数量可能过大且事件可能溢出数据库。此种情况下，建议选择任务设置的两个选项中的一个：

- **保存任务进度相关事件**。此种情况下，数据库仅从运行任务的每个设备接收任务启动、进程和完成信息（成功、带有警告或错误）。
- **仅保存任务执行结果**。此种情况下，数据库仅从运行任务的每个设备接收任务完成信息（成功、带有警告或错误）。

如果策略为大数量设备定义（例如，多于 10,000 台），事件数量可能很大且事件可能溢出数据库。此种情况下，建议在策略设置中仅选择最关键的事件并启用它们的记录。建议您禁用所有其他事件的记录。

为此，您将降低数据库中的事件数量，提高与数据库中事件表分析相关的场景的执行速度，并降低严重事件被大数量事件覆盖的风险。

您也可以降低任务或策略相关事件的存储期限。任务相关事件和策略相关事件的默认期限分别是 7 天和 30 天。当更改事件存储期限时，请考虑您的组织采用的工作程序以及系统管理员用以分析每个事件的时间。

建议在以下情况修改事件存储设置：

- 有关组任务中间状态变化的事件和有关应用策略的事件在 Kaspersky Security Center Linux 数据库的所有事件中占据很高比例。
- 操作系统日志开始显示事件超过存储限制时的自动删除。

基于每天来自每个设备的事件数量不超过 20 的假设来选择事件记录选项。如果必要，您可以稍微增加该限制，但仅是在您网络中的设备数量相对小时（少于 10,000 台）。

# 管理大量设备的管理服务器的最佳实践

## 使用 DBMS 的最佳实践

配置**管理服务器维护**任务以定期运行，特别是在使用 PostgreSQL DBMS 时。

从 IOC 扫描中排除 DBMS 文件夹。

## 策略和配置文件的最佳实践

减少组件（如 Kaspersky Endpoint Security for Windows）的活动策略数量。您可以用策略配置文件替换策略。

## 管理大量设备的管理服务器的最佳实践

减少同时运行的任务数量，尤其是远程安装和补丁管理。

减少与设备分类相关的任务数量并优化其计划。

在策略设置的**事件配置**部分，尽量减少保存的事件类型的数量。

## 存储事件的最佳实践

减少来自应用程序控制组件的单一类型事件的频率。请参阅以下文章了解详情：关于阻止频繁事件。

减少来自组件（例如 Kaspersky Endpoint Security for Windows）的事件和有关已修复漏洞的信息事件的存储期限。

在常见任务（例如更新任务）的任务设置中，启用 **保存任务进度相关事件**选项。有关详细信息，请参阅以下文章：记录有关任务和策略事件的信息。

优化清查任务设置。有关详细信息，请参阅以下文章：清查任务。

# 特别考虑和特定任务的优化设置

特定任务受制于基于网络设备数量的特别考虑。该部分提供了此类任务设置的优化配置建议。

设备发现、数据备份任务、数据库维护任务和更新 Kaspersky Endpoint Security 的组任务是 Kaspersky Security Center Linux 的基本功能部分。

清查任务是漏洞和补丁管理功能的一部分，且在该功能未激活时不可用。

# 设备发现频率

不建议增加设备发现的默认频率，因为这可以增加域控制器负载。相反，建议使用您组织需要的最小频率计划轮询。计算最优计划的建议提供在下表。

设备发现计划

| 网络设备数量 | 建议的设备发现频率 |
| --- | --- |
| 少于 10,000 | 默认频率或更低 |
| 10,000 或更多 | 每天一次或更低 |

# 管理服务器数据备份任务和数据库维护任务

当以下任务运行时管理服务器停止工作：

- 备份管理服务器数据
- 管理服务器维护

当这些任务运行时，数据库无法接收任何数据。

您可能必须重新计划这些任务以便它们和其他管理服务器任务不同时执行。

# 更新 Kaspersky Endpoint Security 的组任务

如果管理服务器作为更新源，Kaspersky Endpoint Security 10 和后续版本的组更新任务的建议计划选项是“**当新更新下载至存储库时**”，其中“**使用任务启动自动随机延迟**”复选框被选中。

如果从 Kaspersky 服务器下载更新到存储库的本地任务已在每个分发点上创建，时段性计划将被建议给 Kaspersky Endpoint Security 组更新任务。随机时段值必须是一小时。

