kaspersky

Kaspersky Anti Targeted Attack Platform

© 2026 AO Kaspersky Lab

目录

Kaspersky Anti Targeted Attack Platform 帮助

Kaspersky Anti Targeted Attack Platform

- 新闻
- 使用 Kaspersky Threat Intelligence Portal
- 分发包
- 硬件和软件要求
  - Kaspersky Endpoint Agent for Windows 版本与 Kaspersky Anti Targeted Attack Platform 版本的兼容性
  - Kaspersky Endpoint Agent for Windows 版本与 EPP 应用程序的兼容性
  - Kaspersky Endpoint Security for Windows 版本与 Kaspersky Anti Targeted Attack Platform 版本的兼容性
  - Kaspersky Endpoint Security for Linux 版本与 Kaspersky Anti Targeted Attack Platform 版本的兼容性
  - Kaspersky Endpoint Security for Mac 与 Kaspersky Anti Targeted Attack Platform 版本的兼容性
  - KUMA 版本与 Kaspersky Anti Targeted Attack Platform 版本的兼容性
  - XDR 版本与 Kaspersky Anti Targeted Attack Platform 版本的兼容性
  - KPSN 版本与 Kaspersky Anti Targeted Attack Platform 版本的兼容性
  - Kaspersky Anti Targeted Attack Platform 与 VK 云的兼容性
- 局限性

数据提供

- 应用程序的服务数据
- Central Node 和 Sensor 组件的数据
  - Sensor 组件的流量数据
  - 检测中的数据
  - 事件中的数据
  - 报告中的数据
  - 存储和隔离区中对象的数据
- Sandbox 组件数据
- 应用程序组件之间传输的数据
- 应用程序跟踪文件中包含的数据
- Kaspersky Endpoint Agent for Windows 的数据
  - 从 Central Node 组件接收的数据
  - 检测与事件中的数据
  - 任务完成报告中包含的数据
  - 安装日志中包含的数据
  - 阻止启动的文件数据
  - 与任务执行有关的数据
- Kaspersky Endpoint Security for Windows 数据
- Kaspersky Endpoint Security for Linux 数据
- Kaspersky Endpoint Security for Mac 数据

应用程序许可

- 关于最终用户授权许可协议
- 关于授权授权许可书
- 关于授权许可
- 关于授权许可密钥
- 关于密钥文件

关于激活码
关于订阅
添加授权许可密钥
替换授权许可密钥
删除授权许可密钥
在 Central Node 的 Web 界面中查看有关添加的授权许可密钥的信息
在 Central Node 的 Web 界面中查看最终用户授权许可协议的文本
在 Central Node 的 Web 界面中查看隐私政策文本
查看应用程序中使用的第三方代码的信息
在 Sandbox 的 Web 界面中查看最终用户授权许可协议的文本
查看 Endpoint Agent 组件的最终用户授权许可协议文本
基于授权许可的应用程序模式
应用程序架构
Sensor 组件
Central Node 组件
Sandbox 组件
Endpoint Agent 组件
应用程序的工作原理
分布式解决方案和多租户
分布式解决方案及多租户模式过渡方案
修改分布式解决方案和多租户模式的应用程序设置
将 PCN 角色分配给一台服务器
将 SCN 角色分配给一台服务器
查看有关租户、PCN 和 SCN 服务器的信息
将租户添加到 PCN 服务器
从 PCN 服务器删除租户
在 PCN 服务器上重命名租户
断开 SCN 与 PCN 的连接
修改断开 SCN 与 PCN 连接的应用程序设置
规模调整指南
部署和安装应用程序组件的常见方案
双服务器部署方案
三服务器部署方案
四台或以上服务器部署方案
使用 Sandbox 组件部署 KEDR 功能的方案
在没有 Sandbox 组件的情况下部署 KEDR 功能的方案
大小计算器
Sensor 组件的计算
Central Node 组件的计算
启用事件链扫描的 Central Node 组件的计算
Sandbox 组件计算
KVM 和 VMware ESXi 虚拟化平台上部署的 Central Node 组件的计算
安装和执行应用程序的初始配置
准备安装应用组件
准备 IT 基础架构以安装应用程序组件
为通过 POP3 与用于接收消息的邮件服务器集成准备 IT 基础构架
为通过 SMTP 与邮件服务器集成准备 IT 基础构架

准备虚拟机以安装 Sandbox 组件
准备包含 Central Node、Sensor 和 Sandbox 组件的安装磁盘镜像
安装和配置应用程序组件的步骤
安装 Sandbox 组件
步骤 1：查看最终用户授权许可协议和隐私策略
步骤 2：选择安装 Sandbox 组件的磁盘
步骤 3：分配主机名
步骤 4：在列表中选择控制网络接口
步骤 5：分配控制接口的地址和网络掩码
步骤 6：添加 DNS 服务器地址
步骤 7：配置静态网络路由
步骤 8：配置 Sandbox 管理员密码的最小密码长度
步骤 9：创建 Sandbox 管理员账户
将带有嵌入式 Sensor 的 Central Node 组件部署为集群
部署存储服务器
步骤 1：查看最终用户授权许可协议和隐私策略
步骤 2：选择服务器角色
步骤 3：选择部署模式
步骤 4：选择安装组件的磁盘
步骤 5：为服务器寻址选择网络掩码
步骤 6：为应用程序组件的寻址选择网络掩码
步骤 7：选择集群网络接口
步骤 8：选择外部网络接口
步骤 9：选择获取网络接口 IP 地址的方法
步骤 10：创建管理员账户并对群集中的服务器进行身份验证
创建管理员账户
验证集群中的服务器
步骤 11：添加 DNS 服务器地址
步骤 12：配置与 NTP 服务器的时间同步
步骤 13：选择用于 Ceph 存储的磁盘
部署处理服务器
步骤 1：查看最终用户授权许可协议和隐私策略
步骤 2：选择服务器角色
步骤 3：选择安装组件的磁盘
步骤 4：为群集服务器寻址选择网络掩码
步骤 5：为应用程序组件的寻址选择网络掩码
步骤 6：选择集群网络接口
步骤 7：选择外部网络接口
步骤 8：选择获取网络接口 IP 地址的方法
步骤 9：验证集群中的服务器
步骤 10：为 NDR 功能选择本地化语言，并配置从 SPAN 端口接收镜像流量
选择 NDR 功能的本地化语言
配置从 SPAN 端口接收镜像流量
清除存储服务器上的硬盘
在服务器上安装带有嵌入式 Sensor 的 Central Node 组件
步骤 1：查看最终用户授权许可协议和隐私策略
步骤 2：选择服务器角色

步骤 3：选择安装组件的磁盘
步骤 4：分配用于针对性攻击分析器组件数据库的磁盘
步骤 5：为服务器寻址选择网络掩码
步骤 6：为应用程序组件的寻址选择网络掩码
步骤 7：选择外部网络接口
步骤 8：选择获取网络接口 IP 地址的方法
步骤 9：创建管理员账户
步骤 10：选择 NDR 功能的本地化语言
步骤 11：添加 DNS 服务器地址
步骤 12：配置与 NTP 服务器的时间同步
步骤 13：配置从 SPAN 端口接收镜像流量
在独立服务器上安装 Sensor 组件
步骤 1：查看最终用户授权许可协议和隐私策略
步骤 2：选择服务器角色
步骤 3：选择安装组件的磁盘
步骤 4：为服务器寻址选择网络掩码
步骤 5：为应用程序组件的寻址选择网络掩码
步骤 6：选择外部网络接口
步骤 7：选择获取网络接口 IP 地址的方法
步骤 8：创建管理员账户
步骤 9：添加 DNS 服务器地址
步骤 10：配置与 NTP 服务器的时间同步
步骤 11：配置从 SPAN 端口接收镜像流量
优化 Sensor 组件的网络接口设置
连接和配置 Sensor 组件的外部存储
配置应用程序的大小设置
配置防火墙规则
装有 Kaspersky Anti Targeted Attack Platform 组件的计算机使用的端口
集群配置中 Kaspersky Anti Targeted Attack Platform 服务使用的端口
作为服务器部署的 Central Node 的服务使用的端口
在独立服务器上安装 Sensor 组件的配置中，服务使用的端口
网络流量分析服务之间的通信端口
配置 Endpoint Agent 组件与 KEDR 功能块的集成
配置与 Kaspersky Endpoint Agent 的受信任连接
配置 Central Node 服务器对 Kaspersky Endpoint Agent TLS 证书的验证并将加密容器上传到 Kaspersky Endpoint Agent
将 Central Node 服务器或 Sensor 的 TLS 证书上传到 Kaspersky Endpoint Agent
在 Kaspersky Endpoint Agent 端配置与 Kaspersky Anti Targeted Attack Platform 的集成和信任连接
配置与 Kaspersky Endpoint Security 的受信任连接
下载 Central Node 服务器的 TLS 证书
在 Kaspersky Anti Targeted Attack Platform 的 Web 界面中为 Central Node 服务器生成 TLS 证书
使用 Kaspersky Anti Targeted Attack Platform 的 Web 界面为 Central Node 服务器上传您自己的 TLS 证书
在 Kaspersky Anti Targeted Attack Platform 的 Web 界面中启用 Endpoint Agent 组件的 TLS 证书验证
在 Kaspersky Anti Targeted Attack Platform 的 Web 界面中生成 Endpoint Agent 组件的 TLS 证书并下载加密容器
使用 Kaspersky Anti Targeted Attack Platform 的 Web 界面上传您自己的 Endpoint Agent 组件的 TLS 证书
在 Kaspersky Anti Targeted Attack Platform 的 Web 界面中查看 Endpoint Agent 组件的 TLS 证书表
在 Kaspersky Anti Targeted Attack Platform 的 Web 界面中过滤和搜索 Endpoint Agent 组件的 TLS 证书

在 Kaspersky Anti Targeted Attack Platform 的 Web 界面中删除 Endpoint Agent 组件的 TLS 证书
配置从 Endpoint Agent 组件到 Sensor 服务器的流量重定向
配置 Endpoint Agent 组件与 NDR 功能块的集成
集成服务器表
准备从 Endpoint Agent 组件接收数据的场景
添加集成服务器
为集成服务器的客户端创建通信数据包
启用或禁用集成服务器
编辑集成服务器设置
删除集成服务器
应用程序使用入门
使用管理员账户开始使用应用程序 Web 界面
应用程序管理员菜单使用入门
在技术支持模式下开始使用应用程序
管理应用程序管理员和用户的账户
创建用于应用程序 Web 界面的管理员账户
创建用于应用程序 Web 界面的用户账户
配置用户账户表显示
查看用户账户表
筛选用户账户
清除账户筛选器
更改用户账户对 PCN 和 SCN 数据的访问权限
启用或禁用用户账户
更改应用程序管理员或用户账户的密码
更改您的账户密码
使用域账户进行身份验证
创建 keytab 文件
配置与 Active Directory 的集成
禁用与 Active Directory 的集成
参与卡巴斯基安全网络并使用卡巴斯基私有安全网络
查看 KSN 声明并配置参与 KSN
配置使用 KPSN
配置与 KPSN 本地信誉数据库的连接
配置要保存到 KPSN 本地信誉数据库的信息
KSN 参与度和 KPSN 使用量下降
通过 Web 界面管理 Sandbox 组件
更新 Sandbox 组件数据库
手动更新数据库
选择数据库更新源
使用卡巴斯基更新实用程序进行更新数据库
使用卡巴斯基更新实用程序下载更新包
启用和禁用更新数据库的代理服务器
配置数据库更新的代理服务器连接设置
配置 Sandbox 和 Central Node 组件间的连接
在 Sandbox Web 界面处理来自 Central Node 服务器的连接请求

- 配置 Sandbox 组件网络接口
  - 配置 DNS 设置
  - 配置管理网络接口的设置
  - 配置用于对已处理对象进行 Internet 访问的网络接口的设置
  - 添加、更改和移除静态网络路由
- 设置 Sandbox 系统的日期和时间
- 准备虚拟机以供使用
- 管理 Sandbox 存储中的操作系统和应用程序镜像
  - 查看 Sandbox 存储中的操作系统和应用程序镜像表
  - 将操作系统和应用程序镜像上传到存储
  - 激活 Sandbox 存储中的操作系统和应用程序镜像
  - 从 Sandbox 存储中删除操作系统和应用程序镜像
- 管理虚拟机模板
  - 创建虚拟机模板
  - 查看模板表格
  - 打开或关闭模板
  - 编辑模板
  - 配置操作系统和软件
    - 缓解 Spectre 和 Meltdown 漏洞。
    - 禁用 Windows Defender
  - 导出模板
  - 导入模板
  - 删除模板
- 管理虚拟机
  - 创建虚拟机
    - 在“虚拟机”部分创建虚拟机
    - 在模板表中创建虚拟机
    - 在模板视图中创建虚拟机
  - 查看具有预设操作系统的虚拟机表
  - 查看具有自定义操作系统的虚拟机表
  - 安装虚拟机
  - 删除虚拟机
  - 下载调试符号
- 设置同时运行的虚拟机的最大数量
- 更改具有自定义操作系统镜像的虚拟机的授权许可密钥数量
- 将 Sandbox 系统日志下载到硬盘驱动器
- 导出 Sandbox 设置
- 导入 Sandbox 设置
- 重新启动 Sandbox 服务器
- 关闭 Sandbox 服务器电源
- 更改 Sandbox 管理员账户密码

对于管理员：应用程序 Web 界面使用入门

- Kaspersky Anti Targeted Attack Platform 界面
- 监控应用程序的性能
  - 关于小组件和布局
  - 在“仪表板”部分选择要管理的租户和服务器
  - 添加小组件到当前布局

- 在当前布局中移动小组件
- 更改 NDR 小部件中信息的显示
- 从当前布局移除小组件
- 保存布局为 PDF
- 配置小部件中的数据显示周期
- 监控传入数据的接收和处理
- 监控由应用程序模块和组件对数据进行处理的队列
- 监控 Sandbox 组件对数据的处理
- 查看应用程序模块和组件的工作状况

管理 Central Node 或 Sensor 服务器信息

- 查看有关 Central Node 或 Sensor 服务器的信息
- 查看网络接口信息
- 识别与网络接口关联的以太网端口

使用应用程序 Web 界面管理 Central Node、PCN 或 SCN 服务器

- 配置服务器上的日期和时间
- 生成或上传服务器的 TLS 证书
- 下载服务器的 TLS 证书
- 服务器的 FQDN 设置
- 配置 DNS 设置
- 配置网络接口的设置
- 配置默认网络路由
- 配置代理服务器连接设置
- 配置邮件服务器连接
- 管理流量节省设置
- 管理保存流量转储文件的设置
- 选择扫描 Sandbox 中的对象时要使用的操作系统
- 密码策略
  - 首次身份验证成功后强制更改密码
  - 强制定期更改密码

管理 Sensor 组件

- 将 Sandbox 组件连接到 Central Node
  - 通过网络自动添加和连接 Sensor 组件
  - 使用通信数据包连接 Sensor 组件
- 删除 Sensor 组件
- 管理 Sensor 组件的证书
  - 在 Sensor 服务器的管理员菜单中为 Sensor 服务器生成 TLS 证书
  - 在 Sensor 服务器的管理员菜单中上传您自己的 TLS 证书
  - 将 Sensor 服务器的 TLS 证书下载到您的计算机
- 登录 Sensor 组件的 Web 界面
- 更改服务器名称
- 管理监控点
  - 添加监控点
  - 重命名监控点
  - 启用监控点
  - 禁用监控点
  - 正在删除监控点
- 配置扫描文件的最大大小

- 配置 HTTP 数据包正文转储
- 配置通过 SMTP 与邮件服务器集成
- 配置通过 ICAP 与代理服务器集成
  - 启用和禁用通过 ICAP 与代理服务器集成
  - 启用或禁用 ICAP 流量实时扫描
  - 配置 ICAP 流量实时扫描
  - 配置通知页面的显示
- 配置 SPAN 端口镜像流量的记录
  - 选择用于从 SPAN 端口接收镜像流量的网络协议
  - 使用 Web 界面配置 SPAN 端口镜像流量的记录
  - 使用 Sensor 组件的管理员菜单配置 SPAN 端口镜像流量的记录
- 配置通过 POP3 与邮件服务器集成

管理集群

- 查看集群的服务器表
- 将服务器添加到集群
- 增加存储服务器上的磁盘空间
- 停用服务器
  - 从集群中删除服务器
- 启动和关闭集群

有关 Central Node 和 Sensor 服务器允许的最大 CPU 和 RAM 负载的通知

- 配置 Central Node 和 Sensor 服务器允许的最大 CPU 和 RAM 负载

配置 SNMP 协议连接

- Kaspersky Anti Targeted Attack Platform 的 MIB 对象描述

管理 Endpoint Agent 主机信息

- 在“Endpoint Agent”部分中选择要管理的租户
- 查看独立 Central Node 服务器上具有 Endpoint Agent 组件的主机表
- 查看有关主机的信息
- 按主机名筛选和搜索具有 Endpoint Agent 组件的主机
- 根据已与网络隔离的 Endpoint Agent 组件筛选和搜索主机
- 按 PCN 和 SCN 服务器名称筛选和搜索具有 Endpoint Agent 组件的主机
- 按计算机 IP 地址筛选和搜索具有 Endpoint Agent 组件的主机
- 按计算机上的操作系统版本筛选和搜索具有 Endpoint Agent 组件的主机
- 按组件版本筛选和搜索具有 Endpoint Agent 组件的主机
- 按活动筛选和搜索具有 Endpoint Agent 组件的主机
- 为具有 Endpoint Agent 组件的主机快速创建筛选器
- 为具有 Endpoint Agent 组件的主机重置筛选器
- 配置 Endpoint Agent 组件的活动指示器
- 删除具有 Endpoint Agent 组件的主机
- 自动删除不活动的主机
- 支持的解释器和进程

配置与 Sandbox 组件的集成

- 查看具有 Sandbox 组件的服务器表
- 使用 Sandbox 组件创建连接到服务器的请求
- 启用和禁用与 Sandbox 组件的连接
- 删除与 Sandbox 组件的连接

从 Endpoint Agent 主机手动发送文件以供 Sandbox 扫描

- 启用和禁用从 Endpoint Agent 主机手动发送文件以供 Sandbox 扫描

- 配置与外部系统的集成
  - 查看外部系统表
  - 处理来自外部系统的请求
  - 从允许集成的列表中移除外部系统
  - 配置处理来自邮件传感器的流量的优先级
- 配置与 Kaspersky Managed Detection and Response 的集成
  - 启用 MDR 集成
  - 禁用 MDR 集成
  - 替换 MDR 配置文件
- 配置与 SIEM 系统的集成
  - 启用和禁用事件信息记录到远程日志
  - 配置 SIEM 系统集成的主要设置
  - 上传 TLS 证书
  - 启用和禁用与 SIEM 系统的连接的 TLS 加密
  - 有关检测的 syslog 邮件的内容和属性
- 更新使用 API 连接到 Central Node 的证书
- 管理连接器
  - 受管理和不受管理的连接器
  - 将事件、应用程序消息和审计记录发送到第三方系统
  - 通过 Cisco 交换机连接器自动控制设备的网络访问
  - 添加连接器
  - 查看连接器表
  - 启用或禁用连接器
  - 编辑连接器设置
  - 为连接器创建新的通信数据包
  - 正在删除连接器
  - 添加和删除连接器类型
    - 查看连接器类型表
    - 添加连接器类型
    - 删除连接器类型
- 管理远程连接的账户凭据 Secret
  - 添加 Secret
  - 查看 Secret 表
  - 连接到远程设备时防止 Secret 泄漏
  - 编辑 Secret 的设置
  - 删除 Secret
- 更新应用程序数据库
  - 选择数据库更新源
  - 手动更新数据库
  - 使用卡巴斯基更新实用程序进行更新数据库
  - 使用卡巴斯基更新实用程序下载更新包
- 创建存档的密码列表
- 与工具集成以解包加密的 SSL/TLS 流量

对于安全人员：应用程序 Web 界面使用入门

- Kaspersky Anti Targeted Attack Platform 界面
- 选择要在应用程序的 Web 界面中管理的租户

监控应用程序的性能
关于小组件和布局
添加小组件到当前布局
在当前布局中移动小组件
更改 NDR 小部件中信息的显示
从当前布局移除小组件
保存布局为 PDF
配置小部件中的数据显示周期
配置小组件显示缩放
“警报”类型小组件管理基础知识
事件小组件中的信息
事件小部件中的信息
查看应用程序模块和组件的工作状况
管理技术
启用或禁用技术
配置设备活动检测模式
管理技术继承
查看警报表
配置警报表显示
筛选、排序和搜索警报
按 VIP 身份筛选警报
按时间筛选和搜索警报
按重要性级别筛选警报
按检测到的对象的类别筛选和搜索警报
按获取的信息筛选和搜索警报
按源地址筛选和搜索警报
按目的地址筛选和搜索警报
按服务器名称筛选和搜索警报
按技术名称筛选和搜索警报
按用户处理状态筛选和搜索警报
按分配了警报的用户的名称过滤和搜索警报
对表中的警报进行排序
快速创建警报筛选器
保存筛选器
重置警报筛选器
警报处理建议
AM 警报处理建议
TAA 警报处理建议
SB 警报处理建议
处理 IOC 警报的建议
YARA 警报处理建议
IDS 警报处理建议
处理 NDR:IDS 和 NDR:EA 警报的建议
查看警报
查看警报详细信息
有关任何类型警报的一般信息
对象信息部分中的信息

- “警报详情”部分中的信息
- “有关使用 NDR 技术进行扫描的信息”部分中的信息
- 扫描结果部分中的信息
- IDS 规则部分中的信息
- URL 部分中的信息
- “检测相关设备的 IP 地址”部分中的信息
- 网络事件部分中的信息
- Sandbox 扫描结果
- IOC 扫描结果
- 主机部分中的信息
- “更改日志”部分中的信息
- 发送警报数据
- 查看警报关系

在警报上执行的用户操作

- 将警报分配给特定用户
- 标记单个警报处理的完成
- 标记警报处理的完成
- 修改 VIP 警报的状态
- 为警报添加注释

监控网络流量事件

- NDR 事件分数和严重程度
- NDR 事件注册技术
- NDR 事件状态
- 已注册 NDR 事件表
- 配置已注册事件表
- 查看嵌套在聚合事件内的事件
- 查看 NDR 事件的详细信息
- 更改 NDR 事件的状态
- 添加标记
- 将 NDR 事件复制到文本编辑器
- 下载事件流量
- 创建用于将事件导出至网络共享的目录

事件数据库威胁追踪

- 在构建器模式下搜索事件
- 在源代码模式下搜索事件
- 转换生成器查询以在源代码模式下搜索事件
- 事件搜索条件
- 运算符
- 对表中的事件进行排序
- 更改事件搜索条件
- 按 EPP 应用程序中的处理结果搜索事件
- 使用 IOC 或 YAML 文件中指定的条件搜索事件
- 根据事件搜索条件创建 TAA (IOA) 规则

事件信息
事件处理建议
遵循建议隔离主机
遵循建议防止文件运行
遵循建议创建任务
有关事件树中事件的信息
查看事件树中的父进程信息
查看事件树中有关父进程发起的事件的信息
查看事件树中的主机信息
查看事件表
配置事件表显示
查看有关事件的信息
有关“进程已启动”事件的信息
有关“进程已终止”事件的信息
有关“模块已加载”事件的信息
有关“远程连接”事件的信息
“防护规则”事件信息
有关“文档被阻止”事件的信息
有关“文件已修改”事件的信息
有关“系统事件日志”事件的信息
有关“注册表更改”事件的信息
有关“端口被侦听”事件的信息
有关“驱动程序已加载”事件的信息
有关“DNS”事件的信息
有关“LDAP”事件的信息
有关“命名管道”事件的信息
有关“WMI”事件的信息
有关“检测”事件的信息
有关“检测处理结果”事件的信息
有关“被解释文件运行”事件的信息
有关“AMSI 扫描”事件的信息
有关“在控制台进行交互式命令输入”事件的信息
有关“代码注入”事件的信息
有关“进程访问”事件的信息
根据 Kaspersky TAA (IOA) 规则进行事件链扫描
启用或禁用根据 Kaspersky TAA (IOA) 规则进行事件链扫描
查看由 Kaspersky TAA (IOA) 规则标记的事件
管理资产
查看设备表
查看设备信息
自动添加和更新设备
手动添加设备
使用设备表时添加设备
在管理拓扑图时添加设备
根据网络交互图上的未知设备节点添加设备
根据拓扑图上非管理交换机添加设备
自动分配设备状态

- 根据条件自动对设备进行分组
  - 根据条件自动对设备进行分组，从组树的根开始
  - 自动将设备分组到选定的设备组中
- 手动将设备分组
  - 将设备添加到组
  - 将多个设备添加到一个组
  - 从组中删除设备
  - 从组中删除多个设备
- 将带有组件和组的服务器移动到网络交互图上的其他组
- 设备组树
- 手动编辑设备组树
  - 添加组
  - 重命名组
  - 删除组
  - 移动组
  - 搜索组
  - 更新树
- 添加和删除设备标签
  - 为单个设备添加标签
  - 为多个设备添加标签
  - 从单个设备上删除标签
  - 清除多个设备的标签列表
- 响应
- 监控设备上的用户
- 监控设备上的文件执行情况
- 主动设备轮询作业
  - 添加主动轮询作业
  - 编辑主动轮询作业
  - 查看主动轮询作业表
  - 启动和停止主动轮询作业
  - 查看有关主动轮询作业运行的一般信息
  - 查看有关主动轮询作业执行的报告
  - 删除主动轮询作业

配置地址空间

- 关于地址空间规则
- 关于地址空间子网
- 添加地址空间
- 为资产管理创建子网列表
  - 添加子网
  - 编辑子网设置
  - 删除子网
- 查看所选子网中具有 IP 地址的设备的信息
- 更改地址空间
- 删除地址空间

使用网络交互图

- 网络交互图上的节点
- 网络交互图上的设备组

网络交互图上的链接
查看对象详细信息
改变网络交互图的比例
定位网络交互图
固定和取消固定节点和组
手动重新排列节点和组
自动排列节点和组
在网络交互图上搜索节点
过滤网络交互图上的对象
节点和链接的全面过滤
使用时间尺度上的时间段进行过滤
按已注册事件进行过滤
节点过滤
按设备状态过滤节点
按设备安全状态过滤节点
按设备类别过滤节点
启用和禁用与过滤节点关联的节点的显示
过滤链接
按严重性分数过滤链接
按通信协议过滤链接
按 OSI 模型层过滤链接
重置过滤器设置
保存和加载网络交互图显示设置
添加新视图，同时保存当前网络交互图显示设置
在保存当前网络交互图显示设置的同时更新视图
重命名网络交互图视图
删除网络交互图视图
在网络交互图上应用保存的视图设置
监控网络会话
网络会话表
查看网络会话详细信息
下载网络会话流量
搜索网络数据包
预配置网络包搜索规则
Kaspersky Anti Targeted Attack Platform 检测到的协议
监控风险
关于漏洞类别中的风险
持续风险管理流程的实施方案
查看风险表
查看风险信息
手动更改风险状态
使用设备表时查看风险详细信息
配置 NDR 事件类型
查看事件类型表
编辑系统事件类型的设置
配置自动保存系统事件类型的流量
配置通过连接器转发事件

- Kaspersky Anti Targeted Attack Platform 中的常见替换变量
- NDR 事件注册技术
- Kaspersky Anti Targeted Attack Platform 中的系统事件类型
  - 入侵检测技术的系统事件类型
  - 资产管理技术的系统事件类型
  - 外部系统技术的系统事件类型
  - 端点保护平台技术的系统事件类型

配置风险类型
- 查看风险类型表
- 更改风险类型的基本分数
- 管理存储风险的设置

Kaspersky Anti Targeted Attack Platform 中的系统事件类型
- 入侵检测技术的系统事件类型
- 资产管理技术的系统事件类型
- 外部系统技术的系统事件类型
- 端点保护平台技术的系统事件类型

管理 Endpoint Agent 主机信息
- 查看具有 Endpoint Agent 组件的主机表
- 配置具有 Endpoint Agent 组件的主机表的显示
- 查看有关主机的信息
- 按主机名筛选和搜索具有 Endpoint Agent 组件的主机
- 根据已与网络隔离的 Endpoint Agent 组件筛选和搜索主机
- 按 PCN 和 SCN 服务器名称筛选和搜索具有 Endpoint Agent 组件的主机
- 按计算机 IP 地址筛选和搜索具有 Endpoint Agent 组件的主机
- 按计算机上的操作系统版本筛选和搜索具有 Endpoint Agent 组件的主机
- 按组件版本筛选和搜索具有 Endpoint Agent 组件的主机
- 按活动筛选和搜索具有 Endpoint Agent 组件的主机
- 为具有 Endpoint Agent 组件的主机快速创建筛选器
- 为具有 Endpoint Agent 组件的主机重置筛选器
- 删除具有 Endpoint Agent 组件的主机
- 支持的解释器和进程

使用 Endpoint Agent 组件对主机进行网络隔离
- 创建一个网络隔离规则
- 添加网络隔离规则中的排除项
- 删除网络隔离规则
- 与网络隔离相关的限制

根据 Kaspersky TAA (IOA) 规则自动从 Kaspersky Endpoint Agent 主机发送文件以供 Sandbox 组件扫描
- 启用和禁用从具有 Endpoint Agent 组件的主机自动发送文件以供 Sandbox 组件扫描

选择扫描 Sandbox 中的对象时要使用的操作系统
- 查看具有 Sandbox 组件的服务器表
- 选择扫描 Sandbox 中的对象时要使用的操作系统

管理任务
- 查看任务表
- 查看有关任务的信息
- 创建获取文件任务
- 创建取证收集任务
- 创建注册表项检索任务

- 创建 NTFS 元文件检索任务
- 创建进程内存转储检索任务
- 创建磁盘镜像检索任务
  - 将文件从 RAW 转换为 EWF 格式
- 创建 RAM 转储检索任务
- 创建进程终止任务
- 创建任务以使用 YARA 规则扫描主机
- 创建服务管理任务
- 创建应用程序执行任务
- 创建文件删除任务
- 创建文件隔离任务
- 创建隔离文件恢复任务
- 创建任务副本
- 删除任务
- 按创建时间筛选任务
- 按类型筛选任务
- 按名称筛选任务
- 按文件名和路径筛选任务
- 按描述筛选任务
- 按服务器名称筛选任务
- 根据创建任务的用户的名称筛选任务
- 按处理状态筛选任务
- 清除任务筛选器

管理策略（防止规则）

- 查看防止规则表
- 配置防止规则表显示
- 查看防止规则
- 创建防止规则
- 导入防止规则
- 启用和禁用防止规则
- 启用和禁用预设
- 删除防止规则
- 按名称筛选防止规则
- 按类型筛选防止规则
- 按文件哈希筛选防止规则
- 按服务器名称筛选防止规则
- 清除防止规则筛选器

管理用户定义的规则

- 使用入侵指标 (IOC) 和攻击指标 (IOA) 进行威胁搜索
- 管理用户定义的 TAA (IOA) 规则
  - 查看TAA（IOA）规则表
  - 根据事件搜索条件创建 TAA (IOA) 规则
  - 导入 TAA (IOA) 规则
  - 查看自定义 TAA (IOA) 规则详细信息
  - 搜索其中触发了 TAA (IOA) 规则的警报和事件
  - 筛选和搜索 TAA (IOA) 规则
  - 重置 TAA (IOA) 规则筛选器

- 启用和禁用 TAA (IOA) 规则
- 修改 TAA (IOA) 规则
- 删除 TAA (IOA) 规则
- 管理用户定义的 IOC 规则
  - 查看 IOC 文件表
  - 查看有关 IOC 文件的信息
  - 上传 IOC 文件
  - 下载 IOC 文件到计算机
  - 扫描主机时启用和禁用 IOC 文件的自动使用
  - 删除 IOC 文件
  - 在 IOC 扫描结果中搜索警报
  - 使用 IOC 文件搜索事件
  - 筛选和搜索 IOC 文件
  - 清除 IOC 文件筛选器
  - 配置 IOC 扫描时间表
- 管理用户定义的入侵检测规则
  - 入侵检测规则
  - 其他入侵检测方法
  - 启用和禁用入侵检测规则集
  - 加载和替换用户定义的入侵检测规则集
  - 删除用户定义的入侵检测规则集
- 管理用户定义的 YARA 规则
  - 查看 YARA 规则表
  - 配置 YARA 规则表显示
  - 导入 YARA 规则
  - 查看 YARA 规则详细信息
  - 筛选和搜索 YARA 规则
  - 清除 YARA 规则筛选器
  - 启用和禁用 YARA 规则
  - 删除 YARA 规则
- 管理存储和隔离区中的对象
  - 查看放入存储中的对象表
  - 使用 Web 界面查看有关手动放置在存储中的对象的信息
  - 查看有关通过获取文件任务放置在存储中的对象的信息
  - 查看有关通过获取数据任务放置在存储中的对象的信息
  - 从存储下载对象
  - 将对象上传到存储
  - 发送存储中的对象进行扫描
  - 删除存储中的对象
  - 按对象类型筛选存储中的对象
  - 按对象描述筛选存储中的对象
  - 根据扫描结果筛选存储中的对象
  - 根据 Central Node、PCN 或 SCN 服务器的名称筛选存储中的对象
  - 按对象源筛选存储中的对象
  - 根据放入存储中的时间筛选对象
  - 清除存储对象筛选器
  - 查看在具有 Kaspersky Endpoint Agent 组件的计算机上被隔离的对象表

查看被隔离对象的信息
从隔离中恢复对象
获取 Kaspersky Anti Targeted Attack Platform 服务器上被隔离对象的副本
从表中删除有关隔离对象的信息
按对象类型筛选有关隔离对象的信息
按对象描述筛选有关隔离对象的信息
按主机名筛选有关隔离对象的信息
按时间筛选有关隔离对象的信息
重置有关隔离对象信息的筛选器
管理报告
管理常见报告
查看模板和报告的表格
创建模板
根据模板创建报告
查看报告
将报告下载到本地计算机
编辑模板
按名称筛选模板
根据创建模板的用户的名称筛选模板
按创建时间筛选模板
清除模板筛选器
删除模板
按创建时间筛选报告
按名称筛选报告
按具有 Central Node 组件的服务器名称筛选报告
根据创建报告的用户的名称筛选报告
清除报告筛选器
删除报告
管理 NDR 报告
查看 NDR 报告模板表
查看 NDR 报告模板详细信息
查看 NDR 报告表
根据模板手动生成 NDR 报告
复制 NDR 报告模板
编辑 NDR 报告模板
将 NDR 报告导出到文件
删除 NDR 报告模板
删除 NDR 报告
取消 NDR 报告生成
管理存储报告文件的设置
管理将 VIP 身份分配给警报的规则
查看 VIP 身份分配规则表
创建 VIP 身份分配规则
删除 VIP 身份分配规则
修改 VIP 身份分配规则
导入 VIP 身份分配规则列表
导出从扫描中排除的数据列表

- 按 VIP 身份分配规则类型筛选和搜索
- 按 VIP 身份规则的值筛选和搜索
- 按 VIP 身份分配规则描述筛选和搜索
- 清除 VIP 身份分配规则筛选器

管理 NDR 事件的允许规则
- 查看允许规则表格
- 使用空白设置或模板中的设置创建允许规则
- 从已注册事件创建允许规则
- 复制允许规则
- 编辑允许规则的设置
- 启用或禁用允许规则
- 删除允许规则

管理扫描排除项列表
- 查看从扫描中排除的数据表
- 添加扫描排除规则
- 删除扫描排除规则
- 编辑添加到扫描排除项的规则
- 导出从扫描中排除的数据列表
- 按条件筛选扫描排除项列表中的规则
- 按值搜索扫描排除项列表中的规则
- 重置扫描排除项列表中的规则筛选器

管理入侵检测规则排除项
- 查看添加到排除项的入侵检测规则表
- 将入侵检测规则添加到排除项
- 编辑添加到排除项的入侵检测规则的描述
- 从排除项中删除入侵检测规则

管理 TAA 排除项
- 查看添加到排除项的 TAA (IOA) 规则表
- 将 TAA (IOA) 规则添加到排除项
- 查看添加到排除项的 TAA (IOA) 规则
- 从排除项中删除 TAA (IOA) 规则

管理 ICAP 排除项
- 查看 ICAP 排除表
- 将规则添加到 ICAP 排除项
- 从 ICAP 排除项中删除规则
- 编辑或禁用 ICAP 排除项列表中的规则
- 按条件筛选 ICAP 排除项列表中的规则
- 按值筛选 ICAP 排除项列表中的规则
- 按状态筛选 ICAP 排除项列表中的规则
- 清除 ICAP 排除项列表中的规则筛选条件

管理 SPAN 端口的镜像流量

创建存档的密码列表

管理 Central Node 或 Sensor 服务器信息

查看服务器设置

查看具有 Sandbox 组件的服务器表

查看用于扫描 Sandbox 中对象的操作系统集的设置

查看外部系统表

管理用户定义的 Sandbox 规则
查看用户定义的 Sandbox 规则表
配置 Sandbox 规则表显示
筛选和搜索 Sandbox 规则
清除 Sandbox 规则筛选器
查看用户定义的 Sandbox 规则信息
创建用户定义的文件扫描 Sandbox 规则
创建用户定义的 URL 扫描 Sandbox 规则
复制用户定义的 Sandbox 规则
导入用户定义的文件扫描 Sandbox 规则
编辑用户定义的 Sandbox 规则
启用或禁用用户定义 Sandbox 规则
导出用户定义的文件扫描 Sandbox 规则
删除用户定义的 Sandbox 规则
文件类别的扩展名列表
发送通知
查看发送通知的规则表
创建发送有关检测的通知的规则
创建用于发送有关应用程序组件操作的通知的规则
启用和禁用发送通知的规则
修改发送通知的规则
删除发送通知的规则
按规则类型筛选和搜索通知转发规则
根据通知主题筛选和搜索通知转发规则
按电子邮件地址筛选和搜索通知转发规则
根据状态筛选和搜索通知转发规则
清除通知转发规则筛选器
管理日志
管理活动日志
启用和禁用在活动日志中记录信息
下载活动日志文件
有关 Web 界面中用户活动的 CEF 消息的内容和属性
管理 NDR 用户活动日志
管理日志存储设置
启用和禁用用户活动审计
查看用户活动审计条目
设置跟踪日志的最大存储空间限制
设置跟踪日志的最大存储空间限制
下载 Kaspersky Anti Targeted Attack Platform 日志
查看应用程序消息
查看已发送至 Kaspersky Anti Targeted Attack Platform 进行扫描的文件的信息
管理 Kaspersky Endpoint Agent for Windows
管理 Kaspersky Endpoint Security for Windows
管理 Kaspersky Endpoint Security for Linux
管理 Kaspersky Endpoint Security for Mac

备份和恢复数据
- 备份和恢复 Central Node 服务器的数据
- 备份和恢复作为集群部署的 Central Node 服务器的数据
- 分布式解决方案和多租户模式下 Central Node 服务器的数据备份和恢复
- 导出数据的内容

升级 Kaspersky Anti Targeted Attack Platform
- 将服务器上安装的 Central Node 从版本 6.1 升级到 7.0.3
- 将作为集群安装的 Central Node 从版本 6.1 升级到版本 7.0.3
- 准备在分布式解决方案和多租户模式下安装升级
- 升级安装在独立服务器上的 Sensor
- 升级 Kaspersky Anti Targeted Attack Platform 时保留的信息内容和数量
- 将 Kaspersky Anti Targeted Attack Platform 从 7.0 版更新至 7.0.1 版
- 将 Kaspersky Anti Targeted Attack Platform 从 7.0.1 版更新至 7.0.3 版

使用 Kaspersky Anti Targeted Attack Platform API KATA 和 KEDR
- 将外部系统与 Kaspersky Anti Targeted Attack Platform 集成
- 用于扫描外部系统对象的 API
  - 请求扫描对象
  - 请求扫描结果
  - 请求删除扫描结果
  - 请求显示对象扫描限制
- 外部系统可用来接收应用程序警报信息的 API
  - 请求显示警报信息
  - 传输数据的范围
    - 有关检测到的对象的数据
    - 有关检测到的威胁的数据
    - 有关检测到的对象的环境数据
- 外部系统可用来接收应用程序事件信息的 API
  - 查询事件信息的请求
  - 用于筛选事件的查询语言
  - 用于筛选事件的字段
- 用于管理威胁响应操作的 API
  - 请求获取具有 Endpoint Agent 组件的主机列表
  - 请求有关网络隔离以及具有 Kaspersky Endpoint Agent 组件的主机是否存在防止规则的信息
  - 主机网络隔离管理
    - 请求启用网络隔离
    - 请求禁用网络隔离
    - 请求将排除项添加到网络隔离规则
  - 管理防止规则
    - 请求创建防止规则
    - 请求删除防止规则
  - 管理应用程序运行任务
    - 请求获取有关任务的信息
    - 请求创建任务
    - 请求删除任务

使用 Kaspersky Anti Targeted Attack Platform API NDR
- 确保使用 Kaspersky Anti Targeted Attack Platform API 时的安全性
- 创建并使用 Kaspersky Anti Targeted Attack Platform API 的连接器

有关应用程序的信息源
联系技术支持服务
如何获得技术支持
通过 Kaspersky CompanyAccount 获得技术支持
词汇表
Central Node
CSRF 攻击
Endpoint Agent 组件
ICAP 客户端
ICAP 数据
IOA
IOC
IOC 文件
Kaspersky Anti Targeted Attack Platform
Kaspersky Secure Mail Gateway
Kaspersky Threat Intelligence Portal
KATA
KEDR
Kerberos 身份验证
Keytab 文件
KPSN 的本地信誉数据库
MIB（管理信息库）
MITRE 技术
NTP 服务器
OpenIOC
Sandbox
Sensor
SIEM 系统
SPAN
Syslog
TAA（IOA）规则
TLS 加密
VIP 身份
YARA
YARA 规则
中间人攻击
入侵检测系统
最终用户授权许可协议
分布式解决方案
卡巴斯基安全网络（KSN）
卡巴斯基私有安全网络
反恶意软件引擎
后门程序
备用数据流
多租户
恶意 Web 地址
新一代威胁

- 服务主体名称 (SPN)
- 检测
- 租户
- 签名
- 网络钓鱼 URL 地址
- 警报
- 转储
- 追踪
- 通信信道带宽
- 针对性攻击
- 针对性攻击分析器
- 镜像流量
- 零日攻击
- 零日漏洞
- 高级持续性威胁（APT）

有关第三方代码的信息

商标声明

Kaspersky Anti Targeted Attack Platform 帮助

新功能

- Kaspersky Anti Targeted Attack Platform 的新增功能

硬件和软件要求

- 硬件和软件要求
- Kaspersky Anti Targeted Attack Platform 与 Kaspersky Endpoint Agent for Windows 的兼容性
- Kaspersky Anti Targeted Attack Platform 与 Kaspersky Endpoint Security for Windows、 Linux和Mac的兼容性

授权许可

- 授权 Kaspersky Anti Targeted Attack Platform

使用入门

- 分布式解决方案和多租户
- 调整 Kaspersky Anti Targeted Attack Platform 大小
- Kaspersky Anti Targeted Attack Platform 的安装和初始配置
- 配置 Kaspersky Anti Targeted Attack Platform 与 Kaspersky Endpoint Agent 组件的集成

开始使用 Kaspersky Anti Targeted Attack Platform Web 界面

- 应用程序 Web 界面入门 — 适用于管理员
- 应用程序 Web 界面入门 — 适用于安全员

附加功能

- 通过 Web 界面管理 Sandbox 组件
- 通过 API 与外部系统交互

更新

- 更新先前版本的 Kaspersky Anti Targeted Attack Platform

联系技术支持服务

- 如何获得技术支持

Kaspersky Anti Targeted Attack Platform

Kaspersky Anti Targeted Attack Platform（以下简称“该应用程序”）是一个设计用来保护企业 IT 基础构架和及时检测诸如*零日攻击*、*针对性攻击*，以及被称为*高级持续性威胁*（以下也称为“*APT*”）的复杂针对性攻击等威胁的解决方案。该解决方案是为企业用户开发的。

Kaspersky Anti Targeted Attack Platform 包括三个功能模块：

- Kaspersky Anti Targeted Attack Platform（以下也称为“KATA”），为企业 IT 基础构架提供边界安全。
- Kaspersky Endpoint Detection and Response（以下也称为“KEDR”），为组织的局域网提供保护。
- 网络检测和响应（以下也称为“NDR”），为企业 LAN 提供保护。

该解决方案可以通过以下方式接收和处理数据：

- 集成到局域网中，接收和处理镜像的*SPAN、ERSPAN 和 RSPAN 流量*，并从 HTTP、HTTP2、FTP、SMTP、DNS、SMB 和 NFS 协议中提取对象和元数据。
- 通过 ICAP 协议连接到代理服务器，接收和处理 HTTP 流量、HTTP2 流量和 FTP 流量以及 HTTPS 流量（如果管理员在代理服务器上配置了 SSL 证书更换）的数据。
- 通过 POP3 (S) 和 SMTP 协议连接到邮件服务器，接收和处理电子邮件消息的副本。
- 与 Kaspersky Secure Mail Gateway 和 Kaspersky Security for Linux 邮件服务器集成，接收并处理电子邮件的副本。
- 使用卡巴斯基 SD-WAN 应用程序接收并处理从远程位置获取的网络流量副本。此功能提高了检测和监控网络活动的灵活性，使您能够分析来自网络不同点的流量并采取适当的措施以确保网络安全。

  有关 Kaspersky Secure Mail Gateway、Kaspersky Security for Linux Mail Server 和 Kaspersky SD-WAN 的详情，请参阅这些应用程序的文档。
- 与 Kaspersky Endpoint Agent 和 Kaspersky Endpoint Security 集成，并从企业 IT 基础架构中运行 Microsoft® Windows®、Linux® 和 Mac® 操作系统的单台计算机接收数据（*事件*）。这些应用程序将持续监控在这些计算机上运行的进程、活动的网络连接和被修改的文件。
- 使用 REST API 接口与外部系统集成并扫描这些系统上的文件。

该解决方案使用以下威胁情报手段：

- 卡巴斯基安全网络（也称为“KSN”）云服务的基础架构，提供对卡巴斯基在线知识库的访问，其中包含有关文件、Web 资源和软件信誉的信息。使用来自卡巴斯基安全网络的数据可确保卡巴斯基应用程序能够更快地响应威胁，提高某些保护组件的性能，并降低误报的可能性。
- 与卡巴斯基私人安全网络 (KPSN) 集成，以访问卡巴斯基安全网络的信誉数据库以及其他统计数据，而无需将数据从用户计算机发送到卡巴斯基安全网络。
- 与被称为 Kaspersky Threat Intelligence Portal 的卡巴斯基信息系统集成，该系统包含并显示有关文件和 URL 信誉的信息。

- IOC（入侵指标）。Kaspersky Anti Targeted Attack Platform 使用符合 OpenIOC 标准的 IOC 文件，该标准是描述入侵指标的开放标准。IOC 文件包含一组与事件指标进行比较的指标。如果比较的指标匹配，应用程序将该事件视为警报。

- IOA（攻击指标）。Kaspersky Anti Targeted Attack Platform 扫描应用程序的事件数据库，并标记与 TAA (IOA) 规则描述的行为相匹配的事件或事件链。

该解决方案可以检测企业 IT 基础架构内发生的以下事件：

- 文件已下载，或试图将文件下载到企业 LAN 计算机。
- 文件已发送到企业 LAN 上的用户的电子邮件地址。
- 网站链接在企业 LAN 计算机上打开。
- 检测到在企业 LAN 计算机的 IP 地址或域名上有网络活动发生。
- 在企业 LAN 计算机上的进程已启动。

应用程序可以通过以下方式向用户提供其运行结果和威胁情报：

- 显示在 Central Node、主 Central Node（以下简称 “PCN”）或从属 Central Node（以下简称 “SCN”）服务器的 Web 界面中完成的工作结果。
- 通过 Syslog 协议向组织中已使用的 SIEM 系统发布警报。
- 通过 REST API 与外部系统集成，并根据需要将解决方案生成的警报信息发送到外部系统。
- 在卡巴斯基私人安全网络的本地信誉数据库中发布有关 Sandbox 组件警报的信息。

具有**高级安全官**或者**安全官**角色的用户可以在应用程序中执行以下操作：

- 监控解决方案的组件。
- 查看检测到的针对性攻击和入侵企业 IT 基础架构的迹象表，筛选和搜索警报，查看和管理每个警报，遵循建议进行评估和调查事件。
- 查看企业 IT 基础架构的计算机和服务器上发生的事件表，搜索威胁，筛选、查看和管理每个事件，遵循建议进行评估和调查事件。
- 在安装有 Kaspersky Endpoint Agent 和 Kaspersky Endpoint Security 的计算机上运行任务：运行应用程序和停止进程、下载和删除文件、在安装有 Kaspersky Endpoint Agent 和 Kaspersky Endpoint Security 的计算机上隔离对象、将文件副本放置在 Kaspersky Anti Targeted Attack Platform 的存储中，从隔离区恢复文件。
- 在安装有 Kaspersky Endpoint Agent 和 Kaspersky Endpoint Security 的选定计算机上，设置策略以防止运行他们认为不安全的文件和进程。
- 将安装有 Kaspersky Endpoint Agent 和 Kaspersky Endpoint Security 的单个计算机与网络隔离。
- 使用 TAA (IOA) 规则对事件进行分类和分析。
- 管理用户定义的针对性攻击分析器 TAA (IOA)、入侵检测系统 (IDS) 和 YARA 规则，上传用于扫描事件和创建警报的规则。
- 使用 OpenIOC 兼容文件（IOC 文件）在具有 Endpoint Agent 组件的主机上和警报数据库中搜索目标攻击、受感染和可能受感染对象的迹象。

- 从扫描中排除卡巴斯基定义的 TAA (IOA) 规则和 IDS 规则。
- 管理隔离区中的对象和存储中对象的副本。
- 管理有关应用程序性能和警报的报告。
- 配置将有关应用程序遇到的警报和问题的通知发送到用户的电子邮件地址。
- 管理 VIP 警报列表和从扫描中排除的数据列表，并填充 KPSN 的本地信誉数据库。
- 存储和下载原始网络流量的副本，以便在外部系统中进行分析。

具有**安全审计员**角色的用户可以在应用程序中执行以下操作：

- 监控解决方案的组件。
- 查看检测到的针对性攻击和入侵企业 IT 基础架构的迹象表，筛选和搜索警报，以及查看每个警报的数据。
- 查看企业 IT 基础架构的计算机和服务器上发生的事件表，搜索威胁，筛选和查看每个事件。
- 查看具有 Endpoint Agent 组件的主机列表以及有关所选主机的信息。
- 查看针对性攻击分析器 TAA (IOA)、入侵检测系统 (IDS) 和 YARA 的用户定义规则。
- 查看卡巴斯基专家定义的扫描排除 TAA (IOA) 规则和 IDS 规则。
- 查看有关应用程序性能和警报的报告。
- 查看 VIP 警报列表以及被从扫描中排除的数据列表。
- 查看在应用程序 Web 界面中进行的所有设置。
- 存储和下载原始网络流量的副本，以便在外部系统中进行分析。

具有“**管理员**”角色的用户可以在应用程序中执行以下操作：

- 编辑应用程序设置。
- 配置分布式解决方案和多租户模式的服务器。
- 设置应用程序与其他应用程序和系统的集成。
- 管理 TLS 证书并在 Central Node 服务器和 Sandbox 服务器之间、Kaspersky Anti Targeted Attack Platform 服务器和 Endpoint Agent 组件之间以及与外部系统之间建立信任连接。
- 管理应用程序用户的账户。
- 监控应用程序健康状况。

新增功能

Kaspersky Anti Targeted Attack Platform 7.0.3 引入了以下新功能：

1. Kaspersky Anti Targeted Attack Platform 的性能得到提升
2. 修复了显示网络会话信息时出现的错误。
3. 修复了安装或升级 Kaspersky Anti Targeted Attack Platform 时出现的错误。
4. 修复了 Suricata 模块中的漏洞。
5. 优化了事件组合规则。
6. 修复了虚拟机状态显示不稳定的问题。
7. 修复了单点登录 (SSO) 身份验证错误。
8. 修复了在网络流量中注册事件时出现的错误。
9. 修复了具有安全官角色的用户尝试访问自定义规则部分时出现的错误。
10. 修复了在 Web 界面的“**控制板**”部分中有关来自 SPAN 端口的镜像流量的信息的显示。

Kaspersky Anti Targeted Attack Platform 7.0.1 目前具有以下功能：

1. 即使下一个下载请求在前一个下载请求完成之前到达，镜像流量的下载也能正确完成。
2. 搜索最近一小时的网络数据包时，所有符合搜索条件的记录都将显示。
3. 在集群配置中，当与邮件服务器集成时，发送电子邮件时的错误现已修复。
4. 修复了将 Central Node 组件（在分布式解决方案或多租户模式下使用）升级至 7.0 版本后 Embedded Sensor 组件出现的错误。
5. 现在，当部署集群时，您可以选择 NDR 功能的本地化语言。

Kaspersky Anti Targeted Attack Platform 7.0 目前具有以下新功能：

1. 现在，您可以在分布式解决方案和多租户模式下将最多 150 台 SCN 服务器连接到单个 PCN 服务器。
2. 现在您可以在以下虚拟化系统中部署应用程序：“Brest”虚拟化软件、“RED Virtualization”、zVirt Node。

3. 现在，您可以使用自定义操作系统镜像中的以下本地化版本，而不会影响对象扫描质量：中文（简体）、阿拉伯语和西班牙语（墨西哥）。

4. 现在，您可以从以 Endpoint Agent 组件角色使用 Kaspersky Endpoint Security for Windows 和 Kaspersky Endpoint Security for Linux 的主机手动发送文件以在 Sandbox 中进行扫描。

5. 现在，您可以使用 Sigma 规则根据 YAML 文件中的事件搜索条件创建 TAA (IOA) 规则。

6. **威胁搜索**部分中，可用于在源代码模式下进行事件搜索的扩展字段列表。

7. Kaspersky Endpoint Security for Windows 12.7 的 Endpoint Agent 的扩展功能：

   - 支持的新事件类型：**代码注入**、**命名管道**、WMI、LDAP、DNS、**进程访问**。
   - **文件已修改**事件的新子类型：**文件读取**、**已创建硬链接**、**符号链接已创建**。
   - **注册表已修改**事件的新子类型：**注册表键已重命名**、**注册表键已保存**。
   - **模块已加载**和**到远程主机的连接**事件的新字段。

8. Kaspersky Endpoint Security for Linux 12.2 的 Endpoint Agent 的扩展功能：

   - 新事件类型：**到远程主机的连接**、**监听的端口**、**模块已加载**、DNS、**进程访问**。
   - **文件已修改**事件的新子类型：**文件读取**。
   - 现在您可以隔离一个对象。
   - 现在您可以创建防御规则。

9. 现在您可以强制更改用户账户密码。

10. 现在支持对从电子邮件中的 URL 下载的加密存档进行扫描。

11. 现在您可以将响应操作应用于多个设备。

12. 扩展的 NDR 功能：

    - 现在您可以查看网络流量中的事件。
    - 警报表现在显示外部分析警报。
    - 添加了组织本地网络上的设备清单。
    - 现在您可以查看以下设备信息：
      - 在设备操作系统中注册的用户账户。
      - 设备上的文件执行情况。
      - 设备的地址空间。
    - 现在您可以显示与设备相关的风险。
    - 现在支持设备的动态 IP 寻址。

- 现在您可以在网络地图上监控设备的网络活动。
- 现在可以主动轮询设备以丰富设备列表中的信息并构建网络拓扑图。
- 增加了分析网络会话的功能。
- 现在您可以识别网络会话中使用的传输协议的名称。
- 现在您可以识别网络会话中使用的应用层协议的名称。
- 现在您可以在流量存储中通过网络数据包查找会话，以及将单个网络数据包和会话的数据下载到文件中。
- 报告的新类型。

13. 更新了管理自定义 IDS 规则的逻辑。

14. 现在 Central Node 和 Sensor 组件之间的交互使用不同的端口：
    - 对于 Central Node 服务器，必须允许到 TCP 端口 13520 和 7423 的入站连接。
    - 对于 Sensor 服务器，必须允许到 TCP 端口 13520 和 7423 的出站连接以及到 TCP 端口 9443 的入站连接。
    - 在分布式解决方案和多租户模式下，必须在 PCN 和 SCN 服务器上启用 TCP 端口 11000:11006 的入站和出站连接。

Kaspersky Endpoint Agent 3.16 for Windows 中的更改：

您可以在 Kaspersky Endpoint Agent for Windows 在线帮助 中查看 Kaspersky Endpoint Agent 3.16 for Windows 中的更改列表。

Kaspersky Endpoint Security 12.7 for Windows 中的更改：

您可以在 Kaspersky Endpoint Security for Windows 在线帮助 中查看 Kaspersky Endpoint Security 12.7 for Windows 中的更改列表。

Kaspersky Endpoint Security 12.2 for Linux 中的更改：

您可以在 Kaspersky Endpoint Security for Linux 在线帮助 中查看 Kaspersky Endpoint Security 12 for Linux 中的更改列表。

使用 Kaspersky Threat Intelligence Portal

有关您认为可疑的文件的其他信息，您可以访问卡巴斯基应用程序 Kaspersky Threat Intelligence 门户网站，该门户网站会分析每个文件以查找恶意代码，并显示文件信誉的相关信息。

Kaspersky Threat Intelligence 应用程序的访问权限付费提供。应用程序网站上的授权要求将应用程序访问证书安装在您计算机上的证书储存中。另外，您必须拥有用于访问应用程序的用户名和密码。

有关 Kaspersky Threat Intelligence Portal 的更多详细信息，请访问卡巴斯基网站。

分发包

Kaspersky Anti Targeted Attack Platform 分发包包含以下文件：

1. 磁盘镜像（带 iso 扩展名的文件），其中包括 Ubuntu® Server 22.04 操作系统以及 Sensor、Central Node 和 Sandbox 组件的安装文件。
2. Sensor、Central Node 组件的存档（.tar.gz 文件），用于基于 Astra Linux Special Edition 1.7.5 创建 iso 镜像。
3. 用于创建基于 Astra Linux Special Edition 1.7.5 的 iso 镜像的 Sandbox 组件的存档（.tar.gz 文件）。
4. Sandbox 组件在其中运行文件的操作系统的磁盘镜像（.iso 文件）。
5. 用于创建基于 Astra Linux Special Edition 1.7.5 的 iso 镜像的实用程序（.tar 文件）。
6. 基于 Ubuntu 和 Astra Linux 操作系统的 Central Node 组件的更新包。
7. 关于 Kaspersky Anti Targeted Attack Platform 中使用的第三方代码的信息文件。

Kaspersky Endpoint Agent 分发包包含以下文件：

Kaspersky Endpoint Agent 分发包

文件	描述
agent\endpointagent.msi	Kaspersky Endpoint Agent 安装包。
agent\endpointagent.kud	用于使用 Kaspersky Security Center 创建Kaspersky Endpoint Agent 安装包的文件。
agent\klcfginst.msi	Kaspersky Security Center 的 Kaspersky Endpoint Agent Management 管理插件的安装包。
agent\kpd.loc\en-us.ini	使用 Kaspersky Security Center 创建英文版Kaspersky Endpoint Agent 安装包所需的配置文件。
agent\kpd.loc\ru-ru.ini	使用 Kaspersky Security Center 创建俄语版Kaspersky Endpoint Agent 安装包所需的配置文件。
agent\en-us\ksn.txt	包含卡巴斯基安全网络参与条款文本的英语文件。
agent\en-us\license.txt	包含最终用户授权许可协议和隐私政策文本的英语文件。
agent\en-us\release_notes.txt	包含 Kaspersky Endpoint Agent 发行说明文本的英语文件。
agent\ru-ru\ksn.txt	包含卡巴斯基安全网络参与条款文本的俄语文件。

文件	描述
agent\ru-ru\license.txt	包含最终用户授权许可协议和隐私政策文本的俄语文件。
agent\ru-ru\release_notes.txt	包含 Kaspersky Endpoint Agent 发行说明文本的俄语文件。

硬件和软件要求

安装 Kaspersky Anti Targeted Attack Platform 的虚拟平台的软件要求

您可以在以下虚拟平台上部署该应用程序：

- VMware ESXi™ 6.7.0 或 7.0
- “Brest” 3.3 虚拟化软件
- “RED Virtualization” 7.3
- zVirt Node 4.2

在 VMware ESXI 虚拟平台上部署应用程序时，必须安装 Hypervisor 的当前更新包。

如果您想在 VMware ESXI Hypervisor 中的 Astra Linux 操作系统上部署应用程序，则需要确保您使用的服务器硬件与 Astra Linux 操作系统兼容。有关受支持的服务器硬件的完整列表，请参阅 Astra Linux 开发者网站。

在 “Brest”、zVirt Node 和 “RED Virtualization” 虚拟平台上部署应用程序时，存在以下限制：

- 如果要在 “Brest” 虚拟平台、zVirt Node 或 “RED Virtualization” 上使用 Sandbox 组件，还必须额外配置使用该组件扫描对象的时间，以增加检测的概率。要配置它，请联系技术支持。
- zVirt Node 或 “RED Virtualization” 虚拟平台不支持该应用程序的高可用性部署。

有关 Central Node、Sensor 和 Sandbox 硬件要求，请参阅大小调整指南。

安装 Endpoint Agent 组件的硬件和软件要求

Endpoint Agent 组件的硬件和软件要求反映了充当Endpoint Agent 组件的应用程序的硬件和软件要求，并在这些应用程序的文档中进行了描述：

- Kaspersky Endpoint Agent for Windows。
- Kaspersky Endpoint Security for Windows。
- Kaspersky Endpoint Security for Linux。
- Kaspersky Endpoint Security for Mac。

使用 Kaspersky Anti Targeted Attack Platform 网页界面的硬件和软件要求

必须在计算机上安装以下浏览器之一，才能使用 Web 界面配置和管理该应用程序：

- Mozilla™ Firefox™ for Linux。
- Mozilla Firefox for Windows。
- Google™ Chrome™ for Windows。
- Google Chrome for Linux。
- Edge (Windows)。
- Safari (Mac)。

使用 Web 界面的最低屏幕分辨率：1366x768。

Kaspersky Endpoint Agent for Windows 版本与 Kaspersky Anti Targeted Attack Platform 版本的兼容性

Kaspersky Endpoint Agent 应用程序使用预定义设置，确定在信息检索和与 Central Node 组件交互的情景下对本地计算机性能的影响。

如果 Central Node 服务器上安装的 Kaspersky Anti Targeted Attack Platform 的版本与公司 LAN 计算机上安装的 Kaspersky Endpoint Agent 的版本不兼容，Kaspersky Anti Targeted Attack Platform 的功能可能会受到限制。

下表列出了有关 Kaspersky Endpoint Agent 组件版本与 Kaspersky Anti Targeted Attack Platform 版本的兼容性信息。

Kaspersky Endpoint Agent for Windows 版本与 Kaspersky Anti Targeted Attack Platform 版本的兼容性