# 清查任务

> 您可以在获取可执行文件相关信息的同时减少数据库的负载。为此，我们建议您在安装了一组标准软件的参考设备上运行 Kaspersky Endpoint Security 清查任务。

管理服务器从单个设备接收的可执行文件数量不能超过 150,000。当 Kaspersky Security Center Linux 达到了该限制，它无法接收任何新文件。

通常，常规客户端设备上的文件数量不超过 60,000。文件服务器上的可执行文件数量可能更大甚至超过 150,000 阈值。

# 管理服务器和受保护设备间的网络负载详情

该部分提供了一定条件下的网络流量测试度量结果。当您计划网络基础架构和您组织网络中（或管理服务器和其他要保护其设备的组织间）吞吐量时，可以参考该信息。知道了网络吞吐量，您也可以估算不同数据传输操作将花费的时间。

## 不同方案下的流量消耗

下表显示不同方案下管理服务器和受管理设备之间流量度量测试的结果。

默认下，设备每 15 分钟或更长间隔与管理服务器同步一次。然而，如果您在管理服务器上修改策略或任务的设置，该策略（或任务）所适用的设备会提前进行同步，从而将新设置传输到设备上。

管理服务器和受管理设备间的流量率

| 方案 | 从管理服务器到每个受管理设备的流量 | 从每个受管理设备到管理服务器的流量 |
|---|---|---|
| 安装带有更新数据库的 Kaspersky Endpoint Security for Linux | 390 MB | 3.3 MB |
| 网络代理安装 | 75 MB | 397 KB |
| 网络代理和 Kaspersky Endpoint Security for Linux 同时安装 | 459 MB | 3.6 MB |
| 反病毒数据库初始更新，不更新软件包中的数据库（如果参与卡巴斯基安全网络被禁用） | 113 MB | 1.8 MB |
| 反病毒数据库每日更新（如果参与卡巴斯基安全网络被启用） | 22 MB | 373 MB |
| 设备数据库更新之前的初始化同步（策略和任务传输） | 382 KB | 446 KB |
| 在设备上更新数据库之后初始同步 | 20 KB | 157 KB |
| 与管理服务器的同步（根据计划） | 18 KB | 23 KB |
| 当组策略中单个设备被更改时同步（设置更改时立即） | 19 KB | 20 KB |
| 当组任务中单个设备被更改时同步（设置更改时立即） | 14 KB | 11 KB |
| 强制同步 | 110 KB | 109 KB |
| **检测到的病毒**事件（1 个病毒） | 44 KB | 50 KB |
| **检测到病毒**事件（10 个病毒） | 58 KB | 77 KB |
| 启用应用程序注册表列表后的一次性流量 | 最多 10 KB | 最多 12 KB |
| 启用应用程序注册表列表后的每日流量 | 最多 840 KB | 最多 1 MB |

## 24 小时平均流量使用

管理服务器和受管理设备之间的 24 小时平均流量使用情况如下所示：

- 从管理服务器到受管理设备的流量为 840 KB。
- 从受管理设备到管理服务器的流量为 1 MB。

流量测量在以下条件下进行：

- 受管理设备已安装网络代理和 Kaspersky Endpoint Security for Linux。
- 设备未被分配为分发点。
- 漏洞和补丁管理未启用。
- 与管理服务器的同步频率是 15 分钟。

# 已知问题

Kaspersky Security Center Linux 具有下列对于应用程序运行并不重要的限制：

- 10373324：如果所有节点均未安装网络代理，则在计算指标状态时仅考虑当前处于活动状态的节点。如果其中一个节点安装了网络代理，则仅当该节点变为活动状态时才会考虑该节点。因此，若要在计算指标状态时考虑所有节点，您必须在每个节点上安装网络代理，并且每个节点都必须至少处于活动状态一次。

- 8994760：如果您拥有虚拟管理服务器的访问权限，但没有主管理服务器的访问权限，并且尝试登录 Kaspersky Security Center Linux，则会发生错误，并且错误消息 **您的请求当前无法被处理。请等待并稍后再试** 不正确。错误文本必须如下：**检查您的访问权限。您必须对主服务器或其中一个虚拟服务器拥有访问权限。请与主管理员联系，然后重试**

- 10085767：迁移到 Kaspersky Security Center Linux 时，报告范围可能显示不正确。

- 10292104：在 Kaspersky Security Center Web Console 版本 15.1 或 15.2 中，如果您将 Kaspersky Endpoint Detection and Response Optimum 插件更新到版本 16.3，则 **警报** 区域可能不会显示警报。

- 10308380：创建应用程序类别后，如果尝试通过单击确认对话框中的 **确定** 按钮来打开其属性，则属性窗口不会打开。

- 10253149：对于应用程序策略，如果您在 **事件配置** 选项卡上选择大量事件，则不会显示 **显示更多** 展开块，其中包含有关此类事件对管理服务器或 DBMS 性能影响的警告。

- 10127434：如果在主管理服务器上登录 Kaspersky Security Center Web Console 时打开 **任务** 区域，然后打开层次结构窗口，虚拟服务器会显示为主服务器。

- 9302142：“**使用网络代理作为 DMZ 连接网关**”选项在 Microsoft Windows on Arm 上不受支持。

- 9065814: 尝试从 Samba 4 域中的 Windows 设备进行域身份验证时，可能会发生错误。

- 9335676: 在高可用性数据库管理系统集群中切换主节点后， Kaspersky Security Center Web Console可能无法访问或访问速度显著降低。如果 Kaspersky Security Center Web Console 超过 10 分钟仍无法访问，请使用以下命令重启 IAM 服务：

  ```
  systemctl restart kliam_srv.service
  ```

- 9157005, 9157085: 在启用了*安装所需更新并修复漏洞*选项的 Windows 受管理设备上运行**在设备重启或关闭时开始安装**任务时，该任务可能会失败并出现错误。当计划安装大量更新时，可能会出现此问题。要解决此问题，请在不启用**在设备重启或关闭时开始安装**选项的情况下运行该任务。

- 9272534: 如果用户表包含超过 50,000 个用户，则仅显示前 50,000 个用户，其余用户将不显示。

- 9291235: 在管理服务器版本16.1上还原备份后， Kaspersky Security Center云控制台会显示登录页面。身份验证成功后，系统会要求输入用于双重身份验证的一次性安全码。输入有效的一次性安全码时，会显示一条错误信息，提示一次性安全码不正确。在这种情况下，请稍等几分钟，然后手动刷新页面，重试登录Kaspersky Security Center云控制台。备份恢复过程完成后，下次尝试登录时即可成功。

- 7939561: 尝试修改受保护的用户账户时，单击账户保护**账户保护取消**按钮会导致错误。

- 8562938: 在管理服务器策略属性中打开移动设备端口不会启用移动设备管理功能，也不会触发移动证书的生成。要启用移动设备管理功能，必须在管理服务器属性中打开移动设备的端口。

- 8732282: 对于在 Active Directory 的帐户属性中启用了**用户无法更改密码**选项的用户，将不会执行 Active Directory 中的**重置密码**响应操作。域控制器管理员必须禁用此用户的**用户无法更改密码**选项或手动重置密码。如果您拥有 Kaspersky Next XDR Optimum 授权许可、启用了与 Active Directory 的集成并且用户包含在 Active Directory 安全组中，则会出现此问题。

- 8688182: 如果用户在 Active Directory 中的账户属性中启用了**密码永不过期**选项，则在执行**重置密码**响应操作后， **密码永不过期**选项将被禁用，并且用户将需要在下次登录时更改其域密码。如果您拥有 Kaspersky Next XDR Optimum 授权许可、启用了与 Active Directory 的集成并且用户包含在 Active Directory 安全组中，则会出现此问题。

- 8703857: 仅当代理服务器支持基本身份验证时，才会建立Kaspersky Security Center Web Console 和管理 Web 插件的代理服务器连接。

- 7911778: 当您**远程卸载应用程序**任务来从运行具有 Arm 架构的操作系统且与管理服务器的时间不同步的设备中卸载网络代理时，即使网络代理已被成功从设备上卸载，任务状态也不会从**运行中**更改为**已完成**。要解决该问题，请在**远程卸载应用程序**之前，将设备上的时间与已安装的网络代理同步，并将设备上的时间与管理服务器同步。