Kaspersky Endpoint Agent 的版本	类型 Kaspersky Endpoint Agent	兼容 KATA 4.0	兼容 KATA 4.1	兼容 KATA 5.0	兼容 KATA 5.1	兼容 KATA 6.0	兼容 KATA 6.1	兼容 KATA 7.0
Endpoint Agent 3.12	独立安装	是	有限制	有限制	有限制	有限制	有限制	有限制
Endpoint Agent 3.13	独立安装	有限制	是	有限制	有限制	有限制	有限制	有限制
Endpoint Agent 3.14	独立安装	有限制	有限制	是	是	是	有限制	有限制
Endpoint Agent 3.15	独立安装	否	否	是	是	是	有限制	有限制
Endpoint Agent 3.16	独立安装	否	否	否	否	是	是	有限制
Endpoint Agent 4.0	独立安装	否	否	否	否	否	是	有限制

Kaspersky Endpoint Agent for Windows 版本与 Kaspersky Anti Targeted Attack Platform 版本有限的兼容性

- Kaspersky Endpoint Agent 3.12 与 Kaspersky Anti Targeted Attack Platform 4.1 的集成。

  Kaspersky Endpoint Agent 发送的数据范围有限：

  - 使用**启动 YARA 扫描**任务扫描自动运行点不受支持。
  - 任务**获取 NTFS 图元文件**、**获取进程内存转储**、**获取注册表键**不受支持。

- Kaspersky Endpoint Agent 3.12 与 Kaspersky Anti Targeted Attack Platform 5.0–6.1 的集成。

  Kaspersky Endpoint Agent 发送的数据范围有限：

  - 使用**启动 YARA 扫描**任务扫描自动运行点不受支持。
  - 以下任务不受支持：**获取 NTFS 图元文件**、**获取进程内存转储**、**获取注册表键**、**获取磁盘镜像**、**获取内存转储**。
  - “**进程已终止**”事件的信息未传输。

- Kaspersky Endpoint Agent 3.12 与 Kaspersky Anti Targeted Attack Platform 7.0 的集成。

  Kaspersky Endpoint Agent 发送的数据范围有限：

  - 使用**启动 YARA 扫描**任务扫描自动运行点不受支持。
  - 以下任务不受支持：**获取 NTFS 图元文件**、**获取进程内存转储**、**获取注册表键**、**获取磁盘镜像**、**获取内存转储**。
  - 不会传输有关以下事件的信息：**进程已终止**、**命名管道**、**WMI**、**LDAP**、**DNS**、**进程访问**。
  - 对于“**文件已修改**”事件，不会传输有关以下子类型的信息：**文件读取**、**已创建硬链接**、**符号链接已创建**。
  - 对于“**注册表已修改**”事件，不会传输有关以下子类型的信息：**注册表键已重命名**、**注册表键已保存**。

- Kaspersky Endpoint Agent 3.13 与 Kaspersky Anti Targeted Attack Platform 4.0 的集成。

  此 Kaspersky Anti Targeted Attack Platform 版本的服务器可以从 Kaspersky Endpoint Agent 应用程序接收有限范围的数据：“**获取 NTFS 图元文件**”、“**获取进程内存转储**”和“**获取注册表键**”任务无法在应用程序的 Web 界面中创建。

- Kaspersky Endpoint Agent 3.13 与 Kaspersky Anti Targeted Attack Platform 4.1–6.1 的集成。

  Kaspersky Endpoint Agent 不支持创建以下任务：“**获取磁盘镜像**”、“**获取内存转储**”。

- Kaspersky Endpoint Agent 3.14 与 Kaspersky Anti Targeted Attack Platform 4.0 的集成。

  此 Kaspersky Anti Targeted Attack Platform 版本的服务器可以从 Kaspersky Endpoint Agent 应用程序接收有限范围的数据：创建**获取 NTFS 图元文件**、**获取进程内存转储**、**获取注册表键**、**获取磁盘镜像**、**获取内存转储**任务在应用程序的 Web 界面中不可用。

- Kaspersky Endpoint Agent 3.14 与 Kaspersky Anti Targeted Attack Platform 4.1 的集成。

  此 Kaspersky Anti Targeted Attack Platform 版本的服务器可以从 Kaspersky Endpoint Agent 应用程序接收有限范围的数据：任务“**获取磁盘镜像**”和“**获取内存转储**”无法在应用程序的 Web 界面中创建。

- Kaspersky Endpoint Agent 3.12–4.0 与 Kaspersky Anti Targeted Attack Platform 7.0 的集成。
  Kaspersky Endpoint Agent 发送的数据范围有限：
  - 不会传输有关以下事件的信息：**命名管道**、**WMI**、**LDAP**、**DNS**、**进程访问**。
  - 对于"**文件已修改**"事件，不会传输有关以下子类型的信息：**文件读取**、**已创建硬链接**、**符号链接已创建**。
  - 对于"**注册表已修改**"事件，不会传输有关以下子类型的信息：**注册表键已重命名**、**注册表键已保存**。

Kaspersky Endpoint Agent for Windows 版本与 EPP 应用程序的兼容性

如果您想使用 Kaspersky Endpoint Agent 应用程序作为Endpoint Agent 组件，您可以仅安装 Kaspersky Endpoint Agent，或者配置 Kaspersky Endpoint Agent 与工作站保护应用程序（Endpoint Protection Platform，以下也称为"EPP"）、Kaspersky Endpoint Security for Windows、Kaspersky Security for Windows Server 和 Kaspersky Security for Virtualization Light Agent 的集成。如果配置了应用程序集成， Kaspersky Endpoint Agent 还会将 EPP 应用程序检测到的威胁信息及其处理结果发送到 Central Node 服务器。

当 Kaspersky Endpoint Agent 安装在虚拟桌面基础架构中的虚拟桌面上时，上述集成方案不起作用。

Kaspersky Endpoint Agent 与 Kaspersky Endpoint Security for Windows 和 Kaspersky Security for Windows Server 集成需要将 Kaspersky Endpoint Agent 作为这些应用程序的一部分进行安装。

Kaspersky Endpoint Agent for Windows 与 Kaspersky Security for Windows Server 版本的兼容性

您可以安装以下版本的 Kaspersky Endpoint Agent 作为 Kaspersky Security for Windows Server 的一部分：

- Kaspersky Endpoint Agent 3.12 作为 Kaspersky Security 11 for Windows Server 的一部分。
- Kaspersky Endpoint Agent 3.10 作为 Kaspersky Security 11.0.1 for Windows Server 的一部分。

当您将 Kaspersky Endpoint Agent 作为 Kaspersky Security for Windows Server 的一部分安装时，相同或早期版本的独立 Kaspersky Endpoint Agent 将被删除。如果作为 Kaspersky Security for Windows Server 的一部分安装的 Kaspersky Endpoint Agent 具有早期版本，则不会安装它。在这种情况下，您必须首先删除独立的 Kaspersky Endpoint Agent 应用程序。

如有必要，您可以升级 Kaspersky Endpoint Agent 应用程序，它已作为 Kaspersky Security for Windows Server 的一部分安装。当 Kaspersky Endpoint Agent 升级和 Kaspersky Security for Windows Server 升级时，应用程序的兼容版本之间的集成都会得到维护。

下表列出了有关 Kaspersky Endpoint Agent 版本与 Kaspersky Security for Windows Server 版本的兼容性的信息。

Kaspersky Endpoint Agent 版本与 Kaspersky Security for Windows Server 版本的兼容性

Kaspersky Security for Windows Server 版本	与 Endpoint Agent 3.8、3.9、3.10 的兼容性	与 Endpoint Agent 3.11、3.12 的兼容性	与 Endpoint Agent 3.13、3.14、3.15、3.16 的兼容性
• KSWS 10.1.2	是	否	否
• KSWS 11	是	是	否
• KSWS 11.0.1	否	是	有限制

与 Kaspersky Endpoint Agent 3.13–3.16 集成时， Kaspersky Security for Windows Server 不会传输“**AMSI 扫描**”事件的信息。

有关安装 Kaspersky Security for Windows Server 的更多详细信息，请参阅 Kaspersky Security for Windows Server 帮助。

Kaspersky Endpoint Agent for Windows 与 Kaspersky Endpoint Security for Windows 版本的兼容性

您可以将以下版本的 Kaspersky Endpoint Agent（Endpoint Sensors）作为 Kaspersky Endpoint Security for Windows 的一部分安装：

- Kaspersky Endpoint Agent 3.7 或 Kaspersky Endpoint Agent (Endpoint Sensors) 3.6.1 作为 Kaspersky Endpoint Security 11.2、11.3 for Windows 的一部分。

  Kaspersky Endpoint Agent（Endpoint Sensors）3.6.1 与 Kaspersky Anti Targeted Attack Platform 版本 4.1 或更高版本不兼容。

  Kaspersky Endpoint Agent 3.7 并非与所有版本的 Kaspersky Anti Targeted Attack Platform 兼容。

- Kaspersky Endpoint Agent 3.12 作为 Kaspersky Endpoint Security 11.4、11.5 的一部分。
- Kaspersky Endpoint Agent 3.10 作为 Kaspersky Endpoint Security 11.6 的一部分。
- Kaspersky Endpoint Agent 3.11 作为 Kaspersky Endpoint Security 11.7、11.8 的一部分。

当您将 Kaspersky Endpoint Agent 3.10 或更高版本作为 Kaspersky Endpoint Security for Windows 的一部分进行安装时，相同或早期版本的独立 Kaspersky Endpoint Agent 应用程序将被删除。如果单独安装的 Kaspersky Endpoint Agent 具有更高版本，则不会安装与 Kaspersky Endpoint Security for Windows 捆绑的应用程序。在这种情况下，您必须首先删除独立的 Kaspersky Endpoint Agent 应用程序。

如有必要，您可以升级已作为 Kaspersky Endpoint Security for Windows 的一部分安装的Kaspersky Endpoint Agent 应用程序。当 Kaspersky Endpoint Agent 升级和 Kaspersky Endpoint Security for Windows 升级时，应用程序兼容版本之间的集成都会得到维护。您只能为 Kaspersky Endpoint Agent 3.7 或更高版本将以前版本的 Kaspersky Endpoint Agent 升级至版本 3.14。

下表列出了有关 Kaspersky Endpoint Agent 版本与 Kaspersky Endpoint Security for Windows 版本的兼容性信息。

Kaspersky Endpoint Agent 版本与 Kaspersky Endpoint Security for Windows 版本的兼容性

Kaspersky Endpoint Security 版本	与 Endpoint Agent 3.8、3.9 的兼容性	与 Endpoint Agent 3.10、3.12 的兼容性	与 Endpoint Agent 3.11 的兼容性	与 Endpoint Agent 3.13、3.14、3.15、3.16 的兼容性
• KES 10 SP2 MR2	否	否	否	否
• KES 10 SP2 MR3/MR4	是	否	否	否
• KES 11.0.0	否	否	否	否
• KES 11.0.1	是	否	否	否
• KES 11.1 • KES 11.1.1	是	是	否	否
• KES 11.2 • KES 11.3	是	是	是	否
• KES 11.4 • KES 11.5	是	是	是	否
• KES 11.6 • KES 11.7 • KES 11.8	是	是	是	是
• KES 版本 12.1 或更高版本	否	否	否	否

有关安装 Kaspersky Endpoint Security 的更多详细信息，请参阅 Kaspersky Endpoint Security for Windows 帮助。

Kaspersky Endpoint Agent 与 Kaspersky Security for Virtualization Light Agent 版本的兼容性

您可以配置单独安装的 Kaspersky Endpoint Agent 和 Kaspersky Security for Virtualization Light Agent 的集成。

下表列出了有关 Kaspersky Endpoint Agent 版本与 Kaspersky Security for Virtualization Light Agent 版本的兼容性信息。

Kaspersky Endpoint Agent 版本和 Kaspersky Security for Virtualization Light Agent 版本的兼容性

Kaspersky Security for Virtualization Light Agent 版本	与 Endpoint Agent 3.8、3.9、3.10 的兼容性	与 Endpoint Agent 3.12 的兼容性	与 Endpoint Agent 3.11、3.13、3.14 的兼容性	与 Endpoint Agent 3.15 的兼容性	与 Endpoint Agent 3.16 的兼容性
• KSV 5.1 LA	是	是	否	否	否
• KSV 5.1.1 LA	是	否	否	否	否
• KSV 5.2 LA	否	是	是	是	是
• KSV 6.0 LA	否	是	是	是	否

安装在虚拟机上的 Kaspersky Endpoint Agent 和 Kaspersky Security for Virtualization Light Agent 在 Central Node 服务器上生成的负载与安装在主机上的 Kaspersky Endpoint Agent 和 Kaspersky Security for Virtualization Light Agent 生成的负载相同。

有关启用 Kaspersky Endpoint Agent 与 Kaspersky Security for Virtualization Light Agent集成的更多详细信息，请参阅 Kaspersky Security for Virtualization Light Agent 帮助。

Kaspersky Endpoint Agent 与 Kaspersky Industrial CyberSecurity for Nodes 版本的兼容性

您可以在安装了 Kaspersky Industrial CyberSecurity for Nodes 的设备上安装 Kaspersky Endpoint Agent。应用程序会自动集成。

Kaspersky Endpoint Agent 版本与 Kaspersky Industrial CyberSecurity for Nodes 版本的兼容性

Kaspersky Industrial CyberSecurity for Nodes 版本	与 Endpoint Agent 3.11、3.12 的兼容性	与 Endpoint Agent 3.13、3.14、3.15 的兼容性	与 Endpoint Agent 3.16 的兼容性
• KICS for Nodes 3.0	是	是	是
• KICS for Nodes 3.1	否	是	是
• KICS for Nodes 3.2	否	否	是

要与 Kaspersky Industrial CyberSecurity for Nodes 集成，必须在 Kaspersky Endpoint Agent中安装相应的授权许可密钥。

如需详细信息，请联系客户经理。

Kaspersky Endpoint Security for Windows 版本与 Kaspersky Anti Targeted Attack Platform 版本的兼容性

您可以使用 Kaspersky Endpoint Security 作为 Endpoint Agent 组件。

下表列出了有关 Kaspersky Endpoint Security 版本与 Kaspersky Anti Targeted Attack Platform 版本的兼容性信息。

Kaspersky Endpoint Security for Windows 版本与 Kaspersky Anti Targeted Attack Platform 版本的兼容性

Kaspersky Endpoint Security 版本	兼容 KATA 4.0	兼容 KATA 4.1	兼容 KATA 5.0	兼容 KATA 5.1	兼容 KATA 6.0	兼容 KATA 6.1	兼容 KATA 7.0
Kaspersky Endpoint Security 12.1、12.2	否	是	是	是	是	否	有限制
Kaspersky Endpoint Security 12.3、12.4	否	是	是	是	是	是	有限制
Kaspersky Endpoint Security 12.5、12.6	否	否	是	是	是	是	有限制
Kaspersky Endpoint Security 12.7	否	否	有限制	有限制	有限制	有限制	是
Kaspersky Endpoint Security 12.8、12.9	否	否	有限制	有限制	有限制	有限制	有限制

要将 Kaspersky Endpoint Security 12.1 或更高版本与 Kaspersky Anti Targeted Attack Platform 集成，您无需安装 Kaspersky Endpoint Agent。

从版本 12.8 开始，Kaspersky Endpoint Security for Windows 可用作 Kaspersky Security for Virtualization 应用程序的 Light Agent for Windows 组件。有关集成的更多详细信息，请参阅 Kaspersky Security for Virtualization Light Agent 帮助。

Kaspersky Endpoint Security for Windows 版本与 Kaspersky Anti Targeted Attack Platform 版本有限的兼容性

- Kaspersky Endpoint Security 12.1–12.6 与 Kaspersky Anti Targeted Attack Platform 7.0 的集成。

  Kaspersky Endpoint Security 发送的数据范围有限：

  - 不会传输有关以下事件的信息：**DNS**、**代码注入**、**命名管道**、**WMI**、**LDAP**。
  - 对于"**文件已修改**"事件，不会处理有关以下子类型的信息：**文件读取**、**已创建硬链接**、**符号链接已创建**。
  - 对于"**注册表已修改**"事件，不会处理有关以下子类型的信息：**注册表键已重命名**、**注册表键已保存**。
  - "**模块已加载**"和"**到远程主机的连接**"事件的新字段不可用。

- Kaspersky Endpoint Security 12.7 与 Kaspersky Anti Targeted Attack Platform 5.0–6.1 的集成。

  这些 Kaspersky Anti Targeted Attack Platform 版本的服务器可以从 Kaspersky Endpoint Security 应用程序接收有限范围的数据：

  - 不会处理有关以下事件的信息：**命名管道**、**WMI**、**LDAP**、**DNS**、**代码注入**。
  - 对于"**文件已修改**"事件，不会处理有关以下子类型的信息：**文件读取**、**已创建硬链接**、**符号链接已创建**。
  - 对于"**注册表已修改**"事件，不会处理有关以下子类型的信息：**注册表键已重命名**、**注册表键已保存**。
  - "**模块已加载**"和"**到远程主机的连接**"事件的新字段不可用。

- Kaspersky Endpoint Security 12.8–12.9 与 Kaspersky Anti Targeted Attack Platform 5.0–6.1 的集成。

  这些 Kaspersky Anti Targeted Attack Platform 版本的服务器可以从 Kaspersky Endpoint Security 应用程序接收有限范围的数据：

  - 不会处理有关以下事件的信息：**命名管道**、**WMI**、**LDAP**、**DNS**、**代码注入**、**USB 设备**。
  - 对于"**文件已修改**"事件，不会处理有关以下子类型的信息：**文件读取**、**已创建硬链接**、**符号链接已创建**。
  - 对于"**注册表已修改**"事件，不会处理有关以下子类型的信息：**注册表键已重命名**、**注册表键已保存**。
  - "**模块已加载**"和"**到远程主机的连接**"事件的新字段不可用。

- Kaspersky Endpoint Security 12.8–12.9 与 Kaspersky Anti Targeted Attack Platform 7.0 的集成。

  此版本的 Kaspersky Anti Targeted Attack Platform 的服务器不处理"**USB 设备**"事件。

Kaspersky Endpoint Security for Linux 版本与 Kaspersky Anti Targeted Attack Platform 版本的兼容性

您可以使用 Kaspersky Endpoint Security 作为 Endpoint Agent 组件。

下表列出了有关 Kaspersky Endpoint Security 版本与 Kaspersky Anti Targeted Attack Platform 版本的兼容性信息。

Kaspersky Endpoint Security for Linux 版本与 Kaspersky Anti Targeted Attack Platform 版本的兼容性

Kaspersky Endpoint Security 版本	兼容 KATA 4.0	兼容 KATA 4.1	兼容 KATA 5.0	兼容 KATA 5.1	兼容 KATA 6.0	兼容 KATA 6.1	兼容 KATA 7.0
Kaspersky Endpoint Security 11.4	否	否	否	有限制	有限制	有限制	有限制
Kaspersky Endpoint Security 12	否	否	有限制	有限制	有限制	有限制	有限制
Kaspersky Endpoint Security 12.1	否	否	否	有限制	有限制	有限制	有限制
Kaspersky Endpoint Security 12.2、12.3	否	否	否	否	有限制	有限制	有限制

要将 Kaspersky Endpoint Security 与 Kaspersky Anti Targeted Attack Platform 集成，您无需安装 Kaspersky Endpoint Agent。

从版本 12 开始，Kaspersky Endpoint Security for Linux 可用作 Kaspersky Security for Virtualization 应用程序的 Light Agent for Linux 组件。有关集成的更多详细信息，请参阅 Kaspersky Security for Virtualization Light Agent 帮助。

当 Kaspersky Endpoint Security for Linux 被用作 Light Agent for Linux 组件时，Kaspersky Endpoint Security for Linux 与 Kaspersky Anti Targeted Attack Platform 的集成将被保留。

Kaspersky Endpoint Security for Linux 版本与 Kaspersky Anti Targeted Attack Platform 版本有限的兼容性

- Kaspersky Endpoint Security 11.4 与 Kaspersky Anti Targeted Attack Platform 5.1、6.1 的集成。
  Kaspersky Endpoint Security 发送的数据范围有限：
  - 不支持创建网络隔离规则。
  - 不支持创建防护规则。
  - 使用 IOC 文件搜索计算机上的入侵指标不受支持。
  - 仅传输以下类型的事件：**进程已启动**、**文件已更改**、**系统事件日志**、**检测**、**检测处理结果**。
  - 仅可使用以下任务：**获取文件**、**运行应用程序**。
- Kaspersky Endpoint Security 12、12.1 与 Kaspersky Anti Targeted Attack Platform 5.1 的集成。
  Kaspersky Endpoint Security 发送的数据范围有限：
  - 不支持创建防止规则。
  - 仅传输以下类型的事件：**进程已启动**、**文件已更改**、**系统事件日志**、**检测**、**检测处理结果**。
  - 仅可使用以下任务：**获取文件**、**运行应用程序**、**删除文件**、**杀死进程**。
- Kaspersky Endpoint Security 12、12.1 与 Kaspersky Anti Targeted Attack Platform 6.0–7.0 的集成。

Kaspersky Endpoint Security 发送的数据范围有限：

- 仅传输以下类型的事件：**进程已终止**、**阻止的应用程序 (防止规则)**、**文件已阻止**。
- 仅可使用以下任务：**获取文件**、**运行应用程序**、**删除文件**、**杀死进程**。

- Kaspersky Endpoint Security 12.2、12.3 与 Kaspersky Anti Targeted Attack Platform 6.0、6.1 的集成。
  Kaspersky Endpoint Security 发送的数据范围有限：
  - 仅传输以下类型的事件：**进程已终止**、**阻止的应用程序 (防止规则)**、**文件已阻止**。
  - 仅可使用以下任务：**获取文件**、**运行应用程序**、**删除文件**、**杀死进程**、**隔离文件**、**从隔离区恢复文件**。
- Kaspersky Endpoint Security 12.2、12.3 与 Kaspersky Anti Targeted Attack Platform 7.0 的集成。
  Kaspersky Endpoint Security 发送的数据范围有限：
  - 仅传输以下类型的事件：**进程已终止**、**阻止的应用程序 (防止规则)**、**文件已阻止**、**代码注入**、DNS。
  - 仅可使用以下任务：**获取文件**、**运行应用程序**、**删除文件**、**杀死进程**、**隔离文件**、**从隔离区恢复文件**。

Kaspersky Endpoint Security for Mac 与 Kaspersky Anti Targeted Attack Platform 版本的兼容性

您可以使用 Kaspersky Endpoint Security for Mac作为Endpoint Agent 组件。

下表列出了有关 Kaspersky Endpoint Security for Mac 版本与 Kaspersky Anti Targeted Attack Platform 版本的兼容性信息。

Kaspersky Endpoint Security for Mac 与 Kaspersky Anti Targeted Attack Platform 版本的兼容性

Kaspersky Endpoint Security 版本	兼容 KATA 4.0	兼容 KATA 4.1	兼容 KATA 5.0	兼容 KATA 5.1	兼容 KATA 6.0	兼容 KATA 6.1	兼容 KATA 7.0
Kaspersky Endpoint Security 12、12.1、12.2	否	否	否	否	有限制	有限制	有限制

Kaspersky Endpoint Security for Mac 版本与 Kaspersky Anti Targeted Attack Platform 版本有限的兼容性

- Kaspersky Endpoint Security 12、12.1、12.2 与 Kaspersky Anti Targeted Attack Platform 6.0–7.0 的集成。
  - 不支持创建网络隔离规则。
  - 不支持创建防护规则。
  - 使用 IOC 文件搜索计算机上的入侵指标不受支持。
  - 仅传输以下类型的事件：**进程已启动**、**进程已终止**、**文件已更改**、**检测**、**检测处理结果**。
  - 仅可使用以下任务：**获取文件**、**运行应用程序**。

KUMA 版本与 Kaspersky Anti Targeted Attack Platform 版本的兼容性

您可以使用 KUMA 作为 SIEM 系统。

下表列出了 KUMA 版本与 Kaspersky Anti Targeted Attack Platform 版本的兼容性信息。

KUMA 版本与 Kaspersky Anti Targeted Attack Platform 版本的兼容性

KUMA 版本	兼容 KATA 4.1	兼容 KATA 5.0	兼容 KATA 5.1	兼容 KATA 6.0	兼容 KATA 6.1	兼容 KATA 7.0
KUMA 2.0	是	是	否	否	否	否
KUMA 2.1	否	是	是	是	否	否
KUMA 3.0.2	否	否	否	是	是	否
KUMA 3.0.3	否	否	否	是	是	否
KUMA 3.2	否	否	否	是	是	否
KUMA 3.3	否	否	否	否	否	是
KUMA 3.4	否	否	否	否	否	是

XDR 版本与 Kaspersky Anti Targeted Attack Platform 版本的兼容性

您可以使用 XDR 作为 SIEM 系统。

下表列出了有关 XDR 版本与 Kaspersky Anti Targeted Attack Platform 版本的兼容性信息。

XDR 版本与 Kaspersky Anti Targeted Attack Platform 版本的兼容性

XDR 版本	兼容 KATA 4.1	兼容 KATA 5.0	兼容 KATA 5.1	兼容 KATA 6.0	兼容 KATA 6.1	兼容 KATA 7.0
XDR 1.0	否	否	是	否	否	否
XDR 1.1	否	否	否	是	是	否
XDR 1.2	否	否	否	否	否	是

KPSN 版本与 Kaspersky Anti Targeted Attack Platform 版本的兼容性

您可以使用卡巴斯基私人安全网络 (KPSN) 而不是卡巴斯基安全网络 (KSN)，以避免将组织的数据发送到公司 LAN 之外。

下表列出了 KPSN 版本与 Kaspersky Anti Targeted Attack Platform 版本的兼容性信息。

KPSN 版本与 Kaspersky Anti Targeted Attack Platform 版本的兼容性

KPSN 版本	兼容 KATA 4.1	兼容 KATA 5.0	兼容 KATA 5.1	兼容 KATA 6.0	兼容 KATA 6.1	兼容 KATA 7.0
KPSN 3.3	是	是	是	是	是	否
KPSN 3.4	否	否	否	是	是	是
KPSN 4.0	否	否	否	否	是	是

Kaspersky Anti Targeted Attack Platform 与 VK 云的兼容性

您可以在 VK Cloud 公有云中创建的虚拟机上部署 Kaspersky Anti Targeted Attack Platform，配置为：一个 Central Node 组件（以单一角色运行），连接一个或多个 KSMG 邮件 Sensor 以及多个沙盒。

在 VK Cloud 公有云中创建的虚拟机上部署 Kaspersky Anti Targeted Attack Platform 时，需遵守以下限制：

- Central Node 必须以单一角色安装在服务器上。
- 仅支持基于 Astra Linux 的应用程序的认证版本。
- 支持安装 KATA 或 KATA+NDR 许可证密钥。
- 仅支持接收和处理来自安装在 VK Cloud 外部的 KSMG 的消息的场景。其他场景不受支持。

为了使 Sandbox 组件正常工作，必须满足以下要求：

- 必须为虚拟机启用嵌套虚拟化。
- 必须正确配置网络接口设置，以便为正在被处理的对象提供 Internet 访问。

  > 仅当可访问互联网的网络接口配置正确时，才能激活 Windows 镜像。

- 用于对已处理对象进行 Internet 访问的网络接口必须与组织的本地网络隔离。
- 处理对象用于访问 Internet 的网络接口必须连接到与控制接口所连接的子网不同的子网。
- 我们建议使用外部防火墙规则，限制处理对象用于访问互联网的网络接口上的入站连接。

限制

Kaspersky Anti Targeted Attack Platform 7.0.3 具有以下已知限制：

1. 不支持依赖系统监控 (Sysmon) 和 Windows 事件日志以外的数据源的 Sigma 规则。
2. 不支持相关 Sigma 规则。
3. 作为与 NDR 功能块集成的一部分，最多 1000 个 Endpoint Agent 组件可以连接到单个 Central Node 组件。
4. 在根据扫描 Web 流量副本的结果创建的文件警报中，如果用户在具有基本身份验证的代理服务器上进行身份验证，“**用户名称**”字段为空。
5. 有关 Endpoint Agent 组件的信息未显示在“**已处理**”小部件的“**控制板**”上。
6. 升级作为集群部署的 Central Node 后，警报表可能不会显示由 IDS 技术生成的新警报。您可以检查该限制是否适用于您，并在必要时采取措施修复它。关于详细信息，请参见“*将 Kaspersky Anti Targeted Attack Platform 从 7.0.1 版更新至 7.0.3 版*”部分
7. 如果正在升级的组件版本中禁用镜像 SPAN 镜像流量的处理，则从版本 6.1 升级Central Node组件将会失败。为了解决此限制，我们强烈建议按照“*更新作为集群安装的 Central Node*”的步骤 1 和“*升级安装在服务器上的 Central Node*”说明中的步骤 4 进行操作。
8. 在极少数情况下，基于Astra Linux操作系统作为集群部署的Central Node从 7.0.1 版本升级到 7.0.3 版本可能会失败，并出现错误“升级任务 UpdateSizing 失败”。

   解决“任务 UpdateSizing 升级失败”错误

   如果在将基于 Astra Linux 部署为集群的 Central Node 从版本 7.0.1 升级到版本 7.0.3 时收到“任务 UpdateSizing 升级失败”信息，请按照以下步骤操作。

   下面描述的所有步骤都必须在使用 `sudo -i` 命令提升用户权限后在技术支持模式下的服务器上执行。

   要解决“任务 UpdateSizing 升级失败”错误，请执行以下操作：

   1. 登录到 Central Node 集群中的任何一台存储服务器，并检查 Ceph 存储是否正常工作。为此，请执行以下命令：

      ```
      ceph -s | grep health:
      ```

      如果返回以下值，则表示 Ceph 存储健康：

      ```
      health: HEALTH_OK
      ```

      如果该值与“`health: HEALTH_OK`”不同，请联系技术支持。

   2. 找出集群中哪些服务器在 Docker Swarm 中具有“管理员”角色。为此，请在任意集群服务器上运行以下命令：

      ```
      docker node ls
      ```

      显示集群服务器的列表。查看列表中的 `MANAGER STATUS` 列：如果服务器在该列中有 `Leader` 或 `Reachable`，则表示它具有“管理者”角色。

3. 以 Docker Swarm 中的"管理员"角色登录服务器，并使用以下命令重新启动 ZooKeeper 服务：

   ```
   docker service update kata_product_main_1_zookeeper --force
   ```

4. 等待 10 分钟，检查 Kafka 服务的状态：

   a. 运行以下命令：

   ```
   docker service ps kata_product_main_1_schema_registry
   ```

   查看"NODE"列中的值以确定哪个服务器具有 Schema Registry。

   b. 登录到具有 Schema Registry 的服务器并运行以下命令：

   ```
   docker exec -it $(docker ps | grep schema_registry | awk '{ print $1 }') curl http://127.0.0.1:8081/subjects
   ```

   如果您获得包含主题列表的 JSON，则表示 Kafka 服务正在运行。在这种情况下，请转到步骤 6。

5. 如果 Kafka 服务不工作，请使用以下命令重新启动它：

   ```
   docker service update kata_product_main_1_kafka --force
   ```

   此后，再次执行步骤 4。如果此后 Kafka 服务仍然无法正常工作，请联系技术支持。

6. 使用以下命令继续升级：

   ```
   source /opt/upgrade_venv/bin/activate
   ```

   ```
   kata-upgrade params --data-dir /data/upgrade/ --user admin --password '<pass>' --ndr-language '<language>' --current-task-index 15
   ```

   在上面的命令中，将<语言>替换成升级过程开始时选择的语言。可能的值：`English`、`Russian`。

9. 将基于 Astra Linux 操作系统作为集群部署的 Central Node 从 6.1 版升级到 7.0.3 版后，"**威胁搜索**"部分中的遥测搜索可能无法正常工作。

   解决搜索事件数据时发生的"内部错误"

   如果在将基于 Astra Linux 部署为集群的 Central Node 从版本 6.1 升级到版本 7.0.3 后，"**威胁搜索**"部分中的搜索事件数据（遥测）不起作用，请按照以下步骤操作。

   下面描述的所有步骤都必须在使用 `sudo -i` 命令提升用户权限后在技术支持模式下的服务器上执行。

   要解决事件数据搜索错误：

   1. 找出集群中哪些服务器在 Docker Swarm 中具有"管理员"角色。为此，请在任意集群服务器上运行以下命令：

      ```
      docker node ls
      ```

      显示集群服务器的列表。查看列表中的 `MANAGER STATUS` 列：如果服务器在该列中有 `Leader` 或 `Reachable`，则表示它具有"管理者"角色。

   2. 以 Docker Swarm 中的"管理员"角色登录服务器并运行以下命令：

      ```
      docker service ps kata_product_main_1_elasticsearch_data
      ```

      查看 `NODE` 列中的值以确定集群中的哪些服务器正在运行 elasticsearch_data 进程。

   3. 在集群中运行 elasticsearch_data 进程的每台服务器上：

      a. 使用以下命令获取正在运行 elasticsearch_data 进程的容器的 ID：

      ```
      docker ps | grep elasticsearch_data | awk '{ print $1 }')
      ```

b. 使用以下命令检查容器日志：

```
docker logs<container ID> | grep "此节点不健康：由于节点锁损坏导致健康检查失败"
```

c. 如果在服务器日志中发现“此节点不健康：由于节点锁损坏导致健康检查失败”字符串，请运行以下命令终止该进程：

```
docker kill <容器 ID>
```

4. 在应用程序 Web 界面中，转到“**威胁搜索**”部分并在事件数据中执行自定义搜索。如果再次收到“内部错误”错误，请联系技术支持。

10. 在服务器上安装 7.0.3 版本的 Central Node 组件时，Kaspersky Anti Targeted Attack Platform 可能会拒绝通过 SMTP 接收的电子邮件。发送者可能会收到“连接被拒绝”错误。您可以去除这个限制。有关详细信息，请参阅*通过 SMTP 配置与邮件服务器的集成*部分。

11. Sensor 组件只能连接到 Central Node 集群中的一个处理服务器。必须**配置此服务器以从 SPAN 端口接收镜像流量**。

    您可以在安装组件时启用镜像流量的接收。如果您在安装阶段禁用了流量接收：

    1. 通过 SSH 或使用终端进入服务器的任何处理服务器的管理控制台。
    2. 运行以下命令：

       ```
       kata-enable-span
       ```

       将启用从 SPAN 端口接收镜像流量。

12. Kaspersky Anti Targeted Attack Platform 可正确处理通过虚拟接口接收的 ERSPAN 流量，速率高达 2 Gbps。ERSPAN 流量速率较高会导致数据丢失。

Kaspersky Anti Targeted Attack Platform 7.0 具有以下已知限制：

1. 不支持依赖系统监控 (Sysmon) 和 Windows 事件日志以外的数据源的 Sigma 规则。
2. 不支持相关 Sigma 规则。
3. 作为与 NDR 功能块集成的一部分，最多 1000 个 Endpoint Agent 组件可以连接到单个 Central Node 组件。如果您想连接更多组件，请联系技术支持。
4. 如果用户没有等待已经开始的下载过程结束，则下载镜像流量时可能会出现错误。
5. 在搜索最近一小时的网络数据包时，即使系统有更多匹配的记录，也不会显示超过 200 条记录。我们建议优化搜索查询以获得具有更少会话的选择。

   限制不适用于流量转储下载。
6. 对于与邮件服务器集成的集群配置，发送电子邮件消息时可能会出现错误：“451 4.3.0 错误：队列文件写入错误”。有关如何消除限制的信息，请参阅“*通过 SMTP 配置与邮件服务器的集成*”部分。

7. Sensor 组件只能连接到 Central Node 集群中的一个处理服务器。必须**配置此服务器以从 SPAN 端口接收镜像流量**。

   您可以在安装组件时启用镜像流量的接收。如果您在安装阶段禁用了流量接收：

   1. 通过 SSH 或使用终端进入服务器的任何处理服务器的管理控制台。
   2. 运行以下命令：

      ```
      kata-enable-span
      ```

      将启用从 SPAN 端口接收镜像流量。

8. 升级到 7.0 版本后，分布式解决方案或多租户模式中使用的 Central Node 组件可能会丢失嵌入式 Sensor。有关如何消除限制的信息，请参阅“*升级安装在服务器上的 Central Node*”部分。

9. 在根据扫描 Web 流量副本的结果创建的文件警报中，如果用户在具有基本身份验证的代理服务器上进行身份验证，“**用户名称**”字段为空。

10. 如果将安装在独立服务器上的 Sensor 组件用作代理服务器，则 Endpoint Agent 组件和 PCN 之间不会建立连接。

11. **忽略 NIC 规则的 MAC 地址**切换开关对应用程序没有影响。

12. 如果 Endpoint Agent 主机运行的是 Windows Server 2016 或更早版本，则 Endpoint Agent 不会发送有关**代码注入**事件的信息。仅当主机运行 Windows Server 2019 或更高版本时，该组件才会发送有关此事件的信息。

13. Kaspersky Anti Targeted Attack Platform 可正确处理通过虚拟接口接收的 ERSPAN 流量，速率高达 2 Gbps。ERSPAN 流量速率较高会导致数据丢失。

一般限制

1. Central Node 和 Sensor 服务器以及 PCN 和 SCN 之间的链路的每个数据包的有效载荷大小（最大传输单元，MTU）的值为 1500。如果您知道您的 ISP 限制解决方案组件之间链接的 MTU 大小，请联系技术支持。

2. 不支持在命令行上更改 Central Node 服务器的名称。

3. 为了使 Central Node、Sensor、PCN 和 SCN 之间的连接正常工作，必须将安装了组件的服务器放置在同一子网中。不支持网络地址转换 (NAT)。此限制不适用于 Endpoint Agent 组件，这些组件可以位于与 Central Node 子网分离的子网中。

将 Central Node 组件部署为集群时适用的限制：

1. Central Node 集群必须至少包含 4 台服务器：2 台存储服务器和 2 台处理服务器。您可以根据规模调整指南扩展集群以增加被处理的流量或连接的主机数量。

2. 建议将硬件配置相同的服务器添加到集群中。否则，无法保证性能按比例提高。

3. 向集群添加额外服务器不会加快处理扫描队列中已有的对象。

4. 如果托管应用程序的服务器出现故障，应用程序的 Web 界面可能会暂时不可用。

5. 如果处理服务器发生故障，您可能会丢失 ICAP、POP3 和 SMTP 流量数据以及等待处理的电子邮件副本以及与其关联的检测。

6. 如果处理服务器被配置为从 SPAN 端口接收镜像流量，则如果该服务器发生故障的话不会处理 SPAN 流量。

7. 如果其中一台集群服务器发生故障或该服务器与 Endpoint Agent 组件之间的连接暂时丢失，事件数据库中的数据可能会暂时无法同步。

8. 如果集群服务器的配置被更改，来自具有 Endpoint Agent 组件的计算机的流量和事件的处理可能会暂时减慢。

9. 将 Kaspersky Anti Targeted Attack Platform 安装为集群或更新集群配置时，嵌入式 Sensor 可能无法启动。

   在这种情况下，我们建议执行以下操作：

   - 如果 Sensor 未连接，请使用 Web 界面将其移除，然后在技术支持模式下运行 `kata-sensor-tool fix-cluster-sensor` 命令。
   - 如果 Sensor 未运行，请在技术支持模式下运行 `kata-sensor-tool fix-cluster-sensor` 命令。

   过一段时间后，Sensor 应该会出现在 Web 界面中。

10. 通过 SMTP 接收电子邮件可能会出现延迟。为了解决这个问题，我们建议采取以下步骤：

    a. 以技术支持模式连接到 Central Node 或 Sensor。

    b. 使用以下命令为 SMTP 集成启用 `DEBUG` 日志记录级别：

    ```
    console-settings-updater set --merge /kata/configuration/product/preprocessor_smtp
    '{"logging":{"level":{"root":"DEBUG"}}}'
    ```

    c. 等待大约 30 秒以使设置同步。

    d. 使用以下命令返回 SMTP 集成的 `ERROR` 日志记录级别：

    ```
    console-settings-updater set --merge /kata/configuration/product/preprocessor_smtp
    '{"logging":{"level":{"root":"ERROR"}}}'
    ```

在分布式解决方案和多租户模式下使用该应用程序时适用的限制：

1. 在 PCN 服务器上，“**资产**” → “**设备**”选项卡仅显示连接到该 PCN 服务器的主机。

2. 只能在 PCN 服务器上更改用户账户密码。

适用于 Sensor 组件的限制：

1. 只有安装在独立服务器上的 Sensor 组件才能被用来以最大 10 Gbps 的速度捕获网络流量。
2. 以 10 Gbps 的最大速度捕获 FTP 流量可能会导致严重丢失。
3. 如果您添加或删除向 Kaspersky Anti Targeted Attack Platform 发送 SPAN 流量的网络接口，则可能会从与您选择的网络接口不同的网络接口下载原始网络流量转储。

适用于 Sandbox 组件的限制：

1. 自定义镜像支持以下操作系统版本：
   - Windows 7
   - Windows 8.1 64 位
   - Windows 10 64 位（最高版本 1909）
2. 自定义操作系统镜像仅完全支持英语和俄语本地化。
3. 不提供用于激活操作系统和软件的授权许可密钥。
4. 如果 Sandbox 服务器上未安装 Central Node 服务器上操作系统集合中选择的某些操作系统，Kaspersky Anti Targeted Attack Platform 不会将对象发送到 Sandbox 组件进行扫描。如果具有 Sandbox 组件的多个服务器连接到具有 Central Node 组件的服务器，则应用程序会将对象发送到其安装的操作系统与 Central Node 上所选集匹配的服务器。

与 Kaspersky Endpoint Agent for Windows 和 Kaspersky Endpoint Security for Windows 集成时适用的限制：

1. 获取RAM 转储和磁盘镜像的任务只能分配给安装有 Kaspersky Endpoint Agent 3.14 或更高版本（适用于 Windows）和 Kaspersky Endpoint Security 12.1 或更高版本（适用于 Windows）的计算机。
2. 获取进程内存转储、NTFS 元文件和注册表项的任务只能分配给安装有 Kaspersky Endpoint Agent 3.14 或更高版本（适用于 Windows）或 Kaspersky Endpoint Security 12.1 或更高版本（适用于 Windows）的计算机。
3. 使用 YARA 规则扫描主机的任务只能分配给安装有 Kaspersky Endpoint Agent 3.14 或更高版本（适用于 Windows）和 Kaspersky Endpoint Security 12.1 或更高版本（适用于 Windows）的计算机。如果您同时将任务分配给安装有 Kaspersky Endpoint Agent 3.14 或更高版本的计算机以及安装有该应用程序早期版本的计算机，则该任务仅在安装有 Kaspersky Endpoint Agent 3.14 或更高版本的计算机上运行。
4. 如果选择自动运行点作为扫描范围，则任务仅在安装有 Kaspersky Endpoint Agent 3.14 或更高版本以及 Kaspersky Endpoint Security 12.1 或更高版本（适用于 Windows）的计算机上运行。
5. **代码注入**、**命名管道**、**WMI**、**LDAP**、**DNS**、**进程访问**事件仅在与 Kaspersky Endpoint Security for Windows 12.7 或更高版本集成时才可用。

与 Kaspersky Endpoint Security for Linux 集成时适用的限制：

1. 以下功能不适用于运行 Kaspersky Endpoint Security for Linux 11.4 的计算机：

   - 主机网络隔离。
   - 创建防御规则。

     在安装有 Kaspersky Endpoint Security 11.4 for Linux 应用程序的计算机上，不会创建有关防御规则应用不成功的通知。
   - 使用 IOC 文件查找计算机上的入侵指标。

     在安装有 Kaspersky Endpoint Security 11.4 for Linux 应用程序的计算机上，不会创建有关入侵指标搜索不成功的通知。

2. 以下功能不适用于运行 Kaspersky Endpoint Security for Linux 12 的计算机：

   - 创建防御规则。

     在安装有 Kaspersky Endpoint Security 12 for Linux 应用程序的计算机上，不会创建有关防御规则应用失败的通知。

3. Kaspersky Endpoint Security 11.4 或 12 for Linux 在事件数据库中记录的事件列表仅限于以下类型：

   - **文件已修改**
   - **进程已启动**
   - **进程已完成**
   - **系统事件日志**
   - **检测**
   - **检测处理结果**

4. 您可以在运行 Kaspersky Endpoint Security 11.4 for Linux 的计算机上创建的任务列表限于以下类型：

   - **获取文件**

     创建任务时，应用程序不会尝试验证可执行文件或要检索的文件的路径。
   - **运行应用程序**

5. 您可以在运行 Kaspersky Endpoint Security 12 for Linux 的计算机上创建的任务列表限于以下类型：

   - **获取文件**

     创建任务时，应用程序不会尝试验证可执行文件或要检索的文件的路径。
   - **运行应用程序**
   - **删除文件**
   - **杀死进程**

6. 您可以在运行 Kaspersky Endpoint Security 12.2 for Linux 的计算机上创建的任务列表限于以下类型：

- **获取文件**

  创建任务时，应用程序不会尝试验证可执行文件或要检索的文件的路径。

- **运行应用程序**
- **删除文件**
- **杀死进程**
- **隔离文件**

7. 在有关 Kaspersky Endpoint Security 11.4 或 12 for Linux 在事件数据库中注册的事件的信息中，“创建时间”字段会显示文件修改时间。

8. 当与 Kaspersky Endpoint Security 12.2 for Linux 或更高版本集成时，**到远程主机的连接**、**监听的端口**、**模块已加载**、**DNS**、**进程访问**事件可用。

与 Kaspersky Endpoint Security 12 for Mac 集成时适用的限制：

1. 以下功能不适用于运行 Kaspersky Endpoint Security 12 for Mac 的计算机：

- 主机网络隔离。
- 创建防御规则。

  在安装有 Kaspersky Endpoint Security 12 for Mac 应用程序的计算机上，不会创建有关防御规则应用失败的通知。

- 使用 IOC 文件查找计算机上的入侵指标。

  在安装有 Kaspersky Endpoint Security 12 for Mac 应用程序的计算机上，不会创建有关入侵指标搜索不成功的通知。

2. Kaspersky Endpoint Security 12 for Mac 在事件数据库中记录的事件列表限于以下类型：

- **文件已修改**
- **进程已启动**
- **进程已完成**
- **检测**
- **检测处理结果**

3. 您可以在运行 Kaspersky Endpoint Security 12 for Mac 的计算机上创建的任务列表限于以下类型：

   - **获取文件**

     创建任务时，应用程序不会尝试验证可执行文件或要检索的文件的路径。

   - **运行应用程序**

4. 在有关 Kaspersky Endpoint Security 12 for Mac 在事件数据库中注册的事件的信息中，创建时间字段会显示文件修改时间。

Kaspersky Endpoint Agent 3.16 for Windows 的限制：

您可以在 Kaspersky Endpoint Agent for Windows 在线帮助 中查看 Kaspersky Endpoint Agent 3.16 for Windows 的限制列表。

Kaspersky Endpoint Security 12.5 for Windows 的限制：

您可以在 Kaspersky Endpoint Agent for Windows 在线帮助 中查看 Kaspersky Endpoint Agent 12.5 for Windows 的限制列表。

Kaspersky Endpoint Security 12 for Linux 的限制：

您可以在 Kaspersky Endpoint Security for Linux 发行备注 中查看 Kaspersky Endpoint Security 12 for Linux 中的限制列表。

Kaspersky Endpoint Security 12 for Mac 的限制：

您可以在 Kaspersky Endpoint Agent for Windows 在线帮助 中查看 Kaspersky Endpoint Agent 12 for Mac 的限制列表。

数据提供

运行 Kaspersky Anti Targeted Attack Platform 的某些组件需要卡巴斯基方的数据处理。未经 Kaspersky Anti Targeted Attack Platform 管理员的同意，组件不会发送数据。

您可以查看数据列表及其使用条款，以及在您的组织与卡巴斯基之间的以下协议中同意数据处理：

- 在最终用户授权许可协议里（比如，安装应用程序期间）。

  根据最终用户授权许可协议条款，您同意自动向卡巴斯基发送在数据提供下的最终用户授权许可协议中列出的信息。最终用户授权许可协议包含在应用程序分发包中。

- 在 KSN 声明里（比如，安装应用程序期间或安装后的管理员菜单中）。

  当您参与卡巴斯基安全网络时，Kaspersky Anti Targeted Attack Platform 运行获得的信息会自动发送至卡巴斯基。传输数据列表在 KSN 声明中指定。Kaspersky Anti Targeted Attack Platform 用户自主决定是否参与 KSN。KSN 声明包含在应用程序分发包中。

  在发送到卡巴斯基之前，KSN 统计数据被积累在托管 Kaspersky Anti Targeted Attack Platform 组件的服务器的缓存中。

卡巴斯基将按照法律和卡巴斯基适用规则规定的方式保护接收到的任何信息。数据通过加密的通信信道发送。

在使用卡巴斯基私有安全网络时，卡巴斯基不会发送关于 Kaspersky Anti Targeted Attack Platform 运行的信息。然而，KSN 统计数据在托管 Kaspersky Anti Targeted Attack Platform 组件的服务器上的缓存中的累积程度与使用卡巴斯基安全网络时的程度相同。如果具有卡巴斯基私有安全网络的服务器位于您的组织之外，那么累积的 KSN 统计数据可能会传输到超出您的组织的范围。

卡巴斯基私有安全网络的管理员必须亲自确保此数据的安全性。

应用程序的服务数据

Kaspersky Anti Targeted Attack Platform 资源不提供限制安装 Central Node 组件的服务器和操作系统用户权限的功能。建议管理员根据自己的判断使用任何系统资源来控制如何允许安装了应用程序的服务器和操作系统的用户访问其他用户的个人数据。

Kaspersky Anti Targeted Attack Platform 的服务数据信息如下表所示。

数据类型	存储地点和期限
• 关于用户账户的数据。 • Central Node 组件的数据。 • 有关租户的数据。 • 有关连接到安装了 Endpoint Agent 组件的 Central Node 组件的计算机的信息。 • 有关预设和防护规则的数据。 • 有关使用 Endpoint Agent 组件分配给计算机的任务的信息。 • 自定义小部件布局数据。 • 有关用户定义的 TAA (IOA) 规则信息。 • 有关用户定义的 IDS 规则信息。 • 有关用户定义的 IOC 规则信息。 • 有关网络隔离规则的数据。 • 有关扫描排除项的数据。 • 关于报告和报告模板的信息。 • 有关 Endpoint Agent 组件证书的信息。	如果服务器上安装了 Central Node 组件，则数据将无限期地存储在托管 Central Node 组件的服务器上的 `/data` 目录中。当 Central Node 组件安装在集群上时，数据将无限期地存储在存储服务器上。
系统事件日志	操作系统日志文件无限期地存储在托管 Central Node 组件的服务器上的 `/var/log` 目录中。
包含应用程序操作信息的日志。	如果该组件安装在服务器上，则日志文件将无限期地存储在托管 Central Node 组件的服务器上的 /data 目录中。当 Central Node 组件安装在集群上时，数据将无限期地存储在存储服务器上。
文件扫描队列。	如果该组件安装在服务器上，文件将存储在托管 Central Node 组件的服务器上的 /data 目录中。当 Central Node 组件后安装在集群上时，数据将存储在存储服务器上。数据将保留直至扫描完成。
从带有 Endpoint Agent 组件的计算机接收的文件。	如果该组件安装在服务器上，文件将存储在托管 Central Node 组件的服务器上的 /data 目录中。当 Central Node 组件后安装在集群上时，数据将存储在存储服务器上。当磁盘空间已满时，数据将被轮换。
包含 YARA 和 IDS 规则（用户定义的和来自卡巴斯基的）的文件。	如果该组件安装在服务器上，文件将无限期地存储在托管 Central Node 组件的服务器上的 /data 目录中。当 Central Node 组件安装在集群上时，数据将无限期地存储在存储服务器上。
包含发送到外部系统的检测数据的文件。	如果该组件安装在服务器上，文件将无限期地存储在托管 Central Node 组件的服务器上的 /data 目录中。当 Central Node 组件安装在集群上时，数据将无限期地存储在存储服务器上。
Sandbox 组件的工件。	如果该组件安装在服务器上，文件将存储在托管 Central Node 组件的服务器上的 /data 目录中。当 Central Node 组件后安装在集群上时，数据将存储在存储服务器上。当磁盘空间已满时，数据将被轮换。
Sandbox 组件为其创建了检测的文件。	如果该组件安装在服务器上，文件将存储在托管 Central Node 组件的服务器上的 /data 目录中。当 Central Node 组件后安装在集群上时，数据将存储在存储服务器上。当磁盘空间已满时，数据将被轮换。

数据类型	存储地点和期限
用于验证应用程序组件的证书文件。	文件将无限期地存储在托管 Central Node、PCN、SCN、Sensor 组件的服务器或具有 Endpoint Agent 组件的计算机上的 /data 目录中。
在应用程序组件之间传输的加密密钥。	文件将无限期地存储在托管 Central Node、PCN、SCN、Sensor 组件的服务器或具有 Endpoint Agent 组件的计算机上的 /data 目录中。
SPAN 端口的镜像流量副本。	文件存储在带有 Sensor 组件的服务器上安装的存储器中。当磁盘空间已满时，数据将被删除。

数据类型	存储地点和期限
ICAP 排除项过滤器。	如果该组件安装在服务器上，文件将无限期地存储在托管 Central Node 组件的服务器上的 /data 目录中。当 Central Node 组件安装在集群上时，数据将无限期地存储在存储服务器上。
• 有关网络会话的信息。 • 设备信息。 • 与 Endpoint Agent 组件集成时的遥测。 • 网络流量事件。 • 用户账户数据。 • 有关可执行文件的信息。 • 与已注册事件相关的流量转储。 • 与网络会话相关的流量转储。	数据存储在 Central Node 服务器的 /data/storage/volumes/nta_database 目录中。当磁盘空间被填满时，数据将被轮换。
• 用户账户 ID。 • 用户账户名称。 • 用户的域名。 • 用户账户角色。 • 用户账户状态。 • 用户账户上次更改密码的日期和时间。	如果该组件安装在服务器上，文件将无限期地存储在托管 Central Node 组件的服务器上的 /data 目录中。当 Central Node 组件安装在集群上时，数据将无限期地存储在存储服务器上。
上传具有用户定义的 IDS 规则的文件的用户账户的用户名。 • 上传具有用户定义的 IDS 规则的文件的日期和时间。 • 用户定义的 IDS 规则的状态。 • 用户定义的 IDS 规则文件中指定的重要性。	
虚拟机配置信息： • 托管 Sandbox 组件的服务器的 IP 地址 • 虚拟机列表	

数据类型	存储地点和期限	
关于用户账户的数据： • 用户账户 ID。 • 用户账户名称。 • 授权用户的计算机的名称。		
网络会话信息： • 网络通讯参与者的姓名。 • 网络通信参与者的 IP 和 MAC 地址。		
有关在应用程序中注册的设备的信息： • 设备名称。 • 设备的 IP 和 MAC 地址。		
作为 NDR 功能的一部分与 Endpoint Agent 组件集成时保存的数据： • 具有 Endpoint Agent 组件的计算机的 IP 和 MAC 地址。 • 具有 Endpoint Agent 组件的计算机的名称。 • 在具有 Endpoint Agent 组件的计算机上注册的用户账户的名称。 • 计算机正在运行的操作系统。 • 用户代理。		
有关网络流量事件的信息：设备的 IP 和 MAC 地址。		
有关作为 NDR 功能的一部分连接的 Endpoint Agent 计算机上的可执行文件的信息： • 文件名。 • 文件路径。 • 文件版本。 • 文件的 MD5 哈希和 SHA256 哈希。		
与记录的网络会话和事件相关的流量转储数据： • 网络通讯参与者的姓名。 • 网络通信参与者的 IP 和 MAC 地址。 • 设备名称。 • 设备的 IP 和 MAC 地址。 • 用户账户名称。 • 用户账户 ID。 • 计算机正在运行的操作系统。 • 用户代理。 • 可执行文件的名称。 • 可执行文件路径。 • 可执行文件的版本。 • 可执行文件的 MD5 哈希和 SHA256 哈希。		

Central Node 和 Sensor 组件的数据

本节包含有关存储在具有 Central Node 组件的服务器上以及具有 Sensor 组件的服务器上的用户数据的以下信息：

- 存储数据的内容
- 存储位置
- 储存期限
- 用户访问数据

Sensor 组件的流量数据

Sensor 组件的流量数据存储在带有 Sensor 组件的服务器上，或者如果 Sensor 和 Central Node安装在同一台服务器上或部署为集群，则存储在带有 Sensor 和 Central Node 组件的服务器上。

流量数据被记录并存储在按顺序创建的文件中。如果出现以下情况，应用程序将停止在一个文件中记录数据并开始在下一个文件中记录数据：

- 已达到最大文件大小（您可以配置此设置）
- 配置的时间间隔已过（您可以配置此设置）
- 流量节省服务或整个Kaspersky Anti Targeted Attack Platform 应用程序被重新启动

随着流量数据累积，Kaspersky Anti Targeted Attack Platform 会筛选数据并仅保留以下信息：

- 与使用针对性攻击分析器技术扫描后生成的警报相关的信息
- PCAP 文件，其中：
  - 源或目的 IP 地址与检测中的 IP 地址匹配。
  - 流量数据属于检测时间后 15 分钟内的时间段。

筛选后的流量数据将被移至单独部分。其余流量数据（不满足筛选条件）将被删除。

筛选后的流量数据被保存在按顺序创建的文件中。如果出现以下情况，应用程序将停止在一个文件中记录数据并开始在下一个文件中记录数据：

- 已达到最大文件大小
- 配置的时间间隔已过

储存的数据流量涵盖过去 24 小时。较旧的数据被删除。

检测中的数据

Kaspersky Anti Targeted Attack Platform 资源不提供限制安装 Central Node 组件的服务器和操作系统用户权限的功能。建议管理员根据自己的判断使用任何系统资源来控制如何允许安装了应用程序的服务器和操作系统的用户访问其他用户的个人数据。

下表列出了创建检测时可能存储的数据的相关信息。

数据类型	存储地点和期限
所有检测的以下数据存储在服务器上： • 检测创建日期和时间。 • 检测修改的日期和时间。 • 检测到的对象的类别。 • 检测到的文件的名称。 • 检测到的文件的类型。 • 检测到的对象的来源。 • 检测到的 URL。 • 检测到的文件的 MD5 哈希和 SHA256 哈希。 • 与检测相关的警报详细信息中添加了用户评论。 • 创建检测所依据的 TAA (IOA) 规则的 ID。 • 生成检测的计算机的 IP 地址和名称。 • 在其上生成检测的计算机的 ID。 • 用户代理。 • 与检测相关的警报被分配到的用户账户。 • 文件列表。 • 警报重要性取决于根据卡巴斯基的经验此警报对计算机或企业局域网可能造成的安全影响。 • 进行检测的技术。 • 与检测相关的警报的状态。 • 与检测相关的警报被分配到的用户的姓名。 • 事件 ID（使用 NDR 功能时）。 • 设备 ID（使用 NDR 功能时）。	如果 Central Node 安装在服务器上，检测信息存储在 Central Node 服务器的 /data 目录中。如果 Central Node 作为集群安装，则检测信息存储在 ceph 存储中。 当单项扫描技术生成的检测记录数量达到 1000000 条时，数据就会轮换。
当与检测相关的警报被修改时，以下信息将存储在服务器上： • 修改警报的用户账户。 • 向其分配了警报的用户账户。 • 警报修改的日期和时间。 • 警报状态。 • 用户评论。	
如果检测是由扫描文件创建的，则以下信息可能存储在服务器上： • 检测到的文件的全名。 • 检测到的文件的 MD5 哈希和 SHA256 哈希。 • 检测到的文件的大小。 • 有关文件签名的信息。	
如果检测是由扫描 FTP 流量创建的，则以下信息可能存储在服务器上： • FTP 请求的 URI。	
如果检测是由扫描 HTTP 流量创建的，则以下信息可能存储在服务器上： • HTTP 请求的 URI。 • 请求源的 URI。 • 用户代理。 • 有关代理服务器的信息。	
如果检测是由于入侵检测技术的扫描而创建的，则以下信息可能存储在服务器上： • 发送数据的计算机的名称。 • 接收数据的计算机的名称。 • 发送数据的计算机的 IP 地址。 • 接收数据的计算机的 IP 地址。 • 传输的数据。 • 数据传输时间。 • 从包含流量、用户代理和方法的文件提取的 URL。 • 包含检测发生处的流量的文件。 • 基于 IDS 数据库的对象类别。 • 用于生成检测的自定义 IDS 规则的名称。 • HTTP 请求正文。 • 检测到的对象的列表。	

数据类型	存储地点和期限
如果检测是由于 URL 信誉技术扫描而创建的，则以下信息可能存储在服务器上： • 发送数据的计算机的名称。 • 接收数据的计算机的名称。 • 发送数据的计算机的 IP 地址。 • 接收数据的计算机的 IP 地址。 • 传输资源的 URI。 • 有关代理服务器的信息。 • 电子邮件的唯一 ID。 • 邮件发件人和收件人的电子邮件地址（包括副本收件人和邮件的密件副本）。 • 电子邮件主题。 • Kaspersky Anti Targeted Attack Platform 接收到邮件的日期和时间，精确到秒。 • 检测到的对象的列表。 • 网络连接时间。 • 网络连接的URL。 • 用户代理。	
如果检测是由扫描 HTTP 流量创建的，则以下信息可能存储在服务器上： • 用于生成检测的应用程序数据库的版本。 • 检测到的对象的类别。 • 检测到的对象名称。 • 检测到的对象的 MD5 哈希。 • 检测到的对象的信息。	
如果检测是由于反恶意软件技术的扫描而创建的，则以下信息可能存储在服务器上： • 用于生成警报的 Kaspersky Anti Targeted Attack Platform 组件的数据库版本。 • 检测到的对象的类别。 • 检测到的对象的列表。 • 检测到的对象的 MD5 哈希。 • 有关检测的其他信息。	
如果检测是因为 DNS 活动检测创建的，则以下信息可能存储在服务器上： • DNS 查询数据。 • DNS 服务器对查询的响应内容。 • 查询的主机列表。	
如果根据用户定义的 IOC 或 TAA (IOA) 规则进行扫描后创建检测，则以下信息可能会存储在服务器上： • 扫描完成的日期和时间。 • 生成检测的计算机的 ID。 • TAA (IOA) 规则的名称。 • IOC 文件的名称。 • 检测到的对象的信息。 • 具有 Endpoint Agent 组件的主机列表。	
如果使用 YARA 规则创建了检测，则可以在服务器上存储以下信息： • 用于生成检测的 YARA 规则的版本。 • 检测到的对象的类别。 • 检测到的对象的名称。 • 检测到的对象的 MD5 哈希。 • 检测到对象的日期和时间。 • 有关警报的其他信息。	