- 6896585: 如果 Kaspersky Security Center Linux 安装在名称中含有西里尔符号的设备上，则受管理设备无法通过 KSN 代理服务连接到 KSN。

- 7523299: 在运行 CentOS 6.6 的受管理设备上终止网络代理进程后，网络代理不会重启。

- 7835858: 如果您在 Kaspersky Security Center Web Console 15.2 或者更高版本中使用**每 N 天**和**按星期几**计划设置创建任务，然后在早期版本的 Kaspersky Security Center Web Console 或管理控制台中打开该任务（例如，当该任务也应用于基于 Linux 和基于 Windows 的辅助管理服务器时），计划设置可能会显示不正确，或者可能会出现错误。

- 7208621: 当您导入*将更新下载到分发点存储库*或*更新验证*任务时，**选择任务将被分配到的设备**选项将启用。这些任务不能分配给设备分类或特定设备。如果将*下载更新分配到分发点存储库*或将*更新验证*任务分配到特定设备，则任务将无法正确导入。

- 6511063: 如果在 Linux 设备上检测到来自**应用程序注册表**部分的应用程序，则应用程序属性不包含有关相关可执行文件的信息。

- 5915107: 在具有字母格式的报告中，分页可能会水平切割文本行。

- 5556109: 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。

- 9093038: 如果 Kaspersky Security Center Linux 管理服务器安装后未启动，且操作系统日志包含与 kladminserver_srv.service 相关的错误 213/SECUREBITS，请以超级用户身份执行以下命令：

```
mkdir -p /etc/systemd/system/kladminserver_srv.service.d
echo "[Service]" > /etc/systemd/system/kladminserver_srv.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/kladminserver_srv.service.d/override.conf
mkdir -p /etc/systemd/system/klwebsrv_srv.service.d
echo "[Service]" > /etc/systemd/system/klwebsrv_srv.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/klwebsrv_srv.service.d/override.conf
```

如果 Kaspersky Security Center Web Console安装后未启动，且操作系统日志包含与 KSCWebConsole.service 相关的错误 213/SECUREBITS，请以超级用户身份执行以下命令：

```
mkdir -p /etc/systemd/system/KSCSvcWebConsole.service.d
echo "[Service]" > /etc/systemd/system/KSCSvcWebConsole.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCSvcWebConsole.service.d/override.conf
mkdir -p /etc/systemd/system/KSCWebConsoleManagement.service.d
echo "[Service]" > /etc/systemd/system/KSCWebConsoleManagement.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsoleManagement.service.d/override.conf
mkdir -p /etc/systemd/system/KSCWebConsoleNATS.service.d
echo "[Service]" > /etc/systemd/system/KSCWebConsoleNATS.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsoleNATS.service.d/override.conf
mkdir -p /etc/systemd/system/KSCWebConsolePlugin.service.d
echo "[Service]" > /etc/systemd/system/KSCWebConsolePlugin.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsolePlugin.service.d/override.conf
mkdir -p /etc/systemd/system/KSCWebConsole.service.d
echo "[Service]" > /etc/systemd/system/KSCWebConsole.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsole.service.d/override.conf
```

如果安装后 kliam_srv 服务未启动，并且操作系统日志包含与该服务相关的 213/SECUREBITS 错误，请以超级用户身份执行以下命令：

```
mkdir -p /etc/systemd/system/kliam_srv.service.d
echo "[Service]" > /etc/systemd/system/kliam_srv.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/kliam_srv.service.d/override.conf
```

- 9165434: NTLM 身份验证不适用于受保护用户组中的用户账户。

# 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。

您可以通过以下任一方式联系技术支持：

- 访问技术支持网站
- 从 Kaspersky CompanyAccount 门户向技术支持团队发送请求

# 通过 Kaspersky CompanyAccount 获得技术支持

Kaspersky CompanyAccount 是面向使用卡巴斯基应用程序的公司的门户。Kaspersky CompanyAccount 门户旨在通过在线请求促进用户和卡巴斯基专家之间的互动。您可以使用 Kaspersky CompanyAccount 来跟踪在线请求状态，并存储它们的历史记录。

您可以将贵组织的所有员工注册到一个 Kaspersky CompanyAccount 账户下。您可以通过一个账户集中管理已注册员工向卡巴斯基发出的电子请求，还可以通过 Kaspersky CompanyAccount 管理这些员工的权限。

Kaspersky CompanyAccount 门户支持以下语言：

- 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 Linux 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 Linux 页面

在 Kaspersky 网站的 Kaspersky Security Center Linux 页面上，您可以查看有关程序、程序功能和特性的一般信息。

## 知识库中的 Kaspersky Security Center Linux 页

*知识库*是 Kaspersky 技术支持网站的一部分。

在 知识库的 Kaspersky Security Center Linux 页面上，您可以阅读文章，这些文章提供了有用的信息、建议以及有关如何购买、安装和使用程序的常见问题解答。

知识库中的文章可能提供关于 Kaspersky Security Center Linux 和 Kaspersky 应用程序的问题的答案。知识库中的文章也可能包含技术支持新闻。

## 在社区讨论 Kaspersky 应用程序

如果您的问题不需要立即回答，您可以在我们的论坛中与卡巴斯基专家和其他用户一起进行讨论。

您可以在论坛上查看讨论主题、发表评论、创建新的讨论主题。

> 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。

# 词汇表

## Cloud Discovery

Cloud Discovery 可管理用户对云服务的访问。云服务包括 Microsoft Teams、Salesforce、Microsoft Office 365 等。云服务分为几类，例如*文件共享*、*通信软件*、*电子邮件*。

## 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。

## Identity and Access Manager (IAM)

管理服务器的一个组件，允许您使用域身份验证（单点登录）。单点登录功能允许用户在 Kaspersky Security Center Web Console 中启用安全身份验证，而无需在公司网络上重新输入密码。

## iOS MDM 服务器

安装在客户端设备上的 Kaspersky Security Center 的一个组件，允许通过 Apple Push Notifications （APNs） 将 iOS 移动设备连接至管理服务器并管理 iOS 移动设备。

## iOS MDM 设备

通过 iOS MDM 协议连接到 iOS MDM 服务器的移动设备。可通过 iOS MDM 协议连接和管理运行 iOS 操作系统的设备。

## JavaScript

一种对网页性能进行扩展的编程语言。使用 JavaScript 创建的网页无需使用来自网络服务器的新数据刷新网页即可执行功能（例如，更改界面元素的视图或打开附加窗口）。要查看使用 JavaScript 创建的页面，请在您的浏览器的配置中启用 JavaScript 支持。

## Kaspersky Security Center Linux Web 服务器

Kaspersky Security Center Linux 组件，与管理服务器一同安装。Web 服务器用于通过网络传输独立安装包、iOS MDM 配置文件、以及共享文件夹的文件。

## Kaspersky Security Center Linux 管理员

通过 Kaspersky Security Center Linux 远程集中管理系统来管理应用程序操作的人。

## Kaspersky Security Center System Health Validator (SHV)

在 Kaspersky Security Center Linux 和 Microsoft NAP 并行运行时，用于检查操作系统运行能力的 Kaspersky Security Center Linux 的一个组件。

## Kaspersky Security Center 操作员

对通过 Kaspersky Security Center 管理的保护系统的状态和操作进行监视的用户。

## Kaspersky 更新服务器

Kaspersky 程序可以从 Kaspersky 的 HTTP(S) 服务器下载数据库和应用程序模块更新。

## Provisioning 配置文件

应用程序在 iOS 移动设备上运行的设置的集合。Provisioning 配置文件包含有关授权许可的信息，它连接至特定的应用程序。

## SSL

互联网和本地网上的使用的数据加密协议。Secure Sockets Layer（SSL）协议用在网络应用程序中，以便在客户端和服务器之间创建安全的连接。

## 不兼容应用程序

第三方开发的反病毒应用程序，或不支持通过 Kaspersky Security Center Linux 管理的 Kaspersky 应用程序。

## 事件严重级别

在 Kaspersky 程序操作过程中遇到的事件的属性。存在以下严重级别：

- 严重事件
- 功能失败

- 警告
- 信息

根据事件发生时的情况，相同类型的事件可能具有不同的严重级别。

## 事件存储库

管理服务器数据库的一部分，用于存储发生在 Kaspersky Security Center Linux 中的事件信息。

## 任务

由 Kaspersky 应用程序执行的功能作为任务来实施，例如：实时文件保护、计算机全盘扫描、数据库更新。

## 任务设置

对于每个任务类型的特别应用程序设置。

## 保护状态

当前保护状态，反映了计算机安全级别。

## 共享证书

证书用于识别用户的移动设备。

## 内部用户

内部用户的账户可用于操作虚拟管理服务器。Kaspersky Security Center Linux 授权应用程序的内部用户拥有真实用户的所有权限。

只能在 Kaspersky Security Center Linux 内创建和使用内部用户账户。系统不会将内部用户的任何数据传送到操作系统。Kaspersky Security Center Linux 将验证内部用户。