数据类型	存储地点和期限
如果检测是由扫描文件创建的，则以下信息可能存储在服务器上： • 邮件发件人和收件人的电子邮件地址（包括邮件副本和密件副本收件人）。 • 电子邮件主题。 • Kaspersky Anti Targeted Attack Platform 接收到邮件的日期和时间，精确到秒。 • 邮件的所有服务标题（如果它们出现在邮件中）。	如果 Central Node 安装在服务器上，检测信息存储在 Central Node 服务器的 /data 目录中。如果 Central Node 作为集群安装，则检测信息存储在 ceph 存储中。 数据将无限期保存。
如果检测是由重新扫描创建的，则以下信息可能存储在服务器上： • 文件名。	

事件中的数据

事件可能包含用户数据。如果服务器上安装了 Central Node，则发生的事件的信息将存储在 `/data` 目录中。如果 Central Node 作为集群安装，则信息存储在 ceph 存储中。

当磁盘变满时，数据会轮换。

Kaspersky Anti Targeted Attack Platform 资源不提供限制安装 Central Node 组件的服务器和操作系统用户权限的功能。建议管理员根据自己的判断使用任何系统资源来控制如何允许安装了应用程序的服务器和操作系统的用户访问其他用户的个人数据。

事件数据可以包含与以下内容相关的信息：

- 发生事件的计算机的名称。
- 具有 Endpoint Agent 组件的计算机的唯一 ID。
- 发生事件的用户账户的名称。
- 用户所属组的名称。
- 事件类型。
- 事件时间。
- 有关为其记录事件的文件的信息：名称、路径、全名。
- 文件的 MD5 哈希和 SHA256 哈希。
- 文件创建时间。
- 文件修改时间。
- 文件访问权限。
- 进程的环境变量。
- 命令行参数。

- 输入到命令行中的命令文本。
- 适配器的本地 IP 地址。
- 本地端口。
- 远程主机名。
- 远程主机 IP 地址。
- 远程主机端口。
- 访问过的网站的 URL 和 IP 地址，以及来自这些网站的链接。
- 网络连接协议。
- HTTP 请求方法。
- HTTP 请求标头。
- 有关 Windows 注册表变量的信息：变量的路径、变量名称、变量值。
- 发送用于 AMSI 扫描的脚本或二进制文件的内容。
- 有关 Windows 日志中事件的信息：事件类型、事件类型 ID、事件 ID、记录事件的用户账户、来自 Windows 事件日志的 XML 格式的事件完整文本。

报告中的数据

如果服务器上安装了 Central Node 组件，则报告数据将无限期地存储在 `/data` 目录中。如果 Central Node 作为集群安装，则信息将无限期地存储在 ceph 存储中。

Kaspersky Anti Targeted Attack Platform 资源不提供限制安装 Central Node 组件的服务器和操作系统用户权限的功能。建议管理员根据自己的判断使用任何系统资源来控制如何允许安装了应用程序的服务器和操作系统的用户访问其他用户的个人数据。

报告可能包含以下信息：

- 报告创建日期。
- 报告中涉及的时间段。
- 生成报告的用户账户的 ID。
- 报告状态。
- 生成报告的中 Central Node 组件。
- 报告文本为HTML代码。
- 报告描述。

- 生成报告的模板的名称。
- 租户 ID。

存储和隔离区中对象的数据

如果服务器上安装了 Central Node 组件，则存储区和隔离区中对象的相关数据将无限期地存储在 /data 目录中。如果 Central Node 作为集群安装，则信息将无限期地存储在 ceph 存储中。

Kaspersky Anti Targeted Attack Platform 资源不提供限制安装 Central Node 组件的服务器和操作系统用户权限的功能。建议管理员根据自己的判断使用任何系统资源来控制如何允许安装了应用程序的服务器和操作系统的用户访问其他用户的个人数据。

备份区和隔离区中的对象数据可能包含以下信息：

- 对象的名称。
- 具有 Endpoint Agent 组件的计算机上的对象路径。
- 文件的 MD5 哈希和 SHA256 哈希。
- 文件大小。
- 隔离对象的用户的 ID。
- 将对象置于存储中的用户的 ID。
- 存储隔离对象的计算机的 IP 地址。
- 存储隔离对象的计算机的名称。
- 存储中存储隔离对象的计算机的唯一 ID。
- 生成检测所依据的 TAA (IOA) 规则的 ID。
- 检测到的对象的类别。
- 使用应用程序的单个模块和技术扫描的对象的结果。
- 文件下载时间。
- 被扫描文件及其来源的元数据。
- 存储中对象的结果状态。

Sandbox 组件数据

对于处理时间，Central Node 组件发送的文件主体以开放形式保存在托管 Sandbox 组件的服务器上。在处理过程中，服务器管理员可以在技术支持模式下访问发送的文件。已扫描文件将定时被特殊脚本删除。默认状态下每 60 分钟一次。

下表中提供了有关使用 Sandbox 组件存储在服务器上的数据的信息。

存储在具有 Sandbox 组件的服务器上的数据

数据范围	存储位置	储存期限	访问数据
扫描的文件	`/var/opt/kaspersky/sandbox/library/`	在 Central Node 组件收到扫描结果后或直到自动删除之时，但存储时间不超过 24 小时。	用户访问权限由管理员使用操义。
文件扫描结果	• `/var/opt/kaspersky/sandbox/library/` • `/tmp/`	在 Central Node 组件收到扫描结果后或直到自动删除之时，但存储时间不超过 24 小时。	用户访问权限由管理员使用操义。
任务设置	• `/var/opt/kaspersky/sandbox/library/` • Sandbox 组件数据库	在 Central Node 组件收到扫描结果后或直到自动删除之时，但存储在目录 `/var/opt/kaspersky/sandbox/library/` 中的时间不超过 `24` 小时。 在 Sandbox 组件数据库中最多存储 90 天。	用户对 `/var/opt/kaspersky/sandl` 目录的访问权限由管理员使用定义。 数据库中的用户身份验证需要动数据库进程的用户和具有 ro 授予对数据库文件的访问权限 仅通过加密的 IPSec 通道提供
跟踪文件	`/var/log/kaspersky/sandbox/`	最多 21 天。	用户访问权限由管理员使用操义。 只有授权用户才能对跟踪文件 有关跟踪文件操作的信息保存件日志中。
更新源设置	`/var/opt/kaspersky/apt-updater`	直至被修改或删除。	用户访问权限由管理员使用操义。
最短密码长度设置	`/var/opt/kaspersky/apt-config-ram-common/validator.conf`	直至被修改或删除。	用户访问权限由管理员使用操义。
虚拟机	`/vm`	直至被修改或删除。	用户访问权限由管理员使用操义。
下载 iso 格式的操作系统和应用程序镜像	`/var/opt/kaspersky/sandbox/custom_images/iso`	直至被修改或删除。	用户访问权限由管理员使用操义。

应用程序组件之间传输的数据

Central Node 和 Endpoint Agent 组件

用作 Endpoint Agent 组件的应用程序向 Central Node 组件发送以下内容：任务完成报告、安装了这些应用程序的计算机上发生的事件和警报的信息、有关终端会话的信息。

如果没有与 Central Node 组件的连接，所有待定信息将会累积起来，直到被发送至 Central Node 组件，或直到被用作 Endpoint Agent 的应用程序被从计算机移除为止，但不会超过 21 天。

所有事件的一般信息

如果用户计算机上发生事件，则应用程序向事件数据库发送以下数据：

- 事件类型。
- 事件时间。
- 事件 ID。
- 事件架构的版本。
- 事件被 Central Node 服务器处理的时间。
- 为其生成事件的用户账户。
- 发生事件的主机的名称。
- 主机的 IP 地址。
- 主机上安装的操作系统类型。
- 操作系统系列。
- 操作系统名称。
- 操作系统版本。
- Endpoint Agent 角色中使用的应用程序用于连接 Central Node 或 Sensor 服务器的网络适配器的 IP 地址。
- 充当 Endpoint Agent 组件角色的应用程序的版本。
- KBD 数据库最后更新的日期。

- SW 数据库最后更新的日期。
- 索引日期。
- 根据 TAA (IOA) 规则标记事件时，将传输以下信息：
  - 触发的攻击指标的 ID。
  - 触发的攻击指标的决定。
  - 触发的攻击指标的来源。
  - 触发的攻击指标的版本。
  - MITRE 技术代码。
  - MITRE 战术代码。
  - 警报重要性取决于根据卡巴斯基的经验此警报对计算机或企业局域网可能造成的安全影响。
  - 检测的置信度（取决于规则引起误报的可能性）：

Central Node 和 Kaspersky Endpoint Agent for Windows

如果用户计算机上发生事件，则应用程序向事件数据库发送以下数据：

1. 文件创建事件。
   - 有关创建文件的进程的信息：进程文件名、进程文件的 MD5 哈希和 SHA256 哈希。
   - 文件名。
   - 文件路径。
   - 文件全名。
   - 文件的 MD5 哈希和 SHA256 哈希。
   - 文件创建和修改日期。
   - 文件大小。
2. 注册表监控事件。
   - 有关修改了注册表的进程的信息：进程 ID、进程文件名称、进程文件的 MD5 哈希和 SHA256 哈希。
   - 注册表项路径。
   - 注册表值名称。
   - 注册表值数据。

- 注册表值类型。
- 以前的注册表项路径。
- 以前的注册表值数据。
- 以前的注册表值类型。

3. 驱动程序加载事件。

- 文件名。
- 文件路径。
- 文件全名。
- 文件的 MD5 哈希和 SHA256 哈希。
- 文件大小。
- 文件创建和修改日期。

4. 监听端口开放事件。

- 有关开放监听端口的进程的详细信息：进程文件名和进程文件的 MD5 哈希和 SHA256 哈希。
- 端口号。
- 适配器 IP 地址。

5. 操作系统日志中的事件。

- 事件时间、发生事件的主机和用户账户名称。
- 事件 ID。
- 信道/日志名称。
- 日志中的事件 ID。
- 提供商名称。
- 认证事件子类型。
- 域名。
- 远程 IP 地址。

- 事件标题字段：ProviderName, EventId, Version, Level, Task, Opcode, Keywords, TimeCreatedSystemTime, EventRecordId, CorellationActivityId, ExecutionProcessID, ThreadID, Channel, Computer。

- 事件主体字段：AccessList, AccessMask, AccountExpires, AllowedToDelegateTo, Application, AuditPolicyChanges, AuthenticationPackageName, CategoryId, CommandLine, DisplayName, Dummy, ElevatedToken, EventCode, EventProcessingFailure, FailureReason, FilterRTID, HandleId, HomeDirectory, HomePath, ImpersonationLevel, IpAddress, IpPort, KeyLength, LayerName, LayerRTID, LmPackageName, LogonGuid, LogonHours, LogonProcessName, LogonType, MandatoryLabel, MemberName, MemberSid, NewProcessId, NewProcessName, NewUacValue, NewValue, NewValueType, ObjectName, ObjectServer, ObjectType, ObjectValueName, OldUacValue, OldValue, OldValueType, OperationType, PackageName, ParentProcessName, PasswordLastSet, PrimaryGroupId, PriviledgeList, ProcessId, ProcessName, ProfileChanged, ProfilePath, Protocol, PublisherId, ResourceAttributes, RestrictedAdminMode, SamAccountName, ScriptPath, ServiceAccount, ServiceFileName, ServiceName, ServiceStartType, ServiceType, SettingType, SettingValue, ShareLocalPath, ShareName, SidHistory, SourceAddress, SourcePort, Status, SubcategoryGuid, Subcategoryld, SubjectDomainName, SubjectLogonId, SubjectUserName, SubjectUserSid, SubStatus, TargetDomainName, TargetLinkedLogonId, TargetLogonId, TargetOutboundDomainName, TargetOutboundUserName, TargetUserName, TargetUserSid, TaskContent, TaskName, TokenElevationType, TransmittedServices, UserAccountControl, UserParameters, UserPrincipalName, UserWorkstations, VirtualAccount, Workstation, WorkstationName。

6. 进程启动事件。

- 有关进程文件的信息：文件名、文件路径、文件的 MD5 或 SHA256 哈希、文件大小、创建和修改日期、颁发文件数字证书的组织名称、数字签名验证结果。

- UniquePID。

- 进程启动选项。

- 进程启动时间。

- 有关父进程的信息：文件路径、进程文件的 UniquePID、MD5 或 SHA256 哈希值、进程启动选项。

7. 进程停止事件。

- 有关进程的文件的信息：文件名、文件路径、文件全名、文件的 MD5 哈希和 SHA256 哈希、文件大小以及进程结束时间。

- UniquePID。

- 进程启动选项。

- 有关父进程的信息：文件路径、进程文件的 UniquePID、MD5 或 SHA256 哈希值、进程启动选项。

8. 模块加载事件。

- 有关加载模块的文件的详细信息：UniquePID、文件名、文件路径、文件全名、文件的 MD5 哈希和 SHA256 哈希以及文件大小。

- DLL 名称。

- DLL 的路径。

- DLL 全名。

- DLL 的 MD5 哈希或 SHA256 哈希。

- DLL 大小。
- DLL 创建和修改日期。
- 颁发 DLL 数字证书的组织名称。
- DLL 数字签名验证结果。

9. 进程启动阻止事件。
   - 有关尝试运行的文件的详细信息：文件名、文件路径、文件全名、文件的 MD5 哈希和 SHA256 哈希、文件大小以及文件创建和修改日期。
   - 命令行参数。
10. 文件启动阻止事件。
    - 有关尝试打开的文件的详细信息：文件名、文件路径、文件全名、文件的 MD5 哈希和 SHA256 哈希、用于文件大小阻止的校验和类型（(0 – MD5, !=0 – SHA256，不用于搜索）。
    - 有关可执行文件的详细信息：文件名、文件路径、文件全名、文件的 MD5 哈希和 SHA256 哈希、文件大小以及文件创建和修改日期。
    - 有关父进程的详细信息：文件名、文件路径、文件全名、文件的 MD5 哈希和 SHA256 哈希以及 UniquePID。
11. 检测事件及其处理结果（当 Kaspersky Endpoint Agent for Windows 与 Kaspersky Endpoint Security for Windows 集成时）。
    - 扫描结果。
    - 检测到的对象的名称。
    - 应用程序数据库中记录的 ID。
    - 用于生成检测的应用程序数据库的发布时间。
    - 对象处理模式。
    - 检测到的对象的类别（例如，病毒的名称）。
    - 检测到的对象的 MD5 哈希。
    - 检测到的对象的 SHA256 哈希。
    - 进程的唯一 ID。
    - Windows任务管理器中显示的进程 PID。
    - 进程启动命令行。
    - 处理对象时出错的原因。
    - 使用 AMSI 扫描的脚本内容。

12. AMSI 扫描事件。

    - 使用 AMSI 扫描的脚本内容。

Central Node 和 Kaspersky Endpoint Security for Windows

如果用户计算机上发生事件，则应用程序向事件数据库发送以下数据：

1. 文件修改事件。

    - 有关创建文件的进程的信息：进程文件名、进程文件的 MD5 哈希和 SHA256 哈希。
    - 有关创建或修改的文件的信息：名称、路径、全名、类型、MD5 哈希、SHA256 哈希、创建日期、修改日期、属性、属性修改日期、大小、区域 ID、文件的应用程序名称、供应商、颁发数字证书的组织名称、描述、数字签名验证结果、数字签名的时间、原始名称、修改前的名称、修改前的路径、修改前的全名。
    - 有关创建链接的文件的信息：MD5 哈希、SHA256 哈希、创建日期、修改日期、属性、属性修改日期、大小、类型、区域 ID、文件的应用程序名称、原始名称、颁发数字证书的组织名称、描述、签名的主题、数字签名验证结果、数字签名的时间、链接文件的全名。

2. 注册表监控事件。

    - 有关修改了注册表的进程的信息：进程 ID、进程文件名称、进程文件的 MD5 哈希和 SHA256 哈希。
    - 注册表项路径。
    - 注册表值名称。
    - 注册表值数据。
    - 注册表值类型。
    - 以前的注册表项路径。
    - 以前的注册表值数据。
    - 以前的注册表值类型。
    - 注册表操作的类型。
    - 保存注册表项的文件的路径。

3. 驱动程序加载事件。

    - 文件名。
    - 原始文件名。
    - 文件路径。
    - 文件全名。

- 文件的 MD5 哈希和 SHA256 哈希。
- 文件大小。
- 文件创建和修改日期。
- 文件属性修改日期。
- 文件大小。
- 文件类型。
- 文件属性。
- 文件区域 ID。
- 文件供应商。
- 文件描述。
- 颁发数字证书的组织名称。
- 签名主题。
- 数字签名验证结果。
- 数字签名的时间。
- 从其检索文件的 URL。
- 从中检索文件的消息的元数据。

4. 监听端口开放事件。

- 有关开放监听端口的进程的详细信息：进程文件名和进程文件的 MD5 哈希和 SHA256 哈希。
- 端口号。
- 适配器 IP 地址。
- 运行状态。

5. 远程连接事件。

- 本地计算机的信息：IP 地址、端口号。
- 有关远程计算机的信息：IP 地址、端口号、FQDN。
- 有关连接的 TLS 加密的信息：协议版本、SNI、加密的 SNI、证书文件的 MD5 哈希、证书文件的 SHA1 哈希、证书颁发者名称、证书序列号、证书验证结果、证书到期日期、Ja3、Ja3s、Ja3 的 MD5 哈希、Ja3s 的 MD5 哈希、套接字类型。
- LANA 号码。
- HTTP 方法。

- 所跟踪的 URL。
- 进程状态。
- 连接方向。

6. DNS 查找事件。
   - DNS 服务器的 IPv4 地址。
   - 正在执行的 DNS 查询的二进制掩码。
   - DNS 响应错误代码。
   - DNS 查询类型 ID。
   - 要解析 DNS 记录的域名。
   - DNS 响应的日期。
7. LDAP 事件。
   - 搜索范围。
   - 搜索查询过滤器。
   - 查询中指定为要返回的属性。
   - 要搜索的 LDAP容器的路径。
8. 进程启动事件。

   有关父进程和祖进程、加载器进程、创建者进程、正在运行的进程的文件的信息：名称、路径、全名、MD5 哈希、SHA256 哈希、创建日期和时间、修改日期和时间、属性、属性修改日期和时间、大小、区域 ID、供应商、颁发数字证书的组织名称、描述、原始名称、数字签名主题、数字签名验证结果、数字签名的日期和时间、文件版本、登录类型、登录会话 ID、用户账户类型、用户名、用户账户 ID、登录计算机的 IP 地址、完整性级别、进程 ID、当前目录。
9. 进程停止事件。
   - 有关进程的文件的信息：文件名、文件路径、文件全名、文件的 MD5 哈希和 SHA256 哈希、文件大小以及进程结束时间。
   - 进程的唯一 ID。
   - 进程启动选项。
   - 有关父进程的信息：文件路径、UniquePID、MD5 和 SHA256 哈希、命令行选项。
10. 进程访问事件。
    - 操作类型。
    - 进程访问权限。

- 调用堆栈。
- 有关接收方进程的文件以及复制句柄的进程的文件的信息：名称、路径、完整路径、MD5 和 SHA256 哈希、创建日期和时间、修改日期和时间、属性修改日期和时间、大小、唯一 ID、系统 ID、命令行选项、从中检索文件的 URL、从中检索文件的消息的元数据。

11. 模块加载事件。

- 有关加载模块的文件的详细信息：UniquePID、文件名、文件路径、文件全名、文件的 MD5 哈希和 SHA256 哈希以及文件大小。
- DLL 名称。
- DLL 的路径。
- DLL 全名。
- DLL 的 MD5 哈希或 SHA256 哈希。
- DLL 大小。
- DLL 属性。
- DLL 区域 ID。
- DLL 应用程序名称。
- 原始 DLL 名称。
- DLL 创建和修改日期。
- 颁发 DLL 数字证书的组织名称。
- DLL 数字签名验证结果。
- DLL 数字签名日期。
- 替换 DLL 的路径。
- DLL 文件类型。
- 从其检索文件的 URL。
- 从中检索文件的消息的元数据。
- .NET 程序集名称。
- .NET 程序集标志。
- .NET 模块标志。

12. 进程启动阻止事件。

- 有关尝试运行的文件的详细信息：文件名、文件路径、文件全名、文件的 MD5 哈希和 SHA256 哈希、文件大小以及文件创建和修改日期。
- 命令行参数。

13. 文件启动阻止事件。

- 有关正在打开的文件的信息：文件名、文件路径、完整文件名、MD5 哈希、SHA256 哈希、触发阻止的校验和类型（MD5 为 0，SHA256 为 !=0，不用于搜索）、下载可执行文件的网站 URL、附加下载的文件的消息的元数据。
- 有关可执行文件的详细信息：文件名、文件路径、文件全名、文件的 MD5 哈希和 SHA256 哈希、文件大小以及文件创建和修改日期。
- 有关父进程的详细信息：文件名、文件路径、文件全名、文件的 MD5 哈希和 SHA256 哈希以及 UniquePID。

14. 命名管道打开并连接的事件。

- 创建或连接到命名管道的进程的文件名。
- 管道操作类型。

15. 威胁检测事件和检测处理结果。

- 检测到的对象的名称。
- 检测到的对象的 MD5 哈希。
- 检测到的对象的 SHA256 哈希。
- 检测对象的类型。
- 扫描结果。
- 应用程序数据库中记录的 ID。
- 用于生成检测的应用程序数据库的版本。
- 对象处理模式。
- 检测到的对象的类别（例如，病毒的名称）。
- 协议。
- 本地计算机的 IPv4 或 IPv6 地址。
- 本地端口号。
- 远程计算机的 IPv4 或 IPv6 地址。
- 远程端口号。

- 从其检索文件的 URL。
- 发件人的电子邮件地址（如果文件是从电子邮件中获取的）。
- 文件加载器的全名、MD5 哈希、SHA256 哈希。
- 进程的唯一 ID。
- Windows任务管理器中显示的进程 PID。
- 进程启动命令行。
- 处理对象时出错的原因。
- 使用 AMSI 扫描的脚本内容和类型。

16. WMI 服务启动事件。
    - 操作类型。
    - WMI 服务的远程启动标志。
    - 启动 WMI 服务的计算机的名称。
    - 启动 WMI 服务的用户的名称。
    - WMI 命名空间。
    - 事件消费者过滤器名称。
    - 创建的事件消费者的名称。
    - 事件消费者源代码。
17. AMSI 扫描事件。
    - 使用 AMSI 扫描的脚本内容。
    - 发送扫描的脚本的内容类型。
    - 发送扫描的脚本的名称。
    - 脚本文件的 MD5 哈希。
    - 脚本文件的 SHA256 哈希。
18. 代码注入事件。
    - 有关接收方进程的信息：应用程序名称、应用程序完整名称、应用程序路径、文件的 MD5 哈希值、文件的 SHA256 哈希值、下载文件的 URL、附加下载的文件的消息的元数据、应用程序的唯一 ID、应用程序的系统 ID、命令行、进程 DLL 的名称、进程 DLL 的路径、进程在地址空间中的地址。
    - 注入方法。
    - 修改的进程的命令行。

- 系统调用参数。
- 拦截注入相关函数时的 API 调用堆栈。

19. 解释文件运行事件。

    有关解释文件的信息：名称、路径、全名、MD5、SHA256、文件创建日期和时间、文件修改日期和时间、大小、类型、属性、属性修改日期和时间、原始名称、描述、区域 ID、颁发数字证书的组织名称、数字签名验证的结果、数字签名的日期和时间、数字签名的主题、获取文件的 URL、附加下载的文件的消息的元数据。

20. 操作系统日志中的事件。

    - 事件时间、发生事件的主机和用户账户名称。
    - 事件 ID。
    - 信道/日志名称。
    - 日志中的事件 ID。
    - 提供商名称。
    - 认证事件子类型。
    - 域名。
    - 远程 IP 地址。

- 事件标题字段：ProviderName, EventId, Version, Level, Task, Opcode, Keywords, TimeCreatedSystemTime, EventRecordId, CorellationActivityId, ExecutionProcessID, ThreadID, Channel, Computer。

- 事件正文字段：AccessList、AccessFiles mask、AccountExpires、AllowedToDelegateTo、Application、AuditPolicyChanges、AuthenticationPackageName、CategoryId、CommandLine、DisplayName、Dummy、ElevatedToken、EventCode、EventProcessingFailure、FailureReason、FilterRTID、HandleId、HomeDirectory、HomePath、ImpersonationLevel、IpAddress、IpPort、KeyLength、LayerName、LayerRTID、LmPackageName、LogonGuid、LogonHours、LogonProcessName、LogonType、MandatoryLabel、MemberName、MemberSid、NewProcessId、NewProcessName、NewUacValue、NewValue、NewValueType、ObjectName、ObjectServer、ObjectType、ObjectValueName、OldUacValue、OldValue、OldValueType、OperationType、PackageName、ParentProcessName、PasswordLastSet、PrimaryGroupId、PriviledgeList、ProcessId、ProcessName、ProfileChanged、ProfilePath、Protocol、PublisherId、ResourceAttributes、RestrictedAdminMode、SamAccountName、ScriptPath、ServiceAccount、ServiceFileName、ServiceName、ServiceStartType、ServiceType、SettingType、SettingValue、ShareLocalPath、ShareName、SidHistory、SourceAddress、SourcePort、Status、SubcategoryGuid、SubcategoryId、SubjectDomainName、SubjectLogonId、SubjectUserName、SubjectUserSid、SubStatus、TargetDomainName、TargetLinkedLogonId、TargetLogonId、TargetOutboundDomainName、TargetOutboundUserName、TargetUserName、TargetUserSid、TaskContent、TaskName、TokenElevationType、TransmittedServices、UserAccountControl、UserParameters、UserPrincipalName、UserWorkstations、VirtualAccount、Workstation、WorkstationName、System、SystemProvider、SystemProviderName、SystemProviderGuid、SystemProviderEventSourceName、SystemEventID、SystemEventIDQualifiers、SystemEventRecordID、SystemChannel、SystemTask、SystemOpcode、SystemVersion、SystemLevel、SystemKeywords、SystemTimeCreated、SystemTimeCreatedSystemTime、SystemCorrelation、SystemCorrelationActivityID、SystemExecution、SystemExecutionProcessID、SystemExecutionThreadID、SystemComputer、SystemSecurity、SystemSecurityUserID、UserData、UserDataEventProcessingFailure、UserDataEventProcessingFailureError、UserDataEventProcessingFailureErrorCode、UserDataEventProcessingFailureEventID、UserDataEventProcessingFailurePublisherID、UserDataLogFileCleared、UserDataLogFileClearedSubjectUserSid、UserDataLogFileClearedSubjectUserName、UserDataLogFileClearedSubjectDomainName、UserDataLogFileClearedSubjectLogonId、UserDataFileIsFull、UserDataOperationStartedOperationalProviderName、UserDataOperationStartedOperationalCode、UserDataOperationStartedOperationalHostProcess、UserDataOperationStartedOperationalProcessID、UserDataOperationStartedOperationalProviderPath、UserDataServiceShutdown、UserDataOperationClientFailure、UserDataOperationClientFailureId、UserDataOperationClientFailureClientMachine、UserDataOperationClientFailureUser、UserDataOperationClientFailureClientProcessId、UserDataOperationClientFailureComponent、UserDataOperationClientFailureOperation、UserDataOperationClientFailureResultCode、UserDataOperationClientFailurePossibleCause、EventData、EventDataData、EventDataDataTaskName、EventDataDataPrivilegeList、EventDataDataAttributeLDAPDisplayName、EventDataDataOperationType、EventDataDataObjectClass、EventDataDataAttributeValue、EventDataDataObjectDN、EventDataDataRelativeTargetName、EventDataDataWorkstationName、EventDataDataServiceName、EventDataDataAllowedToDelegateTo、EventDataDataUserAccountControl、EventDataDataProfileChanged、EventDataDataRuleId、EventDataDataRuleName、EventDataDataSubjectUserSid、EventDataDataSubjectUserName、EventDataDataSubjectDomainName、EventDataDataSubjectLogonId、EventDataDataPreviousTime、EventDataDataNewTime、EventDataDataProcessId、EventDataDataProcessName、EventDataDataObjectType、EventDataDataObjectName、EventDataDataAccessList、EventDataDataAccessMask、EventDataDataServiceFileName、EventDataDataServiceType、EventDataDataServiceStartType、EventDataDataServiceAccount、EventDataDataDomainName、EventDataDataDomainSid、EventDataDataTdoType、EventDataDataTdoDirection、EventDataDataTdoAttributes、EventDataDataSidFilteringEnabled、EventDataDataTargetSid、EventDataDataAccessGranted、EventDataDataTargetUserName、EventDataDataTargetDomainName、EventDataDataSamAccountName、EventDataDataSidHistory、EventDataDataDomainPolicyChanged、EventDataDataMinPasswordAge、EventDataDataMaxPasswordAge、EventDataDataForceLogoff、EventDataDataLockoutThreshold、EventDataDataLockoutObservationWindow、EventDataDataLockoutDuration、EventDataDataProperties、EventDataDataPasswordProperties、EventDataDataMinPasswordLength、EventDataDataPasswordHistoryLength、

EventDataDataMachineAccountQuota、EventDataDataMixedDomainMode、
EventDataDataDomainBehaviorVersion、EventDataDataOemInformation、
EventDataDataGroupTypeChange、EventDataDataLogonGuid、EventDataDataTargetUserSid、
EventDataDataTargetLogonId、EventDataDataTargetLogonGuid、EventDataDataSidList、
EventDataDataWorkstation、EventDataDataStatus、EventDataDataCallerProcessId、
EventDataDataCallerProcessName、EventDataDataForestRoot、EventDataDataForestRootSid、
EventDataDataOperationId、EventDataDataEntryType、EventDataDataFlags、
EventDataDataTopLevelName、EventDataDataDnsName、EventDataDataNetbiosName、
EventDataDataAuditSourceName、EventDataDataEventSourceId、EventDataDataErrorCode、
EventDataDataGPOList、EventDataDataDestinationDRA、EventDataDataSourceDRA、
EventDataDataSourceAddr、EventDataDataNamingContext、EventDataDataOptions、
EventDataDataStatusCode、EventDataDataSessionID、EventDataDataStartUSN、
EventDataDataPackageName、EventDataDataAuthenticationPackageName、
EventDataDataFailureReason、EventDataDataSubStatus、EventDataDataCategoryId、
EventDataDataSubcategoryGuid、EventDataDataAuditPolicyChanges、
EventDataDataUserPrincipalName、EventDataDataHomeDirectory、EventDataDataHomePath、
EventDataDataScriptPath、EventDataDataProfilePath、EventDataDataUserWorkstations、
EventDataDataPasswordLastSet、EventDataDataAccountExpires、EventDataDataPrimaryGroupId、
EventDataDataOldUacValue、EventDataDataNewUacValue、EventDataDataUserParameters、
EventDataDataLogonHours、EventDataDataMemberName、EventDataDataMemberSid、
EventDataDataServiceSid、EventDataDataTicketOptions、EventDataDataTicketEncryptionType、
EventDataDataPreAuthType、EventDataDataCertIssuerName、EventDataDataCertSerialNumber、
EventDataDataCertThumbprint、EventDataDataSettingType、EventDataDataSettingValue、
EventDataDataShareName、EventDataDataShareLocalPath、EventDataDataApplication、
EventDataDataSourceAddress、EventDataDataSourcePort、EventDataDataProtocol、
EventDataDataFilterRTID、EventDataDataLayerName、EventDataDataLayerRTID、
EventDataDataLogonType、EventDataDataLogonProcessName、EventDataDataTransmittedServices、
EventDataDataLmPackageName、EventDataDataKeyLength、EventDataDataIpAddress、
EventDataDataIpPort、EventDataDataImpersonationLevel、EventDataDataRestrictedAdminMode、
EventDataDataTargetOutboundUserName、EventDataDataTargetOutboundDomainName、
EventDataDataVirtualAccount、EventDataDataTargetLinkedLogonId、EventDataDataElevatedToken、
EventDataDataTaskContentNew、EventDataDataTaskContentNewTask、
EventDataDataTaskContentNewTaskRegistrationInfo、
EventDataDataTaskContentNewTaskRegistrationInfoDate、
EventDataDataTaskContentNewTaskRegistrationInfoAuthor、
EventDataDataTaskContentNewTaskTriggers、EventDataDataTaskContentNewTaskPrincipals、
EventDataDataTaskContentNewTaskPrincipalsPrincipal、
EventDataDataTaskContentNewTaskPrincipalsPrincipalid、
EventDataDataTaskContentNewTaskPrincipalsPrincipalRunLevel、
EventDataDataTaskContentNewTaskPrincipalsPrincipalUserId、
EventDataDataTaskContentNewTaskPrincipalsPrincipalLogonType、
EventDataDataTaskContentNewTaskSettings、
EventDataDataTaskContentNewTaskSettingsMultipleInstancesPolicy、
EventDataDataTaskContentNewTaskSettingsDisallowStartIfOnBatteries、
EventDataDataTaskContentNewTaskSettingsStopIfGoingOnBatteries、
EventDataDataTaskContentNewTaskSettingsAllowHardTerminate、
EventDataDataTaskContentNewTaskSettingsStartWhenAvailable、
EventDataDataTaskContentNewTaskSettingsRunOnlyIfNetworkAvailable、
EventDataDataTaskContentNewTaskSettingsIdleSettings、
EventDataDataTaskContentNewTaskSettingsIdleSettingsStopOnIdleEnd、
EventDataDataTaskContentNewTaskSettingsIdleSettingsRestartOnIdle、
EventDataDataTaskContentNewTaskSettingsAllowStartOnDemand、
EventDataDataTaskContentNewTaskSettingsEnabled、
EventDataDataTaskContentNewTaskSettingsHidden、
EventDataDataTaskContentNewTaskSettingsRunOnlyIfIdle、
EventDataDataTaskContentNewTaskSettingsWakeToRun、
EventDataDataTaskContentNewTaskSettingsExecutionTimeLimit、
EventDataDataTaskContentNewTaskSettingsPriority、EventDataDataTaskContentNewTaskActions、

EventDataDataTaskContentNewTaskActionsContext、EventDataDataTaskContentNewTaskActionsExec、
EventDataDataTaskContentNewTaskActionsExecCommand、EventDataDataOldSd、
EventDataDataNewSd、EventDataDataNotificationPackageName、
EventDataDataSecurityPackageName、EventDataDataStopTime、EventDataDataContextInfo、
EventDataDataUserData、EventDataDataPayload、EventDataDataOpCorrelationID、
EventDataDataAppCorrelationID、EventDataDataDSName、EventDataDataDSType、
EventDataDataObjectGUID、EventDataDataFileName、EventDataDataLinkName、
EventDataDataTransactionId、EventDataDataOldObjectDN、EventDataDataNewObjectDN、
EventDataDatabcdCCID、EventDataDatabMaxSlotIndex、EventDataDatabVoltageSupport、
EventDataDatadwProtocols、EventDataDatadwDefaultClock、EventDataDatadwMaximumClock、
EventDataDatabNumClockSupported、EventDataDatadwDataRate、EventDataDatadwMaxDataRate、
EventDataDatabNumDataRateSupported、EventDataDatadwMaxIFSD、
EventDataDatadwSyncProtocols、EventDataDatadwMechanical、EventDataDatadwFeatures、
EventDataDataObjectValueName、EventDataDataHandleId、EventDataDataOldValueType、
EventDataDataOldValue、EventDataDataNewValueType、EventDataDataNewValue、
EventDataDataSubjectUserDomainName、EventDataDataObjectCollectionName、
EventDataDataObjectIdentifyingProperties、EventDataDataObjectProperties、EventDataDataparam、
EventDataDataCVEID、EventDataDataAdditionalDetails、EventDataDataObjectServer、
EventDataDataTaskContent、EventDataDataTaskContentTask、
EventDataDataTaskContentTaskRegistrationInfo、EventDataDataTaskContentTaskRegistrationInfoDate、
EventDataDataTaskContentTaskRegistrationInfoAuthor、EventDataDataTaskContentTaskTriggers、
EventDataDataTaskContentTaskPrincipals、EventDataDataTaskContentTaskPrincipalsPrincipal、
EventDataDataTaskContentTaskPrincipalsPrincipalid、
EventDataDataTaskContentTaskPrincipalsPrincipalRunLevel、
EventDataDataTaskContentTaskPrincipalsPrincipalUserId、
EventDataDataTaskContentTaskPrincipalsPrincipalLogonType、
EventDataDataTaskContentTaskSettings、
EventDataDataTaskContentTaskSettingsMultipleInstancesPolicy、
EventDataDataTaskContentTaskSettingsDisallowStartIfOnBatteries、
EventDataDataTaskContentTaskSettingsStopIfGoingOnBatteries、
EventDataDataTaskContentTaskSettingsAllowHardTerminate、
EventDataDataTaskContentTaskSettingsStartWhenAvailable、
EventDataDataTaskContentTaskSettingsRunOnlyIfNetworkAvailable、
EventDataDataTaskContentTaskSettingsIdleSettings、
EventDataDataTaskContentTaskSettingsIdleSettingsStopOnIdleEnd、
EventDataDataTaskContentTaskSettingsIdleSettingsRestartOnIdle、
EventDataDataTaskContentTaskSettingsAllowStartOnDemand、
EventDataDataTaskContentTaskSettingsEnabled、EventDataDataTaskContentTaskSettingsHidden、
EventDataDataTaskContentTaskSettingsRunOnlyIfIdle、
EventDataDataTaskContentTaskSettingsWakeToRun、
EventDataDataTaskContentTaskSettingsExecutionTimeLimit、
EventDataDataTaskContentTaskSettingsPriority、EventDataDataTaskContentTaskActions、
EventDataDataTaskContentTaskActionsContext、EventDataDataTaskContentTaskActionsExec、
EventDataDataTaskContentTaskActionsExecCommand、EventDataDataOldTargetUserName、
EventDataDataNewTargetUserName、EventDataDataDeviceId、EventDataDataDeviceDescription、
EventDataDataClassId、EventDataDataClassName、EventDataDataVendorIds、
EventDataDataCompatibleIds、EventDataDataLocationInformation、EventDataDataAccountName、
EventDataDataAccountDomain、EventDataDataLogonID、EventDataDataSessionName、
EventDataDataClientName、EventDataDataClientAddress、EventDataDataMajorVersion、
EventDataDataMinorVersion、EventDataDataBuildVersion、EventDataDataQfeVersion、
EventDataDataServiceVersion、EventDataDataBootMode、EventDataDataStartTime、
EventDataDataOldRemark、EventDataDataNewRemark、EventDataDataOldMaxUsers、
EventDataDataNewMaxUsers、EventDataDataOldShareFlags、EventDataDataNewShareFlags、
EventDataDataOldSD、EventDataDataNewSD、EventDataDataTreeDelete、EventDataDataPuaCount、
EventDataDataPuaPolicyId、EventDataDataResourceAttributes、
EventDataDataModifiedObjectProperties、EventDataDataDisplayName、EventDataDataDnsHostName、
EventDataDataServicePrincipalNames、EventDataDataAttributeSyntaxOID、EventDataDataDummy、
EventDataDataComputerAccountChange、EventDataDataMessageNumber、

EventDataDataMessageTotal、EventDataDataScriptBlockText、EventDataDataScriptBlockId、EventDataDataPath、EventDataDataImagePath、EventDataDataStartType、EventDataDataAppName、EventDataDataAppVersion、EventDataDataTerminationTime、EventDataDataExeFileName、EventDataDataReportId、EventDataDataPackageFullName、EventDataDataPackageRelativeAppId、EventDataDataHangType、EventDataDataAccessReason、EventDataDataTargetServerName、EventDataDataTargetInfo、EventDataDataTargetProcessId、EventDataDataTargetProcessName、EventDataDataKerberosPolicyChange、EventDataDataSubcategoryId、EventDataBinary。

Central Node 和 Kaspersky Endpoint Security for Linux

如果用户计算机上发生事件，则应用程序向事件数据库发送以下数据：

1. 文件修改事件。
   - 有关创建文件的进程的信息：进程文件名、进程文件的 MD5 哈希和 SHA256 哈希。
   - 有关创建或修改的文件的信息：名称、路径、全名、类型、MD5 哈希、SHA256 哈希、创建日期、修改日期、属性、属性修改日期、大小、区域 ID、文件的应用程序名称、供应商、颁发数字证书的组织名称、描述、数字签名验证结果、数字签名的时间、原始名称、修改前的名称、修改前的路径、修改前的全名。
   - 有关创建链接的文件的信息：MD5 哈希、SHA256 哈希、创建日期、修改日期、属性、属性修改日期、大小、类型、区域 ID、文件的应用程序名称、原始名称、颁发数字证书的组织名称、描述、签名的主题、数字签名验证结果、数字签名的时间、链接文件的全名。
   - 文件类型。
   - 所有者 ID。
   - 所有者组 ID。
   - 所有者用户名。
   - 所有者组名称。
   - 从其检索文件的 URL。
   - 从中检索文件的消息的元数据。
   - 请求的访问标志。
   - 重启后文件删除的指示。
   - 文件访问标志。
2. 操作系统日志中的事件。
   - 事件时间。
   - 事件类型。
   - 活动名称。

- 操作结果。
- 有关父进程的信息：文件路径、进程文件的 UniquePID、MD5 或 SHA256 哈希、用于启动进程的命令。

3. 进程启动事件。

   有关父进程和祖进程、加载器进程、创建者进程、正在运行的进程的文件的信息：名称、路径、全名、MD5 哈希、SHA256 哈希、创建日期和时间、修改日期和时间、属性、属性修改日期和时间、大小、区域 ID、供应商、颁发数字证书的组织名称、描述、原始名称、数字签名主题、数字签名验证结果、数字签名的日期和时间、文件版本、登录类型、登录会话 ID、用户账户类型、用户名、用户账户 ID、登录计算机的 IP 地址、完整性级别、进程 ID、当前目录、所有者 ID、所有者组 ID、所有者用户名、所有者组名称、真实用户名、真实组名称、有效组名称、有效用户名、文件访问权限标志、下载文件的 URL、获取文件的消息的元数据、进程环境变量、命令行选项、进程类型。

4. 进程停止事件。

   - 有关进程的文件的信息：文件名、文件路径、文件全名、文件的 MD5 哈希和 SHA256 哈希、文件大小以及进程结束时间。
   - UniquePID。
   - 进程启动选项。
   - 有关父进程的信息：文件路径、进程文件的 UniquePID、MD5 或 SHA256 哈希值、进程启动选项。

5. 检测事件及其处理结果。

   - 扫描结果。
   - 检测到的对象的名称。
   - 应用程序数据库中记录的 ID。
   - 用于生成检测的应用程序数据库的发布时间。
   - 对象处理模式。
   - 检测到的对象的类别（例如，病毒的名称）。
   - 检测到的对象的 MD5 哈希。
   - 检测到的对象的 SHA256 哈希。
   - 进程的唯一 ID。
   - 进程的 PID。
   - 进程启动命令行。
   - 处理对象时出错的原因。

6. DNS 查找事件。

   - DNS 服务器的 IPv4 地址。
   - 正在执行的 DNS 查询的二进制掩码。

- DNS 响应错误代码。
- DNS 查询类型 ID。
- 要解析 DNS 记录的域名。
- DNS 响应的日期。

7. 代码注入事件。

- 有关接收方进程的信息：应用程序名称、应用程序完整名称、应用程序路径、文件的 MD5 哈希值、文件的 SHA256 哈希值、下载文件的 URL、附加下载的文件的消息的元数据、应用程序的唯一 ID、应用程序的系统 ID、命令行、进程 DLL 的名称、进程 DLL 的路径、进程在地址空间中的地址。
- 注入方法。
- 修改的进程的命令行。
- 系统调用参数。
- 拦截注入相关函数时的 API 调用堆栈。

Central Node 和 Kaspersky Endpoint Security for Mac

如果用户计算机上发生事件，则应用程序向事件数据库发送以下数据：

1. 文件创建事件。

- 有关创建文件的进程的信息：进程文件名、进程文件的 MD5 哈希和 SHA256 哈希。
- 文件名。
- 文件路径。
- 文件全名。
- 文件类型。
- 文件的 MD5 哈希和 SHA256 哈希。
- 文件创建和修改日期。
- 文件大小。

2. 进程启动事件。

有关父进程和祖进程、加载器进程、创建者进程、正在运行的进程的文件的信息：名称、路径、全名、MD5 哈希、SHA256 哈希、创建日期和时间、修改日期和时间、属性、属性修改日期和时间、大小、区域 ID、供应商、颁发数字证书的组织名称、描述、原始名称、数字签名主题、数字签名验证结果、数字签名的日期和时间、文件版本、登录类型、登录会话 ID、用户账户类型、用户名、用户账户 ID、登录计算机的 IP 地址、完整性级别、进程 ID、当前目录、所有者 ID、所有者组 ID、所有者用户名、所有者组名称、真实用户名、真实组名称、有效组名称、有效用户名、文件访问权限标志、下载文件的 URL、获取文件的消息的元数据、进程环境变量、命令行选项、进程类型。

3. 进程停止事件。

   - 有关进程的文件的信息：文件名、文件路径、文件全名、文件的 MD5 哈希和 SHA256 哈希、文件大小以及进程结束时间。
   - UniquePID。
   - 进程启动选项。
   - 有关父进程的信息：文件路径、进程文件的 UniquePID、MD5 或 SHA256 哈希值、进程启动选项。

4. 威胁检测事件和检测处理结果。

   - 扫描结果。
   - 检测到的对象的名称。
   - 应用程序数据库中记录的 ID。
   - 用于生成检测的应用程序数据库的发布时间。
   - 对象处理模式。
   - 检测到的对象的类别（例如，病毒的名称）。
   - 检测到的对象的 MD5 哈希。
   - 检测到的对象的 SHA256 哈希。
   - 进程的唯一 ID。
   - 进程的 PID。
   - 进程启动命令行。
   - 处理对象时出错的原因。

Central Node 和 Sandbox

Central Node 组件向 Sandbox 组件发送文件以及从网络和邮件流量中提取的 URL。在发送前，文件不会做任何形式的改动。Sandbox 组件将扫描结果发送至 Central Node 组件。

Central Node 和 Sensor

该应用程序可以在 Central Node 和 Sensor 组件之间传输以下数据：

- 文件和电子邮件。
- 入侵检测系统和URL信誉技术生成的警报数据。

- 授权许可信息。
- 被从扫描中排除的数据列表。
- 如果已配置与代理服务器的集成，则端点 Sensor 应用程序的数据。
- 如果已配置从 Central Node 组件接收数据库更新，则为应用程序数据库。

具有 PCN 和 SCN 角色的服务器

如果应用程序在分布式解决方案模式下运行，则在 PCN 和连接的 SCN 之间传输以下相关数据：

- 警报。
- 事件。
- 任务数据。
- 策略数据。
- 使用 IOC、TAA (IOA)、IDS、YARA 用户规则扫描的数据。
- 存储中的文件数据。
- 关于用户账户的数据。
- 关于授权许可。
- 具有 Endpoint Agent 组件的计算机列表。
- 放在存储中的对象。
- 在具有 Endpoint Agent 组件的计算机上被隔离的对象。
- 附加到警报的文件。
- IOC 和 YARA 文件。

应用程序跟踪文件中包含的数据

Kaspersky Anti Targeted Attack Platform 资源不提供限制安装 Central Node 组件的服务器和操作系统用户权限的功能。建议管理员根据自己的判断使用任何系统资源来控制如何允许安装了应用程序的服务器和操作系统的用户访问其他用户的个人数据。

跟踪文件可包括用户的任何个人数据或组织的机密数据。文件无限期地存储在 `/var/log/kaspersky` 目录中。

Kaspersky Endpoint Agent for Windows 的数据

您可以在应用程序的在线帮助中查看有关本地存储和处理的 Kaspersky Endpoint Agent 数据的详细信息:

- 发送至 KATA Central Node 组件的请求中的数据。
- 服务数据。
- 跟踪文件和转储文件中包含的数据。
- 有关接受 KSN 声明的信息。
- Windows 事件日志事件数据。

从 Central Node 组件接收的数据

Kaspersky Endpoint Agent 将从 Central Node 组件接收的设置值保存在计算机的硬盘上。数据以打开的非加密形式保存在文件夹`C:\ProgramData\Kaspersky Lab\Endpoint Agent\protected\data`中。

启用自我防御时，默认情况下，只有具有系统和管理员权限的用户在启用自我防御时才具有对文件的读访问权限。禁用自我防御时，具有系统和管理员权限的用户还可以删除文件、修改其内容并修改对其的访问权限。Kaspersky Endpoint Agent 应用程序不管理对此文件夹或其中任何文件的访问权限。这是决定访问权限的系统管理员。

删除 Kaspersky Endpoint Agent 时，数据也会被删除。

从 Central Node 组件接收的数据可能包含以下信息:

- 关于网络连接的数据。
- 关于安装在具有 Central Node 组件的计算机上的操作系统的数据。
- 关于操作系统用户账户的数据。
- 关于操作系统中用户会话的数据。
- 关于 Windows 事件日志的数据。
- 关于RT_VERSION资源。
- 关于PE文件的内容。
- 关于操作系统服务。
- 具有 Central Node 组件的服务器的证书。
- 访问过的网站的URL和 IP 地址。
- HTTP Referrer 标头。

- 计算机名称。
- MD5 哈希文件。
- 具有 Kaspersky Endpoint Agent 的计算机的唯一 ID。
- Windows 注册表项的名称和值。
- Windows 注册表项路径。
- Windows 注册表变量名称。
- 本地 DNS 缓存条目的名称。
- 来自 IPv4 格式的本地 DNS 缓存条目标地址。
- 来自本地 DNS 缓存的请求主机的 IP 地址或名称。
- 本地 DNS 缓存元素的主机。
- 本地 DNS 缓存元素的域名。
- IPv4 格式的 ARP 缓存元素的地址。
- ARP 缓存元素的物理地址。
- 逻辑驱动器的序列号。
- 本地用户的主文件夹。
- 启动进程的用户账户名称。
- 用户登录系统时运行的脚本的路径。
- 发生事件的用户账户的名称。
- 发生事件的计算机的名称。
- 具有 Kaspersky Endpoint Agent 的计算机上文件的完整路径。
- 具有 Kaspersky Endpoint Agent 的计算机上的文件名称。
- 具有 Kaspersky Endpoint Agent 的计算机上的文件掩码。
- 具有 Kaspersky Endpoint Agent 的计算机上的文件文件夹全称。
- 文件发布者的注释。
- 进程文件镜像的掩码。
- 打开了端口的进程文件镜像的路径。
- 打开端口的进程的名称。
- 端口的本地 IP 地址。

- 可执行模块的数字签名的可信公钥。
- 进程名称。
- 进程段名称。
- 命令行参数。

检测与事件中的数据

事件数据以二进制并且开放未加密的形式保存在 `C:\ProgramData\Kaspersky Lab\Endpoint Agent\protected\kata`文件夹中。

事件数据可以包含与以下内容相关的信息：

- 关于可执行模块的数据。
- 关于网络连接的数据。
- 关于安装在具有 Kaspersky Endpoint Agent 的计算机上的操作系统。
- 关于操作系统中用户会话的数据。
- 关于操作系统用户账户的数据。
- 关于 Windows 事件日志的数据。
- 关于 Kaspersky Endpoint Security for Windows 的警报。
- 关于活动目录的组织单位 (OU)。
- HTTP Referrer 标头。
- 计算机的完全合格域名。
- 文件及其片段的 MD5 哈希和 SHA256 哈希。
- 具有 Kaspersky Endpoint Agent 的计算机的唯一 ID。
- 证书的唯一 ID。
- 证书出版商。
- 证书主题。
- 用于生成证书指纹的算法的名称。
- 本地网络接口的地址和端口。
- 远程网络接口的地址和端口。
- 应用程序供应商。

- 应用程序名称。
- Windows 注册表变量名称。
- Windows 注册表项路径。
- Windows 注册表变量数据。
- 检测到的对象的名称。
- Kaspersky Security Center 网络代理 ID。
- hosts文件的内容。
- 进程启动命令行。

任务完成报告中包含的数据

在被发送至 Central Node 组件前，报告和相关文件被暂时保存在具有 Kaspersky Endpoint Agent 应用程序的计算机的硬盘上。任务完成报告以非加密存档的形式保存在 C:\ProgramData\Kaspersky Lab\Endpoint Agent\protected\kata\data_queue 文件夹里。

启用自我防御时，默认情况下，只有具有系统和管理员权限的用户在启用自我防御时才具有对文件的读访问权限。禁用自我防御时，具有系统和管理员权限的用户还可以删除文件、修改其内容并修改对其的访问权限。Kaspersky Endpoint Agent 应用程序不管理对此文件夹或其中任何文件的访问权限。这是决定访问权限的系统管理员。

任务完成报告包含以下信息：

- 关于任务输出的数据。
- 关于可执行模块的数据。
- 关于操作程序进程的数据。
- 关于用户账户的数据。
- 关于用户会话的数据。
- 计算机的完全合格域名。
- 具有 Kaspersky Endpoint Agent 的计算机的唯一 ID。
- 具有 Kaspersky Endpoint Agent 的计算机的文件。
- NTFS备用流的名称。
- 具有 Kaspersky Endpoint Agent 的计算机上文件的完整路径。
- 具有 Kaspersky Endpoint Agent 的计算机上的文件文件夹全称。

- 进程标准输出的内容。
- 进程标准错误流的内容。

安装日志中包含的数据

在使用命令行安装期间，管理员可以启用 Kaspersky Endpoint Agent 安装日志（使用 msiexec 标准流程）。管理员显示将保存安装日志的文件的路径。

日志记录了安装进程步骤以及包含托管 Central Node 组件的服务器地址和安装日志文件路径的 msiexec 命令行。

阻止启动的文件数据

被阻止启动的文件数据以打开的非加密形式存储在 C:\ProgramData\Kaspersky Lab\Endpoint Agent\protected\kata 文件夹中。

启用自我防御时，默认情况下，只有具有系统和管理员权限的用户在启用自我防御时才具有对文件的读访问权限。禁用自我防御时，具有系统和管理员权限的用户还可以删除文件、修改其内容并修改对其的访问权限。Kaspersky Endpoint Agent 应用程序不管理对此文件夹或其中任何文件的访问权限。这是决定访问权限的系统管理员。

阻止启动的文件数据可能包含以下信息：

- 被阻止文件的完整路径。
- 文件的 MD5 哈希。
- 文件的 SHA256 哈希。
- 进程启动命令。

与任务执行有关的数据

执行将文件放入隔离区的任务时，包含此文件的存档会临时保存在以下一个文件夹中：

- C:\ProgramData\Kaspersky Lab\Endpoint Agent\protected\kata\temp Kaspersky Endpoint Security 的一部分安装的 Kaspersky Endpoint Agent 的临时文件。
- C:\ProgramData\Kaspersky Lab\Endpoint Agent\protected\data\kata\temp Kaspersky Anti Targeted Attack Platform 分发包安装的 Kaspersky Endpoint Agent 的临时文件。

在主机上执行应用程序运行任务时，Kaspersky Endpoint Agent 会以未加密的明文形式在本地存储标准输出流的内容和正在运行的进程的错误，直到任务完成报告被发送到 Central Node 组件。文件存储在以下文件夹之一：

- `C:\ProgramData\Kaspersky Lab\Endpoint Agent\protected\kata\temp` Kaspersky Endpoint Security 的一部分安装的 Kaspersky Endpoint Agent 的临时文件。
- `C:\ProgramData\Kaspersky Lab\Endpoint Agent\protected\data\kata\temp` Kaspersky Anti Targeted Attack Platform 分发包安装的 Kaspersky Endpoint Agent 的临时文件。

启用自我防御时，默认情况下，只有具有系统和管理员权限的用户在启用自我防御时才具有对文件的读访问权限。禁用自我防御时，具有系统和管理员权限的用户还可以删除文件、修改其内容并修改对其的访问权限。Kaspersky Endpoint Agent 应用程序不管理对此文件夹或其中任何文件的访问权限。这是决定访问权限的系统管理员。

Kaspersky Endpoint Security for Windows 数据

有关 Kaspersky Endpoint Security 传输的数据的详细信息，请参阅应用程序的在线帮助：

- 根据最终用户授权许可协议提供数据。
- 使用卡巴斯基安全网络时提供数据。
- 遵守欧盟法律 (GDPR)。
- 使用“检测和响应” → “Kaspersky Anti Targeted Attack Platform (EDR)”解决方案时的提供数据。

Kaspersky Endpoint Security for Linux 数据

有关 Kaspersky Endpoint Security 传输的数据的详细信息，请参阅应用程序的在线帮助。

Kaspersky Endpoint Security for Mac 数据

有关 Kaspersky Endpoint Security 传输的数据的详细信息，请参阅应用程序的在线帮助。

应用程序许可

本节介绍 Kaspersky Anti Targeted Attack Platform 许可的主要方面。

关于最终用户授权许可协议

*最终用户授权许可协议 (EULA)*是用户与 AO Kaspersky Lab 之间的绑定协议，其规定了用户使用该应用程序的条款。

在开始使用该应用程序之前，请仔细阅读最终用户授权许可协议的条款。

您可以通过以下方式查看最终用户授权许可协议 (EULA) 的条款：

- 安装 Kaspersky Anti Targeted Attack Platform 的过程中。
- 通过阅读名为/EULA/License.<language>的文本。
  此文件包含在应用程序分发包中。
- 在应用程序 Web 界面的**设置**部分的**授权许可**子部分，单击 **授权许可协议**按钮。
- 在 Sandbox 组件的 Web 界面中，在 菜单中单击**最终用户授权许可协议**链接。

在安装应用程序时确认您同意最终用户授权许可协议，即表示您接受最终用户授权许可协议 (EULA) 的条款。如果您不接受最终用户授权许可协议的条款，则必须中止应用程序安装并且不得使用该应用程序。

关于授权授权许可书

*授权许可证书*是提供有密钥文件或激活码的一个文档。

授权许可证书包含以下授权许可信息：

- 授权许可 ID 或订单号
- 授权许可持有人的详细信息。
- 有关可以使用授权许可激活的应用程序的信息。
- 授权许可设备（可根据授权许可使用该应用程序的设备）数量限制。
- 授权许可开始日期。
- 授权许可到期日期或授权许可有效期。
- 授权许可类型。

关于授权许可

*授权许可*是根据最终用户授权许可协议 (EULA) 的条款和条件授予的使用 Kaspersky Anti Targeted Attack Platform 的有限时间权利。

服务范围和应用程序使用条款取决于用于激活该应用程序的授权许可的类型。

Kaspersky Anti Targeted Attack Platform 提供以下几种授权许可类型：

- NFR（不得转售）是固定期限内的免费授权许可，旨在让用户熟悉应用程序并执行测试部署。
- 商用版 — 购买应用程序时提供的付费授权许可。

授权许可到期后，应用程序将继续工作，但功能有限。您必须购买商用版授权许可或续订商业版授权许可才能使用该应用程序的所有功能。

我们建议您最迟在授权许可到期日之前续费授权许可，以免中断您的设备对计算机安全威胁的防护。

更新功能（包括反病毒签名更新和代码库更新）可能无法在美国境内使用。

在当前版本的 Kaspersky Anti Targeted Attack Platform 中，应用程序的可用功能还取决于添加的授权许可密钥的类型。

关于授权许可密钥

*授权许可密钥*是根据最终用户授权许可协议来激活并使用应用程序的一串序列。授权许可密钥由卡巴斯基生成。

您可以通过应用*密钥文件*或输入*激活码*向应用程序添加授权许可密钥。将授权许可密钥添加到应用程序后，它将作为唯一的字母数字序列显示在应用程序界面中。

卡巴斯基可以阻止违反最终用户授权许可协议的授权许可密钥。如果授权许可密钥已被阻止，您必须添加不同的授权许可密钥才能使用该应用程序。

在当前版本的 Kaspersky Anti Targeted Attack Platform 中，应用程序的可用功能取决于添加的授权许可密钥的类型：

- **KATA+NDR 和 KEDR 授权许可密钥**。应用程序的完整功能。
- **KEDR 授权许可密钥**。接收和处理来自网络流量和邮件流量的数据有限制。
- **KATA+NDR 授权许可密钥**。Web 界面部分**威胁搜索**、**任务**、**防止**、**自定义规则**、**存储**和**资产**的功能受限。
- **KATA 授权许可密钥**。Web 界面的**威胁搜索**、**任务**、**防止**、**自定义规则**、**存储**、**资产**部分中的功能受到限制，**SPAN 流量处理**部分中的保存和下载网络流量功能受到限制。

关于密钥文件

*密钥文件*是您从卡巴斯基接收的带 .key 扩展名的文件。密钥文件旨在通过添加授权许可密钥来激活应用程序。

密钥文件将发送到您在购买 Kaspersky Anti Targeted Attack Platform 或订购具有 NFR 授权许可类型的 Kaspersky Anti Targeted Attack Platform 后指定的电子邮件地址。

您无需连接到卡巴斯基激活服务器即可通过密钥文件激活应用程序。

如果不小心删除了密钥文件您可以将其恢复。您可能需要密钥文件才能注册 Kaspersky CompanyAccount。

要恢复密钥文件，您必须执行以下操作之一：

- 联系您购买授权许可的供应商。
- 在卡巴斯基网站上使用您的激活码获取密钥文件。

关于激活码

*激活码*是二十个拉丁字符和数字的唯一序列。您输入激活码来添加激活 Kaspersky Anti Targeted Attack Platform 的授权许可密钥。激活码将发送到您在购买 Kaspersky Anti Targeted Attack Platform 或订购具有 NFR 授权许可类型的 Kaspersky Anti Targeted Attack Platform 后指定的电子邮件地址。

要使用激活码激活应用程序，您需要访问互联网以连接到卡巴斯基激活服务器。

如果您在激活应用程序后丢失了激活码，请联系您购买授权许可的卡巴斯基合作伙伴。

关于订阅

*Kaspersky Anti Targeted Attack Platform 订阅*是在所选参数（订阅到期日期、受保护设备数量）下使用解决方案的订单。

订阅是有限制的（例如一年）。要在有限订阅到期后继续使用 Kaspersky Anti Targeted Attack Platform，您必须续费订阅。如果没有续订，Kaspersky Anti Targeted Attack Platform 将继续以有限功能模式运行。

要在订阅下使用 Kaspersky Anti Targeted Attack Platform，您必须输入激活码。应用激活码后，将添加一个授权许可密钥，该密钥决定了在订阅下使用该应用程序的授权许可。有关授权许可密钥的信息显示在Central Node 服务器的 Web 界面上。

通过订阅购买的激活码不能用于激活 Kaspersky Anti Targeted Attack Platform 的先前版本。

添加授权许可密钥

在分布式解决方案模式下，只能在 PCN 服务器上替换密钥。

您可以通过以下方式之一将授权许可密钥添加到 Kaspersky Anti Targeted Attack Platform：

- 输入激活码。
- 上传密钥文件。

要使用激活码将授权许可密钥添加到 Kaspersky Anti Targeted Attack Platform：

1. 在应用程序 Web 界面窗口中，选择**设置**部分的**授权许可**子部分。
2. 在您想要激活的以下功能块部分，点击**输入激活码**：KATA/NDR 或 KEDR。
   这将打开激活窗口。
3. 在该字段中，输入发送到您提供的电子邮件地址的激活码。
4. 仔细阅读卡巴斯基安全网络声明并选择如下选项之一：
   - **我同意参与 KSN**，如果您接受 KSN 声明的条款并希望参与 KSN。
   - **我不同意参与 KSN**，如果您不接受 KSN 声明的条款并且不想参与 KSN。