## 分发点

安装了网络代理并用于更新发布、远程安装应用程序、获取管理组（广播域）中计算机信息的计算机。分发点用来降低发布更新时管理服务器的负载并优化网络流量。分发点可以被自动指定、被管理服务器指定或被管理员手动指定。分发点先前叫做更新代理。

## 卡巴斯基私有安全网络 (KPSN)

“卡巴斯基私有安全网络”允许安装了 Kaspersky 应用程序的设备的用户访问“卡巴斯基安全网络”信誉数据库和其他统计数据，而不从他们的设备发送数据到“卡巴斯基安全网络”。卡巴斯基私有安全网络用于由于以下原因无法参与卡巴斯基安全网络的企业客户：

- 设备未连接到互联网。
- 传输任何数据到国家以外或企业局域网以外被法律或企业安全策略禁止。

## 反病毒保护服务提供商

提供给客户端组织基于 Kaspersky 解决方案的反病毒保护服务的组织。

## 反病毒数据库

包含截至反病毒数据库发布时 Kaspersky 已知的计算机安全威胁信息。反病毒数据库中的条目使得恶意代码在被扫描对象中被检测。反病毒数据库由 Kaspersky 专家创建，每小时更新一次。

## 受管理设备

包括在管理组中的企业网络设备。

## 可用更新

Kaspersky 应用程序模块的更新集，包含特定时间段积累的关键更新和应用程序架构更改。

## 备份文件夹

用于存储使用备份实用工具创建的管理服务器数据副本的专用文件夹。

## 安装包

使用 Kaspersky Security Center 远程管理系统创建的一组用于远程安装 Kaspersky 程序的文件。安装包包含安装应用程序所需的一系列设置，这些设置在安装后立即运行。应用程序默认设置。使用包含在应用程序分发工具中的扩展名为 .kpd 和 .kud 的文件创建安装包。

## 客户端管理员

客户组织中负责监控反病毒保护状态的员工。

## 密钥文件

带有.key扩展名的文件，可以用来以试用或商用授权许可使用 Kaspersky 应用程序。

## 广播域

网络的一个逻辑区域，在这里所有节点可以使用广播通道在 OSI 层（Open Systems Interconnection Basic Reference Model）交换数据。

## 应用程序商店

Kaspersky Security Center Linux 组件。应用程序商店用于安装应用程序到用户 Android 设备。应用程序商店允许您发布应用程序 APK 文件和链接到 Google Play。

## 归属管理服务器

归属管理服务器是网络代理安装过程中指定的管理服务器。归属管理服务器可在网络代理连接配置文件中被使用。

## 手动安装

从分发包安装安全应用程序到企业网络中的设备。手动安装需要管理员或其他 IT 专家的参与。通常情况下，如果远程安装发生错误，则执行手动安装。

## 授权许可期限

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。

## 漏洞

操作系统或应用程序存在的缺陷，恶意软件开发者会利用这种缺陷入侵操作系统或应用程序并破坏其完整性。操作系统中的大量漏洞会使操作系统不安全，因为能够入侵操作系统的病毒会导致操作系统或其上所安装的应用程序发生运行故障。

## 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。

## 病毒爆发

使设备感染病毒的一系列蓄意尝试。

## 直接应用程序管理

通过本地界面进行的应用程序管理。

## 程序设置

对所有任务类型通用并且掌管应用程序总体操作的应用程序设置，例如：应用程序性能设置、报告设置和备份设置。

## 策略

策略决定应用程序设置并管理应用程序在管理组中计算机上的配置。必须为每个应用程序都创建单独的策略。您可以为安装在每个管理组中计算机上的应用程序创建多个策略，但是对于管理组中的每个应用程序，一次只能应用一个策略。