     如果您不同意声明条款，将不会启用卡巴斯基安全网络。
5. 单击**应用**。

   授权许可密钥被添加到应用程序中。

要使用密钥文件将授权许可密钥添加到 Kaspersky Anti Targeted Attack Platform：

1. 在应用程序 Web 界面窗口中，选择**设置**部分的**授权许可**子部分。
2. 在您想要激活的以下功能块部分，点击**上传密钥文件**：KATA/NDR 或 KEDR。
   这将打开激活窗口。
3. 单击**上传**。
   这将打开文件选择窗口。
4. 选择要下载的密钥文件，然后单击**打开**按钮。
   这将关闭文件选择窗口。

5. 仔细阅读卡巴斯基安全网络声明并选择如下选项之一：

- **我同意参与 KSN**，如果您接受 KSN 声明的条款并希望参与 KSN。
- **我不同意参与 KSN**，如果您不接受 KSN 声明的条款并且不想参与 KSN。

> 如果您不同意声明条款，将不会启用卡巴斯基安全网络。

6. 单击**应用**。

授权许可密钥被添加到应用程序中。

替换授权许可密钥

> 在分布式解决方案模式下，只能在 PCN 服务器上替换密钥。

您可以通过以下方式之一将 Kaspersky Anti Targeted Attack Platform 的授权许可密钥替换为不同的授权许可密钥：

- 用激活码替换。
- 用密钥文件替换。

通过输入激活码替换 Kaspersky Anti Targeted Attack Platform 的当前授权许可密钥：

1. 在应用程序 Web 界面窗口中，选择**设置**部分的**授权许可**子部分。
2. 在您想要激活的以下功能块部分，点击**替换**：KATA/NDR 或 KEDR。在显示的下拉列表中，选择**使用激活码替换**。

   这将打开授权许可密钥替换窗口。
3. 在该字段中，输入发送到您提供的电子邮件地址的激活码。
4. 仔细阅读卡巴斯基安全网络声明并选择如下选项之一：

- **我同意参与 KSN**，如果您接受 KSN 声明的条款并希望参与 KSN。
- **我不同意参与 KSN**，如果您不接受 KSN 声明的条款并且不想参与 KSN。

> 如果您不同意声明条款，将不会启用卡巴斯基安全网络。

5. 单击**应用**。

授权许可密钥已替换。

要使用密钥文件将授权许可密钥添加到 Kaspersky Anti Targeted Attack Platform：

1. 在应用程序 Web 界面窗口中，选择**设置**部分的**授权许可**子部分。
2. 在您想要激活的以下功能块部分，点击**替换**：KATA/NDR 或 KEDR。在显示的下拉列表中，选择**使用密钥文件替换**。
   这将打开授权许可密钥替换窗口。
3. 单击**上传**。
   这将打开文件选择窗口。
4. 选择要下载的密钥文件，然后单击**打开**按钮。
   这将关闭文件选择窗口。
5. 仔细阅读卡巴斯基安全网络声明并选择如下选项之一：
   - **我同意参与 KSN**，如果您接受 KSN 声明的条款并希望参与 KSN。
   - **我不同意参与 KSN**，如果您不接受 KSN 声明的条款并且不想参与 KSN。

     如果您不同意声明条款，将不会启用卡巴斯基安全网络。
6. 单击**应用**。

授权许可密钥已替换。

删除授权许可密钥

在分布式解决方案模式下，只能在 PCN 服务器上移除授权许可密钥。

您可以删除已添加到 Kaspersky Anti Targeted Attack Platform 的授权许可密钥。删除授权许可密钥后，应用程序将进入有限功能模式。

要移除授权许可密钥：

1. 在应用程序 Web 界面窗口中，选择**设置**部分的**授权许可**子部分。
2. 在您要删除其授权许可密钥的以下功能块部分中，点击**删除**：KATA/NDR 或 KEDR。
   这将打开授权许可密钥删除确认窗口。
3. 单击**是**。
   密钥移除确认窗口关闭。

授权许可密钥已删除。

在 Central Node 的 Web 界面中查看有关添加的授权许可密钥的信息

在分布式解决方案和多租户模式下，您可以在管理员或应用程序 Web 界面用户的账户下，在 PCN 服务器和所有连接的 SCN 的 Web 界面中查看有关授权许可和添加的密钥的信息。

要查看有关添加的授权许可密钥的信息，

在 Central Node 服务器的 Web 界面中，选择**设置**部分，**授权许可**子部分。

Web 界面将显示有关 KATA/NDR 授权许可密钥的以下信息：

- **序列号**。
- **功能集**。
- **激活日期**。
- **到期日期**。
- **剩余天数**。

Web 界面将显示有关 KEDR 授权许可密钥的以下信息：

- **序列号**。
- **激活日期**。
- **到期日期**。
- **剩余天数**。

在授权许可到期的30天内，**控制板** 部分显示有关续订授权许可的通知。对于所有用户，无论其角色如何，该通知都将显示在具有 Central Node 组件的所有服务器上（在分布式解决方案和多租户模式下 — 在 PCN 和所有连接的 SCN 上）。

在 Central Node 的 Web 界面中查看最终用户授权许可协议的文本

在分布式解决方案和多租户模式下，您可以在本地管理员、管理员或应用程序 Web 界面用户帐户下的 PCN 服务器和所有连接的 SCN 的 Web 界面中查看最终用户授权许可协议的文本。

要查看最终用户授权许可协议的文本，请在托管 Central Node 组件的服务器的 Web 界面中执行以下步骤：

1. 选择**设置**部分的**授权许可**子部分。
2. 单击工作区右上角的**授权许可协议**按钮。

3. 在打开的窗口中，仔细阅读最终用户授权许可协议的文本。

4. 完成后，单击**关闭**按钮。

在 Central Node 的 Web 界面中查看隐私政策文本

在分布式解决方案和多租户模式下，您可以在本地管理员、管理员或应用程序 Web 界面用户账户下的 PCN 服务器和所有连接的 SCN 的 Web 界面中查看隐私政策文本。

要查看隐私政策的文本，请在托管 Central Node 组件的服务器的 Web 界面中执行以下步骤：

1. 选择**设置**部分的**授权许可**子部分。

2. 单击工作区右上角的**隐私策略**按钮。

3. 在打开的窗口中，仔细阅读隐私政策的文本。

4. 完成后，单击**关闭**按钮。

查看应用程序中使用的第三方代码的信息

在分布式解决方案和多租户模式下，您可以在本地管理员、管理员或应用程序 Web 用户账户下的 PCN 服务器和所有连接的 SCN 的 Web 界面中查看 Kaspersky Anti Targeted Attack Platform 中使用的第三方代码的信息。

要查看有关第三方代码的信息，请在托管 Central Node 组件的服务器的 Web 界面中执行以下步骤：

1. 选择**设置**部分的**授权许可**子部分。

2. 单击工作区右上角的**第三方代码**按钮。

3. 在打开的窗口中，查看第三方代码的信息。

4. 完成后，单击**关闭**按钮。

在 Sandbox 的 Web 界面中查看最终用户授权许可协议的文本

要在 Sandbox 服务器的 Web 界面中查看最终用户授权许可协议的文本：

1. 使用您在安装 Sandbox 组件期间指定的帐户凭据登录到 Sandbox Web 界面。

2. 单击Web 界面窗口左下角的按钮。

3. 这将打开一个窗口，其中包含有关 Sandbox 组件的信息。

4. 单击**最终用户授权许可协议**链接可打开包含应用程序最终用户授权许可协议文本的窗口。

5. 仔细阅读最终用户授权许可协议文本。

6. 完成后，单击×按钮。

查看 Endpoint Agent 组件的最终用户授权许可协议文本

您可以查看被用作 Endpoint Agent 组件的应用程序的最终用户授权许可协议文本。有关如何查看最终用户授权许可协议文本的详细信息，请参阅相关应用程序的在线帮助。

关于 Kaspersky Endpoint Agent for Windows 最终用户授权许可协议

关于 Kaspersky Endpoint Security for Windows 最终用户授权许可协议

关于 Kaspersky Endpoint Security for Linux 最终用户授权许可协议

关于 Kaspersky Endpoint Security for Mac 最终用户授权许可协议

基于授权许可的应用程序模式

Kaspersky Anti Targeted Attack Platform 根据添加的授权许可密钥提供不同的操作模式。

未授权

安装应用程序并启动 Web 界面后，应用程序将在此模式下运行，直到您添加授权许可密钥。

未授权许可的模式具有以下限制：

- 应用程序数据库未更新。
- 没有与卡巴斯基安全网络知识库的连接。
- 接收和处理来自网络流量和邮件流量的数据有限制。
- Web 界面部分**威胁搜索**、**任务**、**防止**、**自定义规则**、**存储**和**资产**的功能受限。

商业的

要切换到商业模式，您必须替换授权许可密钥或为商业授权许可添加新的授权许可密钥。

在此模式下，应用程序：

- 更新数据库。
- 连接到卡巴斯基安全网络知识库。

Kaspersky Anti Targeted Attack Platform 当前版本中未授权模式的其他限制的删除取决于所添加的授权许可密钥的类型：

- **KATA+NDR 和 KEDR 授权许可密钥**。应用程序的完整功能。
- **KEDR 授权许可密钥**。接收和处理来自网络流量和邮件流量的数据有限制。
- **KATA+NDR 授权许可密钥**。Web 界面部分**威胁搜索**、**任务**、**防止**、**自定义规则**、**存储**和**资产**的功能受限。
- **KATA 授权许可密钥**。Web 界面的**威胁搜索**、**任务**、**防止**、**自定义规则**、**存储**、**资产**部分中的功能受到限制，**SPAN 流量处理**部分中的保存和下载网络流量功能受到限制。

应用程序架构

应用程序包含以下主要组件：

- *Sensor*。接收和扫描数据，也可以作为在 Endpoint Agent 和 Central Node 之间进行数据交换时的代理服务器。
- *Central Node*。接收和扫描数据、分析对象的行为，并将分析结果发布到应用程序的 Web 界面上。
- *Sandbox*。启动操作系统的虚拟镜像。在这些操作系统中启动文件并跟踪每个操作系统中文件的行为，以检测恶意活动以及针对企业 IT 基础架构的针对性攻击的迹象。
- *Endpoint Agent*。安装在组织 IT 基础架构中的工作站和服务器上。持续监控在这些计算机上运行的进程、活动的网络连接和被修改的文件。

Sensor 组件

该组件可以与 Central Node（嵌入式 Sensor）部署在同一台服务器上，也可以部署在独立的服务器上。

Kaspersky Anti Targeted Attack Platform 的以下模块在每一台 Sensor 服务器上运行：

- *Sensor*。从网络和邮件流量接收数据，并将数据发送到具有 Central Node 组件的服务器进行处理。
- *入侵检测系统*（以下也称为 *IDS*）。扫描 Internet 流量是否存在入侵企业 IT 基础构架的迹象。
- *KSN*。代表 Kaspersky Anti Targeted Attack Platform 检查在卡巴斯基安全网络知识库中的文件和 URL 地址的信誉，并提供有关网站类别的信息（例如，恶意网站、钓鱼网站）。

  卡巴斯基安全网络（以下也称为 *"KSN"*）是一个在线服务的基础架构，提供对卡巴斯基在线知识库的访问，该知识库中包含了有关文件信誉、网站资源和软件的信息。使用来自卡巴斯基安全网络的数据可确保卡巴斯基应用程序能够更快地响应威胁，提高某些保护组件的性能，并降低误报的可能性。

  如果您不想参与 KSN，可以使用*卡巴斯基私人安全网络*（以下也称为"*KPSN*"）。KPSN 是一个允许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，而不从他们自己的计算机实际发送数据到卡巴斯基安全网络的解决方案。

- *URL 信誉*。检测恶意和钓鱼 URL 地址，以及过去黑客在针对性攻击和入侵企业 IT 基础构架时使用的 URL 地址。

在 Sensor 角色中，您还可以使用邮件传感器，它是安装了 Kaspersky Secure Mail Gateway (KSMG) 或 Kaspersky Security for Linux Mail Server (KLMS) 的服务器或虚拟机。这些应用程序将电子邮件发送到 Kaspersky Anti Targeted Attack Platform 进行处理。基于 Kaspersky Anti Targeted Attack Platform 中的电子邮件处理结果，KSMG 和 KLMS 可能会阻止邮件的传输。

Sensor 还可用作来自 Endpoint Agent 组件的传出连接的代理服务器。

如果 KSMG 或 KLMS 是在 Sensor 角色中使用，为邮件收件人配置的扫描排除项名单和文件的 MD5 校验和不会传输到 KSMG 或 KLMS，在邮件由 KSMG 和 KLMS 处理时不应用。

Central Node 组件

该组件可以部署在一台服务器上或部署为一个高可用性集群，该集群含 2 个角色：存储服务器和处理服务器。

高可用性通过存储服务器之间的数据复制和计算资源冗余来实现：如果一台服务器发生故障，其功能将由另一台具有相同角色的服务器执行。与此同时，Kaspersky Anti Targeted Attack Platform 继续工作。

集群中仅允许一台服务器发生故障。如果多台服务器发生故障，集群将无法运行。

以下应用程序模块、内核和技术在具有 Central Node 组件的每个服务器或集群上运行：

- *反恶意软件引擎*（以下也称为 *AM* 或者 *AM 引擎*）。使用反病毒数据库扫描文件和对象以查找企业 IT 基础架构中的病毒和其他威胁。
- *移动攻击分析器*（也称为*MAA*）。使用机器学习技术扫描云基础架构中 APK 格式的可执行文件。扫描的结果是，Kaspersky Anti Targeted Attack Platform 会收到有关检测到的威胁或不存在威胁的信息。
- *YARA*。使用由 Kaspersky Anti Targeted Attack Platform 用户创建的 YARA 规则数据库扫描文件和对象，以发现对企业 IT 基础架构的针对性攻击的迹象。
- *针对性攻击分析器*（以下也称为 *TAA* 或者 *TA 分析器*）。使用 TAA (IOA) 规则分析和监控公司 LAN 计算机上安装的软件的网络活动。搜索 Kaspersky Anti Targeted Attack Platform 的用户应注意的网络活动的迹象，以及对企业 IT 基础架构的针对性攻击的迹象。
- *KSN*。代表 Kaspersky Anti Targeted Attack Platform 检查在卡巴斯基安全网络知识库中的文件和 URL 地址的信誉，并提供有关网站类别的信息（例如，恶意网站、钓鱼网站）。

Sandbox 组件

托管 Sandbox 组件的服务器运行带有操作系统镜像的虚拟机。

Sandbox 组件在这些操作系统中启动对象，并分析对象的行为以检测恶意活动以及对企业 IT 基础构架的针对性攻击的迹象。

文件扫描中涉及的特殊注意事项

在 Sandbox 中扫描文件时，有以下特殊注意事项：

- Sandbox 组件每天能在队列中扫描的最大对象数量为 20000。达到上限时，应用程序会删除排队等待扫描时间最久对象的 10%，并用排队等待扫描的新对象替换它们。被删除的对象保存在应用程序中，状态为 NOT_SCANNED。
- 从一个存档发送的对象总数不得超过 20 个。
- 将扫描嵌套级别低至 3 级（包括 3 级）的文件。

Endpoint Agent 组件

软件组件。

对于 KEDR 功能，可以用以下应用程序来表示：

- Kaspersky Endpoint Agent for Windows
- Kaspersky Endpoint Security for Windows。
- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Mac

对于 NDR 功能，可以用以下应用程序来表示：

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux

应用程序安装在组织 IT 基础架构中的工作站和服务器（以下也称为“计算机”）上。在这些计算机上，应用程序将持续监控进程、活动网络连接和正在被修改的文件，并将该监控数据发送到 Central Node 服务器。

用于安装应用程序的计算机必须满足硬件和软件要求。

应用程序的工作原理

Kaspersky Anti Targeted Attack Platform 应用程序包括三个功能块：

- Kaspersky Anti Targeted Attack（以下也称为“KATA”），它检测企业 IT 基础构架边界上的威胁。
- Kaspersky Endpoint Detection and Response（以下也称为“KEDR”），为组织的局域网提供保护。
- Network Detection and Response（以下也称为“NDR”），为企业 LAN 提供保护。

您可以使用应用程序的全部功能（KATA + NDR 密钥和 KEDR 密钥）或部分功能（仅 KATA/KATA + NDR 密钥或仅 KEDR 密钥）。

Kaspersky Anti Targeted Attack 的工作原理

Kaspersky Anti Targeted Attack 包括以下主要组件：

- Sensor。
- Central Node。
- Sandbox。

Sensor、Central Node 和 Sandbox 交互操作如下：

- Sensor 组件接收镜像的 SPAN、ERSPAN、RSPAN 流量、HTTP、FTP、SMTP 和 DNS 协议的对象和元数据、HTTP 和 FTP 流量数据以及 HTTPS 流量数据（如果管理员已在代理服务器上配置 SSL 证书替换）、电子邮件的副本，并对获取的数据执行以下操作：
  - 使用入侵检测系统技术（以下也称为 IDS）扫描 Internet 流量以查找对企业 IT 基础架构的入侵迹象。

    IDS 技术可以识别和检测 80个协议（特别是 TCP/IP 模型的 53 个应用层协议）中的网络活动，从而检测可疑流量和网络攻击。支持的协议包括 TCP、UDP、FTP、TFTP、SSH、SMTP、SMB、CIF、SSL、HTTP、HTTP/2、HTTPS、TLS、ICMPv4、ICMPv6、IPv4、IPv6、IRC、LDAP、NFS、DNS、RDP、DERPC 、MS-RPC、WebSocket、Citrix 等。
  - 根据卡巴斯基安全网络数据库（以下也称为“KSN”）或卡巴斯基私人安全网络（以下也称为“KPSN”）检查文件和 URL 的信誉。
  - 发送要由 Central Node 组件扫描的对象和文件。

  您还可以使用*邮件传感器*作为 Sensor 组件，它是安装了 Kaspersky Secure Mail Gateway (KSMG) 或 Kaspersky Security for Linux Mail Server (KLMS) 的服务器或虚拟机。

- Central Node 组件使用反病毒数据库、Kaspersky Anti Targeted Attack 用户创建的 YARA 规则数据库扫描文件和对象，并在必要时发送要由 Sandbox 组件扫描的文件和对象。

- Sandbox 组件分析虚拟操作系统中对象的行为，以检测恶意活动和对企业 IT 基础架构的有针对性的攻击迹象，并将扫描结果发送到 Central Node 服务器。

如果检测到任何威胁，Central Node 服务器会在警报数据库中记录相关信息。您可以应用程序 Web 界面的**警报**部分或通过生成警报报告来查看警报表。

警报信息还可以发布到组织中使用的 SIEM 系统以及外部系统。有关 Sandbox 组件警报的信息可以发布在卡巴斯基私人安全网络的本地信誉数据库中。

Kaspersky Endpoint Detection and Response 的工作原理

Kaspersky Endpoint Detection and Response 包括以下组件：

- Central Node。

- Endpoint Agent。

  该组件可以由以下任意应用程序代表：Kaspersky Endpoint Agent for Windows、 Kaspersky Endpoint Security for Windows、 Kaspersky Endpoint Security for Linux、 Kaspersky Endpoint Security for Mac。

- Sandbox。

  可选组件。

  > Sensor 组件可用作Kaspersky Endpoint Agent 传出连接的代理服务器。

Endpoint Agent 和 Central Node 组件互操作如下：

代表 Endpoint Agent 组件的应用程序之一安装在企业 IT 基础架构内的单个计算机上，持续监视进程、开放的网络连接和正在被修改的文件。监控数据被发送到 Central Node 服务器。事件根据这些数据生成。

- Kaspersky Endpoint Agent for Windows 将有关以下事件的数据传输到 Central Node 服务器：**进程已启动**、**进程已终止**、**模块已加载**、**到远程主机的连接**、**阻止的应用程序 (防止规则)**、**文件已阻止**、**文件已更改**、**系统事件日志**、**注册表已修改**、**监听的端口**、**驱动程序已加载**、**进程: 解释文件运行**、**进程: 控制台交互式输入**、**检测**、**检测处理结果**、AMSI **扫描**。

- Kaspersky Endpoint Security for Windows 将有关以下事件的数据传输到 Central Node 服务器：**进程已启动**、**进程已终止**、**模块已加载**、**到远程主机的连接**、**阻止的应用程序 (防止规则)**、**文件已阻止**、**文件已更改**、**系统事件日志**、**注册表已修改**、**监听的端口**、**驱动程序已加载**、**进程: 解释文件运行**、**进程: 控制台交互式输入**、**检测**、**检测处理结果**、AMSI **扫描**、DNS、**代码注入**、**命名管道**、WMI、LDAP。

- Kaspersky Endpoint Security for Linux 将有关以下事件的数据传输到 Central Node 服务器：**进程已启动**、**进程已终止**、**阻止的应用程序 (防止规则)**、**文件已阻止**、**文件已更改**、**系统事件日志**、**检测**、**检测处理结果**、**代码注入**、DNS。

- Kaspersky Endpoint Security for Mac 将有关以下事件的数据传输到 Central Node 服务器：**进程已启动**、**进程已终止**、**文件已更改**、**检测**、**检测处理结果**。

NDR 功能的 Endpoint Agent 单独连接，并且不会将观察信息发送到 Central Node 服务器。

Kaspersky Endpoint Agent for Windows 可与Endpoint Protection Platform（以下简称"EPP"）应用程序集成：

- Kaspersky Endpoint Security for Windows。
- Kaspersky Security for Windows Server。
- Kaspersky Security for Virtualization Light Agent for Windows。

有关 Kaspersky Endpoint Agent for Windows 版本与 EPP 应用程序的兼容性的信息，请参阅Kaspersky Endpoint Agent for Windows 版本与 EPP 应用程序的兼容性部分。

在这种情况下，Kaspersky Endpoint Agent 还会将有关 EPP 应用程序检测到的威胁的信息以及这些应用程序的威胁处理结果发送到 Central Node 服务器。

EPP 应用程序、Kaspersky Endpoint Agent 和 Central Node 组件的互操作如下：

- EPP 应用程序将有关检测到的威胁和威胁处理结果的信息发送到 Kaspersky Endpoint Agent。

  Kaspersky Endpoint Security for Windows 还可以向 Kaspersky Endpoint Agent Security for Windows 提供有关具有反恶意软件扫描接口支持（以下也称为"AMSI"）的第三方应用程序的信息，将对象（例如 PowerShell 脚本）发送到 Kaspersky Endpoint Security for Windows 进行额外扫描。

- Kaspersky Endpoint Agent 将在监控进程、开放网络连接和正在被修改的文件时收集的数据以及从 EPP 应用程序接收的数据发送到 Central Node 服务器。

  Central Node 服务器处理接收到的数据并在应用程序Web 界面中显示相应的事件。

  EPP 应用程序数据处理会生成**检测**、**检测处理结果**、**AMSI 扫描**事件（当 Kaspersky Endpoint Agent for Windows 与 Kaspersky Endpoint Security for Windows 集成时）。

  到达 Central Node 服务器的事件由 TAA (IOA) 规则标记。由于此标记，可以为需要用户注意的事件生成警报。如果您有 Sandbox 组件，您还可以自动从 Kaspersky Endpoint Agent 主机发送文件，以便 Sandbox 组件根据 Kaspersky TAA (IOA) 规则进行扫描。

当 Central Node 服务器与 Kaspersky Endpoint Agent for Windows 和 Kaspersky Endpoint Security for Windows 集成时，您可以执行以下操作来对检测到的威胁做出反应：

- 通过在 Kaspersky Endpoint Agent 主机上运行以下任务来管理文件和应用程序：**杀死进程**，**进行取证**，**启动 YARA 扫描**，**运行应用程序**，**获取文件**，**删除文件**，**隔离文件**，**从隔离区恢复文件**，**管理服务**，**获取磁盘镜像**，**获取内存转储**。
- 配置策略以阻止文件和进程在选定主机上运行。
- 将单个主机与网络隔离。
- 使用 TAA (IOA) 规则对事件进行分类和分析。
- 使用 OpenIOC 兼容文件（IOC 文件）来搜索主机上和警报数据库中的针对性攻击、受感染和可能受感染对象的迹象。
- 使用 API 执行威胁响应操作。

当 Central Node 服务器与 Kaspersky Endpoint Security 11.4 for Linux 和 Kaspersky Endpoint Security for Mac 集成时，您可以执行以下操作来对检测到的威胁做出反应：

- 通过运行**获取文件**、**运行应用程序**任务管理文件和应用程序。
- 使用 TAA (IOA) 规则对事件进行分类和分析。
- 使用 API 执行以下威胁响应操作：管理应用程序运行任务。

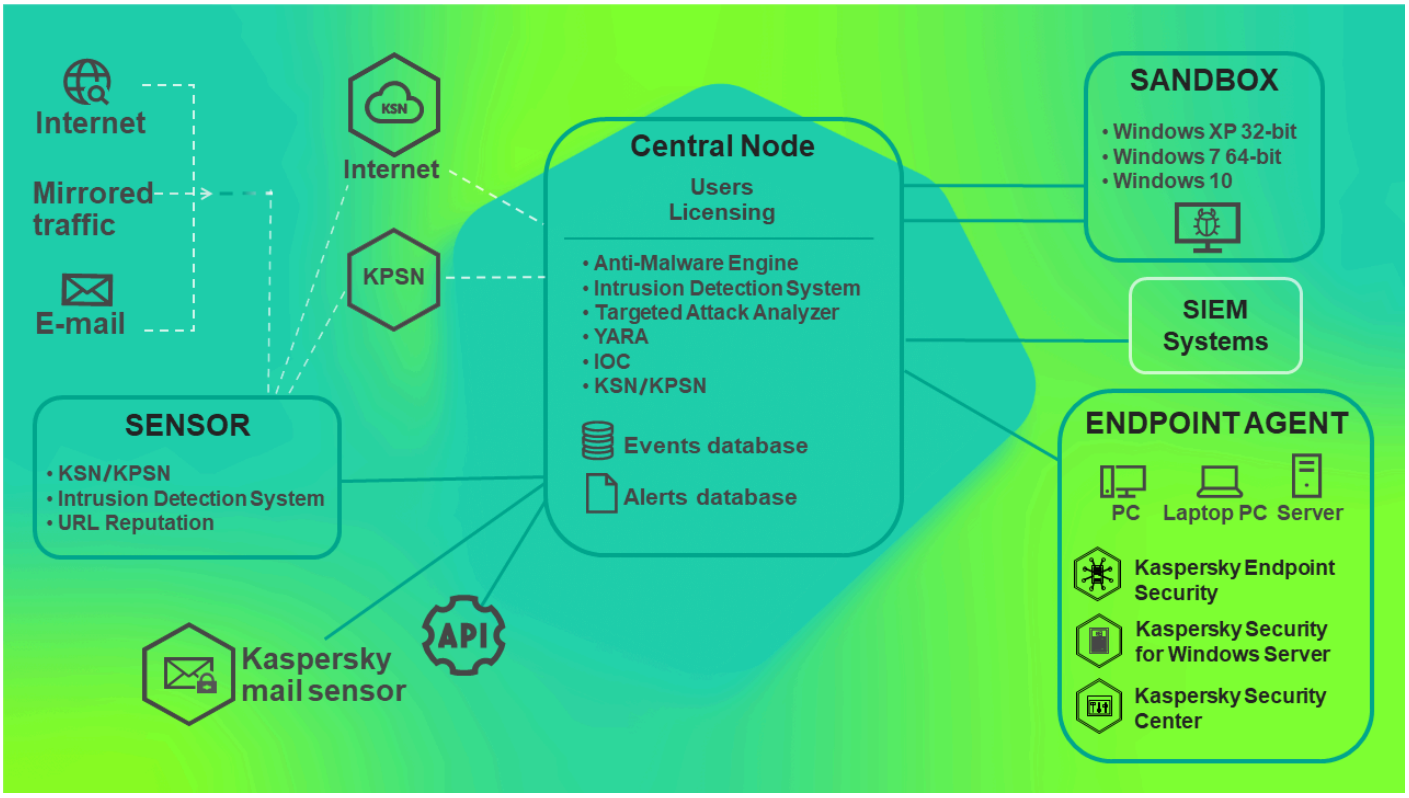
当 Central Node 服务器与 Kaspersky Endpoint Security 12 for Linux 集成时，您可以执行以下操作来对检测到的威胁做出反应：

- 通过运行**获取文件**、**运行应用程序**、**删除文件**、**杀死进程**任务管理文件和应用程序。
- 将单个主机与网络隔离。
- 使用 OpenIOC 兼容文件（IOC 文件）来搜索主机上和警报数据库中的针对性攻击、受感染和可能受感染对象的迹象。
- 使用 API 执行以下威胁响应操作：主机网络隔离管理、管理应用程序运行任务。

当 Central Node 服务器与 Kaspersky Endpoint Security 12.2 for Linux 集成时，您可以执行以下操作来对检测到的威胁做出反应：

- 通过运行以下任务管理文件和应用程序：**获取文件**、**运行应用程序**、**删除文件**、**杀死进程**、**隔离文件**、**从隔离区恢复文件**。
- 配置策略以阻止文件和进程在选定主机上运行。
- 将单个主机与网络隔离。
- 使用 OpenIOC 兼容文件（IOC 文件）来搜索主机上和警报数据库中的针对性攻击、受感染和可能受感染对象的迹象。
- 使用 API 执行以下威胁响应操作：主机网络隔离管理、管理应用程序运行任务、管理防护规则。

Kaspersky Anti Targeted Attack Platform 的工作原理如下图所示。

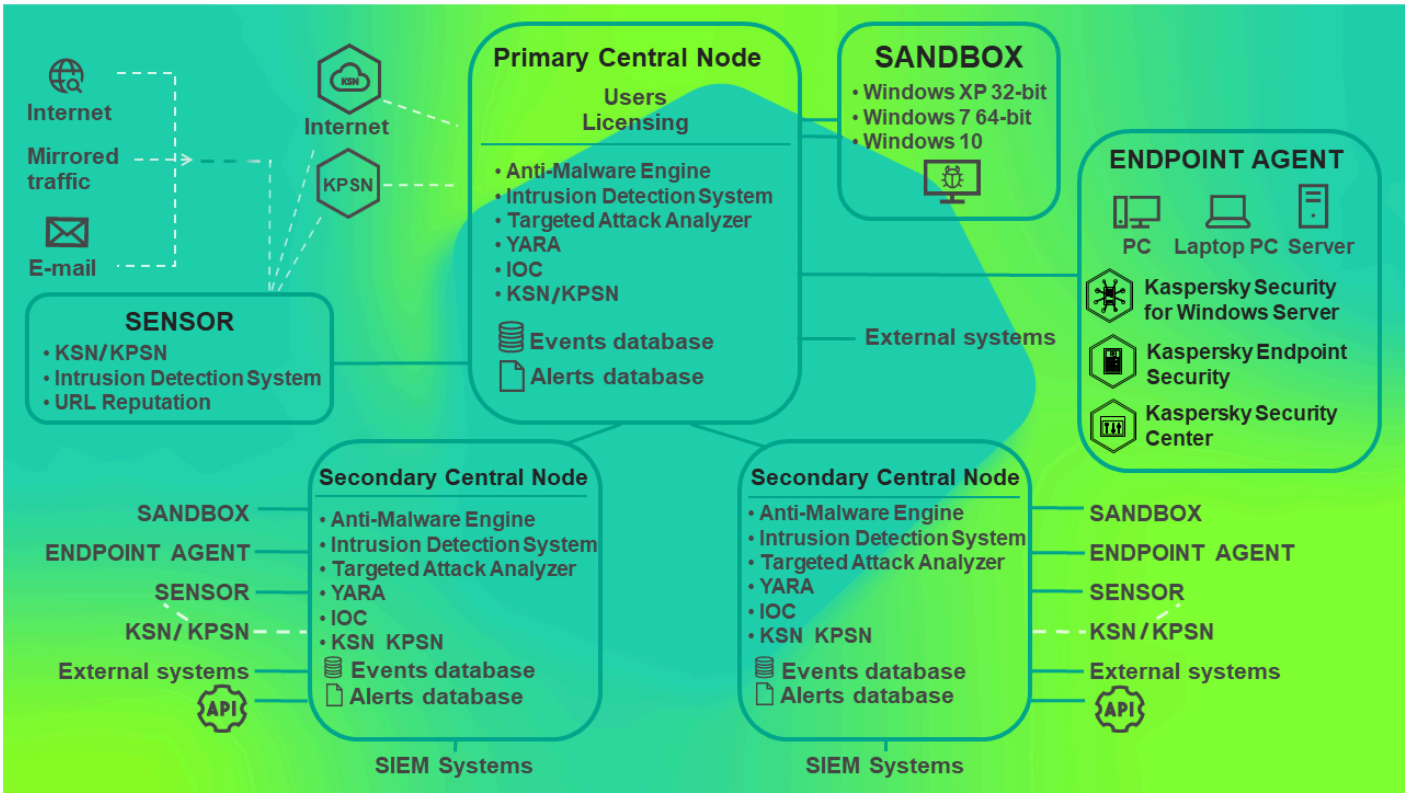


Kaspersky Anti Targeted Attack Platform 的工作原理

您可以单独配置每个 Central Node 组件的设置，也可以在分布式解决方案模式下集中管理多个组件。

分布式解决方案是指 Central Node 服务器的两层架构。该结构将主控制服务器（称为"主 Central Node (PCN)"）和辅助服务器（称为"从属 Central Node (SCN)"）分开。

分布式解决方案模式下 Kaspersky Anti Targeted Attack Platform 的工作原理如下图所示。



分布式解决方案模式下 Kaspersky Anti Targeted Attack Platform 的工作原理

分布式解决方案和多租户

您可以单独配置每个 Central Node 组件的设置，也可以在分布式解决方案模式下集中管理多个组件。

分布式解决方案是指安装有 Central Node 组件的服务器的两层架构。该结构将主控制服务器（称为“*主 Central Node（PCN）*”）和辅助服务器（称为“*从属 Central Node（SCN）*”）分开。服务器的交互要求将 SCN 连接到 PCN。

如果您已将 Central Node 组件部署为集群，则整个集群将充当 PCN 或 SCN 的角色。

PCN 和 SCN 使用与单独管理的Central Node 组件相同的技术来扫描文件和对象。

分布式解决方案允许对应用程序的以下功能区进行集中式管理：

- 用户。
- 警报。
- 威胁搜索。
- 任务。
- 防止。
- 自定义规则。
- 存储。
- Endpoint Agent，包括主机的网络隔离。
- 报告。

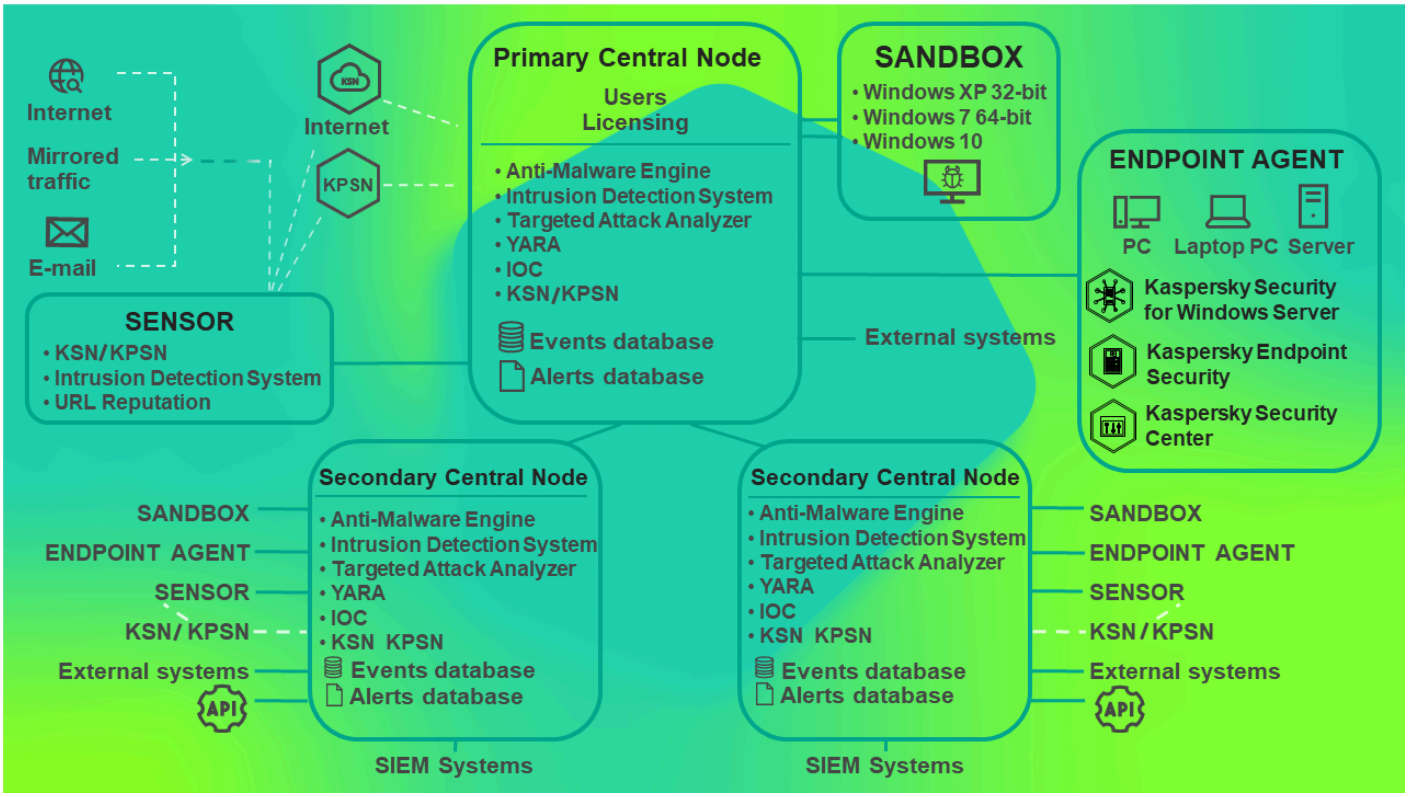
如果您支持多个组织或同一组织的多个分支机构，则可以在多租户模式下使用该应用程序。

多租户模式可让您使用该应用程序同时保护多个组织或同一组织的分支机构（以下也称为“租户”）的基础架构。您可以在每个租户的一个或多个 Central Node 上安装 Kaspersky Anti Targeted Attack Platform。每个租户都可以独立于其他租户管理应用程序。服务提供商可以管理多个租户的数据。

您想要按层次结构组织的 Central Node 组件必须基于相同的操作系统（Ubuntu 或 Astra Linux）。组件的版本必须相同。

对于每个用户账户，同时进行的应用程序管理会话的数量限于一个 IP 地址。如果使用相同的用户名从不同的 IP 地址登录应用程序，则先前的会话将终止。

如果您使用分布式解决方案和多租户模式，则对每个 PCN 和 SCN 服务器分别实施限制。



分布式解决方案模式下的应用程序运行

您可以在以下情况下使用分布式解决方案和多租户模式：

- 为了保护一个租户的 10000 台以上主机
- 用于对租户不同业务部门的应用程序进行集中管理
- 用于集中管理多个租户的服务器上的应用程序
- 用于以最大 10 Gbps 速率处理网络流量，如果您的网络包含多个 10 Gbps 网段并且您想要处理这些网段中的流量

当应用程序切换到分布式解决方案和多租户模式时，所有先前添加的授权许可密钥都将从具有 SCN 角色的服务器中删除。每个连接的 SCN 接收到来自 PCN 的一个密钥。如果应用程序的完整功能用于 PCN（KATA 和 KEDR 密钥），而部分功能用于 SCN（仅 KATA 密钥或仅 KEDR 密钥），则可能会因数据量增加而超出 SCN 服务器负载限制。如果部分应用程序功能用于 PCN（仅 KATA 密钥或仅 KEDR 密钥），而完整功能用于 SCN（KATA 和 KEDR 密钥），则应用程序功能部分不可用。

授权许可密钥只能在 PCN 上管理。

您可以使用以下方案以分布式解决方案和多租户模式部署应用程序：

- 在新的服务器上安装 Central Node 组件并将 PCN 和 SCN 角色分配给那些服务器。
- 将 PCN 和 SCN 角色分配给已经安装了 Central Node 组件的服务器。

  在这种情况下，您必须将 Central Node 组件更新到 7.0 版。

在您将安装了 Central Node 组件的服务器切换为分布式解决方案模式之前，您应该在运行模式更改之后查看将被应用到系统的变更。将 PCN 角色分配给一台服务器是不可逆转的。

分布式解决方案及多租户模式过渡方案

将应用程序切换到分布式解决方案和多租户模式涉及以下步骤：

1. **为要用作 PCN 的 Central Node 服务器分配 DNS 名称**

   如果之前已分配 DNS 名称，请确保正确指定该名称。

2. **将 PCN 角色分配给一台服务器**

3. **在 PCN 服务器上创建应用程序管理员账户**

   您将使用此账户将 SCN 服务器连接到 PCN。如果为 Kaspersky Anti Targeted Attack Platform 配置了 Active Directory 集成，您必须在创建账户时选择“**KATA 用户账户**”身份验证类型。

4. **将 SCN 角色分配给服务器并向 PCN 发送连接请求**

5. **处理 SCN 到 PCN 的连接请求**

切换到分布式解决方案和多租户模式后，应用程序可能需要一些时间来配置组件。在这种情况下，应用程序菜单不会显示在 SCN Web 界面中，而在 PCN Web 界面中，“**控制板**”部分显示“*数据已超过 5 分钟未发送到 SCN。*”错误。设置组件所需的时间取决于累积数据的数量，但平均为 20 到 30 分钟。

修改分布式解决方案和多租户模式的应用程序设置

分布式解决方案模式的应用程序设置修改列在下表中。

切换到分布式解决方案和多租户模式时修改应用程序设置

功能区域	PCN	SCN
用户	分配给它们的用户和角色将被保留。此外，PCN 用户被授予访问权限，以使用 PCN 和所有连接的 SCN。	除部署 Central Node 时创建的用户外，将删除所有的用户。 之后，SCN 从 PCN 请求用户列表，并使用该列表创建具有相同参数的本地用户： 名称 密码 角色 状态 无权访问 SCN 的用户不会显示在用户列表中。
警报	有关来自所有连接的 SCN 的所有警报的信息将添加到 PCN 数据库中。	用户名不再显示在现有的警报信息中。用户数据将从警报操作历史记录中删除。
网络流量事件	没有变化。	没有变化。
控制板	在**警报**选项卡上，您现在可以选择必须在小组件中显示信息的 SCN。 在**系统健康**选项卡上，现在显示 PCN 与连接的 SCN 的连接状态。	在**系统健康**选项卡上，现在显示与 PCN 的连接状态。

功能区域	PCN	SCN
任务	在将分配 PCN 角色分配给 Central Node 服务器之前在 Central Node 服务器上创建的任务，以及在切换到分布式解决方案模式后在 PCN 上创建的任务，适用于所有连接的 SCN。 在 SCN 上创建的任务也会显示在任务列表中。PCN 上无法更改这些任务的设置。	显示在 PCN 上创建的任务，以及在此 SCN 上创建的任务。 在 PCN 上创建的任务设置无法更改。
报告	保留在切换到分布式解决方案模式之前创建的模板和报告。 **服务器**列被添加到报告表中，其中包含警报所属的 SCN 的信息。 切换到分布式解决方案模式后，仅显示在 PCN 上创建的报告。	保留在切换到分布式解决方案模式之前创建的模板和报告。 如果 PCN 具有相同 ID (guid) 的用户，则保留有关创建报告的用户的信息。在其他情况下，用户信息将被删除。 切换到分布式解决方案模式后，仅显示在 SCN 上创建的报告。
防止	在将 PCN 角色分配给 Central Node 服务器之前在 Central Node 服务器上创建的策略，以及在切换到分布式解决方案模式后在 PCN 上创建的策略，适用于所有连接的 SCN。 在 SCN 上创建的策略也会显示在策略列表中。PCN 上无法更改这些策略的设置。	将显示在 PCN 上创建的策略，以及在此 SCN 上创建的策略。 在 PCN 上创建的策略设置无法更改。
存储	保留在切换到分布式解决方案模式之前存储在 PCN 上的所有文件和元数据。在 **Central Node**列中显示 PCN 的名称。 PCN 还保留所有连接的 SCN 的存储内容。	保留在切换到分布式解决方案模式之前存储在 SCN 上的所有文件和元数据。
TAA 排除项	没有变化。	没有变化。
VIP 状态	没有变化。	没有变化。
通知规则	没有变化。	没有变化。
与邮件传感器的集成	没有变化。	没有变化。
威胁搜索	在数据库中的威胁搜索期间，PCN 向所有连接的 SCN 发送请求。处理完搜索查询后，将显示所选租户的 PCN 和 SCN 事件的列表。	没有变化。
自定义规则 - TAA	在被分配 PCN 角色之前在 Central Node 服务器上添加的 TAA (IOA) 规则将仅被应用于 PCN 服务器。服务器获得 PCN 角色后添加的规则也适用于 SCN。	在 PCN 上添加的 TAA (IOA) 规则，以及在切换到分布式解决方案模式之前和之后在此 SCN 上添加的 TAA (IOA) 规则都会显示。
自定义规则 - 入侵检测	没有变化。	没有变化。
自定义规则 - IOC	通过在 Central Node 服务器获得 PCN 角色之前在其上添加的 IOC 文件来搜索危害指标仅在该 PCN 服务器上执行。通过在 Central Node 服务器获得 PCN 角色之后在其上添加的 IOC 文件来搜索入侵指标也会在 SCN 上执行。	在 PCN 上添加的 IOC 文件，以及在切换到分布式解决方案模式之前和之后在此 SCN 上添加的 IOC 文件都会显示。
自定义规则 - YARA	在被分配 PCN 角色之前在 Central Node 服务器上添加的 YARA 规则将仅被应用于 PCN。服务器获得 PCN 角色后添加的规则也适用于 SCN。	在 PCN 上添加的 YARA 规则，以及在切换到分布式解决方案模式之前和之后在此 SCN 上添加的 YARA 规则都会显示。
资产	没有变化。	没有变化。
网络地图	没有变化。	没有变化。
风险和异常	没有变化。	没有变化。
应用程序备份	应用程序的备份仅在未连接 SCN 的 PCN 上可用。 要在 PCN 上备份应用程序，请断开所有 SCN 与 PCN 的连接。	在 SCN 上备份应用程序不可用。 要在 SCN 上备份应用程序，请将该服务器切换到独立服务器模式，从而断开该服务器与 PCN 的连接。

将 PCN 角色分配给一台服务器

将 PCN 角色分配给一台服务器是不可逆转的。将服务器角色更改为 PCN 后，您将无法将该服务器的角色更改为 SCN 或独立服务器。要更改该服务器的角色，您必须重新安装应用程序。

要将 PCN 角色分配给服务器：

1. 利用管理员账户登录应用程序 Web 界面。
   您需要登录要对其分配 PCN 角色的服务器的 Web 界面。
2. 选择 **操作模式** 部分。
3. 单击 **分布式解决方案**。
4. 在**服务器角色** 下拉列表中，选择**主 Central Node**。
5. 在**租户名称**字段中，输入该 Central Node 服务器所属的租户的名称。
6. 单击**分配 PCN 角色**。
   这将打开操作确认窗口。

   > 确认操作后，再次登录应用程序 Web 界面。

7. 单击**是**。

服务器被分配 PCN 角色和租户名称。

使用管理员凭据登录应用程序 Web 界面后，应用程序 Web 界面的**操作模式**部分显示以下信息：

- 当前模式 – 分布式解决方案。
- **服务器角色** – 主 Central Node。
- **证书指纹** –建立与 SCN 连接时，需要服务器的证书指纹用于验证。
- **租户**–有关此服务器和连接的 SCN 服务器所属租户的信息：
  - **IP**–此服务器的主 Central Node 和 SCN 服务器的 IP 地址（连接后）。
  - **服务器**–该服务器的名称和 SCN 服务器的名称（连接后）。
    该名称与安装有应用程序的主机名称无关。您可以更改它。
  - **证书指纹**–该服务器的空白值和 SCN 服务器的证书指纹（连接后）。
  - **状态**– SCN 服务器的连接状态（连接后）以及连接到租户的服务器数量。
- **服务器等待授权**表包含有关连接的 SCN 的信息。

将 SCN 角色分配给一台服务器

要将 SCN 角色分配给服务器：

1. 利用管理员账户登录应用程序 Web 界面。
   您需要登录要对其分配 SCN 角色的服务器的 Web 界面。

2. 在应用程序 Web 界面窗口中选择**操作模式**部分。
3. 单击 **分布式解决方案**。
4. 在**服务器角色**下拉列表中，选择**从属 Central Node**。
5. 在**PCN IP**字段中，输入您希望连接 SCN 并具有 PCN 角色的服务器 IP 地址。
6. 单击**获取证书指纹**。
   具有 PCN 角色的服务器的证书指纹显示在工作区。
7. 联系 PCN 管理员并将您接收的证书指纹与**操作模式**部分的**证书指纹**字段中的 PCN 显示的指纹进行对比。
8. 如果 SCN 和 PCN 上的证书指纹匹配，则在“**用户名称**”和“**密码**”字段中，输入在 PCN 上创建的用于连接 SCN 的管理员账户的用户名和密码。
9. 点击“**发送连接请求**”。
   这将打开一个确认窗口。
10. 单击**是**。

SCN 角色被分配给服务器。

查看有关租户、PCN 和 SCN 服务器的信息

在 PCN 服务器的 Web 界面中，您可以查看有关该服务器以及与其连接的所有 SCN 服务器的信息。

查看多租户模式下 PCN 和 SCN 服务器的信息：

1. 利用管理员账户登录应用程序 Web 界面。
   您需要登录 PCN 服务器的 Web 界面。
2. 在应用程序 Web 界面窗口中选择**操作模式**部分。

工作区将显示有关服务器的以下信息：

- 当前模式 – 分布式解决方案。
- **服务器角色** – 主 Central Node。
- **证书指纹** – PCN 服务器的证书指纹。
- **租户** –有关服务器所属租户的信息，以及连接到 PCN 的所有 SCN 服务器的信息。
  - **IP** –PCN 服务器的主 Central Node 和连接到 PCN 的 SCN 服务器的 IP 地址。
  - **服务器** –服务器名称以及连接到 PCN 的 SCN 服务器的名称。
    该名称与安装有应用程序的主机名称无关。你可以更改它。

- **证书指纹**– PCN 服务器的空白值和等待连接到 PCN 的 SCN 服务器的证书指纹。
- **状态**– SCN 服务器的连接状态以及连接到租户的服务器数量。

- **服务器等待授权**表包含以下信息：
  - **IP**– SCN 服务器的 IP 地址或域名。
  - **服务器**是应用程序 Web 界面中显示的 SCN 服务器的名称。
    该名称与安装有应用程序的主机名称无关。您可以更改它。
  - **证书指纹** – 与连接请求一起发送到 PCN 的 SCN 服务器的证书指纹。
  - **状态** – SCN 到 PCN 连接的状态。

将租户添加到 PCN 服务器

要在 PCN 服务器 Web 界面中添加租户：

1. 利用管理员账户登录应用程序 Web 界面。
   您必须登录要为其添加租户的 PCN 服务器的 Web 界面。
2. 在应用程序 Web 界面窗口中选择**操作模式**部分。
3. 在**租户**工作区右侧，单击**添加**。
4. 在**名称**字段中，输入您要添加的租户的名称。
5. 单击**添加**。

   租户已添加并显示在列表中。

从 PCN 服务器删除租户

要在 PCN 服务器 Web 界面中删除租户：

1. 利用管理员账户登录应用程序 Web 界面。
   您必须登录要为其删除租户的 PCN 服务器的 Web 界面。
2. 在应用程序 Web 界面窗口中选择**操作模式**部分。
3. 在**租户**工作区中，选择要删除的租户。
4. 单击**删除**。
   这将打开操作确认窗口。

该操作不可逆转。该租户的所有全局对象以及报告和报告模板都会丢失。

5. 单击**是**。

租户被删除。

在 PCN 服务器上重命名租户

要在 PCN 服务器的 Web 界面中重命名租户：

1. 利用管理员账户登录应用程序 Web 界面。
   您必须登录要为其重命名租户的 PCN 服务器的 Web 界面。
2. 在应用程序 Web 界面窗口中选择**操作模式**部分。
3. 在**租户**列表中，单击您要重命名的租户旁边的。
   这将打开一个窗口，您可以在其中重命名租户。
4. 在**名称**字段中，输入租户的新名称。
5. 单击**保存**。

租户被重命名。

断开 SCN 与 PCN 的连接

如果要断开 SCN 与 PCN 的连接，请注意以下特殊事项：

- 从 7.0 版本开始，SCN 服务器无法重新连接到任何 PCN 服务器。
- 如果您想将服务器重新连接为 SCN，则需要在此服务器上重新安装 Central Node 组件。
- 断开 SCN 与 PCN 的连接会更改应用程序设置。

Kaspersky Anti Targeted Attack Platform 的管理员负责保密 PCN、SCN 和 Central Node 服务器上的数据。如果您计划将 SCN 服务器从一个租户移至另一个租户，则必须在使用 Kaspersky Anti Targeted Attack Platform 后删除服务器上剩余的所有数据，并重新安装 Kaspersky Anti Targeted Attack Platform，然后再将服务器移交给其他租户。

要断开 SCN 与 PCN 之间的连接：

1. 登录要使用管理员账户从其断开连接 SCN 的 PCN 服务器的 Web 界面。
2. 在应用程序 Web 界面窗口中选择**操作模式**部分。
3. 在服务器列表中，选择您要断开连接的 SCN。

4. 单击 **断开连接**。

   这将打开操作确认窗口。

5. 单击**是**。

SCN 与 PCN 断开连接并继续作为独立的 Central Node 服务器工作。

修改断开 SCN 与 PCN 连接的应用程序设置

下表列出了 SCN 与 PCN 断开连接后应用程序设置的修改。

SCN 与 PCN 断开连接后应用程序设置的修改

功能区域	PCN	SCN
用户	断开连接的 SCN 不会从应用用户权限的服务器列表中删除。 有关对已断开连接的 SCN 具有权限的用户账户更改的信息不会发送到 SCN。	从 PCN 收到的用户账户不会被删除。 您可以再次创建新用户账户，以及禁用和更改现有用户账户的密码。
警报	已删除已断开连接的 SCN 上的警报信息。	保留操作历史记录和所有警报信息。
任务	在已断开连接的 SCN 上创建的任务将被删除。	在 PCN 上创建的任务将被删除。 保留有关在 SCN 上创建任务的用户的信息。
报告	之前创建的有关已断开连接的 SCN 的所有报告都将保留，并且可以保留此服务器筛选报告列表的功能。	模板和报告不会被修改。
防止	在已断开连接的 SCN 上创建的策略将被删除。	在 PCN 上创建的策略将被删除。 保留有关在 SCN 上创建策略的用户的信息。
存储	从存储中删除与断开连接的 SCN 相关的所有对象。	存储中的所有对象都将保留。 指向该任务的链接将停止处理有关作为 PCN 上创建的任务的一部分而接收的对象的信息。
TAA 排除项	没有变化。	没有变化。
VIP 状态	没有变化。	没有变化。
通知规则	没有变化。	没有变化。
与邮件传感器的集成	没有变化。	没有变化。
威胁搜索	处理完搜索查询后，不会显示与已断开连接的 CN 相关的事件。	没有变化。
自定义规则 - TAA和IOC	断开连接的 SCN 的 IOC 和 TAA（IOA）规则被删除。	PCN 上创建的 IOC 和 TAA（IOA）规则被删除。
应用程序备份	应用程序的备份保持不可用。	备份应用程序变为可用。

规模调整指南

要在应用程序的不同操作条件下获得并保持最佳性能，必须考虑联网设备的数量，网络拓扑以及所需的应用程序功能集。

选择最佳应用程序配置包括以下步骤：

1. **选择通用部署方案**
2. **使用大小计算器计算硬件要求**

部署和安装应用程序组件的常见方案

部署和安装应用程序组件的方案取决于应用程序服务器上的计划加载。

Endpoint Agent 组件可以安装在属于组织的 IT 基础架构并运行 Windows 操作系统的任意计算机上。必须允许不使用代理服务器直接从具有 Endpoint Agent 组件的计算机到托管 Central Node 组件的服务器的出站连接。

您可以安装一个或多个 Central Node 组件。如果您安装了多个 Central Node 组件，您可以彼此独立地使用它们或将它们组合起来用于分布式解决方案模式下的集中管理。

部署方案选择取决于所使用的应用程序功能。本手册中列出的所有方案也适用于在虚拟平台上部署应用程序。

全功能（KATA 和 KEDR）

使用 KATA 和 KEDR 功能时，您可以扫描企业局域网计算机上的网络流量、邮件流量和数据。

如果组织内使用超过 5000 台具有 Endpoint Agent 组件的主机，则不建议使用 Central Node 组件来处理流量。

> 您可以使用 Sensor 组件作为代理服务器，将主机连接到 Endpoint Agent 组件和 Central Node。一个 Sensor 组件支持连接最多 1000 台具有 Endpoint Agent 组件的主机。

使用 KATA 和 KEDR 功能时，选择部署方案的条件如下表所示。选择算法如下：

1. 在表的每一行中，选择包含与 IT 基础结构对应的条件值的单元格。
   如果一行中包含两个具有相同值的单元格，则必须选择左侧的单元格。
2. 选择有标记单元格的最右侧列。

使用 KATA 和 KEDR 功能时选择部署方案

条件	双服务器方案	三服务器方案	四台或以上服务器方案	分布式解决方案
无法在同一设备上接收网络流量和邮件流量。	否	是	是	是
Endpoint Agent 主机数量	否	从 5000 到 10000	从 5000 到 10000	10000 以上

条件	双服务器方案	三服务器方案	四台或以上服务器方案	分布式解决方案
通信信道带宽	1 Gbps	1 到 2 Gbps	2 Gbps 以上	2 Gbps 以上
需要分析流量的远程基础架构的数量。	否	一个	两个或以上	两个或以上
一个 Sandbox 组件的容量不足以在可接受的时间范围内分析所有对象。	否	否	是	是

在分布式解决方案模式下，每个应用程序组件必须满足大小计算器中指定的硬件要求。

处理网络流量、邮件流量和 Web 流量（KATA）

如果组织不需要处理企业局域网计算机上的数据，建议使用 KATA 功能。如果是这种情况，则仅处理网络流量和邮件流量。

使用 KATA 功能时选择部署方案的条件如下表所示。选择算法如下：

1. 在表的每一行中，选择包含与 IT 基础结构对应的条件值的单元格。
   如果一行中包含两个具有相同值的单元格，则必须选择左侧的单元格。
2. 选择有标记单元格的最右侧列。

使用 KATA 功能时选择部署方案

条件	双服务器方案	三服务器方案	四台或以上服务器方案
无法在同一设备上接收网络流量和邮件流量。	否	是	是
通信信道带宽	1 Gbps	1 到 2 Gbps	2 Gbps 以上
需要分析流量的远程基础架构的数量。	否	一个	两个或以上
一个 Sandbox 组件的容量不足以在可接受的时间范围内分析所有对象。	否	否	是

处理来自企业局域网计算机 (KEDR) 的数据

如果组织不需要处理流量，建议使用 KEDR 功能。如果是这种情况，则仅处理企业局域网计算机上的数据。

取决于组织中是否存在第三方 Sandbox 解决方案，您可以使用以下部署方案之一：

- 没有 Sandbox 组件
- 使用 Sandbox 组件

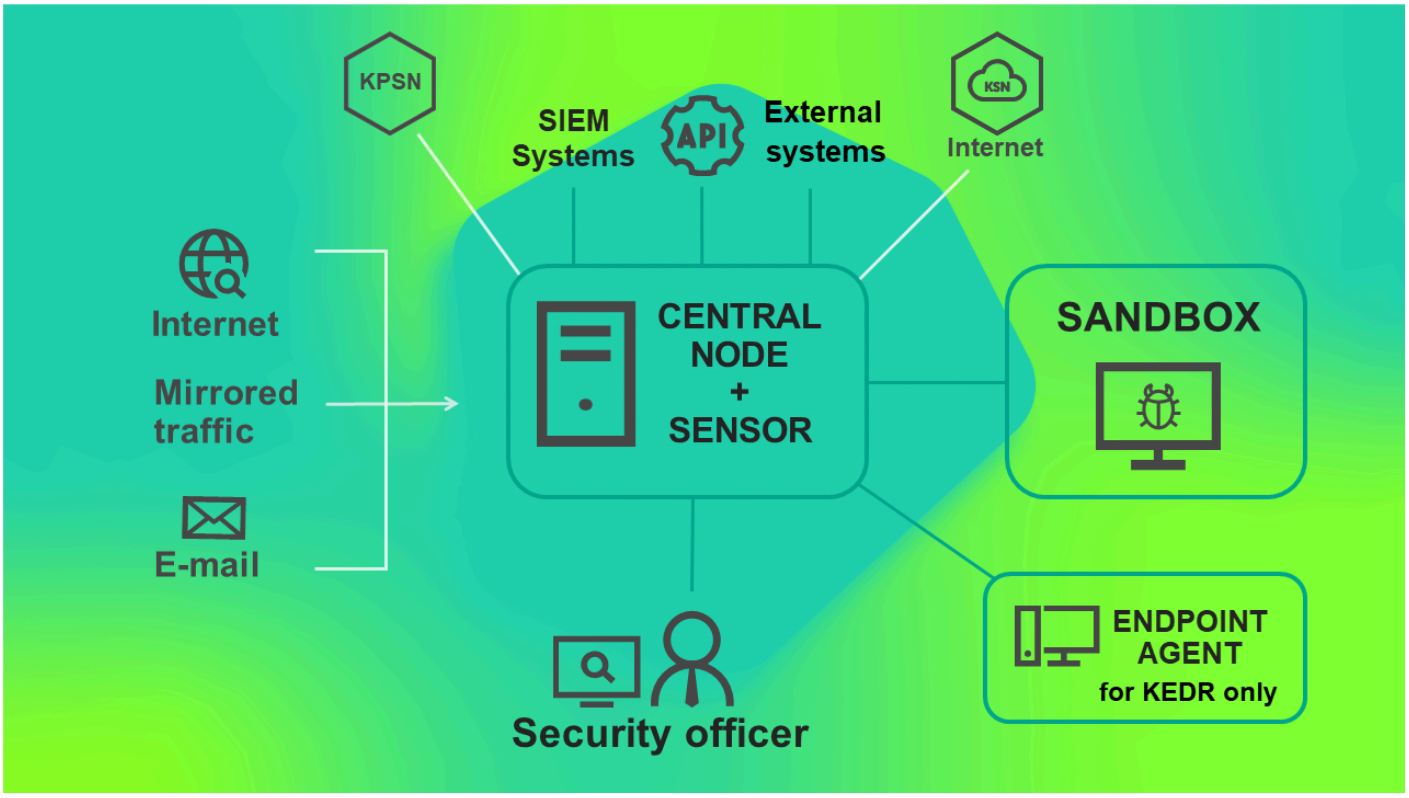
双服务器部署方案

使用 KATA 和 KEDR 功能时，可以在企业局域网计算机上安装 Endpoint Agent 组件。使用 KATA 功能时，Endpoint Agent 组件不会被安装。

使用此部署方案时，Central Node 和 Sensor 组件将被安装在同一服务器或群集上。此服务器或集群可接收流量，执行流量的初始分析并对提取的文件进行更深入的分析。根据扫描结果，组件检测到对组织的 IT 基础架构进行针对性攻击的迹象。

Sandbox 组件安装在另一台服务器上。

部署在两台服务器上的应用程序运行方案如下图所示。



部署在两台服务器上的应用程序运行方案

三服务器部署方案

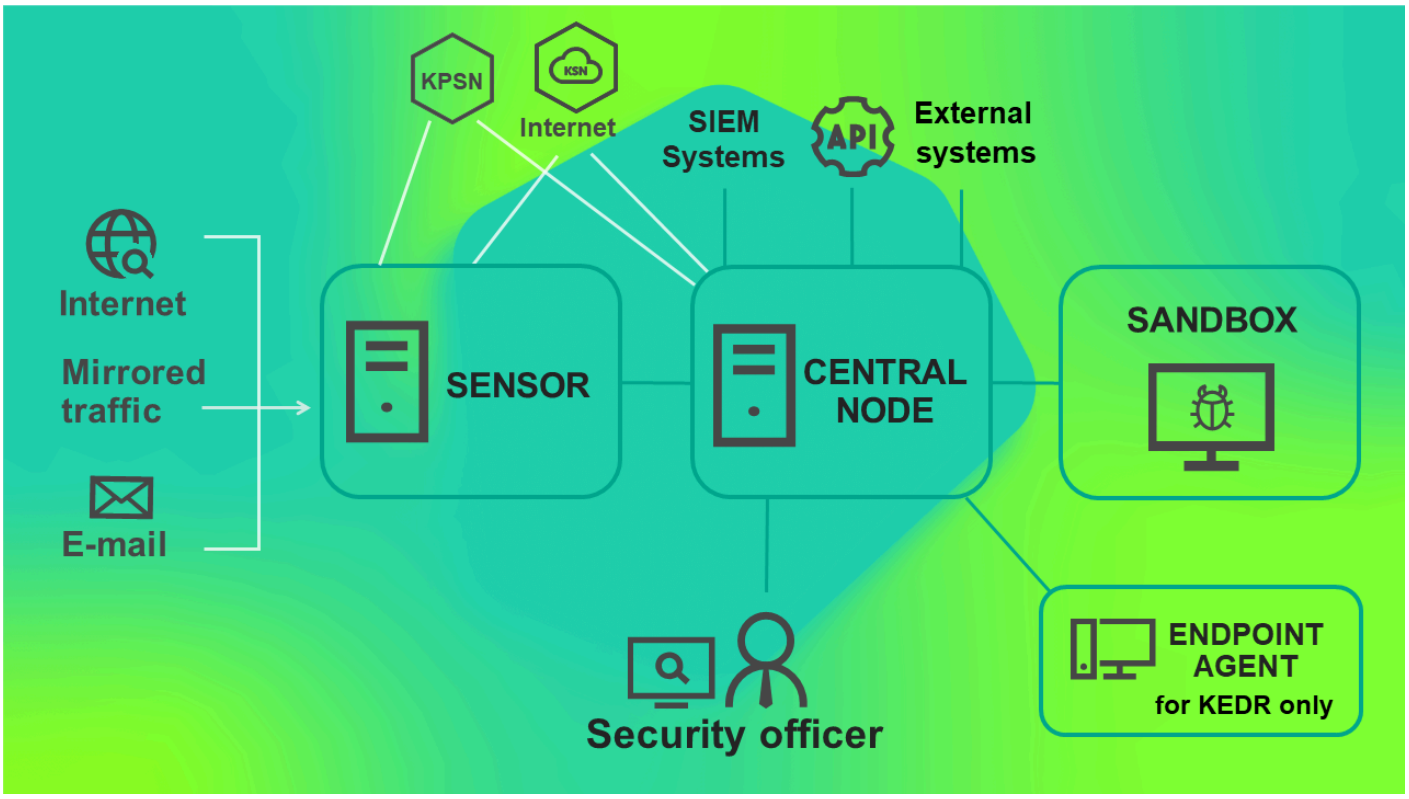
使用 KATA 和 KEDR 功能时，可以在企业局域网计算机上安装 Endpoint Agent 组件。使用 KATA 功能时，Endpoint Agent 组件不会被安装。

使用此部署方案时，Sensor、Central Node 和 Sandbox 组件安装在不同的服务器上。Central Node 组件也可以被部署为集群。Sensor 可接收流量，执行初始分析，提取文件并将它们转发到 Central Node 组件以进行更深入的分析。

使用此部署方案，Central Node 组件可以接收流量并对主基础架构中的数据执行初始分析。在这种情况下，您可以将 Sensor 组件安装在需要分析其流量的远程基础架构的服务器上。如果主基础设施中的链路带宽超过 2 Gbps，我们建议在主基础设施中安装 Sensor。

Central Node 和 Sensor 组件之间交换的流量最多占 Sensor 组件接收的流量的 20%。

部署在三台服务器上的应用程序运行方案如下图所示。



部署在三台服务器上的应用程序运行方案

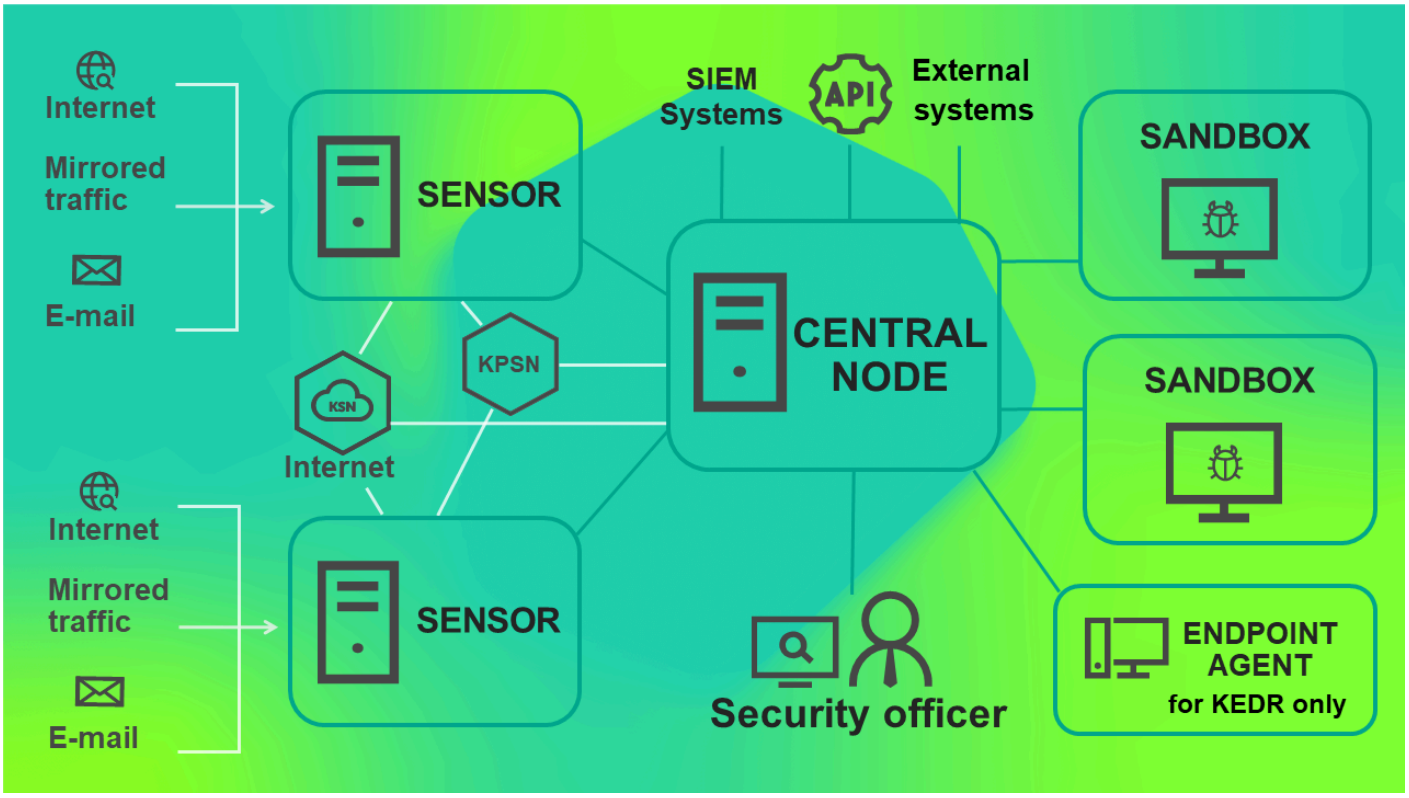
四台或以上服务器部署方案

使用 KATA 和 KEDR 功能时，可以在企业局域网计算机上安装 Endpoint Agent 组件。使用 KATA 功能时，Endpoint Agent 组件不会被安装。

如果存在大量流量，则可以在不同服务器上安装多个 Sensor 组件或多个 Sandbox 组件。建议在大型组织中部署此方案。

您还可以使用一个 Sandbox 组件连接到多个 Central Node 组件。

部署在四台或更多服务器上的应用程序操作原理图如下图所示。

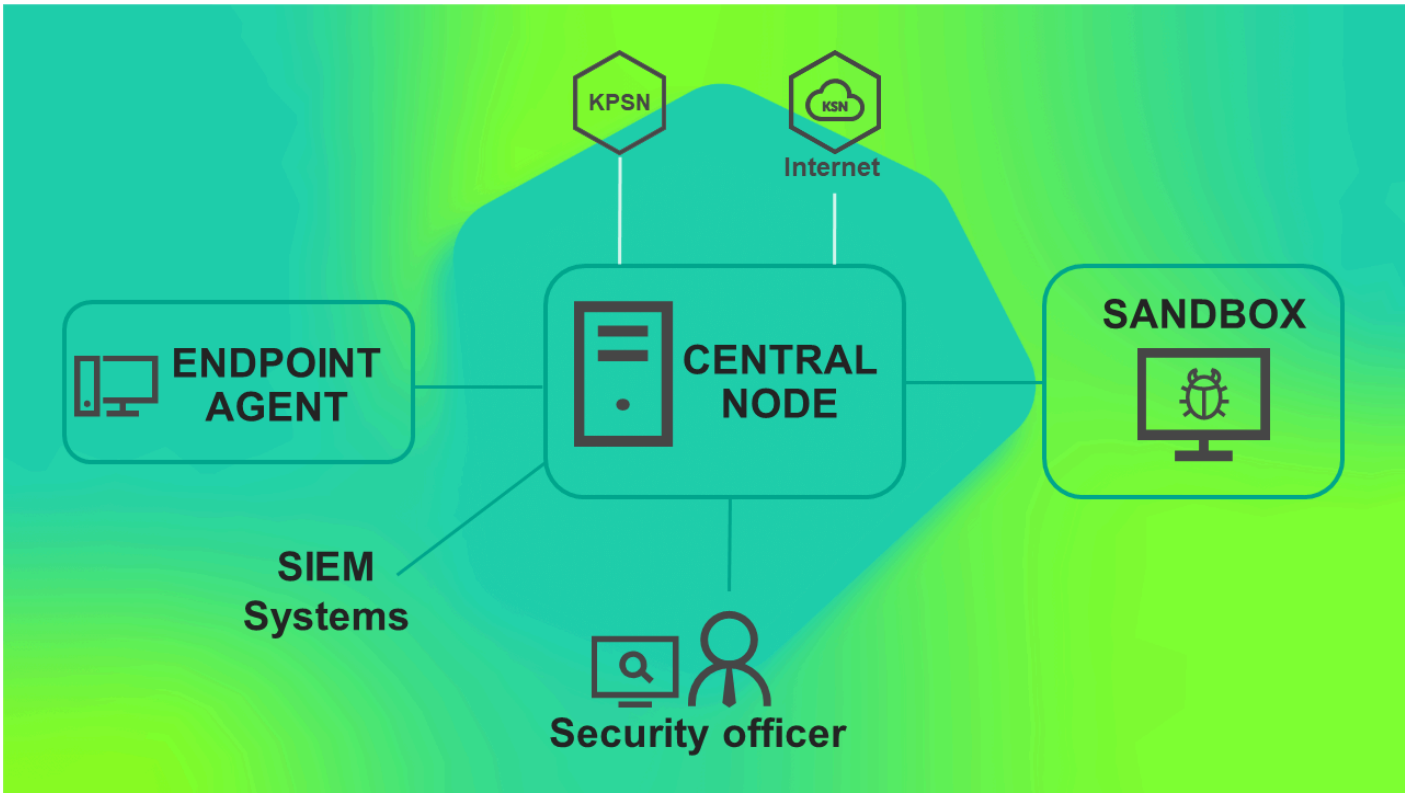


部署在四台及以上服务器上的应用程序运行方案

使用 Sandbox 组件部署 KEDR 功能的方案

如果使用此部署方案，您需要将 Central Node 组件与 Sensor 组件分开安装。

使用 Sandbox 组件部署 KEDR 功能时的应用程序运行方案如下图所示。



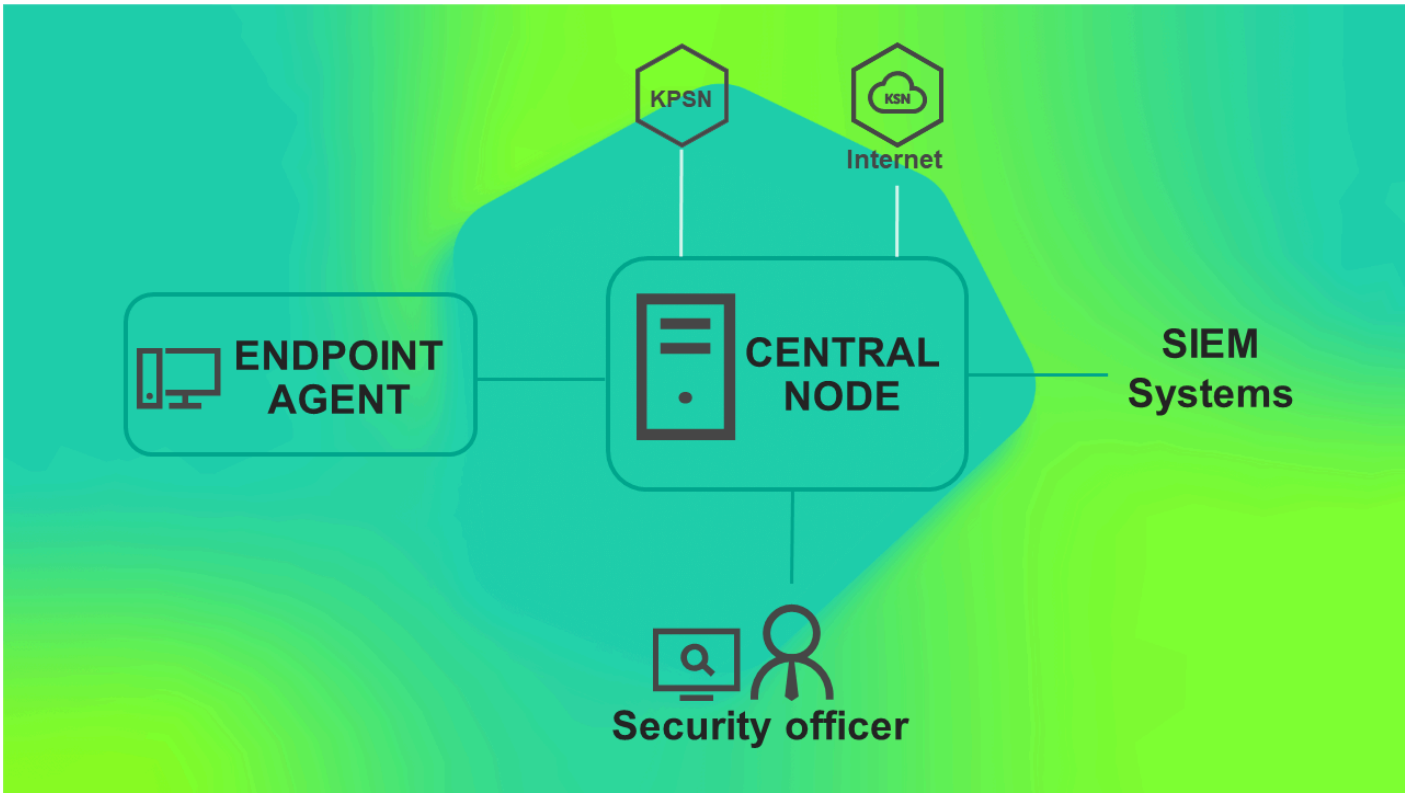
使用 Sandbox 组件部署 KEDR 功能时的应用程序运行方案

在没有 Sandbox 组件的情况下部署 KEDR 功能的方案

您无需安装 Sandbox 组件，只需使用 Central Node 组件来管理 Endpoint Agent 组件和数据分析。

如果使用此部署方案，您需要将 Central Node 组件与 Sensor 组件分开安装。

不使用 Sandbox 组件部署 KEDR 功能时的应用程序运行方案如下图所示。



不使用 Sandbox 组件部署 KEDR 功能时的应用程序运行方案

大小计算器

选择最适合 IT 基础结构的部署方案后，必须计算用于安装应用程序组件的服务器的硬件要求。

7.0 Central Node 服务器的硬件要求与组件先前版本的硬件要求不同。我们强烈建议确保您的服务器配置满足*"Central Node 组件计算"*部分中列出的要求。

Sensor 组件的计算

在计算 Sensor 组件的硬件要求时，请考虑可处理的最大流量为 10 Gbps。此最大流量可以在独立服务器上安装的一个 Sensor 上进行处理，也可以在连接到一个 Central Node 的独立服务器上安装的多个 Sensor 上进行处理。连接到一个 Central Node 的所有 Sensor 的总流量不得超过 10 Gbps。

如果网络中包含多个10 Gbps 网段，并且您需要处理这些网段的流量，则必须采用分布式解决方案。

数据在 Endpoint Agent 工作站和 Central Node 之间交换期间（与 KEDR 功能集成时），您可以将托管 Sensor 的服务器用作代理服务器，以简化网络规则的配置。例如，如果带有 Endpoint Agent 的工作站位于网络的单独段中，则只需配置 Central Node 和 Sensor 服务器之间的连接即可。

当使用 Sensor 作为代理服务器在 Endpoint Agent 组件和 Central Node 组件之间进行通信时，请考虑以下限制：

- 最多 15000 台具有 Endpoint Agent 组件的工作站可以连接到单个 Central Node 组件。
- Sensor 服务器和 Central Node 之间允许的最大数据包丢失率为 10%，数据包延迟最多为 100 毫秒。

Central Node 和 Sensor 服务器之间的链接所需的带宽取决于必须处理的流量，计算如下：

典型负载时 `10%` 的 `SPAN` 端口流量或峰值负载时 `20%` 的 `SPAN` 端口流量 `+` 电子邮件流量 `+` `ICAP` 流量 `+` `Central Node` 和 `Endpoint Agent` 之间的链接要求

Sensor 服务器的硬件要求

Sensor 组件可以与组织的 IT 基础结构集成，如下所示：

- 从 SPAN 端口接收来自网络设备的镜像流量。
- 通过 POP3 协议连接到邮件服务器。
- 通过 SMTP 协议连接到邮件服务器。
- 通过 ICAP 协议从代理服务器接收流量。
- 从 Endpoint Agent 组件接收数据。

下表列出了 Sensor 服务器的硬件要求。这些计算是针对 Sensor 处理来自 SPAN 端口的电子邮件和镜像流量的情况提供的。如果 Sensor 被用作 Endpoint Agent 工作站与 Central Node 之间通信的代理服务器，您还必须考虑链接要求。

Sensor 组件在负载高达 1000 Mbit/s 的虚拟平台上进行了测试；但是，虚拟平台支持更大的负载。如果您想在虚拟平台上部署 Sensor 组件，并计划处理高达 1000 Mbps 的流量，则可以使用下表计算 Sensor 服务器的硬件要求。如果您计划处理更多流量，请联系您的客户经理以获取硬件要求的计算。

Sensor 服务器的硬件要求取决于使用 KATA 和 KEDR 功能时从 SPAN 端口处理的流量

Endpoint Agent 组件的数量（与 KEDR 功能集成）	处理的流量 (Mbps)	最小 RAM (GB)	最小逻辑核心数
10000	100	24	6
15000	500	32	10
15000	1000	40	14
15000	2000	64	24
15000	4000	96	36
15000	7000	152	56
15000	10000	200	76

Sensor 服务器的硬件要求取决于使用 KATA 和 NDR 功能时从 SPAN 端口处理的流量

处理的流量 (Mbps)	最小 RAM (GB)	最小逻辑核心数	保存镜像流量转储时的最小逻辑内核数
100	32	6	8
500	40	10	12
1000	48	14	16
2000	72	24	24

处理的流量 (Mbps)	最小 RAM (GB)	最小逻辑核心数	保存镜像流量转储时的最小逻辑内核数
4000	112	36	40
7000	160	56	60
10000	208	76	80

CPU 必须支持 BMI2、AVX 和 AVX2 指令集。

如果您只想处理电子邮件，而不处理来自 SPAN 端口的镜像流量，我们建议使用安装在与 Central Node 相同的服务器上的 Sensor。有关硬件要求的更多详细信息，请参阅 *Central Node 组件的计算*部分→*Central Node 和 Sensor 服务器的硬件要求*。

如果一个 Sensor 服务器通过多种协议处理流量，则若要计算服务器硬件，您必须考虑到邮件服务器或邮件传感器集成需要禁用 SMTP 流量处理。

Sensor 服务器上的磁盘空间要求

建议使用 RAID 1 磁盘阵列。磁盘总空间必须至少为 600 GB。

保存来自 SPAN 端口的镜像流量转储时的 Sensor 硬件要求

如果要保存来自 SPAN 端口的镜像流量转储，则 Sensor 服务器的以下硬件要求会更高：

- 以 RAID 阵列或 DAS 池的形式安装单独的磁盘存储，其最大带宽使用以下公式计算：

  `<磁盘存储带宽> = 3 * <记录流量的最大吞吐量>`

- 磁盘存储的容量取决于预期的存储时间和保存的最大流量吞吐量，并考虑到筛选器。根据粗略计算，要存储 7 天最大吞吐量为 10 Gbps 的记录流量，需要 750 TiB 的磁盘存储空间。

Central Node 组件的计算

在虚拟平台上部署应用程序比在物理服务器上部署应用程序需要多 10% 的 CPU 资源。在虚拟磁盘设置中，必须选择厚置备磁盘类型。

为了避免在虚拟平台上部署应用程序时可能出现的性能下降，您需要执行以下操作：

- 将延迟敏感度设置为“高”。
- 保留所有内存。
- 保留所有 CPU。

具有 Central Node 和 Sensor 组件的服务器的硬件要求

安装 Central Node 和 Sensor 组件的服务器的硬件要求取决于以下条件：

- 处理的流量

  与未加密流量（来自 SPAN 端口的标准流量）相比，Kaspersky Anti Targeted Attack Platform 对已解密的 SSL/TLS 流量的处理负载增加了 5 倍。此种情况下，要确定用于计算服务器负载的已处理流量，请使用以下公式：

  `<解密流量> = 5 * <未加密流量>`

  要确定 ICAP 服务器上处理的流量以计算服务器上的负载，请使用以下公式：

  `<在 ICAP 服务器上处理的流量> = 5 * <未在 ICAP 服务器上处理的流量>`

- 每秒处理的电子邮件数

- Endpoint Agent 主机数量

  Endpoint Agent 组件可以安装在工作站、终端服务器、文件服务器或网络附加存储 (NAS) 上。

  以下“帮助”部分提供了有关代表 Endpoint Agent 组件的应用程序版本与 Kaspersky Anti Targeted Attack Platform 版本的兼容性的信息：Kaspersky Endpoint Agent for Windows、Kaspersky Endpoint Security for Windows、Kaspersky Endpoint Security for Linux、Kaspersky Endpoint Security for Mac。

  Kaspersky Endpoint Agent for Windows 也可以安装在 SCADA 服务器上。

  要确定具有 Endpoint Agent 组件的有效主机数量来计算服务器负载，可以使用以下公式：

  `K = A+3*B+20*C`

  其中

  - “K”是具有 Endpoint Agent 组件的主机的最大数量。
  - “A”是运行安装了 Endpoint Agent 组件的 Windows 操作系统的终端服务器的工作站和用户数量。
  - “B”是运行安装了 Endpoint Agent 组件的 Linux 或 macOS 操作系统的终端服务器的工作站和用户数量。
  - “C”是服务器数量。

如果处理的流量大于 1 Gbps，则必须在独立服务器上安装 Central Node 和 Sensor 组件。

下表列出了根据所使用的功能对 Central Node 服务器的硬件要求。

请注意，启用事件链扫描功能后，Central Node 服务器将适用不同的硬件要求。请参阅“*启用事件扫描索功能的 Central Node 服务器的硬件要求*”部分。

使用 KEDR 功能时对 Central Node 服务器的硬件要求

具有 Endpoint Agent 组件的最大主机数量	最小 RAM (GB)	3 GHz 时的最小逻辑核心数	第一个磁盘子系统（RAID 1 或 RAID 10）				第二个磁盘子系统 (RAID 10)		
			ROPS（每秒读取操作数）	WOPS（每秒写入操作数）	磁盘阵列大小 (TB)	阵列中的磁盘数量	ROPS（每秒读取操作数）	WOPS（每秒写入操作数）	磁盘阵列大小 (TB)
1000	80	10	100	250	1	4	300	250	大至 12 TB
3000	96	16	100	500	1	4	500	500	
5000	112	20	100	500	1	4	700	600	
10000	160	32	100	500	1	4	1000	800	
15000	208	44	100	500	1	4	1500	1000	

使用 KATA 和 KEDR 功能时，具有 Central Node 组件的服务器的硬件要求

具有 Endpoint Agent 组件的最大主机数量	每秒的最大电子邮件数	来自具有 Central Node 组件的服务器上的 SPAN 端口的最大流量	来自具有 Sensor 组件的服务器上的 SPAN 端口的最大流量 (Mbps)	最小 RAM (GB)	3 GHz 时的最小逻辑核心数	第一个磁盘子系统（RAID 1 或 RAID 10）				第二个磁盘子系统 (RAID 10)	
						ROPS（每秒读取操作数）	WOPS（每秒写入操作数）	磁盘阵列大小 (TB)	阵列中的磁盘数量	ROPS（每秒读取操作数）	WOPS（每秒写入操作数）
1000	1	200	没有处理	128	24	100	1000	1.9	4	300	300
2000	2	500	没有处理	144	32	100	1000	2	4	500	500
5000	1	1000	没有处理	192	48	100	1000	2	4	1000	600
10000	2	1000	没有处理	240	60	100	1000	2	4	2000	800
5000	5	没有处理	2000	176	60	100	1000	1.9	4	1000	600
10000	20	没有处理	4000	240	96	100	1000	1.9	4	2000	800
15000	20	没有处理	4000	288	108	100	1000	1.9	4	2000	800
15000	20	没有处理	7000	320	144	100	1000	1.9	4	2000	800
15000	20	没有处理	10000	336	180	100	1000	1.9	4	2000	800

如果您想在“Brest”或“RED Virtualization”虚拟平台上安装 Central Node 组件并使用 KEDR 或 KATA+KEDR 功能，则需要将最低逻辑内核数增加 20%。如果您想在 Hypervisor 操作系统级别缓解 Spectre 或 Meltdown 类型的漏洞，则需要额外将最小逻辑内核数量增加 1.5 倍。虚拟服务器的其他硬件要求与物理服务器的要求类似，如上表所列。

使用 KATA 功能时对具有 Central Node 组件的服务器的硬件要求

每秒的最大电子邮件数	来自具有 Central Node 组件的服务器上的 SPAN 端口的最大流量	来自具有 Sensor 组件的服务器上的 SPAN 端口的最大流量 (Mbps)	最小 RAM (GB)	3 GHz 时的最小逻辑核心数	第一个磁盘子系统（RAID 1 或 RAID 10）			
					ROPS（每秒读取操作数）	WOPS（每秒写入操作数）	磁盘阵列大小 (TB)	阵列中的磁盘数量
2	500	没有处理	72	24	100	1000	2	4
2	1000	没有处理	88	36	100	1000	2	4
5	没有处理	2000	80	44	100	1000	2	4
20	没有处理	4000	96	72	100	1000	2	2
20	没有处理	7000	128	108	100	1000	2	2
20	没有处理	10000	144	144	100	1000	2	2

如果您想在“Brest”或“RED Virtualization”虚拟平台上安装 Central Node 组件并使用 KATA 功能，则需要将最低逻辑内核数增加 30%。如果您想在 Hypervisor 操作系统级别缓解 Spectre 或 Meltdown 类型的漏洞，则需要额外将最小逻辑内核数量增加 1.5 倍。虚拟服务器的其他硬件要求与物理服务器的要求类似，如上表所列。

使用 KATA、KEDR 和 NDR 功能时，具有 Central Node 组件的服务器的硬件要求

与 KEDR 功能集成的 Endpoint Agent 主机的最大数量	每秒的最大电子邮件数	来自具有 Central Node 组件的服务器上的 SPAN 端口的最大流量	来自具有 Sensor 组件的服务器上的 SPAN 端口的最大流量 (Mbps)	最小 RAM (GB)	3 GHz 时的最小逻辑核心数	第一个磁盘子系统（RAID 1 或 RAID 10）				第二个磁盘子系统 (RAID 10)	
						ROPS（每秒读取操作数）	WOPS（每秒写入操作数）	磁盘阵列大小 (TB)	阵列中的磁盘数量	ROPS（每秒读取操作数）	WOPS（每秒写入操作数）
1000	1	200	没有处理	160	28	100	1000	2	4	400	500
2000	2	500	没有处理	176	40	100	1000	2	4	600	800
5000	1	1000	没有处理	224	56	100	1200	2	4	1200	1000
10000	2	1000	没有处理	272	68	100	1200	2	4	2200	1200
5000	5	没有处理	2000	208	64	100	1200	2	4	1200	1000
10000	20	没有处理	4000	272	104	100	1500	2	4	2200	1200
15000	20	没有处理	4000	320	116	100	1500	2	4	2200	1200
15000	20	没有处理	7000	352	152	200	2000	2	4	2300	1200
15000	20	没有处理	10000	384	188	200	2000	2	4	2300	1200

作为与 NDR 功能块集成的一部分，最多 1000 个 Endpoint Agent 组件可以连接到单个 Central Node 组件。

使用 KATA 和 KEDR 功能时，具有 Central Node 组件的服务器的硬件要求

每秒的最大电子邮件数	来自具有 Central Node 组件的服务器上的 SPAN 端口的最大流量	来自具有 Sensor 组件的服务器上的 SPAN 端口的最大流量 (Mbps)	最小 RAM (GB)	3 GHz 时的最小逻辑核心数	第一个磁盘子系统（RAID 1 或 RAID 10）			
					ROPS（每秒读取操作数）	WOPS（每秒写入操作数）	磁盘阵列大小 (TB)	阵列中的磁盘数量
2	500	没有处理	96	32	100	1000	2	4
2	1000	没有处理	128	44	200	2000	2	4
5	没有处理	2000	112	52	200	2000	2	4
20	没有处理	4000	128	80	200	2000	2	4
20	没有处理	7000	160	116	300	2500	2	4
20	没有处理	10000	192	152	300	2500	2	4

作为与 NDR 功能块集成的一部分，最多 1000 个 Endpoint Agent 组件可以连接到单个 Central Node 组件。

Kaspersky Anti Targeted Attack Platform 不支持对软件 RAID 阵列的操作。

CPU 必须支持 BMI2、AVX 和 AVX2 指令集。

Central Node 服务器的磁盘空间要求

对于 Central Node 服务器，我们建议在第一个磁盘子系统上有 2000 GB 的可用空间，在第二个磁盘子系统上有 2400 GB。第二个磁盘子系统所需的空间量取决于首选存储策略，可以使用以下公式计算：

`150 GB + <Kaspersky Endpoint Agent 或 Kaspersky Endpoint Security for Windows 主机的数量>/15000 * (400 GB + 460 GB * <存储数据的天数>)/0.65`，但不超过 `12 TB`。

如果要使用事件链扫描功能，请使用以下公式计算第二个磁盘子系统上的空间要求：

150 GB + <Kaspersky Endpoint Agent 或 Kaspersky Endpoint Security for Windows 主机的数量>/15000 * (600 GB + 460 GB * <存储数据的天数>)/0.65，但不超过 12 TB。

使用 NDR 功能时，必须按照以下公式在第二个磁盘子系统上分配额外的空间：

(连接到 NDR 功能块的 Endpoint Agent 组件数量> * 0.02 GB + <来自 SPAN 端口的流量 (Gbps)> * 10 GB) * <您要存储多少天的数据>。

这些公式可用于粗略估计所需的磁盘空间。实际存储的数据量取决于组织的流量概况，并且可能与计算结果不同。

如果您没有将 Central Node 安装为高可用性集群，您必须使用以下公式计算“**事件数据库，GB**”和“**存储，GB**”参数的磁盘空间：

A = F - R，GB。

where

- “A”是事件数据库和存储所使用的空间。
- “F”是安装 Central Node 组件的硬盘驱动器的大小。
- “R”是第二个磁盘子系统上根据连接的带有 Endpoint Agent 组件的主机数量保留的可用空间量 (GB)；该参数取自下表。

如果连接到 Central Node 的主机数量在列出的值之间，请在计算中使用较大的数字。

预留的可用空间量取决于 Endpoint Agent 主机的数量

Endpoint Agent 主机数量	预留的可用空间量 (GB)
1000	1000
3000	1200
5000	1400
10000	1900
15000	2400

如果您已配置集成以使用 REST API 扫描外部系统对象，则必须提高对 Central Node 服务器的硬件要求。其他硬件要求如下表所示。

具有集成外部系统的 Central Node 服务器的硬件要求

每秒处理的最大对象数	其他逻辑核心数	附加 Sandbox 服务器的数量
8	2	1
16	4	2
24	7	3

如果您配置了集成以使用 REST API 将事件发送到外部系统，则必须提高对 Central Node 服务器的硬件要求，增加 1 个逻辑内核和 6 GB RAM。

如果要节省网络流量，则必须增加对 Central Node 服务器的硬件要求。有关硬件要求的更多详细信息，请参阅“*Sensor 组件的计算→保存原始网络流量时 Sensor 的硬件要求*”。

分布式解决方案模式下 PCN 服务器的要求

如果使用分布式解决方案模式，需要考虑到当连接最多 10 个 SCN 时，PCN 服务器上的最小 RAM 量和最小逻辑核心数必须比非分布式解决方案模式下的 Central Node 服务器高 10%。SCN 上的负载可以在 Central Node 服务器的硬件要求中指定的限制范围内变化。

如果满足以下条件，则可以将最多 150 个 SCN 连接到一个 PCN：

- 最多可有 5000 个 Endpoint Agent 主机连接到一个 SCN 服务器。
- PCN 服务器的硬件配置需满足以下要求：
  - <Central Node 服务器硬件要求中列出的最小逻辑内核数> + 10。
  - <Central Node 服务器硬件要求中列出的最小 RAM> + 32。
  - <Central Node 服务器硬件要求中列出的 ROPS> + 1500。
  - <Central Node 服务器硬件要求中列出的 WOPS> + 3000。

如果要使用不带内置 Sensor 的 PCN，则 PCN 服务器必须具有以下配置：

- CPU：
  - 时钟频率：2.5 GHz。
  - 线程数：20。
  - 内核数：10。
- RAM：80 千兆字节 (GB)。
- 2 个 SSD (写入密集型 (WI))。

Central Node 服务器的硬件要求如下表所示（见上文）：

- *使用 KEDR 功能时对 Central Node 服务器的硬件要求*。
- *使用 KATA 和 KEDR 功能时对 Central Node 服务器的硬件要求*。
- *使用 KATA 功能时对 Central Node 服务器的硬件要求*。
- *使用 KATA、KEDR 和 NDR 功能时，具有 Central Node 组件的服务器的硬件要求*。
- *使用 KATA 和 KEDR 功能时，具有 Central Node 组件的服务器的硬件要求*。

通信信道要求

您必须确保 Central Node 服务器与每个网段之间有足够的通信信道带宽，具体取决于网段中 Endpoint Agent 主机数量。下表列出了带宽要求，具体取决于 Endpoint Agent 主机数量。

通信信道带宽取决于 Endpoint Agent 主机的数量

Endpoint Agent 主机最大数量	为 Endpoint Agent 主机保留的通信信道所需带宽 (Mbps)
10	1
50	2
100	3
1000	20
10000	200

分布式解决方案模式下 PCN 和 SCN 服务器之间通信信道的最低要求如下表所示。

PCN 和 SCN 服务器之间通信信道的最低要求

Endpoint Agent 主机最大数量	每秒的最大电子邮件数	SPAN 端口的最大流量 (Mbps)	所需通信信道带宽 (Mbps)
5000	5	2000	20
10000	20	4000	30

Central Node 集群服务器的硬件要求

一个集群必须至少包含 4 台服务器：2 台存储服务器和 2 台处理服务器。如果您有多达 15000 台 Endpoint Agent 联机主机，则至少需要 2 台存储服务器和 2 台处理服务器。如果您有 15000 到 30000 台 Endpoint Agent 联机主机，则至少需要 2 台存储服务器和 3 台处理服务器。

每台集群服务器必须有两个网络适配器来配置集群和外部子网。集群子网的速率必须高达 10 Gbps。

集群子网还必须满足以下要求：

- 集群子网必须仅包含集群服务器和网络交换机。
- 集群子网必须被隔离。
- 集群服务器必须全部位于同一 L1 或 L2 网段中。为此，您可以将集群中的所有服务器连接到单个网络交换机或使用软件隧道。例如，L2TPv3 或覆盖传输虚拟化 (OTV)。
- “网络延迟”值必须满足“个位数延迟”要求，即该值必须小于 10 毫秒。

下表列出了使用 KEDR 功能时集群服务器的硬件要求。

使用 KEDR 功能时处理服务器的硬件要求

最小 RAM (GB)	最小逻辑核心数	RAID 磁盘阵列类型	RAID 磁盘阵列中的磁盘数	单硬盘容量 (GB)
256	48	RAID 1	2	1200

使用 KEDR 功能时存储服务器的硬件要求

最小 RAM (GB)	最小逻辑核心数	第一个磁盘子系统			第二个磁盘子系统	
		RAID 磁盘阵列类型	RAID 磁盘阵列中的磁盘数	单硬盘容量 (GB)	磁盘数量	单硬盘容量 (GB)
128	16	RAID 1	2	1200	至少 6	至少 1200

我们建议两个磁盘子系统使用相同大小的磁盘。对于第二个磁盘子系统，您必须使用未组合成 RAID 阵列的磁盘。

磁盘子系统的性能要求相当于“*使用 KEDR 功能时 Central Node 服务器的硬件要求*”表中指定的性能要求（见上文）。

启用事件链扫描的 Central Node 组件的计算

下表列出了启用事件链扫描功能的 Central Node 服务器的硬件要求。

使用 KEDR 功能时对具有 Central Node 组件的服务器的硬件要求

具有 Endpoint Agent 组件的最大主机数量	最小 RAM (GB)	3 GHz 时的最小逻辑核心数	第一个磁盘子系统（RAID 1 或 RAID 10）				第二个磁盘子系统 (RAID 10)		
			ROPS（每秒读取操作数）	WOPS（每秒写入操作数）	磁盘阵列大小 (TB)	阵列中的磁盘数量	ROPS（每秒读取操作数）	WOPS（每秒写入操作数）	磁盘阵列大小 (TB)
1000	96	12	100	250	1	4	300	300	大至 12 TB
3000	96	16	100	500	1	4	700	750	
5000	112	20	100	500	1	4	1000	900	
10000	160	34	100	500	1	4	1500	1200	
15000	224	48	100	750	1	4	1500	1600	

使用 KEDR 功能和 2.1 GHz CPU 时 Central Node 服务器的硬件要求

具有 Endpoint Agent 组件的最大主机数量	最小 RAM (GB)	2.1 GHz 时的最小逻辑核心数	第一个磁盘子系统（RAID 1 或 RAID 10）				第二个磁盘子系统 (RAID 10)		
			ROPS（每秒读取操作数）	WOPS（每秒写入操作数）	磁盘阵列大小 (TB)	阵列中的磁盘数量	ROPS（每秒读取操作数）	WOPS（每秒写入操作数）	磁盘阵列大小 (TB)
1000	96	16	100	250	1	4	300	250	大至 12 TB
3000	96	24	100	500	1	4	700	750	
5000	112	28	100	500	1	4	1000	900	
10000	160	48	100	500	1	4	1500	1200	
15000	224	64	100	750	1	4	1500	1600	

使用 KATA 和 KEDR 功能时，具有 Central Node 组件的服务器的硬件要求

具有 Endpoint Agent 组件的最大主机数量	每秒的最大电子邮件数	来自具有 Central Node 组件的服务器上的 SPAN 端口的最大流量	来自具有 Sensor 组件的服务器上的 SPAN 端口的最大流量 (Mbps)	最小 RAM (GB)	3 GHz 时的最小逻辑核心数	第一个磁盘子系统（RAID 1 或 RAID 10）				第二个磁盘子系统 (RAID 10)	
						ROPS（每秒读取操作数）	WOPS（每秒写入操作数）	磁盘阵列大小 (TB)	阵列中的磁盘数量	ROPS（每秒读取操作数）	WOPS（每秒写入操作数）
1000	1	200	没有处理	144	24	100	1000	1.9	4	300	300
2000	2	500	没有处理	160	32	100	1000	2	4	700	700
5000	1	1000	没有处理	192	48	100	1000	2	4	1000	900
10000	2	1000	没有处理	240	64	100	1000	2	4	1500	1200
5000	5	没有处理	2000	192	60	100	1000	1.9	4	1000	900
10000	20	没有处理	4000	256	100	100	1000	1.9	4	1500	1200
15000	20	没有处理	4000	304	112	100	1000	1.9	4	1500	1600
15000	20	没有处理	7000	320	148	100	1000	1.9	4	1500	1600
15000	20	没有处理	10000	336	184	100	1000	1.9	4	1500	1600

如果您想在“Brest”或“RED Virtualization”虚拟平台上安装 Central Node 组件并使用 KEDR 或 KATA+KEDR 功能，则需要将最低逻辑内核数增加 20%。如果您想在 Hypervisor 操作系统级别缓解 Spectre 或 Meltdown 类型的漏洞，则需要额外将最小逻辑内核数量增加 1.5 倍。虚拟服务器的其他硬件要求与物理服务器的要求类似，如上表所列。

Sandbox 组件计算

具有 Sandbox 组件的服务器的硬件要求取决于已处理流量的类型和数量以及允许的对象扫描时间。

默认情况下，允许的对象扫描时间为 1 个小时。为了缩短这一时间，您需要使用功能更强大的服务器或具有 Sandbox 组件的多台服务器。

建议按如下方式计算 Sandbox 组件的配置：

1. 在一台服务器上安装 Central Node 和 Sensor 组件，在另一台服务器上安装 Sandbox 组件，以便对应用程序进行试运行。

   为了获得足够的统计数据，应用程序必须处理该组织的流量一周。

2. 通过执行以下命令来运行数据记录脚本：

   ```
   sudo kata-run.sh kata-collect --output-dir path-to-folder
   ```

   `--output-dir <目录路径>`

   当脚本完成运行后， *collect.tar.gz*存档将被移至指定目录。

3. 将此存档转发给卡巴斯基工作人员进行分析。

   如果同时启动多个虚拟机，则会增加从队列处理对象的速度。

AMD 处理器不支持 Sandbox 组件。

托管 Sandbox 组件的服务器的硬件要求

使用操作系统预设镜像时，具有 Sandbox 组件的服务器数量的计算如下表所示。

使用操作系统预设镜像时 Sandbox 组件的硬件要求

每秒的最大电子邮件数	SPAN 端口的最大流量 (Mbps)	具有 Endpoint Agent 组件的最大计算机数量	具有 Sandbox 组件的物理服务器的数量	
			使用 所有镜像时	仅使用 两个 Linux 镜像时
1	200	1000	1	1
2	500	3000	1	1
1	1000	5000	1	1
5	2000	5000	1	1
20	4000	10000	2	1
20	7000	15000	4	2
20	10000	15000	5	2

如果要在 VMware ESXi 虚拟机上安装 Sandbox 组件，则需要 5 倍的虚拟服务器才能获得与物理服务器相同的性能。在“Brest”、“RED Virtualization”或“zVirt Node”虚拟平台上安装 Sandbox 组件时，您需要 13 倍的服务器。考虑到需要配置对象扫描持续时间，给出了服务器数量的估计值。

如果您对 Sandbox 服务器使用自定义图像，则可能需要额外的容量。要计算使用自定义操作系统镜像时所需的物理 Sandbox 服务器数量，可以使用以下公式：

```
<根据用户定义的 Sandbox 规则每小时需要处理的文件数量> * <自定义操作系统镜像数量> / 1000
```

要计算使用自定义操作系统镜像时所需的带有 Sandbox 组件的 VMware ESXi 虚拟机的数量，您可以使用以下公式：

```
<根据用户定义的 Sandbox 规则每小时需要处理的文件数量> * <自定义操作系统镜像数量> / 200
```

在“Brest”或 zVirt Node 虚拟化平台上安装 Sandbox 组件时，可以使用以下公式计算使用自定义操作系统镜像时所需的虚拟机数量：

```
<具有 Sandbox 组件的物理服务器的数量> * 5 * 2.6
```

在 RED 虚拟化平台上安装 Sandbox 组件时，可以使用以下公式计算使用自定义操作系统镜像时所需的虚拟机数量：

```
<具有 Sandbox 组件的物理服务器的数量> * 5 * 2.5
```

有关带有 Sandbox 组件的物理服务器数量，请参阅上面的“*使用预设操作系统镜像时 Sandbox 组件的硬件要求*”表。

列出了具有以下配置的服务器的 Sandbox 服务器数量的估计：

- 在物理服务器上安装 Sandbox 组件时：
  - 2 个 CPU：2.6 GHz 或更高频率的 Intel® Xeon® 8 Core™ (HT)
  - 80 GB RAM
  - 2 个 HDD，每个 300 GB，组合成 RAID 1 阵列

  > 在此配置的物理服务器上安装 Sandbox 组件时，您需要将同时运行的虚拟机数量限制设置为 48 台。

- 在虚拟机上安装 Sandbox 组件时：
  - Intel Xeon 15 Core (HT) CPU，主频为 2.1 GHz 或更高

    在“Brest”、zVirt Node 或 RED 虚拟化平台上安装 Sandbox 组件时，我们建议使用 Ice Lake 一代或更高版本的 Intel 处理器。
  - 32 GB RAM。
  - 300 GB HDD。

    在虚拟机上：

    1. 嵌套虚拟化已启用。
    2. 启用高延迟敏感度设置（仅在 VMware ESXi 虚拟机上安装时）。

3. 整个 RAM 被保留。

4. 整个 CPU 频率被保留。

> 在此配置的虚拟机上安装 Sandbox 组件时，您需要将同时运行的虚拟机数量限制设置为 12 个。

如果您计划使用自定义操作系统镜像，我们建议将磁盘空间增加到 600 GB 或更多。

KVM 和 VMware ESXi 虚拟化平台上部署的 Central Node 组件的计算

本节介绍部署在 KVM和VMware ESXi 虚拟平台上并连接有 50 到 750 个 Endpoint Agent 组件的 Central Node 服务器的硬件和软件要求。连接更多 Endpoint Agent 的服务器的硬件要求在*Central Node 组件的计算*部分中提供。

要在 KVM 虚拟平台上部署应用程序，需要使用 QEMU 8.0.2 安装基于 Debian GNU/Linux 12 操作系统的 KVM Hypervisor。

VMware ESXi 虚拟平台的软件要求在*硬件和软件要求*部分提供。

在虚拟平台上部署 Central Node 时，您必须记住以下限制：

- KVM：
  - 该应用程序只能使用 Ubuntu 安装文件进行安装。
  - 只能安装应用程序的非高可用性版本。
  - 仅可使用嵌入式 Sensor。
  - 您只能连接部署在物理服务器上的 KVM 虚拟化平台之外或另一个受支持的虚拟化平台上的 Sandbox 组件。
  - 对于虚拟基础架构中部署的每个 Central Node 服务器，必须使用单独的网络接口来接收镜像 SPAN 流量。
  - 外部系统无法使用API 获取警报信息和应用程序事件。
  - 不保证支持云解决方案中使用的 KVM 虚拟化。
  - 在虚拟机设置中，CPU 设置中的 **type** 参数必须设置为 **host** 值，网络适配器设置中的 **model** 参数必须设置为 **VMware vmxnet3** 值。
- VMware ESXi：
  - 只能安装应用程序的非高可用性版本。
  - 仅可使用嵌入式 Sensor。
  - 对于虚拟基础架构中部署的每个 Central Node 服务器，必须使用单独的网络接口来接收镜像 SPAN 流量。

下表列出了根据所使用的功能对 Central Node 服务器的硬件要求。

使用 KEDR 功能时对 Central Node 服务器的硬件要求

具有 Endpoint Agent 组件的最大主机数量	每分钟的最大电子邮件数	来自具有 Central Node 组件的服务器上的 SPAN 端口的最大流量 (Mbps)	3 GHz 时的最小逻辑核心数	最小RAM (GB)
50	0	0	4	31
100	0	0	4	31
150	0	0	6	31*/32
250	0	0	6	31/32
500	0	0	8	31/34
750	0	0	10	31/38

* 斜线前的值表示安装 Central Node 组件所需的 RAM 数量。安装后，必须将 RAM 数量增加到斜线后的值。

使用 KATA 和 KEDR 功能时对 Central Node 服务器的硬件要求

具有 Endpoint Agent 组件的最大主机数量	每分钟的最大电子邮件数	来自具有 Central Node 组件的服务器上的 SPAN 端口的最大流量 (Mbps)	3 GHz 时的最小逻辑核心数	最小RAM (GB)
100	1	20	6	31*/32
250	5	50	6	31/32
500	30	100	12	31/40
750	30	100	12	31/46

* 斜线前的值表示安装 Central Node 组件所需的 RAM 数量。安装后，必须将 RAM 数量增加到斜线后的值。

安装和执行应用程序的初始配置

本节包含 Kaspersky Anti Targeted Attack Platform 的安装和初始配置说明。

准备安装应用组件

本节提供有关如何为安装 Kaspersky Anti Targeted Attack Platform 组件准备企业 IT 基础架构的信息。

准备 IT 基础架构以安装应用程序组件

本节介绍安装应用程序之前必须配置的端口。为了应用程序组件在安装后能够正确运行，您必须配置防火墙规则。

在安装应用程序前，请准备企业 IT 基础构架以安装 Kaspersky Anti Targeted Attack Platform 组件：

1. 确保服务器、要使用应用程序 Web 界面的计算机以及要安装“Endpoint Agent”组件的计算机均满足硬件和软件要求。
2. 为了保护网络免受被分析对象的攻击，拒绝管理网络接口和用于处理对象的互联网访问的网络接口访问 Sandbox 服务器的本地网络。
3. 按照下表准备企业 IT 基础设施：

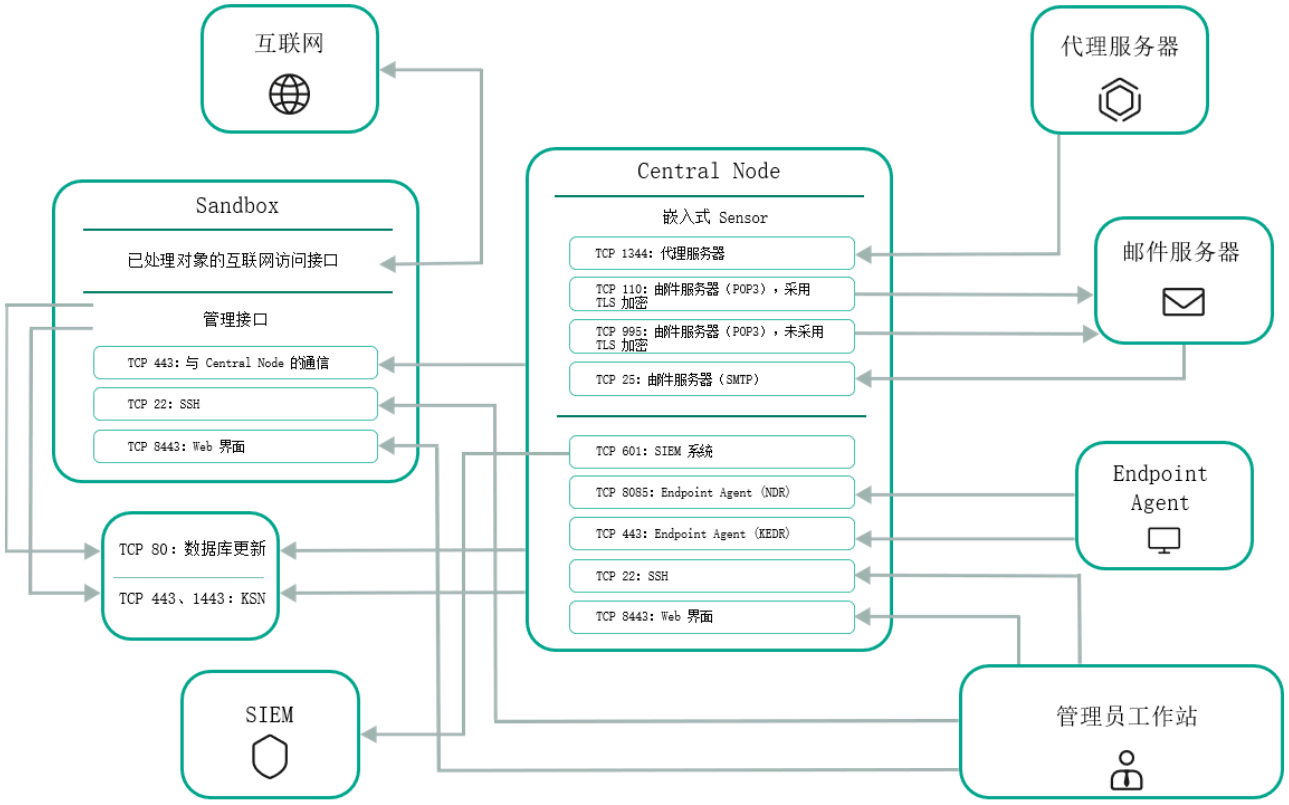
Kaspersky Anti Targeted Attack Platform 组件之间交互的端口

来源	方向	端口或协议	描述
Central Node	入站	TCP 22	通过 SSH 连接到服务器
		TCP 443	从 Endpoint Agent (KEDR) 接收数据
		TCP 8085	从 Endpoint Agent (NDR) 接收数据
		TCP 8443	访问应用程序的 Web 界面
		TCP 7423、8443、9081、13520	与 Sensor 服务器的通信
		UDP 53	
	传出	TCP 80 TCP 443 TCP 1443	与 KSN 服务器和卡巴斯基更新服务器的通信
		TCP 443	将对象发送到 Sandbox 进行扫描
		TCP 601	向 SIEM 系统发送消息
		TCP 9443	与 Sensor 服务器的通信
		UDP 53	
	入站和出站	ESP	用于通过基于 IPSec 协议的安全链路在 Central Node 和 Sensor 之间进行交互

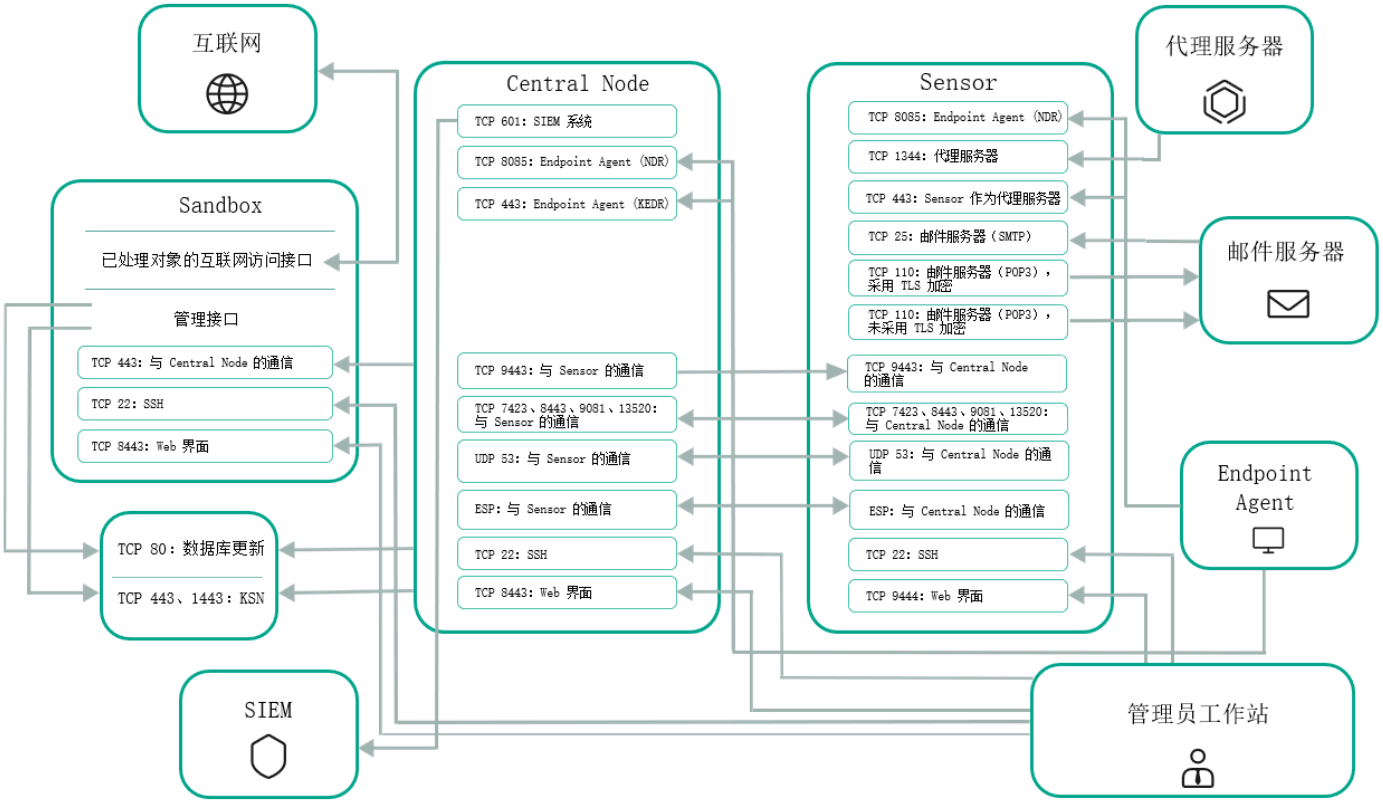
来源	方向	端口或协议	描述
Sensor	入站	TCP 22	通过 SSH 连接到服务器
		TCP 1344	从代理服务器接收流量
		TCP 25	从邮件服务器接收 SMTP 流量
		TCP 443	当 Sensor 用作代理服务器，用于在具有 Endpoint Agent 的工作站和 Central Node 之间进行通信时
		TCP 8085	从 Endpoint Agent (NDR) 接收数据
		TCP 9444	访问组件的 Web 界面。该端口默认是关闭的。
		TCP 9443	与 Central Node 服务器的通信
		UDP 53	
	传出	TCP 80 TCP 443	与 KSN 服务器和卡巴斯基更新服务器的通信
		TCP 995	与邮件服务器集成以实现安全连接
		TCP 110	与邮件服务器集成以辅助不安全的连接
		TCP 7423、8443、9081、13520	与 Central Node 服务器的通信
		UDP 53	
	入站和出站	ESP	用于通过基于 IPSec 协议的安全链路在 Central Node 和 Sensor 之间进行交互
Sandbox	入站（管理 接口）	TCP 22	通过 SSH 连接到服务器
		TCP 443	与 Central Node 交互
		TCP 8443	访问应用程序的 Web 界面
	出站（管理接口）	TCP 80 TCP 443	与卡巴斯基更新服务器通信
	出站和对应的入站（所处理对象的访问接口）	任何	访问互联网以分析已处理对象的网络行为。 拒绝访问企业局域网以保护网络免受被分析对象的攻击。
SCN（使用分布式解决方案模式时）	传出	TCP 8443、8444	用于通过基于 IPSec 协议的安全链路在 SCN 和 PCN 之间进行交互
	入站和出站	TCP 443、53、11000:11006、UDP 53 ESP	
PCN（使用分布式解决方案模式时）	入站	TCP 8443、8444	
	入站和出站	TCP 443、53、11000:11006、UDP 53 ESP	

如果在 VMware ESXi™ 虚拟环境中安装仅接收镜像流量的其他网络接口，请使用 E1000 网络适配器或禁用 VMXNET3 网络适配器上的 LRO（大量接收减负）选项。

下图展示了应用程序组件与应用程序所依赖的系统之间的网络通信图。图中的箭头表示链接的方向：每个箭头从发起连接的对象指向响应的对象。



应用程序组件与应用程序所依赖的系统之间的网络通信图。用嵌入式 Sensor 部署的 Central Node



应用程序组件与应用程序所依赖的系统之间的网络通信图。部署在与 Central Node 不同的服务器上的 Sensor

为通过 POP3 与用于接收消息的邮件服务器集成准备 IT 基础构架

如果使用 Microsoft Exchange 邮件服务器作为您的邮件服务器，并且电子邮件发件人配置了阅读回执通知请求，则必须禁用阅读回执通知。否则，阅读回执通知将从您配置用于 Kaspersky Anti Targeted Attack Platform 接收邮件的电子邮件地址发送出去。您还必须禁用自动处理会议请求，以防止占用 Kaspersky Anti Targeted Attack Platform 接收邮件的邮箱。

要禁用发送来自 Kaspersky Anti Targeted Attack Platform 接收邮件的电子邮件地址的阅读回执通知：

1. 在 Microsoft Exchange 服务器上，检查通知是否已启用。为此，请执行以下命令：

   ```
   Get-MailboxMessageConfiguration -Identity <Kaspersky Anti Targeted Attack Platform 接收邮件的电子邮件地址> | fl
   ```

2. 如果通知已启用，请运行以下命令：

   ```
   Set-MailboxMessageConfiguration -Identity <Kaspersky Anti Targeted Attack Platform 接收邮件的电子邮件地址> -ReadReceiptResponse NeverSend
   ```

   这将禁用来自 Kaspersky Anti Targeted Attack Platform 接收邮件的电子邮件地址的阅读回执通知。

要禁用自动处理会议请求：

1. 在 Microsoft Exchange 服务器上，检查通知是否已启用。为此，请执行以下命令：

   ```
   Get-CalendarProcessing -Identity <Kaspersky Anti Targeted Attack Platform 接收邮件的电子邮件地址> | fl
   ```