## 管理员工作站

在其上打开 Kaspersky Security Center Web Console 的设备。该组件提供了 Kaspersky Security Center Linux 管理界面。

管理员工作站用于配置和管理 Kaspersky Security Center Linux 的服务器部分。使用管理员工作站，管理员基于 Kaspersky 应用程序为企业局域网创建和管理一个集中的反病毒保护系统。

## 管理员权限

在 Exchange 组织内管理 Exchange 对象所需的用户权限。

## 管理控制台

基于 Windows 的 Kaspersky Security Center 的组件（也称为基于 MMC 的管理控制台）。此组件提供管理服务器和网络代理的管理服务用户界面。管理控制台类似于 Kaspersky Security Center Web Console。

## 管理服务器

Kaspersky Security Center Linux 的一个组件，可集中存储企业网络内安装的所有 Kaspersky 应用程序的信息。它也可用于管理这些应用程序。

## 管理服务器客户端（客户端设备）

安装网络代理和运行受管理的 Kaspersky 程序的设备、服务器或工作站。

## 管理服务器数据备份

使用备份实用工具复制管理服务器数据，以便进行备份和后续的恢复。该实用工具可以保存：

- 管理服务器数据库（策略、任务、应用程序设置、管理服务器上保存的事件）
- 有关管理组和客户端设备的结构的配置详情
- 用于远程安装应用程序的安装文件存储库（文件夹内容：软件包、卸载更新）
- 管理服务器证书

## 管理服务器证书

管理服务器用于以下目的的证书：

- 连接到 Kaspersky Security Center Web Console 时的管理服务器身份验证
- 受管理设备上管理服务器和网络代理之间的安全交互
- 将主管理服务器连接到从属管理服务器时的管理服务器身份验证

安装管理服务器时会自动创建证书，然后存储在管理服务器上。

## 管理组

以功能和安装的 Kaspersky 应用程序分组的设备集。设备被分组成一个单一实体以便管理。组可以包含其他组。组策略和组任务可以为组中每个安装的应用程序创建。

## 组任务

为某个管理组定义并在该管理组中所有客户端设备上执行的任务。

## 网络代理

Kaspersky Security Center Linux 的一个组件，它实现了管理服务器和特定网络节点（工作站或服务器）上安装的 Kaspersky 应用程序之间的交互。该组件是公司内所有 Microsoft® Windows® 应用程序的通用组件。对于为 Unix 和 macOS 之类的平台开发的 Kaspersky 产品，分别有不同版本的网络代理。

## 网络位置识别 (NLA)

帮助操作系统识别当前网络的 Windows 服务。NLA 可检测网络变化并调整设备的安全配置。

## 网络保护状态

当前保护状态，它定义了企业网络设备的安全。网络保护状态包括已安装的安全应用程序、授权许可密钥的使用状态及检测到的威胁的数量和类型等因素。

## 网络反病毒保护

一组能够降低病毒和垃圾邮件感染组织网络的可能性并防止网络攻击、钓鱼和其他威胁的技术和组织措施。当您使用安全应用程序和服务和应用企业数据安全策略时，网络安全被增加。

## 虚拟管理服务器

Kaspersky Security Center Linux 组件，用于管理客户端式组织的网络的保护系统。

虚拟管理服务器是从属管理服务器的特例，与物理管理服务器相比，具有以下限制：

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

## 补丁重要级别

补丁属性。有五个 Microsoft 补丁和第三方补丁的重要级别：

- 严重
- 高
- 中
- 低
- 未知

第三方补丁或 Microsoft 补丁的重要级别由补丁需要修复的漏洞的最不利的严重级别决定。

## 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。

## 轻量级 Nagent（LWNGT）

用于与移动设备上的 Kaspersky Endpoint Security 进行交互的协议。LWNGT（又称移动协议）起到网络代理的作用，而无需在移动设备上实际安装网络代理。

## 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、 PostScript 和 Shockwave 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软件基金会在美国和/或其他国家的注册商标或商标。

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。

OpenVPN 是 OpenVPN, Inc. 的注册商标。

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。

Rocky Linux 是 Rocky Enterprise Software Foundation 的商标。

Samsung 是 SAMSUNG 在美国或其他国家/地区的商标。

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。