2. 如果自动处理会议请求已启用，请运行以下命令：

   ```
   Set-CalendarProcessing -Identity <Kaspersky Anti Targeted Attack Platform 接收邮件的电子邮件地址> -AutomateProcessing:None
   ```

   这将禁用自动处理会议请求。

为通过 SMTP 与邮件服务器集成准备 IT 基础构架

要为通过 SMTP 协议集成 Kaspersky Anti Targeted Attack Platform 与邮件服务器而准备企业 IT 基础构架：

1. 在外部邮件服务器上配置规则，以便将要发送的用于 Kaspersky Anti Targeted Attack Platform 扫描的邮件副本转发到 Kaspersky Anti Targeted Attack Platform 指定的地址中。

2. 指定将电子邮件转发到 Sensor 服务器的路由。

   建议指定一个静态路由 — Sensor 服务器的 IP 地址。

3. 配置组织的防火墙以允许从正在转发电子邮件信息副本的邮件服务器到 Sensor 服务器端口 25 的入站连接。

您也可以通过 SMTP 协议提高 Kaspersky Anti Targeted Attack Platform 与邮件服务器集成的安全性。

要通过 SMTP 协议提高 Kaspersky Anti Targeted Attack Platform 与邮件服务器集成的安全性。

1. 在为 Kaspersky Anti Targeted Attack Platform 转发电子邮件的邮件服务器端，配置 Kaspersky Anti Targeted Attack Platform 服务器的认证。
2. 在为 Kaspersky Anti Targeted Attack Platform 转发电子邮件的邮件服务器上配置强制加密流量。
3. 在 Kaspersky Anti Targeted Attack Platform 端，配置为 Kaspersky Anti Targeted Attack Platform 转发电子邮件的邮件服务器的认证。

准备虚拟机以安装 Sandbox 组件

准备虚拟机以安装 Sandbox 组件：

1. 运行 VMware ESXi hypervisor。
2. 打开虚拟机管理控制台。
3. 在要安装 Sandbox 组件的虚拟机的上下文菜单中，选择**编辑设置**。
   这将打开虚拟机属性窗口。
4. 在**虚拟硬件**选项卡上，展开CPU设置组并选中**向来宾操作系统公开硬件辅助虚拟化**复选框。
5. 在**虚拟机选项**选项卡上的**延迟敏感度**下拉列表中，选择**高**。
6. 单击**确定**。

虚拟机已准备好安装 Sandbox 组件。

准备包含 Central Node、Sensor 和 Sandbox 组件的安装磁盘镜像

安装应用程序之前，您需要准备好基于 Astra Linux 操作系统的安装盘 iso 镜像，其中包含 Central Node、Sensor 和 Sandbox 组件。

可用于创建 iso 镜像的设备的最低硬件要求：

- CPU：4 核，时钟频率 2500 MHz 或更高。
- RAM：8 千兆字节 (GB)。
- 可用磁盘空间：100 GB。

软件要求：

- 基于最新 Linux 内核的操作系统。
- Docker 20 或更高版本

- 提供 Astra Linux Special Edition 1.7.5 的 iso 镜像

  Kaspersky Anti Targeted Attack Platform 不支持其他版本的 Astra Linux 操作系统。

要挂载基于 Astra Linux 操作系统、包含 Central Node 和 Sensor 或 Sandbox 组件的 iso 镜像：

1. 从分发包中，下载 Central Node 和 Sensor 组件分发包（kata-cn-distribution-7.0.3.520-x86_64_en-ru-zh.tar.gz）、Sandbox 组件分发包（kata-sb-distribution-7.0.3.520-x86_64_en-ru.tar.gz）和名为 iso-builder-7.0.3.520-x86_64_en-ru.tar 的文件。

2. 创建**包含以下内容的**iso_builder.sh 文件。

   # $1 - absolute source_iso_host_path

   # $2 - absolute distribution_host_path

   # $3 - absolute iso_builder_image_host_path

   # $4 - absolute build_host_path

   # $5 - absolute target_iso_name

   docker load -i $3

   docker run -v $1:$1 -v $2:$2 -v $4:/build kaspersky/kata/deployment/iso_builder:6.0 --source-iso-uri file://$1 --kata-distribution-uri file://$2 --target-iso-name $5

3. 运行`mkdir /var/kata_builder`命令。

4. 将步骤 1 中列出的文件放入新创建的 /var/kata_builder 目录中。确保 Astra Linux Special Edition 1.7.5 iso 镜像被命名为“installation-1.7.5.16-06.02.24_14.21.iso”。如果 iso 镜像的名称不同，请对其进行重命名。

5. 运行以下命令：

   - 如果您正在准备包含 Central Node 和 Sensor 组件的磁盘镜像：`sudo ./iso_builder.sh /var/kata_builder/installation-1.7.5.16-06.02.24_14.21.iso /var/kata_builder/kata-cn-distribution-7.0.3.520-x86_64_en-ru-zh.tar.gz /var/kata_builder/iso-builder-7.0.3.520-x86_64_en-ru.tar /var/kata_builder buildCNSensorAstra.iso`

   - 如果您正在准备包含 Sandbox 组件的磁盘镜像：`sudo ./iso_builder.sh /var/kata_builder/installation-1.7.5.16-06.02.24_14.21.iso /var/kata_builder/kata-sb-distribution-7.0.3.520-x86_64_en-ru.tar.gz /var/kata_builder/iso-builder-7.0.3.520-x86_64_en-ru.tar /var/kata_builder buildSandboxAstra.iso`

运行命令后，包含 Central Node 和 Sensor 组件的安装磁盘镜像（名为 buildCNSensorAstra.iso 和 buildSandboxAstra.iso）位于 /var/kata_builder 目录中。

如果您使用其他目录存放文件，可以执行以下命令：`sudo ./iso_builder.sh <source_iso_host_path> <distribution_host_path> <iso_builder_image_host_path> <build_host_path> <target_iso_name>`，其中：

- source_iso_host_path 是 Astra Linux Special Edition 1.7.5 的分发包的路径。
- distribution_host_path 是分发套件的路径：kata-cn-distribution-7.0.3.520-x86_64_en-ru-zh.tar.gz 或 kata-sb-distribution-7.0.3.520-x86_64_en-ru.tar.gz。
- iso_builder_image_host_path 是 iso-builder-7.0.3.520-x86_64_en-ru.tar 文件的路径。
- build_host_path 是挂载的 ISO 镜像必须所在的路径，无需指定分配给 ISO 镜像的名称。
- target_iso_name 是分配给 ISO 镜像的名称。

安装和配置应用程序组件的步骤

安装和配置应用程序涉及以下步骤：

1. **安装包含 Sandbox 组件的磁盘镜像**
2. **通过 Sandbox Web 界面配置 Sandbox 组件**
3. **安装 Microsoft Windows 操作系统和 Sandbox 组件应用程序的磁盘镜像**
4. **安装 Central Node 和 Sensor 组件**

   您可以采用以下配置之一安装 Central Node 和 Sensor 组件：

   - 集群。
   - 服务器。

   如果有多个 Central Node 组件，则可以在分布式解决方案模式下使用该应用程序。
5. **安装 Sensor 组件**

   如果有多个 Sensor 组件，则可以在必要数量的服务器上安装和配置 Sensor 组件。
6. **配置 Central Node 和 Sensor 组件。**
7. **在公司 IT 基础架构的计算机上安装 Endpoint Agent 组件。**

   作为 Endpoint Agent 组件，您可以使用以下应用程序： Kaspersky Endpoint Agent for Windows、 Kaspersky Endpoint Security for Windows、 Kaspersky Endpoint Security for Linux、 Kaspersky Endpoint Security for Mac。

   以下“帮助”部分提供了有关代表 Endpoint Agent 组件的应用程序版本与 Kaspersky Anti Targeted Attack Platform 版本的兼容性的信息： Kaspersky Endpoint Agent for Windows、Kaspersky Endpoint Security for Windows、Kaspersky Endpoint Security for Linux、Kaspersky Endpoint Security for Mac。

Kaspersky Endpoint Agent 应用程序可在以下配置中使用：

- 不与 EPP 应用程序集成。

  在这种情况下，您只需安装Kaspersky Endpoint Agent for Windows。

- 与 EPP 应用程序集成。

  在这种情况下，Kaspersky Endpoint Agent 还会将有关 EPP 应用程序检测到的威胁的信息以及该应用程序的威胁处理结果发送到 Central Node 服务器。

Kaspersky Endpoint Agent for Windows 可以与以下 EPP 应用程序集成：

- Kaspersky Endpoint Security for Windows

  Kaspersky Endpoint Agent for Windows 与 Kaspersky Endpoint Security for Windows 集成

  要集成这些应用程序，您必须将 Kaspersky Endpoint Agent 作为 Kaspersky Endpoint Security 的一部分进行安装。不支持集成单独安装的应用程序。

  要将 Kaspersky Endpoint Agent 作为 Kaspersky Endpoint Security 的一部分进行安装：

  1. 开始安装 Kaspersky Endpoint Security 应用程序，该应用程序的分发包中包含 Kaspersky Endpoint Agent。

     有关安装 Kaspersky Endpoint Security 的更多详细信息，请参阅*Kaspersky Endpoint Security for Windows 帮助*。

  2. 在安装过程中，选择 Endpoint Agent 组件。

  安装带有 Endpoint Agent 组件的应用程序后，已安装的应用程序列表会包括 Kaspersky Endpoint Security 和 Kaspersky Endpoint Agent。

  如有必要，您可以升级已作为 Kaspersky Endpoint Security 的一部分安装的 Kaspersky Endpoint Agent 应用程序。当 Kaspersky Endpoint Agent 应用程序升级和 Kaspersky Endpoint Security 应用程序升级时，应用程序兼容版本之间的集成都会得到维护。您可以升级 Kaspersky Endpoint Agent 版本 3.7 或更高版本的先前版本。

- Kaspersky Security for Windows Server。

  Kaspersky Endpoint Agent for Windows 与 Kaspersky Security for Windows Server 集成

  要集成这些应用程序，您必须将 Kaspersky Endpoint Agent 作为 Kaspersky Security for Windows Server 的一部分进行安装。不支持集成单独安装的应用程序。

  要将 Kaspersky Endpoint Agent 作为 Kaspersky Security for Windows Server 的一部分进行安装：

  1. 开始安装 Kaspersky Security for Windows Server 应用程序，该应用程序的分发包中包含Kaspersky Endpoint Agent。

     有关安装 Kaspersky Security for Windows Server 的更多详细信息，请参阅*Kaspersky Security for Windows Server 帮助*。

  2. 在安装过程中，选择 Kaspersky Endpoint Agent 组件。

  安装带有 Kaspersky Endpoint Agent 组件的应用程序后，已安装的应用程序列表包括 Kaspersky Security for Windows 和 Kaspersky Endpoint Agent。

  如有必要，您可以升级 Kaspersky Endpoint Agent 应用程序，它已作为 Kaspersky Security for Windows Server 的一部分安装。当 Kaspersky Endpoint Agent 升级和 Kaspersky Security for Windows Server 升级时，应用程序的兼容版本之间的集成都会得到维护。

- Kaspersky Security for Virtualization Light Agent for Windows。

  Kaspersky Endpoint Agent for Windows 与 Kaspersky Security for Virtualization Light Agent 的集成

  Kaspersky Endpoint Agent 和 Kaspersky Security for Virtualization Light Agent 单独安装。Kaspersky Endpoint Agent 无法作为 Kaspersky Security for Virtualization Light Agent 的一部分进行安装。

  要启用 Kaspersky Endpoint Agent 与 Kaspersky Security for Virtualization Light Agent 的集成：

  1. 如果尚未安装 Kaspersky Security for Virtualization Light Agent，请安装。
  2. 启用Light Agent 与 Kaspersky Endpoint Agent 的集成。

     您可以在安装或升级 Light Agent 期间启用与 Kaspersky Endpoint Agent 的集成。您还可以使用 Light Agent 已安装组件集的修改过程来启用与 Kaspersky Endpoint Agent 的集成。

     有关安装、启用集成、升级应用程序以及修改已安装应用程序组件集的过程的更多详细信息，请参阅 *Kaspersky Security for Virtualization Light Agent在线帮助*。
  3. 如果尚未在虚拟机上安装 Kaspersky Endpoint Agent 应用程序，请使用 Light Agent 安装它。

  > 要与 Kaspersky Security for Virtualization Light Agent 5.2 集成，我们建议使用 Kaspersky Endpoint Agent 3.14。如有必要，您可以升级 Kaspersky Endpoint Agent 应用程序和 Kaspersky Security for Virtualization Light Agent。升级应用程序时，兼容版本之间的集成将保持不变。

- Kaspersky Industrial CyberSecurity for Nodes。

  Kaspersky Endpoint Agent for Windows 与 Kaspersky Industrial CyberSecurity for Nodes 的集成

  要启用 Kaspersky Endpoint Agent 与 Kaspersky Industrial CyberSecurity for Nodes 的集成：

  1. 如果尚未安装 Kaspersky Industrial CyberSecurity for Nodes 应用程序，请安装该应用程序。

     有关安装的更多详细信息，请参阅*Kaspersky Industrial CyberSecurity for Nodes 帮助*。
  2. 如果尚未安装 Kaspersky Endpoint Agent 应用程序，请在同一设备上安装它。

     应用程序会自动集成。

  > 要与 Kaspersky Industrial CyberSecurity for Nodes 集成，必须在 Kaspersky Endpoint Agent中安装相应的授权许可密钥。

  如需详细信息，请联系客户经理。

有关 Kaspersky Endpoint Agent for Windows 版本与 EPP 应用程序的兼容性的信息，请参阅Kaspersky Endpoint Agent for Windows 版本与 EPP 应用程序的兼容性部分。

有关安装 Kaspersky Endpoint Security 的详细信息，请参阅应用程序的在线帮助：

- 安装 Kaspersky Endpoint Security for Windows
- 安装 Kaspersky Endpoint Security for Linux
- 安装 Kaspersky Endpoint Security for Mac

如果您的主机安装了早期版本的应用程序，您可以升级它们。有关详细信息，请参阅以下部分。

安装 Sandbox 组件

本节提供有关安装 Sandbox 组件的分步说明。

要开始 Sandbox 组件的安装：

1. 运行包含 Sandbox 组件的磁盘镜像。

   安装向导启动。

2. 单击**确定**。

步骤 1：查看最终用户授权许可协议和隐私策略

要继续安装，您必须阅读并接受 AO Kaspersky Lab 的最终用户授权许可协议和隐私策略的条款和条件（以下分别称为“最终用户授权许可协议”和“隐私策略”）。仅当您接受最终用户授权许可协议和隐私政策的条款后，安装才能继续进行。

要在安装基于 Ubuntu Server 操作系统的 Sandbox 组件时接受 AO Kaspersky Lab 的最终用户授权许可协议和隐私策略的条款和条件：

1. 在列表中选择用于查看最终用户授权许可协议和隐私策略的语言，然后按 **Enter**。

   要向上和向下移动，您可以使用以下键：↑、↓、**PageUp** 和 **PageDown**。

   这将打开显示最终用户授权许可协议文本的窗口。

2. 请阅读最终用户授权许可协议。

3. 如果您接受最终用户授权许可协议的条款和条件，请选择“**我接受**”并按 **Enter**。

   这将打开一个显示隐私政策文本的窗口。

4. 请仔细阅读隐私政策。

5. 如果您接受隐私策略的条款和条件，请选择“**我接受**”并按 **Enter**。

   安装向导将继续执行下一步。

要在安装基于 Astra Linux 操作系统的 Sandbox 组件时接受 AO Kaspersky Lab 的最终用户授权许可协议和隐私策略的条款和条件：

1. 如果您使用 BIOS 进行安装，请按“**F1**”键，从列表中选择用于查看 Astra Linux 操作系统的最终用户授权许可协议、最终用户授权许可协议和隐私策略的语言，然后按“**Enter**”。

   这将打开一个窗口，其中包含 Astra Linux 最终用户授权许可协议的文本。

2. 阅读 Astra Linux 操作系统的最终用户授权许可协议。

   要向上和向下移动，您可以使用以下键：↑、↓、**PageUp** 和 **PageDown**。

3. 如果您接受 Astra Linux 操作系统的最终用户授权许可协议的条款和条件，请选择“**Yes**”并按 **Enter**。

   这将打开一个窗口，其中包含 AO Kaspersky Lab 最终用户授权许可协议的文本。

4. 请阅读最终用户授权许可协议。
5. 如果您接受最终用户授权许可协议的条款和条件，请选择"**I accept**"并按 **Enter**。
   这将打开一个显示隐私政策文本的窗口。
6. 请仔细阅读隐私政策。
7. 如果您接受隐私策略的条款和条件，请选择"**I accept**"并按 **Enter**。

安装向导将继续执行下一步。

步骤 2：选择安装 Sandbox 组件的磁盘

选择用于安装 Sandbox 组件的物理磁盘。

要选择用于安装组件的磁盘：

1. 选择用于安装组件的建议驱动器之一，然后按**Enter**。
   确认窗口将显示。
2. 单击**安装**。
   包含安装文件的存档将被解压到磁盘。服务器将重新启动。

安装向导将继续执行下一步。

步骤 3：分配主机名

分配由 DNS 服务器使用的服务器主机名称。

为服务器分配主机名：

1. 在**主机名**字段中，输入服务器的完整域名。
   以 FQDN 格式指定服务器名称（例如：host.domain.com 或 host.domain.subdomain.com）。
2. 单击**确定**。

安装向导将继续执行下一步。

步骤 4：在列表中选择控制网络接口

为保证 Sandbox 组件正常运行，必须连接至少两个网卡，并配置以下网络接口：

- 管理网络接口。该接口用于提供对 Sandbox 服务器的 SSH 访问；Sandbox 服务器也使用此接口从 Central Node 接收对象。
- 用于对已处理对象进行 Internet 访问的网络接口。由 Sandbox 处理的对象可以使用此接口尝试在互联网上活动，并且 Sandbox 可以分析其行为。如果阻止互联网访问，则 Sandbox 无法分析互联网上对象的行为，因此将只分析无互联网访问的对象的行为。

  > 用于对已处理对象进行 Internet 访问的网络接口必须与组织的本地网络隔离。

选择想要用作控制接口的网络接口。

要选择管理网络接口：

1. 在网络接口列表中，选择您想要用作管理接口的网络接口。
2. 按下“**Enter**”。

   安装向导将继续执行下一步。

步骤 5：分配控制接口的地址和网络掩码

要分配管理网络接口的 IP 地址和网络掩码：

1. 在**地址**字段中，输入想要分配给此网络接口的 IP 地址。
2. 在**网络掩码**字段中，输入想使用此网络接口的网络掩码。
3. 单击**确定**。

安装向导将继续执行下一步。

步骤 6：添加 DNS 服务器地址

添加 DNS 服务器地址：

1. 在 **DNS 服务器**窗口中，选择**新建**并按 **ENTER**。
   这将打开 DNS 服务器地址输入窗口。
2. 在 **DNS 服务器**文本框中，以 IPv4 格式输入主 DNS 服务器的 IP 地址。

3. 单击**确定**。
   DNS 服务器地址输入窗口关闭。
4. 如果要添加其他 DNS 服务器的 IP 地址，请重复 **DNS 服务器**窗口中的步骤。
5. 添加完 DNS 服务器后，在 **DNS 服务器**窗口中，选择**继续**并按 **ENTER**。

安装向导将继续执行下一步。

步骤 7：配置静态网络路由

要配置静态网络路由：

1. 在**IPv4 路由器**窗口中，选择**新建**并按**ENTER**。
   这将打开 **IPv4 静态路由**窗口。
2. 在**地址/掩码**字段中，输入要为其配置网络路由的子网的 IP 地址和掩码。
3. 如果要使用默认网络路由，请输入 0.0.0.0/0。
4. 在**网关**字段中，输入网关的 IP 地址。
5. 单击**确定**。
6. 如果要添加其他网络路由，请重复**IPv4 静态路由**窗口中的步骤。
7. 如果您已完成添加网络路由，请单击**继续**。

安装向导将继续执行下一步。

步骤 8：配置 Sandbox 管理员密码的最小密码长度

要设置 Sandbox 组件的管理员密码的最小长度：

1. 在**最小长度**中，输入长度（以字符为单位）。建议密码长度为 12 个或更多字符。
2. 单击**确定**。

安装向导将继续执行下一步。

步骤 9：创建 Sandbox 管理员账户

创建一个管理员账户，用于在 Sandbox Web 界面、管理员菜单以及具有 Sandbox 组件的服务器的管理控制台中工作。

要创建 Sandbox 管理员账户：

1. 在**用户名**字段中，输入管理员账户名称。默认使用'admin'账户。
2. 在**密码**字段中，输入管理员账户的密码。
   密码必须满足以下要求：
   - 必须包含至少 8 个字符。
   - 必须包含至少三种字符：
     - 大写字母 (A-Z)。
     - 小写字母 (a-z)。
     - 数字。
     - 特殊字符。
   - 不能与用户名完全或基本相同。
3. 在**确认密码**字段中，再次输入密码。
4. 单击**确定**。
   这将打开一个窗口，其中包含 Sandbox 服务器的 IP 地址。您可以在 Web 浏览器中输入此地址以打开 Sandbox Web 界面。要登录，请使用您创建的 Sandbox 管理员账户。
   Sandbox 服务器将重新启动。

继续通过 Web 界面配置 Sandbox 组件。

将带有嵌入式 Sensor 的 Central Node 组件部署为集群

一个集群必须至少包含 4 台服务器：2 台存储服务器和 2 台处理服务器。您可以使用"规模调整指南"来确定适合您组织的服务器数量。

以集群形式部署带有嵌入式 Sensor 的 Central Node 组件包括以下步骤：

1. **部署第一台存储服务器**
   第一步是部署存储服务器。部署存储服务器后，您可以向集群添加其他存储和处理服务器。
2. **部署处理服务器**和**附加存储服务器**
   您可以按任何顺序部署服务器。
3. **配置应用程序的大小设置**
   在集群部署的最后阶段，您需要配置应用程序的扩展设置：指定计划的 SPAN 流量、电子邮件流量、具有 Endpoint Agent 组件的主机数量以及存储和事件数据库的大小。

Central Node 组件始终与 Sensor 组件一起安装。如果您需要单独使用 Central Node 组件，则在部署处理服务器时，请在步骤 10中关闭从 SPAN 端口接收镜像流量。

如果您在物理服务器上部署了群集，并且想要向这些服务器添加更多的硬盘驱动器，或者更换一些现有驱动器，然后重新安装群集，则在安装组件之前，您必须清除存储服务器上以前分配给 OSD (Object Storage Daemon) 的驱动器。否则，不能保证应用程序正常运行。如果您想完全断开驱动器并且不再计划将其重新连接到服务器，则无需清除驱动器。

部署存储服务器

要部署数据存储服务器，您需要运行具有 Central Node 和 Sensor 组件的磁盘镜像。

如果执行安装向导步骤时出现错误，请联系技术支持。

步骤 1. 查看最终用户授权许可协议和隐私策略

要继续安装，您必须阅读最终用户授权许可协议和隐私政策并接受其条款和条件。仅当您接受最终用户授权许可协议和隐私政策的条款后，安装才能继续进行。

安装基于 Ubuntu 操作系统的组件时接受最终用户授权许可协议和隐私政策的条款和条件：

1. 在列表中选择用于查看 AO Kaspersky Lab 最终用户授权许可协议和隐私策略的语言，然后按 **Enter**。
   这将打开一个窗口，其中包含 AO Kaspersky Lab 最终用户授权许可协议的文本。
2. 阅读 AO Kaspersky Lab 最终用户授权许可协议。
   要向上和向下移动，您可以使用以下键：↑、↓、**PageUp** 和 **PageDown**。
3. 如果您接受 AO Kaspersky Lab 最终用户授权许可协议，请选择“**我接受**”并按“**Enter**”。
   这将打开一个显示 AO Kaspersky Lab 隐私策略文本的窗口。
4. 阅读 AO Kaspersky Lab 隐私策略。
5. 如果您接受 AO Kaspersky Lab 隐私策略的条款和条件，请选择“**我接受**”并按 **Enter**。

安装向导将继续执行下一步。

安装基于 Astra Linux 操作系统的组件时接受最终用户授权许可协议和隐私政策的条款和条件：

1. 按 **F1** 键从列表中选择查看 Astra Linux 操作系统最终用户授权许可协议的语言，然后按 **Enter**。
   这将打开一个窗口，其中包含 Astra Linux 最终用户授权许可协议的文本。
2. 阅读 Astra Linux 操作系统的最终用户授权许可协议。
   要向上和向下移动，您可以使用以下键：↑、↓、**PageUp** 和 **PageDown**。
3. 如果您接受 Astra Linux 操作系统的最终用户授权许可协议的条款和条件，请选择“**Yes**”并按 **Enter**。
   这将打开一个窗口，您可以在其中选择查看 AO Kaspersky Lab 最终用户授权许可协议和隐私策略的语言。

4. 在列表中选择用于查看 AO Kaspersky Lab 最终用户授权许可协议和隐私策略的语言，然后按 **Enter**。
   这将打开一个窗口，其中包含 AO Kaspersky Lab 最终用户授权许可协议的文本。

5. 阅读 AO Kaspersky Lab 最终用户授权许可协议。
   要向上和向下移动，您可以使用以下键：↑、↓、**PageUp** 和 **PageDown**。

6. 如果您接受 AO Kaspersky Lab 最终用户授权许可协议的条款和条件，请选择“**I accept**”并按“**Enter**”。
   这将打开一个显示 AO Kaspersky Lab 隐私策略文本的窗口。

7. 阅读 AO Kaspersky Lab 隐私策略。

8. 如果您接受 AO Kaspersky Lab 隐私策略的条款和条件，请选择“**I accept**”并按“**Enter**”。

安装向导将继续执行下一步。

步骤 2：选择服务器角色

要选择服务器角色：

1. 选择以下选项之一：

   - **storage**。
     该角色用于安装存储服务器，以将 Central Node 组件部署为集群。
   - **processing**。
     该角色用于安装处理服务器，以将 Central Node 组件部署为集群。

     > 该角色还包括 Sensor 组件的安装和配置。

   - **single**。
     该角色用于在同一服务器上安装 Central Node 和 Sensor 组件。
   - **sensor**。
     此角色用于在独立服务器上安装 Sensor 组件。

2. 按下“**Enter**”。

安装向导将继续执行下一步。

步骤 3：选择部署模式

选择部署模式：

1. 选择以下选项之一：

   - **首个节点安装**。
     当部署集群中的第一台服务器时选择此值。

- **向集群添加额外节点**。
  当部署将被添加到现有集群的服务器时选择此值。

2. 按下“**Enter**”。

安装向导将继续执行下一步。

步骤 4：选择安装组件的磁盘

您至少需要 150 GB 的磁盘空间。如果可用磁盘空间少于 150 GB，安装将完成并出现错误。

要选择用于安装组件的磁盘：

1. 选择用于安装组件的建议驱动器之一，然后按**Enter**。
   确认窗口将显示。
2. 选择**是**，然后按 **Enter** 键。

安装向导将继续执行下一步。

步骤 5：为服务器寻址选择网络掩码

我们建议使用默认值。

该网络掩码可能与组织基础架构中使用的网络掩码不匹配。

要指定服务器寻址的网络掩码：

- 如果要使用网络掩码的预定义值，请选择“**确定**”按钮，然后按 **Enter**。
  默认值：198.18.0.0/16。
- 如果要指定不同的网络掩码，请在“**子网**”字段中输入您的值，选择“**确定**”按钮，然后按 **Enter**。
  掩码必须与模板匹配：xx0.0/16。

安装向导将继续执行下一步。

步骤 6：为应用程序组件的寻址选择网络掩码

我们建议使用默认值。

应用程序组件寻址的网络不得与集群服务器寻址的网络重叠。

要指定用于寻址应用程序主要组件的网络掩码：

- 如果要使用网络掩码的预定义值，请选择“**确定**”按钮，然后按 **Enter**。
  默认值：198.19.0.0/16。
- 如果要指定不同的网络掩码，请在“**Bridge/Overlay 子网**”字段中输入您的值，选择“**确定**”按钮，然后按 **Enter**。
  掩码必须与模板匹配：xx0.0/16。

安装向导将继续执行下一步。

步骤 7：选择集群网络接口

集群网络接口用于集群服务器之间的通信。

要选择集群网络接口：

1. 选择包含用于内部网络的网络接口的行。
   要选择一行，您可以使用 ↑、↓、PageUp 和 PageDown 键。所选行以红色突出显示。
2. 按下“**Enter**”。

安装向导将继续执行下一步。

步骤 8：选择外部网络接口

外部网络接口用于通过 SSH 访问服务器、管理 Kaspersky Anti Targeted Attack Platform 的 Web 界面以及其他外部连接。

要选择外部网络接口：

1. 选择包含用于外部网络的网络接口的行。
   要选择一行，您可以使用 ↑、↓、PageUp 和 PageDown 键。所选行以红色突出显示。
2. 按下“**Enter**”。

安装向导将继续执行下一步。

步骤 9：选择获取网络接口 IP 地址的方法

要选择用于获取网络接口 IP 地址的方法：

1. 选择包含**配置类型：**的行，然后按**Enter**。
   要选择一行，您可以使用 ↑、↓、PageUp 和 PageDown 键。所选行以红色突出显示。

2. 在打开的窗口中，选择以下选项之一：

   - **dhcp**。
   - **static**。

3. 如果您选择了 **static**：

   a. 选择包含参数的行然后按**Enter**键。

   b. 在打开的窗口中输入所需的数据，然后按**Enter**两次。

   > 您需要为每个参数指定一个值。

4. 选择包含**Save**的行。

5. 按下“**Enter**”。

安装向导将继续执行下一步。

步骤 10：创建管理员账户并对群集中的服务器进行身份验证

在此步骤中，您需要执行以下操作之一：

- 如果您要部署集群中的第一台服务器，请创建一个管理员账户。
- 如果您要部署其他存储服务器，请对集群中的服务器进行身份验证。

创建管理员账户

> 仅在部署集群中的第一台服务器时才需要管理员账户。如果您在部署额外的存储服务器，应用程序不会打开提示您创建管理员账户的窗口，而是提示您对集群中的服务器进行身份验证。

在部署集群中的第一台服务器时，您需要创建一个管理员账户。该用户账户用于管理应用程序的 Web 界面、应用程序的管理员菜单以及在技术支持模式下管理应用程序。

默认情况下，管理员账户的用户名为*admin*。您必须输入该用户账户的密码。

输入管理员用户账户的密码：

1. 这将打开一个窗口；在该窗口中，在“**最小长度**”字段中输入最小密码长度。您必须输入 8 或更大的值。
2. 选择**确定**，然后按 ENTER 键。
   这将打开密码创建窗口。
3. 这将打开一个窗口；在该窗口的“**密码**”字段中，输入管理员账户的密码。
   要选择一行，您可以使用 ↑、↓、PageUp 和 PageDown 键。所选行以红色突出显示。

4. 在**确认**字段中，再次输入新密码。

5. 选择**确定**，然后按 **ENTER** 键。

安装向导将继续执行下一步。

验证集群中的服务器

仅当部署额外的存储服务器时才需要对集群中的服务器进行身份验证。如果您正在部署集群中的第一台服务器，应用程序会提示您创建管理员账户，而不是对服务器进行身份验证。

要对集群中的服务器进行身份验证，您需要输入部署集群中第一台服务器时设置的管理员账户密码。

对集群中的服务器进行身份验证：

1. 在**密码**字段中，输入管理员账户的密码。

2. 选择**确定**，然后按 **Enter** 键。
   要选择按钮，可以使用 ↑、↓、PageUp 和 PageDown 键。

集群中的服务器将得到身份验证。安装向导将继续执行下一步。

步骤 11：添加 DNS 服务器地址

如果您正在部署集群中的第一台服务器，则此步骤可用。

为具有应用程序组件的服务器的运行配置 DNS 设置。

添加 DNS 服务器地址：

1. 选择“**添加**”字段然后按 **Enter** 键。

2. 以 IPv4 格式输入 DNS 服务器的 IP 地址。

3. 如果要添加其他 DNS 服务器的 IP 地址，请选择“**添加**”字段，按 **Enter** 并输入服务器的地址。

4. 添加所有 DNS 服务器后，选择“**继续**”字段并按 **Enter**。

安装向导将继续执行下一步。

步骤 12：配置与 NTP 服务器的时间同步

如果您正在部署集群中的第一台服务器，则此步骤可用。

配置服务器时间与 NTP 服务器的同步。

1. 选择“**添加**”字段然后按 **Enter** 键。
2. 输入 NTP 服务器的 IP 地址或名称。
3. 如果要添加其他 NTP 服务器的 IP 地址或名称，请选择“**添加**”字段，按 **Enter**，然后输入 NTP 服务器的 IP 地址或名称。
4. 添加所有 NTP 服务器后，选择“**继续**”字段并按 **Enter**。

安装向导将继续执行下一步。

为了使集群正常运行，集群服务器上的时间必须同步。确保您添加的 NTP 服务器正常工作并能保证集群服务器之间的时间同步。

步骤 13：选择用于 Ceph 存储的磁盘

选择用于 Ceph 存储的磁盘。磁盘数量根据“规模调整指南”确定。

要为 Ceph 存储选择磁盘：

1. 选择包含所需驱动器的行。

   要选择一行，您可以使用 ↑、↓、PageUp 和 PageDown 键。所选行以红色突出显示。
2. 按下“**Enter**”。
3. 如果要选择多个驱动器，请重复步骤 1 到 2 以选择更多驱动器。
4. 选择“**应用并完成**”字段并按 **Enter**。

   确认窗口将显示。
5. 选择**是**，然后按 **Enter** 键。

配置可能需要一些时间。然后安装完成。您可以继续配置集群的服务器。

部署处理服务器

要部署处理服务器，您需要运行带有 Central Node 和 Sensor 组件的磁盘镜像。

如果执行安装向导步骤时出现错误，请联系技术支持。

步骤 1：查看最终用户授权许可协议和隐私策略

要继续安装，您必须阅读最终用户授权许可协议和隐私政策并接受其条款和条件。仅当您接受最终用户授权许可协议和隐私政策的条款后，安装才能继续进行。

安装基于 Ubuntu 操作系统的组件时接受最终用户授权许可协议和隐私政策的条款和条件：

1. 在列表中选择用于查看 AO Kaspersky Lab 最终用户授权许可协议和隐私策略的语言，然后按 **Enter**。
   这将打开一个窗口，其中包含 AO Kaspersky Lab 最终用户授权许可协议的文本。
2. 阅读 AO Kaspersky Lab 最终用户授权许可协议。
   要向上和向下移动，您可以使用以下键：↑、↓、**PageUp** 和 **PageDown**。
3. 如果您接受 AO Kaspersky Lab 最终用户授权许可协议，请选择“**我接受**”并按“**Enter**”。
   这将打开一个显示 AO Kaspersky Lab 隐私策略文本的窗口。
4. 阅读 AO Kaspersky Lab 隐私策略。
5. 如果您接受 AO Kaspersky Lab 隐私策略的条款和条件，请选择“**我接受**”并按 **Enter**。

安装向导将继续执行下一步。

安装基于 Astra Linux 操作系统的组件时接受最终用户授权许可协议和隐私政策的条款和条件：

1. 按 **F1** 键从列表中选择查看 Astra Linux 操作系统最终用户授权许可协议的语言，然后按 **Enter**。
   这将打开一个窗口，其中包含 Astra Linux 最终用户授权许可协议的文本。
2. 阅读 Astra Linux 操作系统的最终用户授权许可协议。
   要向上和向下移动，您可以使用以下键：↑、↓、**PageUp** 和 **PageDown**。
3. 如果您接受 Astra Linux 操作系统的最终用户授权许可协议的条款和条件，请选择“**Yes**”并按 **Enter**。
   这将打开一个窗口，您可以在其中选择查看 AO Kaspersky Lab 最终用户授权许可协议和隐私策略的语言。
4. 在列表中选择用于查看 AO Kaspersky Lab 最终用户授权许可协议和隐私策略的语言，然后按 **Enter**。
   这将打开一个窗口，其中包含 AO Kaspersky Lab 最终用户授权许可协议的文本。
5. 阅读 AO Kaspersky Lab 最终用户授权许可协议。
   要向上和向下移动，您可以使用以下键：↑、↓、**PageUp** 和 **PageDown**。
6. 如果您接受 AO Kaspersky Lab 最终用户授权许可协议的条款和条件，请选择“**I accept**”并按“**Enter**”。
   这将打开一个显示 AO Kaspersky Lab 隐私策略文本的窗口。
7. 阅读 AO Kaspersky Lab 隐私策略。
8. 如果您接受 AO Kaspersky Lab 隐私策略的条款和条件，请选择“**I accept**”并按“**Enter**”。

安装向导将继续执行下一步。

步骤 2：选择服务器角色

要选择服务器角色：

1. 选择以下选项之一：

   - **storage**。
     该角色用于安装存储服务器，以将 Central Node 组件部署为集群。
   - **processing**。
     该角色用于安装处理服务器，以将 Central Node 组件部署为集群。

     > 该角色还包括 Sensor 组件的安装和配置。

   - **single**。
     该角色用于在同一服务器上安装 Central Node 和 Sensor 组件。
   - **sensor**。
     此角色用于在独立服务器上安装 Sensor 组件。

2. 按下“**Enter**”。

安装向导将继续执行下一步。

步骤 3：选择安装组件的磁盘

> 您至少需要 150 GB 的磁盘空间。如果可用磁盘空间少于 150 GB，安装将完成并出现错误。

要选择用于安装组件的磁盘：

1. 选择用于安装组件的建议驱动器之一，然后按**Enter**。
   确认窗口将显示。
2. 选择**是**，然后按 **Enter** 键。

安装向导将继续执行下一步。

步骤 4：为群集服务器寻址选择网络掩码

> 我们建议使用默认值。

> 该网络掩码可能与组织基础架构中使用的网络掩码不匹配。

要指定集群服务器寻址的网络掩码：

- 如果要使用网络掩码的预定义值，请选择“**确定**”按钮，然后按 **Enter**。
  默认值：198.18.0.0/16。
- 如果要指定不同的网络掩码，请在“**子网**”字段中输入您的值，选择“**确定**”按钮，然后按 **Enter**。
  掩码必须与模板匹配：xx0.0/16。

安装向导将继续执行下一步。

步骤 5：为应用程序组件的寻址选择网络掩码

我们建议使用默认值。

应用程序组件寻址的网络不得与集群服务器寻址的网络重叠。

要指定用于寻址应用程序主要组件的网络掩码：

- 如果要使用网络掩码的预定义值，请选择“**确定**”按钮，然后按 **Enter**。
  默认值：198.19.0.0/16。
- 如果要指定不同的网络掩码，请在“**Bridge/Overlay 子网**”字段中输入您的值，选择“**确定**”按钮，然后按 **Enter**。
  掩码必须与模板匹配：xx0.0/16。

安装向导将继续执行下一步。

步骤 6：选择集群网络接口

集群网络接口用于集群服务器之间的通信。

要选择集群网络接口：

1. 选择包含用于内部网络的网络接口的行。
   要选择一行，您可以使用 ↑、↓、PageUp 和 PageDown 键。所选行以红色突出显示。
2. 按下“**Enter**”。

安装向导将继续执行下一步。

步骤 7：选择外部网络接口

外部网络接口用于通过 SSH 访问服务器、管理 Kaspersky Anti Targeted Attack Platform 的 Web 界面以及其他外部连接。

要选择外部网络接口：

1. 选择包含用于外部网络的网络接口的行。
   要选择一行，您可以使用 ↑、↓、PageUp 和 PageDown 键。所选行以红色突出显示。
2. 按下“**Enter**”。

安装向导将继续执行下一步。

步骤 8：选择获取网络接口 IP 地址的方法

要选择用于获取网络接口 IP 地址的方法：

1. 选择包含**配置类型：**的行，然后按**Enter**。
   要选择一行，您可以使用 ↑、↓、PageUp 和 PageDown 键。所选行以红色突出显示。
2. 在打开的窗口中，选择以下选项之一：
   - **dhcp**。
   - **static**。
3. 如果您选择了 **static**:
   a. 选择包含参数的行然后按**Enter**键。
   b. 在打开的窗口中输入所需的数据，然后按**Enter**两次。

   > 您需要为每个参数指定一个值。

4. 选择包含**Save**的行。
5. 按下“**Enter**”。

安装向导将继续执行下一步。

步骤 9：验证集群中的服务器

要对集群中的服务器进行身份验证，您需要输入部署集群中第一台服务器时设置的管理员账户密码。

对集群中的服务器进行身份验证：

1. 在**密码**字段中，输入管理员账户的密码。
2. 选择**确定**，然后按 **Enter** 键。
   要选择按钮，可以使用 ↑、↓、PageUp 和 PageDown 键。

集群中的服务器将得到身份验证。安装向导将继续执行下一步。

步骤 10：为 NDR 功能选择本地化语言，并配置从 SPAN 端口接收镜像流量

如果您正在部署集群的第一个工作服务器，则在此步骤中，您必须按照以下顺序完成安装向导的步骤：

1. 选择 NDR 功能的本地化语言。
2. 配置从 SPAN 端口接收镜像流量。

如果您正在部署额外的工作服务器，则可以省略 NDR 本地化选择步骤。对集群中的服务器进行认证后，安装向导将继续执行配置从 SPAN 端口接收镜像流量的步骤。

选择 NDR 功能的本地化语言

所选语言用于显示与 NDR 功能有关的应用程序部分。

要选择 NDR 功能的本地化语言：

在列表中选择它并按 Enter。

选择 NDR 功能的本地化语言。安装向导将继续进行配置从 SPAN 端口接收镜像流量的步骤。

配置从 SPAN 端口接收镜像流量

为了使应用程序正常工作，必须在群集中的一个处理服务器上启用从 SPAN 端口接收镜像流量。如果您实际上不需要处理来自 SPAN 端口的镜像流量，请在配置大小时将 SPAN 流量指定为 0。

必须仅在群集中的一个处理服务器上启用镜像流量处理。

要开启从 SPAN 端口接收镜像流量：

1. 这将打开一个窗口，在该窗口中，选择**“是”**并按 **Enter**。
2. 在显示的列表中，选择要从中捕获网络流量的网络接口。
3. 选择包含“**应用并完成**”的行，然后按 **Enter**。

配置可能需要一些时间。然后安装完成。为了使应用程序正常工作，您必须配置服务器。

要关闭从 SPAN 端口接收镜像流量：

在打开的窗口中，选择“**否**”并按 **Enter**。

配置可能需要一些时间。然后安装完成。为了使应用程序正常工作，您必须配置服务器。

清除存储服务器上的硬盘

如果您已经在服务器上部署了群集，并且想要向这些服务器添加更多的硬盘驱动器，或者更换一些现有驱动器，然后重新安装群集，则在安装组件之前，必须清除存储服务器上以前分配给 OSD (Object Storage Daemon) 的驱动器。否则，不能保证应用程序正常运行。

要清除活动存储服务器上分配给 OSD 的磁盘：

1. 通过 SSH 或终端登录到要清除磁盘的服务器的管理控制台。
2. 通过运行 `sudo systemctl stop kata-osd-starter.service` 停止 OSD 启动服务。
3. 通过运行 `sudo docker ps --filter name=osd -q | xargs docker stop` 停止 OSD 容器。
4. 通过运行 `sudo ceph-volume --cluster ceph lvm list | grep devices` 获取 OSD 磁盘列表。
5. 使用 `sudo wipefs -af /dev/<磁盘名称>` 命令从这些磁盘中删除文件系统签名和分区表。

   您必须对在步骤 4 中获得的每个驱动器运行此命令。例如：`sudo wipefs -af /dev/sda`。
6. 通过运行 `sudo ceph-volume lvm zap --destroy /dev/<磁盘名称>`清除这些磁盘。

   您必须对在步骤 4 中获得的每个驱动器运行此命令。例如：`sudo ceph-volume lvm zap --destroy /dev/sda`。

OSD 守护进程被从磁盘中删除。

如果服务器不在活动状态，则必须从为 OSD 分配的每个磁盘中删除有关卷组的信息。

要从非活动服务器上为 OSD 分配的每个磁盘中删除有关卷组的信息：

1. 使用备用操作系统启动服务器。
2. 使用 `sudo pvs` 命令获取为 OSD 分配的每个磁盘的组 ID。

   该命令输出一个表，其中 `PV` 表示物理卷，`VG` 表示逻辑组成员身份，`Fmt` 表示卷格式，`Size` 表示物理卷大小。
3. 通过运行 `sudo vgremove <卷组 ID>` 删除相关卷组。

分配给 OSD 的磁盘上的卷组信息被删除。

在服务器上安装带有嵌入式 Sensor 的 Central Node 组件

在服务器上部署带有嵌入式 Sensor 的 Central Node 组件涉及以下步骤：

1. **安装带有嵌入式 Sensor 的 Central Node 组件**

   要在物理服务器上安装组件，您需要从带有 Central Node 和 Sensor 组件的磁盘镜像启动。

   要在虚拟服务器上安装组件，您需要将带有 Central Node 和 Sensor 组件的磁盘镜像连接到所选虚拟机并运行它。虚拟机启动后安装立即开始。您可以使用虚拟机的控制台管理安装过程。

2. **配置应用程序的大小设置**

   在集群部署的最后阶段，您需要配置应用程序的扩展设置：指定计划的 SPAN 流量、电子邮件流量、具有 Endpoint Agent 组件的主机数量以及存储和事件数据库的大小。

Central Node 组件始终与 Sensor 组件一起安装。如果您需要单独使用 Central Node 组件，请在步骤 10 中关闭从 SPAN 端口接收镜像流量。

如果执行安装向导步骤时出现错误，请联系技术支持。

步骤 1：查看最终用户授权许可协议和隐私策略

要继续安装，您必须阅读最终用户授权许可协议和隐私政策并接受其条款和条件。仅当您接受最终用户授权许可协议和隐私政策的条款后，安装才能继续进行。

安装基于 Ubuntu 操作系统的组件时接受最终用户授权许可协议和隐私政策的条款和条件：

1. 在列表中选择用于查看 AO Kaspersky Lab 最终用户授权许可协议和隐私策略的语言，然后按 **Enter**。

   这将打开一个窗口，其中包含 AO Kaspersky Lab 最终用户授权许可协议的文本。

2. 阅读 AO Kaspersky Lab 最终用户授权许可协议。

   要向上和向下移动，您可以使用以下键：↑、↓、**PageUp** 和 **PageDown**。

3. 如果您接受 AO Kaspersky Lab 最终用户授权许可协议，请选择“**我接受**”并按“**Enter**”。

   这将打开一个显示 AO Kaspersky Lab 隐私策略文本的窗口。

4. 阅读 AO Kaspersky Lab 隐私策略。

5. 如果您接受 AO Kaspersky Lab 隐私策略的条款和条件，请选择“**我接受**”并按 **Enter**。

安装向导将继续执行下一步。

安装基于 Astra Linux 操作系统的组件时接受最终用户授权许可协议和隐私政策的条款和条件：

1. 按 **F1** 键从列表中选择查看 Astra Linux 操作系统最终用户授权许可协议的语言，然后按 **Enter**。
   这将打开一个窗口，其中包含 Astra Linux 最终用户授权许可协议的文本。
2. 阅读 Astra Linux 操作系统的最终用户授权许可协议。
   要向上和向下移动，您可以使用以下键：↑、↓、**PageUp** 和 **PageDown**。
3. 如果您接受 Astra Linux 操作系统的最终用户授权许可协议的条款和条件，请选择“**Yes**”并按 **Enter**。
   这将打开一个窗口，您可以在其中选择查看 AO Kaspersky Lab 最终用户授权许可协议和隐私策略的语言。
4. 在列表中选择用于查看 AO Kaspersky Lab 最终用户授权许可协议和隐私策略的语言，然后按 **Enter**。
   这将打开一个窗口，其中包含 AO Kaspersky Lab 最终用户授权许可协议的文本。
5. 阅读 AO Kaspersky Lab 最终用户授权许可协议。
   要向上和向下移动，您可以使用以下键：↑、↓、**PageUp** 和 **PageDown**。
6. 如果您接受 AO Kaspersky Lab 最终用户授权许可协议的条款和条件，请选择“**I accept**”并按“**Enter**”。
   这将打开一个显示 AO Kaspersky Lab 隐私策略文本的窗口。
7. 阅读 AO Kaspersky Lab 隐私策略。
8. 如果您接受 AO Kaspersky Lab 隐私策略的条款和条件，请选择“**I accept**”并按“**Enter**”。

安装向导将继续执行下一步。

步骤 2：选择服务器角色

要选择服务器角色：

1. 选择以下选项之一：

   - **storage**。
     该角色用于安装存储服务器，以将 Central Node 组件部署为集群。
   - **processing**。
     该角色用于安装处理服务器，以将 Central Node 组件部署为集群。

     > 该角色还包括 Sensor 组件的安装和配置。

   - **single**。
     该角色用于在同一服务器上安装 Central Node 和 Sensor 组件。

- **sensor**。
  此角色用于在独立服务器上安装 Sensor 组件。

2. 按下“**Enter**”。

安装向导将继续执行下一步。

步骤 3：选择安装组件的磁盘

您至少需要 150 GB 的磁盘空间。如果可用磁盘空间少于 150 GB，安装将完成并出现错误。

要选择用于安装组件的磁盘：

1. 选择用于安装组件的建议驱动器之一，然后按**Enter**。
   确认窗口将显示。
2. 选择**是**，然后按 **Enter** 键。

安装向导将继续执行下一步。

步骤 4：分配用于针对性攻击分析器组件数据库的磁盘

为了实现针对性攻击分析器组件的最佳性能，建议您在服务器上为组件数据库分配至少 1 TB 的物理磁盘。

在此步骤中，您可以为针对性攻击分析器分析组件数据库分配物理磁盘，或拒绝为其分配物理磁盘。

分配用于针对性攻击分析器组件数据库的磁盘：

1. 为针对性攻击分析器组件数据库选择建议的驱动器之一。
   如果您不需要 Targeted Attack Analyzer 组件的数据库，请选择“**不为 TAA 分配单独的磁盘**”行。
   确认窗口将显示。
2. 选择**是**，然后按 **Enter** 键。

安装向导将继续执行下一步。

步骤 5：为服务器寻址选择网络掩码

我们建议使用默认值。

该网络掩码可能与组织基础架构中使用的网络掩码不匹配。

要指定服务器寻址的网络掩码：

- 如果要使用网络掩码的预定义值，请选择“**确定**”按钮，然后按 **Enter**。
  默认值：198.18.0.0/16。
- 如果要指定不同的网络掩码，请在“**子网**”字段中输入您的值，选择“**确定**”按钮，然后按 **Enter**。
  掩码必须与模板匹配：xx0.0/16。

安装向导将继续执行下一步。

步骤 6：为应用程序组件的寻址选择网络掩码

我们建议使用默认值。

应用程序组件寻址的网络不得与服务器寻址的网络重叠。

要指定用于寻址应用程序主要组件的网络掩码：

- 如果要使用网络掩码的预定义值，请选择“**确定**”按钮，然后按 **Enter**。
  默认值：198.19.0.0/16。
- 如果要指定不同的网络掩码，请在“**Bridge/Overlay 子网**”字段中输入您的值，选择“**确定**”按钮，然后按 **Enter**。
  掩码必须与模板匹配：xx0.0/16。

安装向导将继续执行下一步。

步骤 7：选择外部网络接口

外部网络接口用于通过 SSH 访问服务器、管理 Kaspersky Anti Targeted Attack Platform 的 Web 界面以及其他外部连接。

要选择外部网络接口：

1. 选择包含用于外部网络的网络接口的行。
   要选择一行，您可以使用 ↑、↓、PageUp 和 PageDown 键。所选行以红色突出显示。
2. 按下“**Enter**”。

安装向导将继续执行下一步。

步骤 8：选择获取网络接口 IP 地址的方法

要选择用于获取网络接口 IP 地址的方法：

1. 选择包含**配置类型：**的行，然后按**Enter**。
   要选择一行，您可以使用 ↑、↓、PageUp 和 PageDown 键。所选行以红色突出显示。
2. 在打开的窗口中，选择以下选项之一：
   - **dhcp**。
   - **static**。
3. 如果您选择了 **static**:
   a. 选择包含参数的行然后按**Enter**键。
   b. 在打开的窗口中输入所需的数据，然后按**Enter**两次。

   > 您需要为每个参数指定一个值。

4. 选择包含**Save**的行。
5. 按下“**Enter**”。

安装向导将继续执行下一步。

步骤 9：创建管理员账户

管理员账户用于管理应用程序的 Web 界面，应用程序的管理员菜单，以及在技术支持模式下管理应用程序。

默认情况下，管理员账户的用户名为*admin*。您必须输入该用户账户的密码。

输入管理员用户账户的密码：

1. 这将打开一个窗口；在该窗口中，在“**最小长度**”字段中输入最小密码长度。您必须输入 8 或更大的值。
2. 选择**确定**，然后按 **ENTER** 键。
   这将打开密码创建窗口。
3. 这将打开一个窗口；在该窗口的“**密码**”字段中，输入管理员账户的密码。
   要选择一行，您可以使用 ↑、↓、PageUp 和 PageDown 键。所选行以红色突出显示。
4. 在**确认**字段中，再次输入新密码。
5. 选择**确定**，然后按 **ENTER** 键。

安装向导将继续执行下一步。

步骤 10：选择 NDR 功能的本地化语言

所选语言用于显示与 NDR 功能有关的应用程序部分。

要选择 NDR 功能的本地化语言：

在列表中选择它并按 Enter。

步骤 11：添加 DNS 服务器地址

为具有应用程序组件的服务器的运行配置 DNS 设置。

添加 DNS 服务器地址：

1. 选择“**添加**”字段然后按 **Enter** 键。
2. 以 IPv4 格式输入 DNS 服务器的 IP 地址。
3. 如果要添加其他 DNS 服务器的 IP 地址，请选择“**添加**”字段，按 **Enter** 并输入服务器的地址。
4. 添加所有 DNS 服务器后，选择“**继续**”字段并按 **Enter**。

安装向导将继续执行下一步。

步骤 12：配置与 NTP 服务器的时间同步

配置服务器时间与 NTP 服务器的同步。

1. 选择“**添加**”字段然后按 **Enter** 键。
2. 输入 NTP 服务器的 IP 地址或名称。
3. 如果要添加其他 NTP 服务器的 IP 地址或名称，请选择“**添加**”字段，按 **Enter**，然后输入 NTP 服务器的 IP 地址或名称。
4. 添加所有 NTP 服务器后，选择“**继续**”字段并按 **Enter**。

安装向导将继续执行下一步。

步骤 13：配置从 SPAN 端口接收镜像流量

即使您仅使用 KEDR 功能单元，也必须启用镜像流量的接收。

要开启从 SPAN 端口接收镜像流量：

1. 这将打开一个窗口，在该窗口中，选择**“是”**并按 **Enter**。
2. 在显示的列表中，选择要从中捕获网络流量的网络接口。
3. 选择包含“**应用并完成**”的行，然后按 **Enter**。

配置可能需要一些时间。然后安装完成。为了使应用程序正常工作，您必须配置服务器。

在独立服务器上安装 Sensor 组件

要在物理服务器上安装 Sensor 组件，您需要运行包含 Central Node 和 Sensor 组件的磁盘镜像。

要在虚拟服务器上安装 Sensor 组件，您需要将带有 Central Node 和 Sensor 组件的磁盘镜像连接到所选虚拟机并运行它。虚拟机启动后安装立即开始。您可以使用虚拟机的控制台管理安装过程。

步骤 1：查看最终用户授权许可协议和隐私策略

要继续安装，您必须阅读最终用户授权许可协议和隐私政策并接受其条款和条件。仅当您接受最终用户授权许可协议和隐私政策的条款后，安装才能继续进行。

安装基于 Ubuntu 操作系统的组件时接受最终用户授权许可协议和隐私政策的条款和条件：

1. 在列表中选择用于查看 AO Kaspersky Lab 最终用户授权许可协议和隐私策略的语言，然后按 **Enter**。
   这将打开一个窗口，其中包含 AO Kaspersky Lab 最终用户授权许可协议的文本。
2. 阅读 AO Kaspersky Lab 最终用户授权许可协议。
   要向上和向下移动，您可以使用以下键：↑、↓、**PageUp** 和 **PageDown**。
3. 如果您接受 AO Kaspersky Lab 最终用户授权许可协议，请选择“**我接受**”并按“**Enter**”。
   这将打开一个显示 AO Kaspersky Lab 隐私策略文本的窗口。
4. 阅读 AO Kaspersky Lab 隐私策略。
5. 如果您接受 AO Kaspersky Lab 隐私策略的条款和条件，请选择“**我接受**”并按 **Enter**。

安装向导将继续执行下一步。

安装基于 Astra Linux 操作系统的组件时接受最终用户授权许可协议和隐私政策的条款和条件：

1. 按 **F1** 键从列表中选择查看 Astra Linux 操作系统最终用户授权许可协议的语言，然后按 **Enter**。
   这将打开一个窗口，其中包含 Astra Linux 最终用户授权许可协议的文本。
2. 阅读 Astra Linux 操作系统的最终用户授权许可协议。
   要向上和向下移动，您可以使用以下键：↑、↓、**PageUp** 和 **PageDown**。

3. 如果您接受 Astra Linux 操作系统的最终用户授权许可协议的条款和条件，请选择“**Yes**”并按 **Enter**。
   这将打开一个窗口，您可以在其中选择查看 AO Kaspersky Lab 最终用户授权许可协议和隐私策略的语言。
4. 在列表中选择用于查看 AO Kaspersky Lab 最终用户授权许可协议和隐私策略的语言，然后按 **Enter**。
   这将打开一个窗口，其中包含 AO Kaspersky Lab 最终用户授权许可协议的文本。
5. 阅读 AO Kaspersky Lab 最终用户授权许可协议。
   要向上和向下移动，您可以使用以下键：↑、↓、**PageUp** 和 **PageDown**。
6. 如果您接受 AO Kaspersky Lab 最终用户授权许可协议的条款和条件，请选择“**I accept**”并按“**Enter**”。
   这将打开一个显示 AO Kaspersky Lab 隐私策略文本的窗口。
7. 阅读 AO Kaspersky Lab 隐私策略。
8. 如果您接受 AO Kaspersky Lab 隐私策略的条款和条件，请选择“**I accept**”并按“**Enter**”。

安装向导将继续执行下一步。

步骤 2：选择服务器角色

要选择服务器角色：

1. 选择以下选项之一：
   - **storage**。
     该角色用于安装存储服务器，以将 Central Node 组件部署为集群。
   - **processing**。
     该角色用于安装处理服务器，以将 Central Node 组件部署为集群。

     > 该角色还包括 Sensor 组件的安装和配置。

   - **single**。
     该角色用于在同一服务器上安装 Central Node 和 Sensor 组件。
   - **sensor**。
     此角色用于在独立服务器上安装 Sensor 组件。
2. 按下“**Enter**”。

安装向导将继续执行下一步。

步骤 3：选择安装组件的磁盘

> 您至少需要 150 GB 的磁盘空间。如果可用磁盘空间少于 150 GB，安装将完成并出现错误。

要选择用于安装组件的磁盘：

1. 选择用于安装组件的建议驱动器之一，然后按**Enter**。
   确认窗口将显示。
2. 选择**是**，然后按 **Enter** 键。

安装向导将继续执行下一步。

步骤 4：为服务器寻址选择网络掩码

我们建议使用默认值。

该网络掩码可能与组织基础架构中使用的网络掩码不匹配。

要指定服务器寻址的网络掩码：

- 如果要使用网络掩码的预定义值，请选择“**确定**”按钮，然后按 **Enter**。
  默认值：198.18.0.0/16。
- 如果要指定不同的网络掩码，请在“**子网**”字段中输入您的值，选择“**确定**”按钮，然后按 **Enter**。
  掩码必须与模板匹配：xx0.0/16。

安装向导将继续执行下一步。

步骤 5：为应用程序组件的寻址选择网络掩码

我们建议使用默认值。

应用程序组件寻址的网络不得与服务器寻址的网络重叠。

要指定用于寻址应用程序主要组件的网络掩码：

- 如果要使用网络掩码的预定义值，请选择“**确定**”按钮，然后按 **Enter**。
  默认值：198.19.0.0/16。
- 如果要指定不同的网络掩码，请在“**Bridge/Overlay 子网**”字段中输入您的值，选择“**确定**”按钮，然后按 **Enter**。
  掩码必须与模板匹配：xx0.0/16。

安装向导将继续执行下一步。

步骤 6：选择外部网络接口

外部网络接口用于通过 SSH 访问服务器、管理 Kaspersky Anti Targeted Attack Platform 的 Web 界面以及其他外部连接。

要选择外部网络接口：

1. 选择包含用于外部网络的网络接口的行。

   要选择一行，您可以使用 ↑、↓、PageUp 和 PageDown 键。所选行以红色突出显示。

2. 按下“**Enter**”。

安装向导将继续执行下一步。

步骤 7：选择获取网络接口 IP 地址的方法

要选择用于获取网络接口 IP 地址的方法：

1. 选择包含**配置类型：**的行，然后按**Enter**。

   要选择一行，您可以使用 ↑、↓、PageUp 和 PageDown 键。所选行以红色突出显示。

2. 在打开的窗口中，选择以下选项之一：

   - **dhcp**。
   - **static**。

3. 如果您选择了 **static**:

   a. 选择包含参数的行然后按**Enter**键。

   b. 在打开的窗口中输入所需的数据，然后按**Enter**两次。

   > 您需要为每个参数指定一个值。

4. 选择包含**Save**的行。

5. 按下“**Enter**”。

安装向导将继续执行下一步。

步骤 8：创建管理员账户

管理员账户用于管理应用程序的 Web 界面，应用程序的管理员菜单，以及在技术支持模式下管理应用程序。

默认情况下，管理员账户的用户名为*admin*。您必须输入该用户账户的密码。

输入管理员用户账户的密码：

1. 这将打开一个窗口；在该窗口中，在“**最小长度**”字段中输入最小密码长度。您必须输入 8 或更大的值。
2. 选择**确定**，然后按 **ENTER** 键。
   这将打开密码创建窗口。
3. 这将打开一个窗口；在该窗口的“**密码**”字段中，输入管理员账户的密码。
   要选择一行，您可以使用 ↑、↓、PageUp 和 PageDown 键。所选行以红色突出显示。
4. 在**确认**字段中，再次输入新密码。
5. 选择**确定**，然后按 **ENTER** 键。

安装向导将继续执行下一步。

步骤 9：添加 DNS 服务器地址

为具有应用程序组件的服务器的运行配置 DNS 设置。

添加 DNS 服务器地址：

1. 选择“**添加**”字段然后按 **Enter** 键。
2. 以 IPv4 格式输入 DNS 服务器的 IP 地址。
3. 如果要添加其他 DNS 服务器的 IP 地址，请选择“**添加**”字段，按 **Enter** 并输入服务器的地址。
4. 添加所有 DNS 服务器后，选择“**继续**”字段并按 **Enter**。

安装向导将继续执行下一步。

步骤 10：配置与 NTP 服务器的时间同步

配置服务器时间与 NTP 服务器的同步。

1. 选择“**添加**”字段然后按 **Enter** 键。
2. 输入 NTP 服务器的 IP 地址或名称。
3. 如果要添加其他 NTP 服务器的 IP 地址或名称，请选择“**添加**”字段，按 **Enter**，然后输入 NTP 服务器的 IP 地址或名称。
4. 添加所有 NTP 服务器后，选择“**继续**”字段并按 **Enter**。

安装向导将继续执行下一步。

步骤 11：配置从 SPAN 端口接收镜像流量

要开启从 SPAN 端口接收镜像流量：

1. 在显示的列表中，选择要从中捕获网络流量的网络接口。
2. 选择包含“**应用并完成**”的行，然后按 **Enter**。

   配置可能需要一些时间。然后安装完成。

优化 Sensor 组件的网络接口设置

如果应用程序在处理网络流量时遇到网络数据包丢失或性能问题，请按照这些说明进行操作。

要减少网络数据包丢失和从流量中提取文件不完整的情况，请执行以下操作：

1. 指定 RSS 队列的最大数量：
   - 如果网络上的数据传输速率小于 1 Gbps，请将数字设置为 1。
   - 如果网络上的数据传输速率大于 1 Gbps，请将数字设置为 16。

   如果您的网络接口不允许将 RSS 队列的最大数量设置为 16，请将其设置为受支持的最大数量。
2. 为网络接口配置对称 RSS 哈希。有关配置 RSS 哈希的详细信息，请参阅网络适配器的供应商文档。
3. 创建**包含以下内容**的 interrupts.sh 文件。

```
#!/usr/bin/env bash

set -e

dev=$1
min_cpu=$2
max_cpu=$3
step=$4

irs=($(cat /proc/interrupts | grep "$dev" | awk '{split($1,a,":"); print a[1]}'))

cpu=$min_cpu
for ir in ${irs[@]}; do
echo $cpu > /proc/irq/$ir/smp_affinity_list
cpu=$(((cpu + step) % max_cpu))
cat "/proc/irq/$ir/smp_affinity_list"
done
```

4. 运行以下命令：

`sudo bash interrupts.sh <dev> <min_cpu> <max_cpu> <step>`，其中

- `<dev>`是您想要在内核之间分配中断的网络接口。
- `<min_cpu>`是网络适配器中断分配范围内的第一个内核。
- `<max_cpu>`是网络适配器中断分配范围内的最后一个内核。
- `<step>`是选择下一个分配给中断的内核的增量。

  示例：

  ```
  sudo bash interrupts.sh ens192 2 11 1
  ```

5. 如果您使用 NVIDIA Mellanox 网络适配器 (mlx4)，请通过运行以下命令配置 RSS 队列数和 RSS 哈希：

   ```
   ethtool -L $dev rx 16
   ethtool -X $dev equal 16
   ethtool -X $dev hfunc xor
   ```

6. 如果您使用的是 Intel 网络适配器 (i40e)，请配置 RSS 队列数和 RSS 哈希：

   ```
   rmmod i40e && modprobe i40e
   ifconfig $dev down
   ethtool -L $dev combined 16
   ethtool -K $dev rxhash on
   ethtool -K $dev ntuple on
   ifconfig $dev up
   ethtool -X $dev hkey
   6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:
   5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A equal 16
   ethtool -A $dev rx off
   ethtool -C $dev adaptive-rx off adaptive-tx off rx-usecs 125
   ethtool -G $dev rx 1024
   ethtool -N $dev rx-flow-hash tcp4 sdfn
   ethtool -N $dev rx-flow-hash tcp6 sdfn
   ethtool -N $dev rx-flow-hash udp4 sdfn
   ethtool -N $dev rx-flow-hash udp6 sdfn
   ```

网络接口已配置。

重新启动应用程序后，您必须按照说明重新配置网络接口。

连接和配置 Sensor 组件的外部存储

Kaspersky Anti Targeted Attack Platform 将从网络接口接收的流量保存为网络流量转储文件。如果要确保网络流量转储文件的长期存储，您可以连接并配置外部存储。您可以使用外部存储中的网络流量转储文件将网络流量下载为 PCAP 文件。我们建议使用 SSD 驱动器作为外部存储。

要在安装了 Sensor 和 Central Node 组件的服务器上连接和配置网络流量转储文件的外部存储：

1. 连接一个您想要用作外部存储、至少有 100 GB 的磁盘。
2. 进入技术支持模式。
3. 运行以下命令：

   ```
   sudo -i
   fdisk -l
   ```

   确保您连接的外部存储磁盘显示在控制台中。
4. 运行以下命令：

   ```
   mke2fs -t ext4 -L DATA -m 0 /dev/<连接的磁盘名称>
   sudo nano /etc/fstab
   ```

   这将在文本编辑器中打开 fstab 文件。
5. 在文件末尾添加以下行：

   ```
   /dev/<连接的磁盘名称> /data/volumes/dumps/ ext4 defaults 0 0
   ```
6. 关闭文本编辑器。
7. 运行以下命令：

   ```
   mount
   rm -r /data/volumes/dumps/*
   ```

   > 这些命令会从连接的磁盘中删除所有数据。

   连接的磁盘将配置为用作外部存储器。
8. 运行以下命令：

   ```
   chown kluser:klusers /data/volumes/dumps/
   ls -lah /data/volumes/dumps/
   lsblk
   ```

   确保在 **MOUNTPOINTS** 列中，**/data/volumes/dumps** 显示在已连接的磁盘名称旁边。
9. 运行以下命令：

   ```
   docker service update kata_product_main_1_preprocessor_span --force
   docker ps | grep preprocessor_span
   ```

   等待 控制台显示**“最多 2 秒”**。
10. 运行以下命令：

    ```
    docker exec -it $(docker ps | grep preprocessor_span | awk '{print $1}') bash
    lsblk
    ```

    确保在 **MOUNTPOINTS** 列中，**/mnt/kaspersky/nta/dumps** 值显示在已连接的磁盘名称旁边。
11. 在应用程序 Web 界面窗口中选择**Sensor 服务器**部分。

12. 单击相关 Sensor 组件的卡片。
    这将打开一个窗口，其中包含有关组件的信息。

13. 单击**"编辑"**。

14. 选择"**外部存储**"选项卡，然后使用"**为流量转储文件连接外部存储**"开关启用外部存储模式。

15. 在**"最大大小"**下设置存储流量转储文件的空间限制。
    您可以选择大小限制的计量单位：**MB** 或 **GB**。

16. 如果必要，在"**使用 BPF 过滤**"部分，启用过滤并输入使用 BPF (Berkley Packet Filter) 技术进行过滤的表达式。BPF 过滤表达式的写入格式为 libpcap。有关语法的更多详细信息，请参阅 pcap-filter 手册页。

17. 如有必要，在"**存储时间限制**"部分中，对文件的最短存储时间进行限制，并指定相关的天数。

18. 单击"**保存**"。

安装了 Sensor 和 Central Node 的服务器上网络流量转储文件的外部存储已连接并配置。

要在安装了 Sensor 组件的独立服务器上连接和配置网络流量转储文件的外部存储：

1. 连接一个您想要用作外部存储、至少有 100 GB 的磁盘。

2. 进入技术支持模式。

3. 运行以下命令：
   ```
   sudo -i
   fdisk -l
   ```
   确保您连接的外部存储磁盘显示在控制台中。

4. 运行以下命令：
   ```
   mke2fs -t ext4 -L DATA -m 0 /dev/<连接的磁盘名称>
   sudo nano /etc/fstab
   ```
   这将在文本编辑器中打开 fstab 文件。

5. 在文件末尾添加以下行：
   ```
   /dev/<连接的磁盘名称> /data/volumes/dumps/ ext4 defaults 0 0
   ```

6. 关闭文本编辑器。

7. 运行以下命令：
   ```
   rm -r /data/volumes/dumps/*
   ```

   这些命令会从连接的磁盘中删除所有数据。

8. 在应用程序 Web 界面窗口中选择**Sensor 服务器**部分。

9. 单击相关 Sensor 组件的卡片。
   这将打开一个窗口，其中包含有关组件的信息。

10. 单击**"编辑"**。

11. 选择"**外部存储**"选项卡，然后使用"**为流量转储文件连接外部存储**"开关启用外部存储模式。

12. 在**"最大大小"**下设置存储流量转储文件的空间限制。

    您可以选择大小限制的计量单位：**MB** 或 **GB**。

13. 如果必要，在"**使用 BPF 过滤**"部分，启用过滤并输入使用 BPF (Berkley Packet Filter) 技术进行过滤的表达式。BPF 过滤表达式的写入格式为 libpcap。有关语法的更多详细信息，请参阅 pcap-filter 手册页。

14. 如有必要，在"**存储时间限制**"部分中，对文件的最短存储时间进行限制，并指定相关的天数。

15. 单击"**保存**"。

安装了 Sensor 组件的独立服务器上网络流量转储文件的外部存储已连接并配置。

配置应用程序的大小设置

如果您使用分布式解决方案和多租户模式，请使用要为其配置参数的 PCN 或 SCN 服务器的 Web 界面。

您可以更改 Central Node 组件上的运行负载。例如，您可以将其他主机（带有 Endpoint Agent 组件）或服务器（带有 Sensor 组件）连接到 Central Node 组件。为此，您需要指定计划的 SPAN 流量、邮件流量、安装了 Endpoint Agent 组件的主机数量，以及存储和事件数据库的大小。Kaspersky Anti Targeted Attack Platform 将根据指定的设置确定 Central Node 服务器的最佳配置。

如果 Central Node 组件被部署为集群，则应用程序会确定集群中所有服务器的最佳配置。

为了使集群正常运行，在配置大小参数后，必须在集群的服务器上同步时间。在配置大小参数之前，请确保为集群中至少一台服务器配置了与正常运行的 NTP 服务器的集成。

您可以在 Kaspersky Anti Targeted Attack Platform 的 Web 界面或集群中任何服务器上的组件管理员菜单中配置 NTP 服务器集成。如果您之前没有配置 NTP 服务器集成，我们建议在配置后重新启动集群服务器。

配置 Central Node 服务器：

1. 在任何一台允许访问 Central Node 服务器的计算机的浏览器中，将具有 Central Node 组件的服务器的 IP 地址输入地址栏中。

   如果您使用的是应用程序的高可用性版本，则可以输入 Central Node 集群的任何服务器的 IP 地址或**集群的完全限定域名 (FQDN)**。

   为了保证程序 Web 界面的访问不间断，可以在DNS 服务器上配置轮询调度算法功能。为此，请登录 Central Node 集群的第一台正常服务器的 Web 界面。

   Kaspersky Anti Targeted Attack Platform 用户的账户凭证输入窗口打开。

2. 输入用户名(“admin”)以及在安装应用程序期间设置的密码。

3. 单击**登录**。

4. 前往**服务器配置**部分。

5. 在“**Endpoint Agent 数量**”字段，指定基础架构的 Endpoint Agent 主机有效数量。

   有关如何计算 Endpoint Agent 主机有效数量的详细信息，请参阅扩展指南。

   如果您不使用 KEDR 授权许可密钥，请指定 0。

6. 在“**邮件流量，每秒消息数**”字段中，指定计划每秒发送的电子邮件数量。

   如果您不使用 KATA 授权许可密钥，请指定 0。

7. 在**SPAN 流量，Mbps**字段中，指定来自具有 Sensor 组件的服务器上的 SPAN 端口的计划流量。

   如果您不使用 KATA 授权许可密钥，请指定 0。

8. 如果您在服务器上安装了 Central Node，则在“**磁盘空间**”部分中，在“**事件数据库，GB**”和“**存储，GB**”字段中保留默认值。

9. 如果您将 Central Node 安装为集群，则在“**可用磁盘空间**”部分中，通过以下方式之一指定事件数据库和存储的大小：

   - 将分隔**事件数据库**和**存储**的滑块向左或向右移动。

     请记住，减少事件数据库或存储的大小会根据轮换规则不可逆地删除最旧的数据。扩大事件数据库或存储不会导致数据丢失。

   - 指定**事件数据库，GB**和**存储，GB**字段中的值。

     如果将 Central Node 组件部署为高可用性集群，请使用“规模调整指南”来计算事件数据库的大小。

   - 如有必要，您可以通过移动右侧的最后一个滑块在磁盘上留下可用空间。

   安装 Central Node 组件时，会自动为警报数据库保留磁盘空间。

10. 单击**配置**。

    如果服务器上安装了 Central Node，Kaspersky Anti Targeted Attack Platform 会根据指定的参数确定最佳服务器配置。如果 Central Node 作为集群安装，则应用程序将配置集群的服务器。

配置防火墙规则

应用程序及其组件的正常运行需要在连接到已安装应用程序组件的计算机的网络设备上配置防火墙规则。您可以使用 iptables 工具配置规则。这些端口以 iptables 术语描述。

组件的操作系统已预配置防火墙规则。我们强烈建议不要更改这些规则。

装有 Kaspersky Anti Targeted Attack Platform 组件的计算机使用的端口

所描述的规则适用于所有类型的主机，无论配置如何。这些规则通过 kata-firewall systemd 服务应用，仅适用于 INPUT 和 DOCKER-USER 链。

INPUT 链

该链管理与具有 Kaspersky Anti Targeted Attack Platform 组件的计算机的所有连接。

网络规则如下表所列。

INPUT 链的网络规则

目标服务或协议	端口	协议	sport	dport	外部网络访问
SSH	22	TCP	—	✓	✓
SMTP	25	TCP	—	✓	✓
DNS	53	TCP	—	✓	✓
HTTP	80	TCP	—	✓	✓
SNMPD	161	UDP	—	✓	✓
HTTPS	443	TCP	—	✓	✓
preprocessor_icap	1334	TCP	—	✓	✓
docker swarm	2377	TCP	✓	✓	—
etcd	2379	TCP	—	✓	✓
etcd	2380	TCP	—	✓	✓
ceph_mon	3300	TCP	—	✓	✓
VXLAN	4789	TCP/UDP	✓	✓	—
ceph_mon	6789	TCP	—	✓	✓
ceph OSD	6800:6900	TCP	—	✓	✓
docker swarm	7946	TCP/UDP	✓	✓	—
ipsec_manager	8084	TCP	✓	✓	—
pcap_manager	8085	TCP	—	✓	✓
HTTPS	8443	TCP/UDP	—	✓	✓

目标服务或协议	端口	协议	sport	dport	外部网络访问
HTTPS	8444	TCP/UDP	—	✓	✓
suricata_metrics_exporter	9103	TCP	✓	✓	—
node_exporter	9141	TCP	✓	✓	—
cadvisor	9142	TCP	✓	✓	—
preprocessor_metrics_exporter	9191	TCP	✓	✓	—
pcap_manager_metrics_exporter	9192	TCP	✓	✓	—
ceph_mgr	9283	TCP	—	✓	✓
ceph_rgw	9284	TCP	—	✓	✓
NDR Sensor	9443	TCP	—	✓	✓
kafka bootstrap	11000:11006	TCP	—	✓	✓

DOCKER-USER 链

该链管理用于应用程序组件寻址的网络连接。网络规则如下表所列。

DOCKER-USER 链的网络规则

目标服务或协议	端口	协议	sport	dport
SMTP	25	TCP	—	✓
DNS	53	TCP/UDP	—	✓
HTTP	80	TCP	—	✓
HTTPS	443	TCP	—	✓
preprocessor_icap	1344	UDP	—	✓
NDR NATS (KICKS NAT)	7423	TCP	—	✓
NDR public API	8070	TCP	—	✓
deployment API	8080	TCP	✓	✓
部署管理 API	8090	TCP	✓	✓
授权服务	8091	TCP	✓	✓
HTTPS	8443	TCP	—	✓
apt collector ssl	9081	TCP	—	✓
Sensor	9443	TCP	—	✓
NDR EKA	13520	TCP	—	✓

集群配置中 Kaspersky Anti Targeted Attack Platform 服务使用的端口

为了使应用程序在集群配置中正常工作，您必须根据下表为我们的传出连接配置网络访问。

集群配置中 Kaspersky Anti Targeted Attack Platform 服务使用的端口

服务	端口	协议
agent_database_configurator	2379	TCP
agent_database_configurator	5432	TCP
agent_database_synchronizer	2379	TCP
agent_database_synchronizer	5432	TCP
agent_database_synchronizer	9092	TCP
agent_database_synchronizer	9100	TCP
agent_database_synchronizer	10000:10010	TCP
agent_server	1080	TCP
agent_server	2379	TCP
agent_server	5432	TCP
agent_server	8100	TCP
agent_server	9090	TCP
agent_server	9284	TCP
antiapt_database_configurator	2379	TCP
antiapt_database_configurator	5432	TCP
authorization_service	2379	TCP
authorization_service	4567	TCP
authorization_service	8090	TCP
authorization_service	8443	TCP
authorization_service	8701	TCP
authorization_service	8899	TCP
cadvisor	任何	任何
ceph_management_api	2379	TCP
ceph_management_api	3300	TCP
ceph_management_api	6789	TCP
ceph_management_api	8765	TCP
ceph_management_api	8080	TCP
ceph_management_api	9283	TCP
ceph_management_api	9284	TCP
ceph_mgr	2379	TCP
ceph_mgr	3300	TCP
ceph_mgr	6789	TCP
ceph_mgr	6800:6900	TCP
ceph_mgr	9141	TCP
ceph_mgr	9142	TCP
ceph_mgr	9283	TCP
ceph_mgr	9284	TCP
ceph_mon	2379	TCP
ceph_mon	3300	TCP
ceph_mon	6789	TCP

服务	端口	协议
ceph_mon	6800:6900	TCP
ceph_mon	9141	TCP
ceph_mon	9142	TCP
ceph_mon	9283	TCP
ceph_mon	9284	TCP
ceph_osd	2379	TCP
ceph_osd	3300	TCP
ceph_osd	6789	TCP
ceph_osd	6800:6900	TCP
ceph_osd	9141	TCP
ceph_osd	9142	TCP
ceph_osd	9283	TCP
ceph_osd	9284	TCP
ceph_rgw	2379	TCP
ceph_rgw	3300	TCP
ceph_rgw	6789	TCP
ceph_rgw	6800:6900	TCP
ceph_rgw	9141	TCP
ceph_rgw	9142	TCP
ceph_rgw	9283	TCP
ceph_rgw	9284	TCP
ceph_rgw_configurator	2379	TCP
ceph_rgw_configurator	3300	TCP
ceph_rgw_configurator	6789	TCP
ceph_rgw_configurator	6800:6900	TCP
ceph_rgw_configurator	9141	TCP
ceph_rgw_configurator	9142	TCP
ceph_rgw_configurator	9283	TCP
ceph_rgw_configurator	9284	TCP
clickhouse	2379	TCP
clickhouse	8123	TCP
clickhouse	9000	TCP
clickhouse_database_configurator	2379	TCP
clickhouse_database_configurator	9000	TCP
clickhouse_metrics_importer	2379	TCP
clickhouse_metrics_importer	6379	TCP
clickhouse_metrics_importer	8123	TCP
clickhouse_metrics_importer	9000	TCP
clickhouse_metrics_importer	9090	TCP
coredns	53	TCP
coredns	53	TCP

服务	端口	协议
coredns	2379	TCP
deployment_api	22	TCP
deployment_api	2377	TCP
deployment_api	2379	TCP
deployment_api	4567	TCP
deployment_api	8080	TCP
deployment_api	8443	TCP
deployment_api	8701	TCP
deployment_api	9141	TCP
deployment_api	9284	TCP
deployment_management_api	53	TCP
deployment_management_api	2379	TCP
deployment_management_api	4567	TCP
deployment_management_api	8091	TCP
deployment_management_api	8443	TCP
deployment_management_api	8701	TCP
deployment_management_api	8702	TCP
deployment_management_api	8765	TCP
deployment_management_api	8899	TCP
deployment_management_api	9141	TCP
dhcp_server	任何	任何
edr_synchronizer	25	TCP
edr_synchronizer	80	TCP
edr_synchronizer	514	TCP
edr_synchronizer	514	UDP
edr_synchronizer	2379	TCP
edr_synchronizer	5432	TCP
edr_synchronizer	6379	TCP
edr_synchronizer	8081	TCP
edr_synchronizer	8082	TCP
edr_synchronizer	8083	TCP
edr_synchronizer	9092	TCP
edr_synchronizer	10000:10010	TCP
edr_synchronizer	33334	TCP
elasticsearch	2379	TCP
elasticsearch	9200	TCP
elasticsearch	9300	TCP
elasticsearch_data	2379	TCP
elasticsearch_data	9200	TCP
elasticsearch_data	9300	TCP
elasticsearch_exporter	2379	TCP

服务	端口	协议
elasticsearch_exporter	9200	TCP
elasticsearch_exporter	9300	TCP
etcd	2379	TCP
etcd	2380	TCP
events_api	80	TCP
events_api	2379	TCP
events_api	5432	TCP
events_api	8080	TCP
events_api	8081	TCP
events_api	9092	TCP
events_api	9100	TCP
events_api	9284	TCP
events_api	10000:10010	TCP
fastsearch	2379	TCP
fastsearch	8080	TCP
fastsearch	8180	TCP
fastsearch_events_cleaner	9200	TCP
fastsearch_events_importer	2379	TCP
fastsearch_events_importer	8081	TCP
fastsearch_events_importer	9092	TCP
fastsearch_events_importer	9100	TCP
fastsearch_events_importer	9200	TCP
fastsearch_events_importer	10000:10010	TCP
hunts_database_configurator	2379	TCP
hunts_database_configurator	5432	TCP
hunts_database_synchronizer	2379	TCP
hunts_database_synchronizer	5432	TCP
hunts_database_synchronizer	9092	TCP
hunts_database_synchronizer	10000:10010	TCP
hunts_event_processor	2379	TCP
hunts_event_processor	5432	TCP
hunts_event_processor	8080	TCP
hunts_event_processor	8081	TCP
hunts_event_processor	9092	TCP
hunts_event_processor	9100	TCP
hunts_event_processor	10000:10010	TCP
hunts_statistics_api	2379	TCP
hunts_statistics_api	5432	TCP
hunts_statistics_api	8080	TCP
hunts_statistics_api	8081	TCP
hunts_statistics_api	9092	TCP

服务	端口	协议
hunts_statistics_api	9100	TCP
hunts_statistics_api	10000:10010	TCP
hunts_statistics_processor	2379	TCP
hunts_statistics_processor	5432	TCP
hunts_statistics_processor	8080	TCP
hunts_statistics_processor	8081	TCP
hunts_statistics_processor	9092	TCP
hunts_statistics_processor	9100	TCP
hunts_statistics_processor	9200	TCP
hunts_statistics_processor	10000:10010	TCP
edr_synchronizer	25	TCP
edr_synchronizer	80	TCP
ids_alert_syncer	514	UDP
ids_alert_syncer	2379	TCP
ids_alert_syncer	5432	TCP
ids_alert_syncer	777	TCP
ids_alert_syncer	8083	TCP
ids_alert_syncer	9092	TCP
ids_alert_syncer	9200	TCP
ids_alert_syncer	10000:10010	TCP
ids_alert_syncer	33334	TCP
ioa_update_validator	2379	TCP
ipsec_manager	80	TCP
ipsec_manager	2379	TCP
kafka	2379	TCP
kafka	2181	TCP
kafka	9092	TCP
kafka	9095	TCP
kafka	10000:10010	TCP
kafka_configurator	2181	TCP
kafka_configurator	2379	TCP
kafka_configurator	9092	TCP
kafka_configurator	10000:10010	TCP
kafka_exporter	2379	TCP
kafka_exporter	9092	TCP
kafka_exporter	9100	TCP
kafka_exporter	10000:10010	TCP
kafka_proxy	任何	任何
kata_scanner	25	TCP
kata_scanner	80	TCP
kata_scanner	514	TCP

服务	端口	协议
kata_scanner	514	UDP
kata_scanner	443	TCP
kata_scanner	2379	TCP
kata_scanner	5432	TCP
kata_scanner	6379	TCP
kata_scanner	7777	TCP
kata_scanner	8081	TCP
kata_scanner	8082	TCP
kata_scanner	8083	TCP
kata_scanner	9081	TCP
kata_scanner	9090	TCP
kata_scanner	9092	TCP
kata_scanner	9100	TCP
kata_scanner	9284	TCP
kata_scanner	10000:10010	TCP
kata_scanner	33334	TCP
ksb_agent_server	80	TCP
ksb_agent_server	2379	TCP
ksb_agent_server	5432	TCP
ksb_agent_server	8082	TCP
ksb_agent_server	8083	TCP
ksb_agent_server	9898	TCP
ksn_proxy	80	TCP
ksn_proxy	443	TCP
ksn_proxy	514	TCP
ksn_proxy	514	UDP
ksn_proxy	2379	TCP
ksn_proxy	7777	TCP
ksn_proxy	8083	TCP
ksn_proxy	9092	TCP
ksn_proxy	9102	TCP
ksn_proxy	10000:10010	TCP
ksn_proxy	1:65535	TCP
ksqldb_configurator	2379	TCP
ksqldb_configurator	5432	TCP
ksqldb_configurator	8083	TCP
ksqldb_configurator	8088	TCP
ksqldb_configurator	9092	TCP
ksqldb_configurator	10000:10010	TCP
ksqldb_server	2379	TCP
ksqldb_server	5432	TCP

服务	端口	协议
ksqldb_server	9092	TCP
ksqldb_server	11000:11006	TCP
management_ui	2379	TCP
management_ui	8091	TCP
monitoring_grafana	3000	TCP
monitoring_prometheus	2379	TCP
monitoring_prometheus	9090	TCP
monitoring_prometheus	9100	TCP
monitoring_prometheus	9102	TCP
monitoring_prometheus	9141	TCP
monitoring_prometheus	9142	TCP
monitoring_prometheus	9191	TCP
monitoring_prometheus	9192	TCP
monitoring_prometheus	9283	TCP
multitenancy_management_api	2379	TCP
multitenancy_management_api	4567	TCP
multitenancy_management_api	8443	TCP
multitenancy_management_api	8701	TCP
multitenancy_management_api	8090	TCP
multitenancy_management_api	8899	TCP
nginx_exporter	2379	TCP
nginx_gateway	80	TCP
nginx_gateway	81	TCP
nginx_gateway	443	TCP
nginx_gateway	2379	TCP
nginx_gateway	4443	TCP
nginx_gateway	4567	TCP
nginx_gateway	6379	TCP
nginx_gateway	8080	TCP
nginx_gateway	8081	TCP
nginx_gateway	8082	TCP
nginx_gateway	8083	TCP
nginx_gateway	8085	TCP
nginx_gateway	8090	TCP
nginx_gateway	8100	TCP
nginx_gateway	8443	TCP
nginx_gateway	8444	TCP
nginx_gateway	8701	TCP
nginx_gateway	8702	TCP
nginx_gateway	8899	TCP
nginx_gateway	9393	TCP

服务	端口	协议
nginx_gateway	9898	TCP
node_exporter	任何	任何
nta_core	25	TCP
nta_core	80	TCP
nta_core	2379	TCP
nta_core	5433	TCP
nta_core	8082	TCP
nta_core	8083	TCP
nta_core	9443	TCP
nta_database	-	-
nta_database_configurator	2379	TCP
nta_database_configurator	5432	TCP
nta_database_configurator	5432	TCP
nta_sensor_configurator	2379	TCP
nta_sensor_configurator	8084	TCP
nta_sensor_configurator	9443	TCP
nta_sensor_configurator	50051	TCP
nta_syncer	80	TCP
nta_syncer	2379	TCP
nta_syncer	5422	TCP
nta_syncer	5423	TCP
nta_syncer	7777	TCP
nta_syncer	8084	TCP
nta_syncer	9092	TCP
nta_syncer	10000:10010	TCP
nta_syncer	50051	TCP
postfix	25	TCP
postfix	2379	TCP
postgresql_exporter	2379	TCP
postgresql_exporter	5432	TCP
postgresql_exporter	9100	TCP
postgresql_server	2379	TCP
postgresql_server	5432	TCP
preprocessor	任何	任何
preprocessor_icap	80	TCP
preprocessor_icap	1514	TCP
preprocessor_icap	1514	UDP
preprocessor_icap	2379	TCP
preprocessor_icap	4223	TCP
preprocessor_icap	6379	TCP
preprocessor_icap	7777	TCP

服务	端口	协议
preprocessor_icap	8081	TCP
preprocessor_icap	8082	TCP
preprocessor_icap	8083	TCP
preprocessor_icap	9092	TCP
preprocessor_icap	9192	TCP
preprocessor_icap	9284	TCP
preprocessor_icap	10000:10010	TCP
preprocessor_pop	110	TCP
preprocessor_pop	514	TCP
preprocessor_pop	514	UDP
preprocessor_pop	2379	TCP
preprocessor_pop	4223	TCP
preprocessor_pop	6379	TCP
preprocessor_pop	7777	TCP
preprocessor_pop	8081	TCP
preprocessor_pop	8082	TCP
preprocessor_pop	8083	TCP
preprocessor_pop	9081	TCP
preprocessor_pop	9092	TCP
preprocessor_pop	10000:10010	TCP
preprocessor_pop	1:65535	TCP
preprocessor_smtp	514	TCP
preprocessor_smtp	514	UDP
preprocessor_smtp	2379	TCP
preprocessor_smtp	4223	TCP
preprocessor_smtp	6379	TCP
preprocessor_smtp	7777	TCP
preprocessor_smtp	8081	TCP
preprocessor_smtp	8082	TCP
preprocessor_smtp	8083	TCP
preprocessor_smtp	9081	TCP
preprocessor_smtp	9092	TCP
preprocessor_smtp	10000:10010	TCP
preprocessor_span	任何	任何
primary_database_configurator	2379	TCP
primary_database_configurator	5432	TCP
redis	2379	TCP
redis	6379	TCP
response_actions_processor	514	TCP
response_actions_processor	514	UDP
response_actions_processor	2379	TCP

服务	端口	协议
response_actions_processor	5432	TCP
response_actions_processor	8081	TCP
response_actions_processor	9092	TCP
response_actions_processor	9100	TCP
response_actions_processor	10000:10010	TCP
response_api	514	TCP
response_api	514	UDP
response_api	2379	TCP
response_api	5432	TCP
response_api	8080	TCP
response_api	9092	TCP
response_api	9100	TCP
response_api	10000:10010	TCP
s3rotator	80	TCP
s3rotator	1080	TCP
s3rotator	2379	TCP
s3rotator	9283	TCP
s3rotator	9284	TCP
schema_registry	2379	TCP
schema_registry	8081	TCP
schema_registry	9092	TCP
schema_registry	10000:10010	TCP
sensor_event_processor	2379	TCP
sensor_event_processor	8080	TCP
sensor_event_processor	8081	TCP
sensor_event_processor	9092	TCP
sensor_event_processor	9100	TCP
sensor_event_processor	10000:10010	TCP
services_configurator	2379	TCP
siem_proxy	80	TCP
siem_proxy	514	TCP
siem_proxy	514	UDP
siem_proxy	1080	TCP
siem_proxy	1514	TCP
siem_proxy	1514	UDP
siem_proxy	2080	TCP
siem_proxy	2379	TCP
siem_proxy	9284	TCP
siem_proxy	任何	任何
snmpd	161	TCP
snmpd	2379	TCP

服务	端口	协议
updater	80	TCP
updater	443	TCP
updater	514	TCP
updater	514	TCP
updater	2379	TCP
updater	5432	TCP
updater	6379	TCP
updater	7777	TCP
updater	8083	TCP
updater	9100	TCP
updater	9500	TCP
updater	1:65535	TCP
updates_consistency_checker	80	TCP
updates_consistency_checker	2379	TCP
updates_consistency_checker	6379	TCP
updates_consistency_checker	8083	TCP
updates_consistency_checker	9092	TCP
updates_consistency_checker	10000:10010	TCP
web_backend	25	TCP
web_backend	80	TCP
web_backend	443	TCP
web_backend	514	TCP
web_backend	514	UDP
web_backend	1080	TCP
web_backend	2379	TCP
web_backend	5432	TCP
web_backend	6379	TCP
web_backend	7777	TCP
web_backend	8080	TCP
web_backend	8081	TCP
web_backend	8082	TCP
web_backend	8083	TCP
web_backend	8085	TCP
web_backend	8090	TCP
web_backend	8123	TCP
web_backend	8283	TCP
web_backend	8443	TCP
web_backend	8444	TCP
web_backend	8899	TCP
web_backend	9090	TCP
web_backend	9092	TCP

服务	端口	协议
web_backend	9284	TCP
web_backend	9500	TCP
web_backend	10000:10010	TCP
web_backend	33334	TCP
zookeeper	2181	TCP
zookeeper	2379	TCP
zookeeper	2888	TCP
zookeeper	3888	TCP
zookeeper	9092	TCP
zookeeper	10000:10010	TCP

作为服务器部署的 Central Node 的服务使用的端口

为了使应用程序能够与作为服务器部署的 Central Node 组件正确协同工作，必须按照下表为传出连接配置网络访问。

在 Central Node 组件作为服务器部署的配置中，服务使用的端口

服务	端口	协议
agent_database_configurator	2379	TCP
agent_database_configurator	5432	TCP
agent_database_synchronizer	2379	TCP
agent_database_synchronizer	5432	TCP
agent_database_synchronizer	9092	TCP
agent_database_synchronizer	9100	TCP
agent_database_synchronizer	10000:10010	TCP
agent_server	1080	TCP
agent_server	2379	TCP
agent_server	5432	TCP
agent_server	8100	TCP
agent_server	9090	TCP
agent_server	9284	TCP
antiapt_database_configurator	2379	TCP
antiapt_database_configurator	5432	TCP
authorization_service	2379	TCP
authorization_service	4567	TCP
authorization_service	8090	TCP
authorization_service	8443	TCP
authorization_service	8701	TCP
authorization_service	8899	TCP
cadvisor	任何	任何
clickhouse	2379	TCP

服务	端口	协议
clickhouse	8123	TCP
clickhouse	9000	TCP
clickhouse_database_configurator	2379	TCP
clickhouse_database_configurator	9000	TCP
clickhouse_metrics_importer	2379	TCP
clickhouse_metrics_importer	6379	TCP
clickhouse_metrics_importer	8123	TCP
clickhouse_metrics_importer	9000	TCP
clickhouse_metrics_importer	9090	TCP
coredns	53	TCP
coredns	53	TCP
coredns	2379	TCP
deployment_api	22	TCP
deployment_api	2377	TCP
deployment_api	2379	TCP
deployment_api	4567	TCP
deployment_api	8080	TCP
deployment_api	8443	TCP
deployment_api	8701	TCP
deployment_api	9141	TCP
deployment_api	9284	TCP
deployment_management_api	53	TCP
deployment_management_api	2379	TCP
deployment_management_api	4567	TCP
deployment_management_api	8091	TCP
deployment_management_api	8443	TCP
deployment_management_api	8701	TCP
deployment_management_api	8702	TCP
deployment_management_api	8765	TCP
deployment_management_api	8899	TCP
deployment_management_api	9141	TCP
dhcp_server	任何	任何
edr_synchronizer	25	TCP
edr_synchronizer	80	TCP
edr_synchronizer	514	TCP
edr_synchronizer	514	UDP
edr_synchronizer	2379	TCP
edr_synchronizer	5432	TCP
edr_synchronizer	6379	TCP
edr_synchronizer	8081	TCP
edr_synchronizer	8082	TCP

服务	端口	协议
edr_synchronizer	8083	TCP
edr_synchronizer	9092	TCP
edr_synchronizer	10000:10010	TCP
edr_synchronizer	33334	TCP
elasticsearch	2379	TCP
elasticsearch	9200	TCP
elasticsearch	9300	TCP
elasticsearch_data	2379	TCP
elasticsearch_data	9200	TCP
elasticsearch_data	9300	TCP
elasticsearch_exporter	2379	TCP
elasticsearch_exporter	9200	TCP
elasticsearch_exporter	9300	TCP
etcd	2379	TCP
etcd	2380	TCP
events_api	80	TCP
events_api	2379	TCP
events_api	5432	TCP
events_api	8080	TCP
events_api	8081	TCP
events_api	9092	TCP
events_api	9100	TCP
events_api	9284	TCP
events_api	10000:10010	TCP
fastsearch	2379	TCP
fastsearch	8080	TCP
fastsearch	8180	TCP
fastsearch_events_cleaner	9200	TCP
fastsearch_events_importer	2379	TCP
fastsearch_events_importer	8081	TCP
fastsearch_events_importer	9092	TCP
fastsearch_events_importer	9100	TCP
fastsearch_events_importer	9200	TCP
fastsearch_events_importer	10000:10010	TCP
hunts_database_configurator	2379	TCP
hunts_database_configurator	5432	TCP
hunts_database_synchronizer	2379	TCP
hunts_database_synchronizer	5432	TCP
hunts_database_synchronizer	9092	TCP
hunts_database_synchronizer	10000:10010	TCP
hunts_event_processor	2379	TCP

服务	端口	协议
hunts_event_processor	5432	TCP
hunts_event_processor	8080	TCP
hunts_event_processor	8081	TCP
hunts_event_processor	9092	TCP
hunts_event_processor	9100	TCP
hunts_event_processor	10000:10010	TCP
hunts_statistics_api	2379	TCP
hunts_statistics_api	5432	TCP
hunts_statistics_api	8080	TCP
hunts_statistics_api	8081	TCP
hunts_statistics_api	9092	TCP
hunts_statistics_api	9100	TCP
hunts_statistics_api	10000:10010	TCP
hunts_statistics_processor	2379	TCP
hunts_statistics_processor	5432	TCP
hunts_statistics_processor	8080	TCP
hunts_statistics_processor	8081	TCP
hunts_statistics_processor	9092	TCP
hunts_statistics_processor	9100	TCP
hunts_statistics_processor	9200	TCP
hunts_statistics_processor	10000:10010	TCP
edr_synchronizer	25	TCP
edr_synchronizer	80	TCP
ids_alert_syncer	514	UDP
ids_alert_syncer	2379	TCP
ids_alert_syncer	5432	TCP
ids_alert_syncer	777	TCP
ids_alert_syncer	8083	TCP
ids_alert_syncer	9092	TCP
ids_alert_syncer	9200	TCP
ids_alert_syncer	10000:10010	TCP
ids_alert_syncer	33334	TCP
ioa_update_validator	2379	TCP
ipsec_manager	80	TCP
ipsec_manager	2379	TCP
kafka	2379	TCP
kafka	2181	TCP
kafka	9092	TCP
kafka	9095	TCP
kafka	10000:10010	TCP
kafka_configurator	2181	TCP

服务	端口	协议
kafka_configurator	2379	TCP
kafka_configurator	9092	TCP
kafka_configurator	10000:10010	TCP
kafka_exporter	2379	TCP
kafka_exporter	9092	TCP
kafka_exporter	9100	TCP
kafka_exporter	10000:10010	TCP
kafka_proxy	任何	任何
kata_scanner	25	TCP
kata_scanner	80	TCP
kata_scanner	514	TCP
kata_scanner	514	UDP
kata_scanner	443	TCP
kata_scanner	2379	TCP
kata_scanner	5432	TCP
kata_scanner	6379	TCP
kata_scanner	7777	TCP
kata_scanner	8081	TCP
kata_scanner	8082	TCP
kata_scanner	8083	TCP
kata_scanner	9081	TCP
kata_scanner	9090	TCP
kata_scanner	9092	TCP
kata_scanner	9100	TCP
kata_scanner	9284	TCP
kata_scanner	10000:10010	TCP
kata_scanner	33334	TCP
ksb_agent_server	80	TCP
ksb_agent_server	2379	TCP
ksb_agent_server	5432	TCP
ksb_agent_server	8082	TCP
ksb_agent_server	8083	TCP
ksb_agent_server	9898	TCP
ksn_proxy	80	TCP
ksn_proxy	443	TCP
ksn_proxy	514	TCP
ksn_proxy	514	UDP
ksn_proxy	2379	TCP
ksn_proxy	7777	TCP
ksn_proxy	8083	TCP
ksn_proxy	9092	TCP

服务	端口	协议
ksn_proxy	9102	TCP
ksn_proxy	10000:10010	TCP
ksn_proxy	1:65535	TCP
ksqldb_configurator	2379	TCP
ksqldb_configurator	5432	TCP
ksqldb_configurator	8083	TCP
ksqldb_configurator	8088	TCP
ksqldb_configurator	9092	TCP
ksqldb_configurator	10000:10010	TCP
ksqldb_server	2379	TCP
ksqldb_server	5432	TCP
ksqldb_server	9092	TCP
ksqldb_server	11000:11006	TCP
management_ui	2379	TCP
management_ui	8091	TCP
monitoring_grafana	3000	TCP
monitoring_prometheus	2379	TCP
monitoring_prometheus	9090	TCP
monitoring_prometheus	9100	TCP
monitoring_prometheus	9102	TCP
monitoring_prometheus	9141	TCP
monitoring_prometheus	9142	TCP
monitoring_prometheus	9191	TCP
monitoring_prometheus	9192	TCP
monitoring_prometheus	9283	TCP
multitenancy_management_api	2379	TCP
multitenancy_management_api	4567	TCP
multitenancy_management_api	8443	TCP
multitenancy_management_api	8701	TCP
multitenancy_management_api	8090	TCP
multitenancy_management_api	8899	TCP
nginx_exporter	2379	TCP
nginx_gateway	80	TCP
nginx_gateway	81	TCP
nginx_gateway	443	TCP
nginx_gateway	2379	TCP
nginx_gateway	4443	TCP
nginx_gateway	4567	TCP
nginx_gateway	6379	TCP
nginx_gateway	8080	TCP
nginx_gateway	8081	TCP

服务	端口	协议
nginx_gateway	8082	TCP
nginx_gateway	8083	TCP
nginx_gateway	8085	TCP
nginx_gateway	8090	TCP
nginx_gateway	8100	TCP
nginx_gateway	8443	TCP
nginx_gateway	8444	TCP
nginx_gateway	8701	TCP
nginx_gateway	8702	TCP
nginx_gateway	8899	TCP
nginx_gateway	9393	TCP
nginx_gateway	9898	TCP
node_exporter	任何	任何
nta_core	25	TCP
nta_core	80	TCP
nta_core	2379	TCP
nta_core	5433	TCP
nta_core	8082	TCP
nta_core	8083	TCP
nta_core	9443	TCP
nta_database	-	-
nta_database_configurator	2379	TCP
nta_database_configurator	5432	TCP
nta_database_configurator	5432	TCP
nta_sensor_configurator	2379	TCP
nta_sensor_configurator	8084	TCP
nta_sensor_configurator	9443	TCP
nta_sensor_configurator	50051	TCP
nta_syncer	80	TCP
nta_syncer	2379	TCP
nta_syncer	5422	TCP
nta_syncer	5423	TCP
nta_syncer	7777	TCP
nta_syncer	8084	TCP
nta_syncer	9092	TCP
nta_syncer	10000:10010	TCP
nta_syncer	50051	TCP
postfix	25	TCP
postfix	2379	TCP
postgresql_exporter	2379	TCP
postgresql_exporter	5432	TCP

服务	端口	协议
postgresql_exporter	9100	TCP
postgresql_server	2379	TCP
postgresql_server	5432	TCP
preprocessor	任何	任何
preprocessor_icap	80	TCP
preprocessor_icap	1514	TCP
preprocessor_icap	1514	UDP
preprocessor_icap	2379	TCP
preprocessor_icap	4223	TCP
preprocessor_icap	6379	TCP
preprocessor_icap	7777	TCP
preprocessor_icap	8081	TCP
preprocessor_icap	8082	TCP
preprocessor_icap	8083	TCP
preprocessor_icap	9092	TCP
preprocessor_icap	9192	TCP
preprocessor_icap	9284	TCP
preprocessor_icap	10000:10010	TCP
preprocessor_pop	110	TCP
preprocessor_pop	514	TCP
preprocessor_pop	514	UDP
preprocessor_pop	2379	TCP
preprocessor_pop	4223	TCP
preprocessor_pop	6379	TCP
preprocessor_pop	7777	TCP
preprocessor_pop	8081	TCP
preprocessor_pop	8082	TCP
preprocessor_pop	8083	TCP
preprocessor_pop	9081	TCP
preprocessor_pop	9092	TCP
preprocessor_pop	10000:10010	TCP
preprocessor_pop	1:65535	TCP
preprocessor_smtp	514	TCP
preprocessor_smtp	514	UDP
preprocessor_smtp	2379	TCP
preprocessor_smtp	4223	TCP
preprocessor_smtp	6379	TCP
preprocessor_smtp	7777	TCP
preprocessor_smtp	8081	TCP
preprocessor_smtp	8082	TCP
preprocessor_smtp	8083	TCP

服务	端口	协议
preprocessor_smtp	9081	TCP
preprocessor_smtp	9092	TCP
preprocessor_smtp	10000:10010	TCP
preprocessor_span	任何	任何
primary_database_configurator	2379	TCP
primary_database_configurator	5432	TCP
redis	2379	TCP
redis	6379	TCP
response_actions_processor	514	TCP
response_actions_processor	514	UDP
response_actions_processor	2379	TCP
response_actions_processor	5432	TCP
response_actions_processor	8081	TCP
response_actions_processor	9092	TCP
response_actions_processor	9100	TCP
response_actions_processor	10000:10010	TCP
response_api	514	TCP
response_api	514	UDP
response_api	2379	TCP
response_api	5432	TCP
response_api	8080	TCP
response_api	9092	TCP
response_api	9100	TCP
response_api	10000:10010	TCP
s3proxy	80	TCP
s3proxy	1080	TCP
s3proxy	2379	TCP
s3rotator	80	TCP
s3rotator	1080	TCP
s3rotator	2379	TCP
s3rotator	9283	TCP
s3rotator	9284	TCP
schema_registry	2379	TCP
schema_registry	8081	TCP
schema_registry	9092	TCP
schema_registry	10000:10010	TCP
sensor_event_processor	2379	TCP
sensor_event_processor	8080	TCP
sensor_event_processor	8081	TCP
sensor_event_processor	9092	TCP
sensor_event_processor	9100	TCP

服务	端口	协议
sensor_event_processor	10000:10010	TCP
services_configurator	2379	TCP
siem_proxy	80	TCP
siem_proxy	514	TCP
siem_proxy	514	UDP
siem_proxy	1080	TCP
siem_proxy	1514	TCP
siem_proxy	1514	UDP
siem_proxy	2080	TCP
siem_proxy	2379	TCP
siem_proxy	9284	TCP
siem_proxy	任何	任何
snmpd	161	TCP
snmpd	2379	TCP
updater	80	TCP
updater	443	TCP
updater	514	TCP
updater	514	TCP
updater	2379	TCP
updater	5432	TCP
updater	6379	TCP
updater	7777	TCP
updater	8083	TCP
updater	9100	TCP
updater	9500	TCP
updater	1:65535	TCP
updates_consistency_checker	80	TCP
updates_consistency_checker	2379	TCP
updates_consistency_checker	6379	TCP
updates_consistency_checker	8083	TCP
updates_consistency_checker	9092	TCP
updates_consistency_checker	10000:10010	TCP
web_backend	25	TCP
web_backend	80	TCP
web_backend	443	TCP
web_backend	514	TCP
web_backend	514	UDP
web_backend	1080	TCP
web_backend	2379	TCP
web_backend	5432	TCP
web_backend	6379	TCP

服务	端口	协议
web_backend	7777	TCP
web_backend	8080	TCP
web_backend	8081	TCP
web_backend	8082	TCP
web_backend	8083	TCP
web_backend	8085	TCP
web_backend	8090	TCP
web_backend	8123	TCP
web_backend	8283	TCP
web_backend	8443	TCP
web_backend	8444	TCP
web_backend	8899	TCP
web_backend	9090	TCP
web_backend	9092	TCP
web_backend	9284	TCP
web_backend	9500	TCP
web_backend	10000:10010	TCP
web_backend	33334	TCP
zookeeper	2181	TCP
zookeeper	2379	TCP
zookeeper	2888	TCP
zookeeper	3888	TCP
zookeeper	9092	TCP
zookeeper	10000:10010	TCP

在独立服务器上安装 Sensor 组件的配置中，服务使用的端口

为了使应用程序在 Sensor 组件安装在独立服务器上的配置下正常工作，您必须根据下表为传出连接配置网络访问。

在独立服务器上安装 Sensor 组件的配置中，服务使用的端口

服务	端口	协议
cadvisor	任何	任何
ksn_proxy	80	TCP
ksn_proxy	443	TCP
ksn_proxy	514	TCP
ksn_proxy	514	UDP
ksn_proxy	2379	TCP
ksn_proxy	7777	TCP

服务	端口	协议
ksn_proxy	8083	TCP
ksn_proxy	9092	TCP
ksn_proxy	9102	TCP
ksn_proxy	10000:10010	TCP
monitoring_prometheus	2379	TCP
monitoring_prometheus	9090	TCP
monitoring_prometheus	9100	TCP
monitoring_prometheus	9102	TCP
monitoring_prometheus	9141	TCP
monitoring_prometheus	9142	TCP
monitoring_prometheus	9191	TCP
monitoring_prometheus	9192	TCP
nginx_gateway	443	TCP
nginx_gateway	2379	TCP
nginx_gateway	8085	TCP
nginx_gateway	8100	TCP
nginx_gateway	8283	TCP
node_exporter	任何	TCP
preprocessor_icap	443	TCP
preprocessor_icap	1080	TCP
preprocessor_icap	1344	TCP
preprocessor_icap	1514	TCP
preprocessor_icap	1514	UDP
preprocessor_icap	2379	TCP
preprocessor_icap	4223	TCP
preprocessor_icap	6379	TCP
preprocessor_icap	7777	TCP
preprocessor_icap	8081	UDP
preprocessor_icap	8082	TCP
preprocessor_icap	8082	UDP
preprocessor_icap	8083	TCP
preprocessor_icap	8085	TCP
preprocessor_icap	9092	TCP
preprocessor_pop3	1514	TCP
preprocessor_pop3	1514	UDP
preprocessor_pop3	2379	TCP
preprocessor_pop3	4223	TCP
preprocessor_pop3	6379	TCP
preprocessor_pop3	7777	TCP
preprocessor_pop3	8081	TCP
preprocessor_pop3	8081	UDP

服务	端口	协议
preprocessor_pop3	8082	UDP
preprocessor_pop3	8083	TCP
preprocessor_pop3	9081	TCP
preprocessor_pop3	9092	TCP
preprocessor_pop3	11000	TCP
preprocessor_smtp	1514	TCP
preprocessor_smtp	1514	UDP
preprocessor_smtp	2379	TCP
preprocessor_smtp	4223	TCP
preprocessor_smtp	6379	TCP
preprocessor_smtp	7777	TCP
preprocessor_smtp	8081	TCP
preprocessor_smtp	8081	UDP
preprocessor_smtp	8082	UDP
preprocessor_smtp	8083	TCP
preprocessor_smtp	9081	TCP
preprocessor_smtp	9092	TCP
preprocessor_smtp	11000	TCP
preprocessor_span	任何	任何
preprocessor_span	13520	TCP
preprocessor_span	8081	UDP
preprocessor_span	8082	UDP
preprocessor_span	9081	TCP
preprocessor_span	7777	TCP
preprocessor_span	9092	TCP
preprocessor_span	8083	TCP
preprocessor_span	2379	TCP
preprocessor_span	6379	TCP
redis	2379	TCP
redis	6379	TCP
s3proxy	80	TCP
s3proxy	1080	TCP
s3proxy	2379	TCP
s3rotator	80	TCP
s3rotator	1080	TCP
s3rotator	2379	TCP
s3rotator	9284	TCP
sensor_management_api	任何	任何
services_configurator	2379	TCP
siem_proxy	80	TCP
siem_proxy	514	TCP

服务	端口	协议
siem_proxy	514	UDP
siem_proxy	1080	TCP
siem_proxy	1514	TCP
siem_proxy	1514	UDP
siem_proxy	2080	TCP
siem_proxy	2379	TCP
siem_proxy	9284	TCP
snmpd	161	TCP
snmpd	2379	TCP

网络流量分析服务之间的通信端口

为了使应用程序正常工作，您必须确保网络流量分析服务可以通过下表列出的端口进行通信。默认情况下允许服务的入站连接。

网络流量分析服务之间的通信端口

服务	端口	目标服务	协议
nta_database_configurator	5433	nta_database	TCP
nta_core	5433	nta_database	TCP
nta_core	2379	etcd	TCP
nta_core	80	web_backend	TCP
nta_core	9443	互联网	TCP
nta_syncer	9092	kafka	TCP
nta_syncer	2379	etcd	TCP
nta_syncer	5432	postgresql_server	TCP
nta_syncer	5433	nta_database	TCP
nta_syncer	50051	nta_core	TCP
nta_syncer	8084	nta_core	TCP
nta_sensor_configurator	50051	nta_core	UDP
nta_sensor_configurator	9443	nta_core	TCP
preprocessor_span	13520	nta_core	TCP
preprocessor_span	8081	kata_scanner	UDP
preprocessor_span	8082	kata_scanner	UDP
preprocessor_span	9081	kata_scanner	TCP
preprocessor_span	7777	ksn_proxy	TCP
preprocessor_span	9092	kafka	TCP
preprocessor_span	8083	updater	TCP
preprocessor_span	2379	etcd	TCP
preprocessor_span	6379	redis	TCP
preprocessor_icap	9092	kafka	TCP
preprocessor_icap	7777	ksn_proxy	TCP

服务	端口	目标服务	协议
preprocessor_icap	8081	kata_scanner	UDP
preprocessor_icap	8082	kata_scanner	UDP
preprocessor_icap	2379	etcd	TCP
preprocessor_icap	8083	updater	TCP
preprocessor_icap	4223	preprocessor_span	TCP
preprocessor_smtp	8081	kata_scanner	UDP
preprocessor_smtp	8082	kata_scanner	UDP
preprocessor_smtp	9081	kata_scanner	TCP
preprocessor_smtp	7777	ksn_proxy	TCP
preprocessor_smtp	9092	kafka	TCP
preprocessor_smtp	8083	updater	TCP
preprocessor_smtp	2379	etcd	TCP
preprocessor_smtp	6379	redis	TCP
preprocessor_smtp	4223	preprocessor_span	TCP
preprocessor_pop3	8081	kata_scanner	UDP
preprocessor_pop3	8082	kata_scanner	UDP
preprocessor_pop3	9081	kata_scanner	TCP
preprocessor_pop3	7777	ksn_proxy	TCP
preprocessor_pop3	9092	kafka	TCP
preprocessor_pop3	8083	updater	TCP
preprocessor_pop3	2379	etcd	TCP
preprocessor_pop3	6379	redis	TCP
preprocessor_pop3	4223	preprocessor_span	TCP

配置 Endpoint Agent 组件与 KEDR 功能块的集成

本节包含有关配置 KEDR 功能块与 Endpoint Agent 组件角色中使用的应用程序的集成的信息。

配置与 Kaspersky Endpoint Agent 的受信任连接

配置受信任连接的操作可在 Kaspersky Anti Targeted Attack Platform 端通过 Web 界面和应用程序管理员菜单执行，也可在 Kaspersky Endpoint Agent 端通过 KSC 管理控制台执行。

您可以使用以下选项之一来配置信任连接：

- 无需在 Kaspersky Anti Targeted Attack Platform端验证 Kaspersky Endpoint Agent TLS 证书。
  - 配置与 Central Node 服务器的连接，无需验证 Kaspersky Anti Targeted Attack Platform 中 Kaspersky Endpoint Agent 的 TLS 证书。

    Kaspersky Endpoint Agent 使用 Central Node 服务器的 TLS 证书与 Kaspersky Anti Targeted Attack Platform 建立受信任连接。当 Kaspersky Endpoint Agent 尝试连接时，Kaspersky Anti Targeted Attack Platform 不会验证 Kaspersky Endpoint Agent 的 TLS 证书。

    如果您使用此替代配置进行信任连接，则过程如下：

    1. 在 Central Node 的 Web 界面中生成或上传独立准备的 Central Node 服务器的 TLS 证书（如果之前未创建 Central Node 的 TLS 证书）。
    2. 将 Central Node 服务器的 TLS 证书下载到您的计算机。
    3. 使用管理控制台 (MMC) 将 Central Node 服务器的 TLS 证书上传到 Kaspersky Endpoint Agent。
  - 配置与 Sensor 服务器的连接，无需验证 Kaspersky Anti Targeted Attack Platform 中 Kaspersky Endpoint Agent 的 TLS 证书。

    到 Sensor 服务器的流量重定向是在 Kaspersky Anti Targeted Attack Platform 中配置的。Kaspersky Endpoint Agent 使用 Sensor 服务器的 TLS 证书与 Kaspersky Anti Targeted Attack Platform 建立信任连接。当 Kaspersky Endpoint Agent 尝试连接时，Kaspersky Anti Targeted Attack Platform 不会验证 Kaspersky Endpoint Agent 的 TLS 证书。

    如果您使用此替代配置进行信任连接，则过程如下：

    1. 启用从 Kaspersky Endpoint Agent 到 Sensor 服务器的流量重定向。
    2. 在 Central Node 服务器上授权 Sensor 组件。
    3. 在 Sensor 服务器的管理员菜单中为 Sensor 服务器生成或上传独立准备的 TLS 证书。
    4. 将 Sensor 服务器的 TLS 证书下载到您的计算机。
    5. 使用管理控制台 (MMC) 将 Sensor 服务器的 TLS 证书上传到 Kaspersky Endpoint Agent。

- 验证 Kaspersky Anti Targeted Attack Platform 端的 Kaspersky Endpoint Agent TLS 证书。

  - 配置与 Central Node 服务器的连接，并验证 Kaspersky Anti Targeted Attack Platform 中 Kaspersky Endpoint Agent 的 TLS 证书。

    Kaspersky Endpoint Agent 使用 Central Node 服务器的 TLS 证书与 Kaspersky Anti Targeted Attack Platform 建立受信任连接。额外的连接安全性在 Kaspersky Endpoint Agent 中得到配置，Kaspersky Endpoint Agent 的 TLS 证书得到上传。当 Kaspersky Endpoint Agent尝试连接时，Kaspersky Anti Targeted Attack Platform 会验证 Kaspersky Endpoint Agent 的 TLS 证书。

    如果您使用此替代配置进行信任连接，则过程如下：

    1. 在 Central Node 的 Web 界面中生成或上传独立准备的 Central Node 服务器的 TLS 证书（如果之前未创建 Central Node 的 TLS 证书）。
    2. 将 Central Node 服务器的 TLS 证书下载到您的计算机。
    3. 使用管理控制台 (MMC) 将 Central Node 服务器的 TLS 证书上传到 Kaspersky Endpoint Agent。
    4. 在 Kaspersky Anti Targeted Attack Platform 的 Web 界面中启用 Kaspersky Endpoint Agent TLS 证书验证。
    5. 使用 Kaspersky Endpoint Agent 的 TLS 证书生成并下载加密容器，或使用 Kaspersky Anti Targeted Attack Platform 的 Web 界面上传独立准备的 Kaspersky Endpoint Agent TLS 证书。

       如果您想自行准备 Kaspersky Endpoint Agent 的 TLS 证书，则必须使用您的证书创建 PFX 加密容器。有关管理 TLS 证书的详细信息，请参阅 OpenSSL 文档。

    6. 使用管理控制台 (MMC) 将带有 Kaspersky Endpoint Agent 证书的加密容器上传到 Kaspersky Endpoint Agent。

  - 配置与 Sensor 服务器的连接，并验证 Kaspersky Anti Targeted Attack Platform 中 Kaspersky Endpoint Agent 的 TLS 证书。

    到 Sensor 服务器的流量重定向是在 Kaspersky Anti Targeted Attack Platform 中配置的。Kaspersky Endpoint Agent 使用 Sensor 服务器的 TLS 证书与 Kaspersky Anti Targeted Attack Platform 建立信任连接。额外的连接安全性在 Kaspersky Endpoint Agent 中得到配置，Kaspersky Endpoint Agent 的 TLS 证书得到上传。当 Kaspersky Endpoint Agent尝试连接时，Kaspersky Anti Targeted Attack Platform 会验证 Kaspersky Endpoint Agent 的 TLS 证书。

    如果您使用此替代配置进行信任连接，则过程如下：

    1. 启用从 Kaspersky Endpoint Agent 到 Sensor 服务器的流量重定向。
    2. 在 Central Node 服务器上授权 Sensor 组件。
    3. 在 Sensor 服务器的管理员菜单中为 Sensor 服务器生成或上传独立准备的 TLS 证书。
    4. 将 Sensor 服务器的 TLS 证书下载到您的计算机。
    5. 使用管理控制台 (MMC) 将 Sensor 服务器的 TLS 证书上传到 Kaspersky Endpoint Agent。
    6. 在 Kaspersky Anti Targeted Attack Platform 的 Web 界面中启用 Kaspersky Endpoint Agent TLS 证书验证。

7. 使用 Kaspersky Endpoint Agent 的 TLS 证书生成并下载加密容器，或使用 Kaspersky Anti Targeted Attack Platform 的 Web 界面上传独立准备的 Kaspersky Endpoint Agent TLS 证书。

   如果您想自行准备 Kaspersky Endpoint Agent 的 TLS 证书，则必须使用您的证书创建 PFX 加密容器。有关管理 TLS 证书的详细信息，请参阅 OpenSSL 文档。

8. 使用 KSC 管理控制台将带有 Kaspersky Endpoint Agent 证书的加密容器上传到 Kaspersky Endpoint Agent。

配置 Central Node 服务器对 Kaspersky Endpoint Agent TLS 证书的验证并将加密容器上传到 Kaspersky Endpoint Agent

要配置 Central Node 服务器对 Kaspersky Endpoint Agent TLS 证书的验证并将带有 Kaspersky Endpoint Agent 证书的加密容器上传到 Kaspersky Endpoint Agent：

1. 打开 KSC 控制台。
2. 在控制台树中，打开**策略**文件夹。
3. 在 Kaspersky Endpoint Agent 策略部分中，选择所需的策略并双击它以打开其属性。
   所选策略的属性将得到显示。
4. 在**KATA 集成**部分中，选择**KATA Central Node**子部分。
5. 单击**配置附加安全性**。
6. 在打开的窗口中，选择**使用客户端证书保护连接**复选框。
7. 单击**上传**。
   这将在您的本地计算机上打开文件选择窗口。
8. 选择在 Kaspersky Anti Targeted Attack Platform 服务器上生成并下载到您计算机硬盘上的 Kaspersky Endpoint Agent 证书的加密容器文件。
9. 单击“**确定**”。
   窗口关闭。
10. 确保设置组右上角的切换开关位于**策略下方**位置。
11. 单击“**确定**”。

带有 Kaspersky Endpoint Agent 证书的加密容器将被上传到 Kaspersky Endpoint Agent。现在，当 Kaspersky Endpoint Agent 尝试连接时，Kaspersky Anti Targeted Attack Platform 会验证 Kaspersky Endpoint Agent 的 TLS 证书。

将 Central Node 服务器或 Sensor 的 TLS 证书上传到 Kaspersky Endpoint Agent

将 Central Node 服务器或 Sensor 的 TLS 证书上传到 Kaspersky Endpoint Agent

1. 打开 KSC 控制台。
2. 在控制台树中，打开**策略**文件夹。
3. 在 Kaspersky Endpoint Agent 策略部分中，选择所需的策略并双击它以打开其属性。
   所选策略的属性将得到显示。
4. 在**KATA 集成**部分中，选择**KATA 集成设置**子部分。
5. 选择**启用 KATA 集成**复选框。
6. 在**地址**字段中，输入要配置与其集成的 Kaspersky Anti Targeted Attack Platform 程序的 Central Node 服务器的地址，然后选择用于连接的端口。默认使用端口 443。
7. 选择**使用固定证书来保护连接**复选框。
8. 单击**添加 TLS 证书...**。
   这将打开**添加 TLS 证书**窗口。
9. 要添加先前在 Kaspersky Anti Targeted Attack Platform 端创建并下载的 TLS 证书，请执行以下操作之一：
   - 添加证书文件。为此，请单击**浏览...**；在显示的窗口中选择证书文件，单击**打开**。
   - 将证书文件的内容粘贴到**粘贴 TLS 证书数据：**字段。

   Kaspersky Endpoint Agent 只能为 Kaspersky Anti Targeted Attack Platform 服务器存储一个 TLS 证书。如果您之前添加过 TLS 证书并正在再次添加 TLS 证书，则仅使用最后添加的证书。

   如果您使用 Sensor 组件配置了到服务器的流量重定向，则必须下载 Sensor 服务器的 TLS 证书，然后在此处上传。
10. 单击**添加**。
    有关添加的 TLS 证书的信息显示在与 Kaspersky Anti Targeted Attack Platform 集成的部分中。
11. 确保设置组右上角的切换开关位于**策略下方**位置。
12. 单击“**确定**”。

Central Node 服务器的 TLS 证书被下载到 Endpoint Agent。

在 Kaspersky Endpoint Agent 端配置与 Kaspersky Anti Targeted Attack Platform 的集成和信任连接

要在 Kaspersky Endpoint Agent 端配置与 Kaspersky Anti Targeted Attack Platform 的集成：

1. 打开 KSC 控制台。
2. 在控制台树中，打开**策略**文件夹。
3. 在 Kaspersky Endpoint Agent 策略部分中，选择所需的策略并双击它以打开其属性。
   所选策略的属性将得到显示。
4. 在**KATA 集成**部分中，选择**KATA 集成设置**子部分。
5. 选择**启用 KATA 集成**复选框。
6. 在**地址**字段中，输入要配置与其集成的 Kaspersky Anti Targeted Attack Platform 程序的 Central Node 服务器的地址，然后选择用于连接的端口。默认使用端口 443。
7. 选择**使用固定证书来保护连接**复选框。
8. 单击**添加 TLS 证书...**。
   这将打开**添加 TLS 证书**窗口。
9. 要添加先前在 Kaspersky Anti Targeted Attack Platform 端创建并下载的 TLS 证书，请执行以下操作之一：
   - 添加证书文件。为此，请单击**浏览...**；在显示的窗口中选择证书文件，单击**打开**。
   - 将证书文件的内容粘贴到**粘贴 TLS 证书数据：**字段。

   Kaspersky Endpoint Agent 只能为 Kaspersky Anti Targeted Attack Platform 服务器存储一个 TLS 证书。如果您之前添加过 TLS 证书并正在再次添加 TLS 证书，则仅使用最后添加的证书。

   如果您使用 Sensor 组件配置了到服务器的流量重定向，则必须下载 Sensor 服务器的 TLS 证书，然后在此处上传。
10. 单击**添加**。
    有关添加的 TLS 证书的信息显示在与 Kaspersky Anti Targeted Attack Platform 集成的部分中。
11. 单击**添加客户端证书...**。
12. 在显示的窗口中，选择**使用客户端证书保护**复选框。
13. 单击**下载**。
    这将在您的本地计算机上打开文件选择窗口。

14. 选择在 Kaspersky Anti Targeted Attack Platform 服务器上生成并下载到您计算机硬盘上的 Kaspersky Endpoint Agent 证书的加密容器文件。

15. 单击“**确定**”。

    窗口关闭。

16. 在**超时期限（秒）：** 字段中，输入Kaspersky Anti Targeted Attack Platform Central Node 服务器的最大响应超时（以秒为单位）。

17. 在**每隔（分钟）向 KATA 服务器发送同步请求**字段中，输入时间段（以分钟为单位）。

18. 如果您不希望 Kaspersky Endpoint Agent 将有关进程重复运行的信息发送到 Kaspersky Anti Targeted Attack Platform 服务器，请选择**应用事件传输的 TTL 周期**复选框。如果该进程在下一个 TTL 周期到期后启动，Kaspersky Endpoint Agent 不会认为这是该进程的重复启动。

19. 如果已设置“应用事件传输的 TTL 周期”复选框，请在**TTL 周期（分钟）**字段中指定时间。

20. 确保设置组右上角的切换开关位于**策略下方**位置。

21. 单击“**确定**”。

    在 Kaspersky Endpoint Agent 端与 Kaspersky Anti Targeted Attack Platform 集成得到配置。

配置与 Kaspersky Endpoint Security 的受信任连接

要配置受信任连接，您必须在 Kaspersky Anti Targeted Attack Platform 端和 Kaspersky Endpoint Security 端执行操作。

您可以使用以下选项之一来配置信任连接：

- **配置与 Central Node 服务器的连接，无需验证 Kaspersky Anti Targeted Attack Platform 中 Kaspersky Endpoint Security 的 TLS 证书。**

  Kaspersky Endpoint Security 使用 Central Node 服务器的 TLS 证书与 Kaspersky Anti Targeted Attack Platform 建立受信任连接。当 Kaspersky Endpoint Security 尝试连接时，Kaspersky Anti Targeted Attack Platform 不会验证 Kaspersky Endpoint Security 的 TLS 证书。

  如果您使用此替代配置进行信任连接，则过程如下：

  1. 在 Central Node 的 Web 界面中生成或上传独立准备的 Central Node 服务器的 TLS 证书（如果之前未创建 Central Node 的 TLS 证书）。

  2. 下载 Central Node 服务器的 TLS 证书。

  3. 将安装有 Kaspersky Endpoint Security 的计算机连接到 Central Node 服务器：

     - 连接 Kaspersky Endpoint Security for Windows。
     - 连接 Kaspersky Endpoint Security for Linux。
     - 连接 Kaspersky Endpoint Security for Mac。

- **配置与 Central Node 服务器的连接，并验证 Kaspersky Anti Targeted Attack Platform 端 Kaspersky Endpoint Security 的 TLS 证书。**

  Kaspersky Endpoint Security 使用 Central Node 服务器的 TLS 证书与 Kaspersky Anti Targeted Attack Platform 建立受信任连接。额外的连接安全性在 Kaspersky Endpoint Security 中得到配置，Kaspersky Endpoint Security 的 TLS 证书得到上传。当 Kaspersky Endpoint Security 尝试连接时，Kaspersky Anti Targeted Attack Platform 会验证 Kaspersky Endpoint Security 的 TLS 证书。

  如果您使用此替代配置进行信任连接，则过程如下：

  1. 在 Central Node 的 Web 界面中生成或上传独立准备的 Central Node 服务器的 TLS 证书（如果之前未创建 Central Node 的 TLS 证书）。
  2. 下载 Central Node 服务器的 TLS 证书。
  3. 在 Kaspersky Anti Targeted Attack Platform 的 Web 界面中启用 Kaspersky Endpoint Security TLS 证书验证。
  4. 使用 Kaspersky Endpoint Security 的 TLS 证书生成并下载加密容器，或使用 Kaspersky Anti Targeted Attack Platform 的 Web 界面上传独立准备的 Kaspersky Endpoint Security TLS 证书。

     如果您想自行准备 Kaspersky Endpoint Security 的 TLS 证书，则必须使用您的证书创建 PFX 加密容器。有关管理 TLS 证书的详细信息，请参阅 OpenSSL 文档。

  5. 将安装有 Kaspersky Endpoint Security 的计算机连接到 Central Node 服务器：
     - 连接 Kaspersky Endpoint Security for Windows。
     - 连接 Kaspersky Endpoint Security for Linux。
     - 连接 Kaspersky Endpoint Security for Mac。

下载 Central Node 服务器的 TLS 证书

下载服务器的 TLS 证书：

1. 在应用程序 Web 界面窗口中，选择**设置**部分的**证书**子部分。
2. 在**服务器证书**部分，单击**下载**。

服务器证书文件将被保存在浏览器下载文件夹中。

在 Kaspersky Anti Targeted Attack Platform 的 Web 界面中为 Central Node 服务器生成 TLS 证书

如果您已在使用 Central Node 服务器 TLS 证书，则生成新证书会导致当前使用的证书被删除并替换为新生成的证书。

在使用旧证书的所有地方都必须输入新证书的数据。

如果您替换 TLS 证书，您将需要:

- 重新授权 Central Node 上的邮件 Sensor (KSMG、KLMS)。
- 重新配置 Central Node、PCN、SCN 与 Sandbox 的连接。
- 重新配置从 Endpoint Agent 到 Sensor 的流量转发以及与 Endpoint Agent 的受信任连接。
- 将新证书上传到 Active Directory (如果您正在使用 Active Directory)。

请确保删除所有 Endpoint Agent 主机隔离规则。与隔离主机的连接将丢失，您将无法管理它们。

为 Central Node 服务器生成 TLS 证书:

1. 使用管理员凭据登录 Kaspersky Anti Targeted Attack Platform Web 界面。
2. 在应用程序 Web 界面窗口中，选择**设置**部分的**证书**子部分。
3. 在“**服务器证书**”部分，单击“**生成**”。
   这将打开操作确认窗口。
4. 单击**是**。

   Kaspersky Anti Targeted Attack Platform 生成新的 TLS 证书。页面会自动刷新。

使用 Kaspersky Anti Targeted Attack Platform 的 Web 界面为 Central Node 服务器上传独立准备的 TLS 证书

您可以选择自行准备 TLS 证书并使用 Kaspersky Anti Targeted Attack Platform Web 界面上传。

准备上传的 TLS 证书文件必须满足以下要求:

- 文件必须包含证书本身和用于连接的私人加密密钥。
- 文件必须是 PEM 格式。

该应用程序不支持其他格式的证书。

如果您准备了其他格式的证书，则必须将其转换为 PEM 格式。

- 私钥长度必须为 2048 位或更长。

要获取准备 TLS 证书进行导入的更多详细信息，请参阅 Open SSL 文档。

如果您已在使用 Central Node 服务器 TLS 证书，则上传新证书会导致当前使用的证书被删除并替换为上传的证书。

在使用旧证书的所有地方都必须输入新证书的数据。

如果您替换 TLS 证书，您将需要:

- 重新授权 Central Node 上的邮件 Sensor (KSMG、KLMS)。
- 重新配置 Central Node、PCN、SCN 与 Sandbox 的连接。
- 重新配置从 Endpoint Agent 到 Sensor 的流量转发以及与 Endpoint Agent 的受信任连接。

删除所有 Endpoint Agent 主机隔离规则。与隔离主机的连接被切断，您无法管理它们。

要使用 Kaspersky Anti Targeted Attack Platform Web 界面上传独立准备的 TLS 证书:

1. 使用管理员凭据登录 Kaspersky Anti Targeted Attack Platform Web 界面。
2. 在应用程序 Web 界面窗口中，选择**设置**部分的**证书**子部分。
3. 在**服务器证书**部分，单击**上传**。
   这将打开文件选择窗口。
4. 选择要下载的 TLS 证书文件，然后单击**打开**按钮。
   这将关闭文件选择窗口。
   TLS 证书已添加到 Kaspersky Anti Targeted Attack Platform。
   重新配置从 Endpoint Agent 到 Sensor 的流量转发以及与 Endpoint Agent 的受信任连接。

请确保删除所有 Endpoint Agent 主机隔离规则。与隔离主机的连接将丢失，您将无法管理它们。

在 Kaspersky Anti Targeted Attack Platform 的 Web 界面中启用 Endpoint Agent 组件的 TLS 证书验证

要打开与在 Endpoint Agent 组件角色中使用的应用程序的受信任连接，请执行以下操作：

1. 使用管理员凭据登录 Kaspersky Anti Targeted Attack PlatformWeb 界面。
2. 在 Kaspersky Anti Targeted Attack Platform Web 界面窗口中，选择**设置**部分的**证书**子区域。
3. 在**Endpoint Agent 证书**部分，打开**验证 Endpoint Agent TLS 证书**开关。

   当充当 Endpoint Agent 组件角色的应用程序尝试连接到 Kaspersky Anti Targeted Attack Platform 时，Kaspersky Anti Targeted Attack Platform 将检查 TLS 证书数据。

在 Kaspersky Anti Targeted Attack Platform 的 Web 界面中生成 Endpoint Agent 组件的 TLS 证书并下载加密容器

要为 Kaspersky Anti Targeted Attack Platform 与 Endpoint Agent 组件角色中使用的应用程序的连接生成 TLS 证书：

1. 使用管理员凭据登录 Kaspersky Anti Targeted Attack PlatformWeb 界面。
2. 在 Kaspersky Anti Targeted Attack Platform Web 界面窗口中，选择**设置**部分的**证书**子区域。
3. 在**Endpoint Agent 证书**部分，单击**生成和导出**。

   新的 TLS 证书将显示在 TLS 证书表中。带有 PFX 格式的 Kaspersky Endpoint Agent 证书的加密容器文件将被下载到本地计算机上的浏览器下载文件夹中。

当尝试连接到 Kaspersky Anti Targeted Attack Platform 时，您可以使用加密容器来配置 Central Node 服务器对 Kaspersky Endpoint Agent TLS 证书的验证。

默认情况下，加密容器不受密码保护。您可以使用密码保护加密容器。有关管理 TLS 证书的详细信息，请参阅 OpenSSL 文档。

加密容器仅包含证书文件，但不包含私钥文件。Kaspersky Anti Targeted Attack Platform 不会存储用于连接的 TLS 加密的私钥。

使用 Kaspersky Anti Targeted Attack Platform 的 Web 界面上传独立准备的 Endpoint Agent 组件的 TLS 证书

您可以选择自行准备 TLS 证书并使用 Kaspersky Anti Targeted Attack Platform Web 界面上传。

准备上传的 TLS 证书文件必须满足以下要求：

- 文件必须包含证书本身和用于连接的私人加密密钥。
- 文件必须是 PEM 格式。
- 私人密钥长度必须为 2048 位或更长。

要获取准备 TLS 证书进行导入的更多详细信息，请参阅 Open SSL 文档。

如果您想自行准备 Kaspersky Endpoint Agent 的 TLS 证书，必须使用您的证书创建 PFX 加密容器并将加密容器上传到 Kaspersky Endpoint Agent。

当尝试连接到 Kaspersky Anti Targeted Attack Platform 时，您可以使用加密容器来配置 Central Node 服务器对 Kaspersky Endpoint Agent TLS 证书的验证。

有关管理 TLS 证书的详细信息，请参阅 OpenSSL 文档。

> 加密容器必须仅包含证书文件，但不包含私钥文件。Kaspersky Anti Targeted Attack Platform 不会存储用于连接的 TLS 加密的私钥。

要使用 Kaspersky Anti Targeted Attack Platform Web 界面上传独立准备的 TLS 证书：

1. 使用管理员凭据登录 Kaspersky Anti Targeted Attack Platform Web 界面。
2. 在 Kaspersky Anti Targeted Attack Platform Web 界面窗口中，选择**设置**部分的**证书**子区域。
3. 在**Endpoint Agent 证书**部分，单击**上传**。
   这将打开文件选择窗口。
4. 选择要下载的 TLS 证书文件，然后单击**打开**按钮。
   这将关闭文件选择窗口。

TLS 证书已添加到 Kaspersky Anti Targeted Attack Platform。

在 Kaspersky Anti Targeted Attack Platform 的 Web 界面中查看 Endpoint Agent 组件的 TLS 证书表

要使用 Kaspersky Anti Targeted Attack Platform Web 界面查看用于与在 Endpoint Agent 组件角色中使用的应用程序连接的 TLS 证书列表，请执行以下操作：

1. 使用管理员凭据登录 Kaspersky Anti Targeted Attack PlatformWeb 界面。
2. 在 Kaspersky Anti Targeted Attack Platform Web 界面窗口中，选择**设置**部分的**证书**子区域。

3. **Endpoint Agent 证书**部分显示 TLS 证书列表，其中包含每个证书的以下详细信息：

   - **TLS 证书**– 证书的指纹。
   - **序列号** – 证书的序列号。
   - **到期** – 证书的到期日期。

在 Kaspersky Anti Targeted Attack Platform 的 Web 界面中过滤和搜索 Endpoint Agent 组件的 TLS 证书

您可以按一列或两列筛选表中显示的 TLS 证书（**TLS 证书**和**序列号**）或输入搜索条件按这些列搜索 TLS 证书。

要筛选并搜索表中的 TLS 证书：

1. 使用管理员凭据登录 Kaspersky Anti Targeted Attack PlatformWeb 界面。
2. 在 Kaspersky Anti Targeted Attack Platform Web 界面窗口中，选择**设置**部分的**证书**子区域。
3. **Endpoint Agent 证书**部分显示 TLS 证书列表，其中包含每个证书的以下详细信息：

   - **TLS 证书**– 证书的指纹。
   - **序列号** – 证书的序列号。
   - **到期** – 证书的到期日期。

4. 如果您想通过证书指纹筛选或搜索 TLS 证书：

   a. 单击**TLS 证书**链接打开筛选配置窗口。

   b. 在**TLS 证书**文本框中输入证书指纹的几个字符。

   c. 单击**应用**。

5. 如果您想按序列号筛选或搜索 TLS 证书：

   a. 单击**序列号**链接打开筛选配置窗口。

   b. 在**序列号**文本框中输入序列号的几个字符。

   c. 单击**应用**。

该表仅显示与您设置的筛选条件匹配的 TLS 证书。

要清除一个或多个筛选条件的筛选器：

单击您想清除其筛选条件的表列标题右侧的。

如果要清除多个筛选条件，请执行必要的操作以清除每个筛选条件。

选定筛选器将被清除。

在 Kaspersky Anti Targeted Attack Platform 的 Web 界面中删除 Endpoint Agent 组件的 TLS 证书

要使用 Kaspersky Anti Targeted Attack Platform Web 界面删除用于与在 Endpoint Agent 组件角色中使用的应用程序连接的一个或多个 TLS 证书，请执行以下操作：

1. 使用管理员凭据登录 Kaspersky Anti Targeted Attack Platform Web 界面。
2. 在 Kaspersky Anti Targeted Attack Platform Web 界面窗口中，选择**设置**部分的**Endpoint Agent 证书**子区域。
   Endpoint Agent 证书部分显示 TLS 证书列表。
3. 选择要删除的一个或多个 TLS 证书旁边的复选框。
4. 单击**删除**。
   这将打开操作确认窗口。
5. 单击**是**。

选定的 TLS 证书将被删除。

配置从 Endpoint Agent 组件到 Sensor 服务器的流量重定向

您可以将 Sensor 服务器用作代理服务器以在 Endpoint Agent 组件和 Central Node 之间进行通信，以减轻 Central Node 的负担。为此，在连接充当 Endpoint Agent 组件的应用程序时，在该应用程序端，需要指定 Sensor 服务器的 IP 地址，而不是 Central Node 服务器的 IP 地址。Sensor 必须安装在与 Central Node 不同的服务器上。

配置流量重定向时，请记住以下限制：

- Sensor 的最大传入流量不得超过 1 Gbps。
- Central Node 和 Sensor 服务器之间的推荐通道带宽必须是 SPAN 端口流量的 15%。
- Sensor 服务器和 Central Node 之间允许的最大数据包丢失率为 10%，数据包延迟最多为 100 毫秒。

要将 Sensor 用作代理服务器，请将 Sensor 连接到 Central Node。

配置 Endpoint Agent 组件与 NDR 功能块的集成

如果您使用 NDR 功能，您可以配置 Kaspersky Anti Targeted Attack Platform 与 Kaspersky Endpoint Security 12.7 for Windows 和 Kaspersky Endpoint Security 12.2 Linux 所代表的 Endpoint Agent 组件的集成，以接收有关安装该组件的设备的以下信息：

- 由于 EPP 技术触发而记录在事件数据库中的有关 NDR 事件的信息（工作站和服务器保护事件）。
- 设备信息（例如，操作系统版本、型号或供应商信息）。
- 有关网络交互图上设备连接的信息。
- 有关用于建立设备间连接的协议的信息。

> 您可以将最多 1000 个 Endpoint Agent 组件连接到单个 Central Node 组件。

要集成 NDR 功能，必须使用 *KESB Advanced* 或 *KESB Total* 授权许可密钥激活 Kaspersky Endpoint Security 12.7 for Windows 或 Kaspersky Endpoint Security 12.2 Linux。

安装了 Endpoint Agent 组件的计算机的数据通过*集成服务器*发送到 Kaspersky Anti Targeted Attack Platform。任何安装了 Kaspersky Anti Targeted Attack Platform 组件（Central Node 或 Sensor）的服务器都可以作为集成服务器。为了与 Endpoint Agent 集成，请将集成服务器添加到从具有 Endpoint Agent 的计算机接收数据的服务器。

托管 Endpoint Agent 的计算机通过 HTTPS 协议与集成服务器建立安全连接。连接由 Central Node 服务器颁发的证书保护。以下证书可用于连接：

- 集成服务器证书。每次建立连接时，Endpoint Agent 计算机都会验证此证书。直到证书验证成功后才建立连接。
- 客户端证书。此证书用于对具有 Endpoint Agent 的计算机集成服务器客户端进行身份验证。同一个客户端证书可以被多台装有 Endpoint Agent 的计算机使用。默认情况下，集成服务器不会验证客户端证书，但您可以启用验证以提高连接的安全性。

证书和公钥使用 Kaspersky Endpoint Security for Windows 或 Kaspersky Endpoint Security for Linux 分发给 Endpoint Agent 计算机。要将这些数据上传到 Kaspersky Endpoint Security，您可以使用通信数据包，该数据包必须在添加集成服务器后在 Kaspersky Anti Targeted Attack Platform 中创建。

只有具有**管理员**角色的用户才能配置来自 Endpoint Agent 组件的数据接收。具有**安全审计员**角色的用户可以查看集成服务器列表。

集成服务器表

集成服务器表显示在“**设置**”部分，“**连接服务器**”子部分中，“**集成服务器**”选项卡上。该表显示已在安装了应用程序组件的服务器上添加的集成服务器的信息。

集成服务器我表包含以下信息：

- **节点名称** – 安装了应用程序组件的服务器的名称。
- **IP 地址** – Kaspersky Anti Targeted Attack Platform 组件服务器所有网络接口上的 IP 地址列表（未为集成服务器配置特定网络接口和 IP 地址，因为计算机的任何可用网络接口和 IP 地址都可用于到集成服务器的外部连接）。
- **每秒请求数** – 从客户端到集成服务器的成功处理请求的平均数量。
- **状态** – 集成服务器的当前状态。
- **验证客户端证书** – 指示是否启用或禁用客户端证书验证（如果禁用验证，则表单元格为空）。

准备从 Endpoint Agent 组件接收数据的场景

准备从 Endpoint Agent 组件接收数据的场景涉及以下步骤：

1. **在受控制网络的计算机上安装 Endpoint Agent 组件**

   在此步骤中，您必须在想要在 Kaspersky Anti Targeted Attack Platform 中接收信息的所有计算机上安装 Kaspersky Endpoint Security for Windows 或 Kaspersky Endpoint Security for Linux （作为 Endpoint Agent 组件）。这些计算机必须与装有 Sensor 组件的其中一台服务器位于同一网络上。

   > Kaspersky Anti Targeted Attack Platform 的当前版本仅在与 Kaspersky Endpoint Security for Windows 12.7 及更高版本或 Kaspersky Endpoint Security for Linux 12.2 及更高版本集成时支持接收和处理数据。

2. **为 Kaspersky Anti Targeted Attack Platform 组件添加集成服务器**

   此阶段涉及完成将集成服务器添加到 Endpoint Agent 组件将连接到的服务器的过程。服务器与 Endpoint Agent 组件之间的网络交互仅可通过未用作监控点的网络接口来实现。没有为集成服务器配置特定的网络接口和 IP 地址，因为计算机的任何可用网络接口和 IP 地址都可以用于与集成服务器的外部连接。

3. **为集成服务器的客户端创建通信数据包**

   在此阶段，您必须创建和下载通信数据包，应用程序在其中存储用于将客户端连接到集成服务器的证书和密钥。每个通信数据包都是一个包含以下数据的存档：

   - 集成服务器证书的公钥。
   - 集成服务器的客户端证书（带有私钥）。如果集成服务器上启用了客户端证书验证，则会添加此证书。证书和密钥使用创建通信数据包时指定的密码加密。

4. **将连接集成服务器的数据上传到客户端计算机**

   我们建议使用 Kaspersky Security Center 来执行此操作。对于 Kaspersky Anti Targeted Attack Platform 集成服务器，客户端是装有 Endpoint Agent 组件的计算机。使用 Endpoint Agent 管理插件将通信数据包中的证书和/或密钥上传到 Kaspersky Security Center 管理服务器。然后，在 Kaspersky Security Center 中创建策略，以便将数据上传到 Endpoint Agent 计算机。有关管理数据和创建策略的信息，请参阅 Kaspersky Endpoint Security for Windows 和 Kaspersky Endpoint Security for Linux 的文档。

对于每个集成服务器，必须创建至少一条策略，其中包含要上传到客户端计算机的以下数据：

- 集成服务器证书的公钥。
- 用于连接集成服务器的 IP 地址。您可以指定集成服务器节点的任意可用 IP 地址。您可以在 Web 界面的“**设置**”部分，“**连接服务器**”子部分中，“**集成服务器**”选项卡上查看 IP 地址。默认情况下，使用端口 8070 进行连接。
- 集成服务器的客户端证书（带有私钥）。如果集成服务器上启用了客户端证书验证，则会添加此证书。

5. **启用集成服务器**

   应用策略并将数据上传到带有 Endpoint Agent 组件的计算机后，此阶段即完成。在此阶段，您需要启用所有要向其发送 EPP 应用程序数据的集成服务器。

该场景的结果是，Kaspersky Anti Targeted Attack Platform 开始接收和处理来自 EPP 应用程序的数据。

添加集成服务器

要添加集成服务器：

1. 使用应用程序管理员账户登录 Web 界面。
2. 选择应用程序 Web 界面窗口中“**设置**”部分的“**连接服务器**”子部分。
3. 在“**集成服务器**”选项卡上，单击“**添加 Endpoint Agent 集成服务器**”按钮。
4. 在“**节点**”下拉列表中，选择要向其中添加集成服务器的已安装 Central Node 或 Sensor 组件的服务器。

   您只能选择尚未添加集成服务器的节点。
5. 如有必要，请使用“**验证客户端证书**”切换开关启用客户端身份验证的证书验证。
6. 如果您启用了客户端证书验证，请为集成服务器客户端创建一个或多个证书。要创建证书，请单击“**创建新证书**”。如有必要，您可以单击包含证书指纹的字段右侧的 图标从列表中删除不必要的证书。

   若您创建了多个客户端证书，您可以在创建通讯数据包时选择证书。
7. 单击“**保存**”。

集成服务器已添加。

为集成服务器的客户端创建通信数据包

添加集成服务器或更改其设置后，您需要为该服务器的客户端创建并下载通信数据包。

要为集成服务器的客户端创建新的通信数据包：

1. 使用应用程序管理员账户登录 Web 界面。
2. 选择应用程序 Web 界面窗口中“**设置**”部分的“**连接服务器**”子部分。

3. 在“**集成服务器**”选项卡上，选择要为其客户端创建新的通信数据包的服务器。
   详细信息区域显示在 Web 界面窗口的右侧。

4. 单击“**获取客户端的通信数据包**”。

5. 如果为集成服务器启用了客户端证书验证，则会显示“**生成新的通信数据包**”窗口。执行以下操作：

   a. 在“**客户端证书**”下拉列表中，选择用于集成服务器客户端身份验证的相关证书。

   b. 指定所选证书的访问密码。指定的密码用于加密连接器通信数据包中的证书。

   c. 单击“**创建通信数据包**”。

Central Node 为所选集成服务器的客户端生成新的通信数据包，然后浏览器保存下载的文件。根据您的浏览器的设置，屏幕上可能会显示一个窗口，您可以在其中指定下载文件的路径和名称。

您需要将通信数据包的内容上传到集成服务器客户端计算机。您可以使用 Kaspersky Security Center 管理服务器策略上传它。在 Kaspersky Security Center 策略中，指定用于连接到集成服务器的 IP 地址（您可以使用所选集成服务器的详细信息区域中列出的可用 IP 地址之一）。有关创建和配置 Kaspersky Security Center 策略的更多详细信息，请参阅 Kaspersky Endpoint Security for Windows 或 Kaspersky Endpoint Security for Linux 的文档。

启用或禁用集成服务器

可以启用或禁用集成服务器。默认情况下，创建后，集成服务器被禁用，因此 Kaspersky Anti Targeted Attack Platform 不会处理来自其客户端的数据。

要启用或禁用集成服务器：

1. 使用应用程序管理员账户登录 Web 界面。

2. 选择应用程序 Web 界面窗口中“**设置**”部分的“**连接服务器**”子部分。

3. 在“**集成服务器**”选项卡上，选择要启用或禁用的服务器。
   详细信息区域显示在 Web 界面窗口的右侧。

4. 单击“**启用**”或“**禁用**”。

服务器被启用或禁用。

编辑集成服务器设置

编辑集成服务器设置时，您可以替换集成服务器本身的证书、启用或禁用客户端证书验证以及更改客户端的证书列表。

要编辑集成服务器设置：

1. 使用应用程序管理员账户登录 Web 界面。

2. 选择应用程序 Web 界面窗口中“**设置**”部分的“**连接服务器**”子部分。

3. 在“**集成服务器**”选项卡上，选择要更改其客户端设置的服务器。
   详细信息区域显示在 Web 界面窗口的右侧。
4. 在工具栏上，单击“**编辑**”按钮。
5. 如果要替换集成服务器自身的证书（颁发新证书），请点击“**重新颁发证书**”。

   更换集成服务器证书会导致旧证书无效。

6. 如果要启用或禁用客户端身份验证的证书验证，请使用“**验证客户端证书**”切换开关。
7. 如果启用了客户端证书验证并且您想要修改客户端的证书列表，请单击“**创建新证书**”和/或包含证书指纹的字段的右侧的 × 图标。
8. 单击**“保存”**。

集成服务器设置已修改。

如果您为集成服务器颁发了新证书或生成了新的客户端证书，则需要重新创建并下载通信数据包，以将这些证书的信息传播到客户端计算机。

删除集成服务器

要删除集成服务器：

1. 使用应用程序管理员账户登录 Web 界面。
2. 选择应用程序 Web 界面窗口中“**设置**”部分的“**连接服务器**”子部分。
3. 在“**集成服务器**”选项卡上，选择要删除的服务器。
   详细信息区域显示在 Web 界面窗口的右侧。
4. 单击“**删除**”。
   这将打开一个确认提示窗口。
5. 在提示窗口中，单击“**确定**”。

集成服务器被删除。

应用程序使用入门

本节包含有关如何在 Web 界面、管理员菜单以及技术支持模式下开始管理应用程序的信息。

使用管理员账户开始使用应用程序 Web 界面

仅当用于管理应用程序 Web 界面的浏览器提供 HTTP POST 请求的 Referrer 标头时，Kaspersky Anti Targeted Attack Platform 的 Web 界面才受保护免受 **CSRF 攻击**并运行。确保用于使用 Kaspersky Anti Targeted Attack Platform 的 Web 界面的浏览器不会修改 HTTP POST 请求的 Referrer 头信息。如果与 Kaspersky Anti Targeted Attack Platform 的 Web 界面的连接是通过组织的代理服务器建立的，请确保代理服务器不会修改 HTTP POST 请求的 Referrer 头信息。

跨站请求伪造（也称为“XSRF 攻击”）。利用 HTTP 协议的漏洞攻击网站用户。这种攻击使得黑客能够打着授权用户的幌子在易受攻击的网站中执行操作。例如，在易受攻击的网站中，黑客可以打着授权用户的幌子秘密地向外部支付系统的服务器发送请求，以便将资金转移到黑客的账户。

安装 Kaspersky Anti Targeted Attack Platform 后，您必须管理应用程序的大小设置。

如果未配置 Kaspersky Anti Targeted Attack Platform 的大小设置，则无法登录应用程序 Web 界面。

要使用管理员账户开始使用应用程序 Web 界面：

1. 在任何一台允许访问 Central Node 服务器的计算机的浏览器中，将具有 Central Node 组件的服务器的 IP 地址输入地址栏中。

   如果您使用的是应用程序的高可用性版本，则可以输入 Central Node 集群的任何服务器的 IP 地址或**集群的完全限定域名 (FQDN)**。

   为了保证程序 Web 界面的访问不间断，可以在DNS 服务器上配置轮询调度算法功能。为此，请登录 Central Node 集群的第一台正常服务器的 Web 界面。

   Kaspersky Anti Targeted Attack Platform 用户的账户凭证输入窗口打开。

2. 输入用户名“admin”以及部署 Central Node 组件时设置的密码。

3. 单击**登录**。

   应用程序 Web 界面的**控制板**页面将显示。

您可以通过管理员账户开始使用应用程序。

对于每个用户账户，同时进行的应用程序管理会话的数量限于一个 IP 地址。如果使用相同的用户名从不同的 IP 地址登录应用程序，则先前的会话将终止。

应用程序管理员菜单使用入门

您可以在安装应用程序组件的每台服务器的管理控制台的管理员菜单中管理每个应用程序的 Sensor、Central Node 和 Sandbox 组件的设置。

确保只能从您授予此类访问权限的计算机访问 Kaspersky Anti Targeted Attack Platform 管理员菜单和服务器管理控制台。

确保您授予访问权限的计算机位于网络的安全范围内。

您可以使用 iptables 命令行实用程序配置从某些计算机对 Kaspersky Anti Targeted Attack Platform 管理员菜单和服务器管理控制台的访问。有关管理 iptables 的详细信息，请参阅 iptables 文档。

要在托管所需组件的服务器管理中的 Sandbox、Sensor 或 Central Node 组件管理员菜单中开始工作，请执行以下操作：

1. 登录到要通过 SSH 协议或终端更改其设置的服务器的管理控制台。

   显示应用程序组件管理员菜单。

2. 系统提示时，请输入管理员用户名和安装应用程序期间设置的密码。

   显示应用程序组件管理员菜单。

您可以开始使用 Sensor 或 Sandbox 组件管理员菜单。

在技术支持模式下开始使用应用程序

技术支持模式下任何未经技术支持人员批准和/或不建议的操作都是被禁止的，并且是撤销技术支持的理由。

您可以在技术支持模式下管理应用程序的 Sensor、Central Node 和 Sandbox 组件。

技术支持模式为 Kaspersky Anti Targeted Attack Platform 管理员提供对应用程序及其所有存储数据（包括个人信息）的无限制访问权限（根）。

在具有超级用户账户权限的技术支持模式下从管理控制台使用 Kaspersky Anti Targeted Attack Platform，您可以：

- 使用配置文件管理应用程序操作设置。

  在应用程序节点间传输数据时，您还可以修改数据加密的设置，以及用于存储和处理被扫描对象的设置。

在这种情况下，数据以未加密的形式传输。Kaspersky Anti Targeted Attack Platform 管理员必须独立使用这些数据来确保服务器受到保护。Kaspersky Anti Targeted Attack Platform 管理员负责修改应用程序的配置文件。

- 管理跟踪日志设置。

跟踪文件可能包含用户的机密数据。此类文件将无限期保留，并且可以由 Kaspersky Anti Targeted Attack Platform 的管理员手动删除。跟踪文件的路径由 Kaspersky Anti Targeted Attack Platform 的管理员指定。

要开始在技术支持模式下使用 Sandbox、Sensor 或 Central Node 组件：

1. 登录到要通过 SSH 协议或终端更改其设置的服务器的管理控制台。
2. 系统提示时，请输入管理员用户名和安装组件期间指定的密码。
   显示应用程序组件管理员菜单。
3. 在应用程序管理员菜单中，选择**技术支持模式**。
4. 按 **ENTER** 键。
   这将打开技术支持模式确认窗口。
5. 确认您想要在技术支持模式下管理应用程序。为此，请选择**是**并按 **ENTER**。

您可以继续在技术支持模式下管理 Central Node、Sensor 或 Sandbox 组件。

管理应用程序管理员和用户的账户

Kaspersky Anti Targeted Attack Platform 为具有以下组件的服务器提供账户：

- Sensor。用于管理组件 Web 界面、管理员菜单和服务器管理控制台（技术支持模式下）的管理员账户。默认情况下使用在组件安装期间创建的“admin”账户。
- Sandbox。用于管理组件 Web 界面、管理员菜单和服务器管理控制台（技术支持模式下）的管理员账户。默认情况下使用在组件安装期间创建的“admin”账户。
- Central Node。以下账户：
  - 用于在应用程序管理员菜单和服务器管理控制台（在技术支持模式下）中工作的管理员账户。默认情况下使用在组件安装期间创建的“admin”账户。
  - 应用程序 Web 界面的管理员账户。
  - 具有**安全审计员**、**安全官**和 **高级安全官**角色的应用程序 Web 界面用户账户。

来自于每个此类账户的数据被储存在托管该账户所属的应用程序组件的服务器上。

在分布式解决方案和多租户模式中，来自每个账户的数据都存储在 PCN 上以及托管该账户所属的应用程序组件的服务器上。

用于在服务器管理控制台中工作的管理员账户拥有无限权限来管理托管该账户所属的应用程序组件的服务器（超级用户权限）。在此账户下，您可以关闭或重启服务器，或在服务器管理控制台中修改应用程序在技术支持模式下的设置。

在服务器（管理员）的管理控制台中工作的管理员账户可以无限制地访问该服务器上的数据。用于在服务器管理控制台中工作的管理员账户的密码必须是强密码。管理员必须采取步骤确保服务器的安全。管理员具有访问储存在服务器上的数据的责任。

您可以使用“**管理员**”角色的账户来管理应用程序用户账户以及应用程序 Web 界面管理员可用的应用程序设置。在分布式解决方案和多租户模式下，用户账户在 PCN 上进行管理。

一个具有“**安全审计员**”角色的账户可以查看管理员和安全官可用的 Web 界面的所有部分。具有**安全审计员**角色的用户可以查看数据，但不能编辑该数据。

“**高级安全官**”和“**安全官**”角色专供组织的员工使用，这些员工的工作涉及管理 Kaspersky Anti Targeted Attack Platform 的事件、警报和任务，以及管理响应操作。在具有这些角色的账户下登录应用程序时，您可以看到安全官可以使用的应用程序 Web 界面的所有部分。具有**高级安全官**角色的用户有权访问所有操作。对具有**安全官**角色的用户的限制如下表所示。

具有**安全官**角色的应用程序用户的访问限制

功能范围/Web 界面部分	限制
控制板	VIP 组事件的小组件不可用。 无法使用小组件上的链接转到"**警报**"部分。
警报	如下操作不可用: • 查看警报详细信息。 • 标记 VIP 组警报处理的完成。 • 对多个警报执行操作。 • 导出所有警报的列表。
资产: **设备**	设备分组不可用。
资产: Endpoint Agent	查看 Endpoint Agent 工作站表的权限；查看任务、策略和网络隔离详细信息的限制。
网络流量事件	无法执行与 VIP 组警报相关的事件的操作。
威胁搜索	如下操作不可用: • 从 VIP 组的警报中查看与工作站相关的事件 • 根据事件搜索条件创建 TAA (IOA) 规则
任务	无法访问。
防护规则	无法访问。
自定义规则: IOC	读取。
自定义规则: YARA	仅能访问以导出规则。
自定义规则: TAA	读取。
用户定义的 Sandbox 规则和入侵检测规则	无法访问。
日志	无法访问应用程序 Web 界面中的审计日志和用户活动日志。
存储	无法访问由于任务而被放置在存储中的对象。 完全访问用户手动下载的对象。
隔离	无法访问。
报告	无法访问。
设置	如下操作不可用: • 创建警报通知规则（完全访问发送有关应用程序遇到的问题的通知的规则） • 管理 Kaspersky TAA (IOA) 规则的排除项和扫描（读取访问）排除项 无法访问以下功能: • 管理 Endpoint Agent • 本地 KPSN 信誉数据库连接设置 • 为警报分配 VIP 状态的规则 • 允许规则 • Sandbox 连接设置 • 扫描 Sandbox 中的对象时要使用的操作系统设置 • 存档密码

如果您使用分布式解决方案和多租户模式，则可以允许或拒绝每个账户对租户和 SCN 服务器的 Web 界面的访问。

创建用于应用程序 Web 界面的管理员账户

要创建应用程序管理员账户:

1. 使用应用程序管理员账户登录 Web 界面。
2. 在应用程序 Web 界面窗口中，选择**设置**部分的**用户**子部分。
3. 单击**添加**。
   这将打开**新用户**窗口。

4. 要启用账户，请打开**状态**切换开关。
   默认情况下，该账户已启用。

   如果启用了用户账户，则允许用户访问应用程序 Web 界面。如果用户账户被禁用，则禁止用户访问应用程序 Web 界面。

5. 在**角色**下拉列表中，选择**管理员**。

6. 在**身份验证类型**下面，选择以下选项之一：

   - KATA **用户账户**。
     在这种情况下，若要连接到应用程序 Web 界面，用户必须输入创建账户时配置的用户名和密码。
   - **域用户账户**。
     在这种情况下，若要连接到应用程序 Web 界面，用户不必输入用户名和密码；用户将通过域账户进行身份验证。

   如果配置了 Active Directory 集成，则KATA **用户账户**和**域用户账户**字段可用。

7. 如果您选择了KATA **用户账户**：

   a. 在**用户名称**字段中，输入要创建的账户的用户名。
      用户名必须满足以下要求：

      - 在用户名列表中必须是唯一的（区分大小写）。
      - 必须包含不超过 32 个字符。
      - 可以包含字母 A–Z、a–z、数字 0–9、连字符 (-) 和下划线 (_)。
      - 必须以字母（A-Z 或 a-z）开头。

   b. 在**新密码**字段中，输入将要用于访问 Web 界面的用户密码。
      密码必须满足以下要求：

      - 不能与用户名相同。
      - 不得包含字典单词、常用字母组合或键盘布局示例（例如 Qwerty 或 passw0rd）。
      - 必须包含至少 8 个字符。
      - 必须包含至少三种字符：
        - 大写字母 (A-Z)。
        - 小写字母 (a-z)。

- 数字。
- 特殊字符。

c. 在**确认密码**字段中，再次输入将要用于访问 Web 界面的用户密码。

8. 如果您选择了**域用户账户**， 在**用户名称**字段中输入用户的域名。
9. 单击**添加**。

应用程序管理员账户已创建。

如果您使用分布式解决方案和多租户模式，则 PCN 服务器的管理员账户可以访问与该服务器关联的所有组织的数据。

创建用于应用程序 Web 界面的用户账户

您可以创建具有**高级安全官**、**安全官**和**安全审计员**角色的用户账户。

要为应用程序 Web 界面创建用户账户：

1. 使用应用程序管理员账户登录 Web 界面。
2. 在应用程序 Web 界面窗口中，选择**设置**部分的**用户**子部分。
3. 单击**添加**。

   这将打开**新用户**窗口。
4. 如有必要，请使用**状态**切换开关禁用用户账户。

   默认情况下，该账户已启用。

   如果启用了用户账户，则允许用户访问应用程序 Web 界面。如果用户账户被禁用，则禁止用户访问应用程序 Web 界面。
5. 在**身份验证类型**下面，选择以下选项之一：

   - KATA **用户账户**。

     在这种情况下，若要连接到应用程序 Web 界面，用户必须输入创建账户时配置的用户名和密码。
   - **域用户账户**。

     在这种情况下，若要连接到应用程序 Web 界面，用户不必输入用户名和密码；用户将通过域账户进行身份验证。

     如果您选择了**域用户账户**身份验证类型，请注意，用户将无法使用不同的用户账户登录应用程序 Web 界面。

   如果配置了 Active Directory 集成，则KATA **用户账户**和**域用户账户**字段可用。

6. 在**角色**下拉列表中，选择以下角色之一：

   - **高级安全官。**
   - **安全官**。
   - **安全审计员。**

7. 如果您选择KATA **用户账户**：

   a. 在**用户名称**字段中，输入要创建的账户的用户名。
   用户名必须满足以下要求：

      - 在用户名列表中必须是唯一的（区分大小写）。
      - 必须包含不超过 32 个字符。
      - 可以包含字母 A–Z、a–z、数字 0–9、连字符 (-) 和下划线 (_)。
      - 必须以字母（A-Z 或 a-z）开头。

   b. 在**新密码**字段中，输入将要用于访问 Web 界面的用户密码。
   密码必须满足以下要求：

      - 不能与用户名相同。
      - 不得包含字典单词、常用字母组合或键盘布局示例（例如 Qwerty 或 passw0rd）。
      - 必须包含至少 8 个字符。
      - 必须包含至少三种字符：
         - 大写字母 (A-Z)。
         - 小写字母 (a-z)。
         - 数字。
         - 特殊字符。

   c. 在**确认密码**字段中，再次输入将要用于访问 Web 界面的用户密码。

8. 如果您选择了**域用户账户**， 在**用户名称**字段中输入用户的域名。

9. 在**访问**部分，配置访问权限：

   a. 打开**SCN Web 界面**切换开关可让用户不仅访问该 PCN 服务器的 Web 界面，还可以访问所有可用 SCN 服务器的 Web 界面。

   b. 在**租户**设置标题右侧，选择您要授予其 Web 界面访问权限的一个或多个租户的复选框。
   您可以使用**全选**和**全部清除**链接选择或取消选择所有租户。

10. 单击**添加**。

配置用户账户表显示

您可以显示或隐藏列以及更改应用程序 Web 界面用户账户表中列的顺序。

要配置应用程序 Web 界面用户账户表的显示：

1. 使用应用程序管理员账户登录 Web 界面。
2. 在应用程序 Web 界面窗口中，选择**设置**部分的**用户**子部分。
3. 在表格的标题部分，单击 。
   这将打开**定制表格**窗口。
4. 如果要在表中显示列，请选择要在表中显示的参数名称旁边的复选框。
   如果要隐藏表中的参数，请清除该复选框。

   > 必须选择至少一个复选框。

5. 如果要更改表格中列的顺序，请将鼠标光标移动到具有相关参数的行，单击 并将该行移动到新位置。
6. 如果要恢复默认表格显示设置，请单击**默认**。
7. 单击**应用**。

用户账户表显示得到配置。

查看用户账户表

用户账户表显示在应用程序 Web 界面窗口的“**设置**”部分，“**用户**”子部分。您可以按**用户名称**、**角色**、**租户**和**状态**列对表中的事件进行排序。

表包含以下信息：

1. **用户名称**是创建账户时配置的用户名。
2. **身份验证类型**是用户的身份验证类型。可能值：
   - KATA **用户账户**。
     如果选择此身份验证类型，若要连接到应用程序 Web 界面，用户必须输入创建账户时配置的用户名和密码。
   - **域用户账户**。
     如果选择此身份验证类型，则连接到应用程序 Web 界面时，用户无需输入用户名和密码；用户通过域账户进行身份验证。
3. **角色**是分配给用户的角色。

4. **租户**是用户有权访问的租户列表。
   该列仅在分布式解决方案和多租户模式下显示。

5. **状态**是账户的状态。可以有以下值：

   - **已启用。**
     如果启用了用户账户，则允许用户访问应用程序 Web 界面。
   - **已禁用。**
     如果用户账户被禁用，则禁止用户访问应用程序 Web 界面。

筛选用户账户

要按所需条件筛选或搜索用户账户：

1. 使用应用程序管理员账户登录 Web 界面。
2. 在应用程序 Web 界面窗口中，选择**设置**部分的**用户**子部分。
3. 根据筛选条件，执行以下操作：

   - **按用户名**

     a. 单击**用户名称**链接以打开筛选菜单。

     b. 在下拉列表中，选择以下筛选运算符之一：

     - **包含**
     - **不包含**

     c. 在文本框中，键入用户名或用户名中的字符序列。

     d. 单击**应用**。

   - **按身份验证类型**

     a. 单击**身份验证类型**链接以打开筛选菜单。

     b. 选择要包含在筛选条件中的账户旁边的复选框：

     - KATA **用户账户**。
     - **域用户账户**。

     c. 单击**应用**。

- **按角色**

  a. 单击**角色**链接以打开筛选菜单。

  b. 选择与要添加到筛选条件的角色对应的复选框。

  - **管理员**。
  - **高级安全官**。
  - **安全官**。
  - **安全审计员**。

  您可以选择多个复选框。

  c. 单击**应用**。

- **按用户有权访问的租户名称**

  a. 单击**租户**链接以打开筛选菜单。

  b. 选择与要添加到筛选条件的租户相对应的复选框。
  您可以选择多个复选框。

  c. 单击**应用**。

- **按状态**

  a. 单击**状态**展开筛选器设置列表。

  b. 选择以下选项之一：

  - **所有。**
  - **已启用。**
  - **已禁用。**

该表显示与配置的筛选条件相对应的账户。

> 您可以同时使用多个筛选器。

清除账户筛选器

要按一个或多个过滤条件清除用户账户过滤器：

1. 使用应用程序管理员账户登录 Web 界面。
2. 在应用程序 Web 界面窗口中，选择**设置**部分的**用户**子部分。

3. 单击您想清除其过滤条件的用户账户表列标题右侧的 。

> 如果要清除多个筛选条件，请执行必要的操作以清除每个筛选条件。

选定筛选器将被清除。

该表仅显示与指定条件匹配的用户账户。

更改用户账户对 PCN 和 SCN 数据的访问权限

如果您正使用分布式解决方案和多租户模式，您可以更改具有**高级安全官**和**安全官**角色的用户对 PCN 和 SCN 服务器数据的访问权限以及对这些服务器所属的租户的访问权限。

要更改应用程序 Web 界面用户账户的访问权限，请在 PCN 的 Web 界面中执行以下操作：

1. 使用应用程序管理员账户登录 Web 界面。
2. 在应用程序 Web 界面窗口中，选择**设置**部分的**用户**子部分。
3. 选择您要更改其访问权限的账户。
   这将打开**编辑用户账户**窗口。
4. 如果您想启用或禁用账户，请移动**状态**切换开关。
5. 必要时在**访问**部分移动**SCN Web 界面**切换开关：
   - 如果您想要授权用户除了此 PCN 服务器的 Web 界面之外还可以访问所有可用 SCN 服务器的 Web 界面，请将切换开关设为**已启用**。
   - 如果您只想授权用户访问此 PCN 服务器的 Web 界面，请将切换开关设为**已禁用**。
6. 在**租户**设置名称的右侧，选择或清除要为其更改服务器 Web 界面访问权限的一个或多个租户的复选框。
   您可以使用**全选**和**全部清除**链接选择或取消选择所有租户。
7. 单击**保存**。

账户的访问权限已更改。

启用或禁用用户账户

如果您正使用分布式解决方案和多租户模式，请在 PCN 的 Web 界面中执行以下步骤。用户账户状态管理在 SCN 的 Web 界面中不可用。

要启用或禁用用户账户：

1. 使用应用程序管理员账户登录 Web 界面。
2. 在应用程序 Web 界面窗口中，选择**设置**部分的**用户**子部分。
3. 在账户列表中，选择要启用或禁用的用户账户。
4. 在**状态**列中，执行以下操作之一：
   - 如果您想启用用户账户，将用户账户名称旁边的切换开关设置为“**已启用**”。
   - 如果您想禁用用户账户，将用户账户名称旁边的切换开关设置为“**已禁用**”。

   操作确认窗口将显示。
5. 单击**是**。

账户的状态已修改。

管理员账户无法被禁用。

更改应用程序管理员或用户账户的密码

仅具有KATA **用户账户**身份验证类型的用户可以更改其用户账户的密码。

要更改应用程序管理员账户或用户账户的密码，请在 PCN 的 Web 界面中执行以下操作：

1. 使用应用程序管理员账户登录 Web 界面。
2. 在应用程序 Web 界面窗口中，选择**设置**部分的**用户**子部分。在账户列表中，选择要更改其密码的用户账户。这将打开**编辑用户账户**窗口。
3. 在**新密码**字段中，输入程序 Web 界面的新密码。
   密码必须满足以下要求：
   - 不能与用户名相同。
   - 不得包含字典单词、常用字母组合或键盘布局示例（例如 Qwerty 或 passw0rd）。
   - 必须包含至少 8 个字符。
   - 必须包含至少三种字符：
     - 大写字母 (A-Z)。
     - 小写字母 (a-z)。

- 数字。
- 特殊字符。

4. 在**确认密码**字段中，再次输入新密码。
5. 单击**保存**。

应用程序管理员账户或用户账户的密码被更改。

修改您账户的密码

仅具有KATA **用户账户**身份验证类型的用户可以更改其用户账户的密码。

要修改您的用户账户的密码：

1. 利用您的账户登录程序 Web 界面。
2. 在程序 Web 界面窗口的下部，单击包含您帐户名称的链接以展开操作列表。
3. 选择**更改密码**操作。
   这将打开**更改密码**窗口。
4. 在**旧密码**字段中，输入应用程序 Web 界面的当前密码。
5. 在**新密码**字段中，输入程序 Web 界面的新密码。
   密码必须满足以下要求：
   - 不能与用户名相同。
   - 不得包含字典单词、常用字母组合或键盘布局示例（例如 Qwerty 或 passw0rd）。
   - 必须包含至少 8 个字符。
   - 必须包含至少三种字符：
     - 大写字母 (A-Z)。
     - 小写字母 (a-z)。
     - 数字。
     - 特殊字符。
6. 在**确认密码**字段中，再次输入新密码。
7. 单击**更改密码**。

用来访问应用程序 Web 界面的用户账号密码被更改。

使用域账户进行身份验证

如果配置了使用域账户的身份验证，则用户无需输入 Kaspersky Anti Targeted Attack Platform 账户凭据即可连接到应用程序 Web 界面。

要启用使用域账户进行身份验证：

1. 配置与 Active Directory 的集成。

   要设置 Active Directory 集成，您必须创建一个 keytab 文件，其中包含要为其设置集成的 Central Node 服务器的服务主体名称（以下也称为“SPN”）。

2. 选择创建账户时用户的**域用户账户**身份验证类型。

创建 keytab 文件

您可以创建一个用户账户以在多个 Central Node 服务器上进行身份验证。服务主体名称 (SPN) 为此，您必须创建一个keytab 文件，其中包含每个服务器的*服务主体名称（以下也称为 SPN）*。创建 keytab 文件时，必须使用属性来生成*salt*（哈希函数输入修饰符）。

> 生成的 salt 必须以任何方便的方式保存，以便将来向 keytab 文件添加更多 SPN。

您还可以为要为其设置 Kerberos 身份验证的每个 Central Node 服务器创建单独的 Active Directory 用户账户。

要使用一个用户账户创建 keytab 文件：

1. 在域控制器上的**Active Directory 用户和计算机**管理单元中，创建一个用户账户（例如，使用`control-user`作为其名称）。

2. 如果要使用 AES256-SHA1 加密算法，请在**Active Directory 用户和计算机**管理单元中：

   a. 打开您创建的用户账户的属性。

   b. 在**账户**选项卡上，选择**此账户支持 Kerberos AES 256 位加密**复选框。

3. 使用 ktpass 实用程序为控制用户创建 keytab 文件。为此，请在命令行中运行以下命令：

   `C:\Windows\system32\ktpass.exe -princ HTTP/<Central Node 服务器的完全限定域名 (FQDN)>@<大写的 Active Directory 域的领域名称> -mapuser control-user@<大写的 Active Directory 域的领域名称> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * +dumpsalt -out <文件路径>\<文件名>.keytab`

   该实用程序在执行命令时请求 `control-user` 密码。

   所选服务器的 SPN 将被添加到创建的 keytab 文件中。生成的盐显示在屏幕上：使用盐“<哈希值>”对密码进行哈希处理。

4. 将每个后续 Central Node 服务器的 SPN 记录添加到 keytab 文件中。为此，请运行以下命令：

C:\Windows\system32\ktpass.exe -princ HTTP/<Central Node 服务器的完全限定域名 (FQDN)>@<大写的 Active Directory 域的领域名称> -mapuser control-user@<大写的 Active Directory 域的领域名称> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in <先前创建的文件的路径和名称>.keytab -out <路径和新名称>.keytab -setupn -setpass -rawsalt "<在第 3 步创建keytab文件时获得的盐的哈希值>"

该实用程序在执行命令时请求 control-user 密码。

keytab 文件已创建。此文件包含所选服务器的所有添加的 SPN。

示例：

例如，您需要创建一个包含 3 个服务器的 SPN 名称的 keytab 文件：control-01.test.local、 secondary-01.test.local 和 secondary-02.test.local。

要在 C:\keytabs\ 中创建包含服务器的 SPN 的 filename1.keytab 文件，请运行以下命令：

```
C:\Windows\system32\ktpass.exe -princ HTTP/control-01.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * +dumpsalt -out C:\keytabs\filename1.keytab
```

假设您有“TEST.LOCALHTTPcontrol-01.test.local”作为盐。

要添加另一个 SPN，请运行以下命令：

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-01.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename1.keytab -out C:\keytabs\filename2.keytab -setupn -setpass -rawsalt "TEST.LOCALHTTPcontrol-01.test.local"
```

要添加第三个 SPN：

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-02.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename2.keytab -out C:\keytabs\filename3.keytab -setupn -setpass -rawsalt "TEST.LOCALHTTPcontrol-01.test.local"
```

这将创建一个 filename3.keytab 文件，其中包含所有三个添加的 SPN。

要使用每个 Central Node 服务器的单独账户创建 keytab 文件：

1. 在域控制器服务器上的**Active Directory 用户和计算机**管理单元中，为每台服务器创建单独的用户账户（例如，control-user、 secondary1-user、 secondary2-user等）。

2. 如果要使用 AES256-SHA1 加密算法，请在**Active Directory 用户和计算机**管理单元中：

   a. 打开您创建的用户账户的属性。

   b. 在**账户**选项卡上，选择**此账户支持 Kerberos AES 256 位加密**复选框。

3. 使用 ktpass 实用程序为控制用户创建 keytab 文件。为此，请在命令行中运行以下命令：

   C:\Windows\system32\ktpass.exe -princ HTTP/<Central Node 服务器的完全限定域名 (FQDN)>@<大写的 Active Directory 域的领域名称> -mapuser control-user@<大写的 Active Directory 域的领域名称> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -out <文件路径>\<文件名>.keytab

   该实用程序在执行命令时请求 control-user 密码。

   所选服务器的 SPN 将被添加到创建的 keytab 文件中。

4. 将每个后续 Central Node 服务器的 SPN 记录添加到 keytab 文件中。为此，请运行以下命令：

   C:\Windows\system32\ktpass.exe -princ HTTP/<Central Node 服务器的完全限定域名 (FQDN)>@<大写的 Active Directory 域的领域名称> -mapuser secondary1-user@<大写的 Active Directory 域的领域名称> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in <先前创建的文件的路径和名称>.keytab -out <路径和新名称>.keytab

   该实用程序在执行命令时请求 secondary1-user 密码。

keytab 文件已创建。此文件包含所选服务器的所有添加的 SPN。

示例：

例如，您需要创建一个包含 3 个服务器的 SPN 名称的 keytab 文件：`control-01.test.local`、`secondary-01.test.local` 和 `secondary-02.test.local`。

要在 C:\keytabs\ 中创建包含服务器的 SPN 的 `filename1.keytab` 文件，请运行以下命令：

```
C:\Windows\system32\ktpass.exe -princ HTTP/control-01.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -out C:\keytabs\filename1.keytab
```

要添加另一个 SPN，请运行以下命令：

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-01.test.local@TEST.LOCAL -mapuser secondary1-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename1.keytab -out C:\keytabs\filename2.keytab
```

要添加第三个 SPN：

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-02.test.local@TEST.LOCAL -mapuser secondary2-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename2.keytab -out C:\keytabs\filename3.keytab
```

这将创建一个`filename3.keytab`文件，其中包含所有三个添加的 SPN。

配置与 Active Directory 的集成

要配置与 Active Directory 的集成：

1. 使用应用程序管理员账户登录 Web 界面。
2. 在应用程序 Web 界面窗口中，选择**设置**部分的**用户**子部分。
3. 前往**Active Directory 集成**选项卡。
4. 如果您想要启用与 Active Directory 的集成，请选择**集成**复选框。
5. 单击**浏览**上传keytab 文件。
6. 选择 keytab 文件并单击**打开**。

   上传文件后，以下字段将显示：

   - Keytab 文件状态。可能值:
     - **文件包含该服务器的 SPN**表示上传的 keytab 文件包含该 Kaspersky Anti Targeted Attack Platform 服务器的 SPN。
     - **该服务器没有 SPN**表示上传的 keytab 文件不包含该 Kaspersky Anti Targeted Attack Platform 服务器的 SPN。
   - **文件内容**是文件包含的 SPN 列表。
7. 单击**应用**。

与 Active Directory 的集成已配置。

在分布式解决方案和多租户模式下，PCN 服务器上配置的 Active Directory 集成设置**不会**应用于连接到该 PCN 服务器的 SCN 服务器。如果要在单个 SCN 服务器上设置 Active Directory 集成，您必须在每个选定的 SCN 服务器上完成上述步骤。

禁用与 Active Directory 的集成

与 Active Directory 的集成被禁用时，无法使用域账户进行用户身份验证。

要禁用与 Active Directory 的集成：

1. 使用应用程序管理员账户登录 Web 界面。
2. 在应用程序 Web 界面窗口中，选择**设置**部分的**用户**子部分。
3. 前往**Active Directory 集成**选项卡。
4. 清除**集成**复选框。
5. 单击**应用**。

与 Active Directory 的集成已禁用。上传的 keytab 文件被永久删除。

在分布式解决方案和多租户模式下，PCN 服务器上配置的 Active Directory 集成设置**不会**应用于连接到该 PCN 服务器的 SCN 服务器。如果要在单个 SCN 服务器上禁用 Active Directory 集成，您必须在每个选定的 SCN 服务器上完成上述步骤。

参与卡巴斯基安全网络并使用卡巴斯基私有安全网络

为了更有效地保护用户的计算机，Kaspersky Anti Targeted Attack Platform 使用从全球用户获取的数据。*卡巴斯基安全网络* 旨在获取此类数据。

卡巴斯基安全网络（以下也称为“KSN”）是一个在线服务的基础架构，提供对卡巴斯基在线知识库的访问，该知识库中包含了有关文件信誉、网站资源和软件的信息。使用 Kaspersky Security Network 提供的数据可确保 Kaspersky Anti Targeted Attack Platform 更快地响应尚未添加到反病毒数据库的新对象，提高某些保护组件的性能，并降低误报的可能性。

感谢参与 Kaspersky Security Network 的用户，卡巴斯基能够及时接收有关尚未添加到反病毒数据库的对象的类型和来源的信息，开发抵御它们的解决方案，并最大限度地减少错误警报的数量。用户参与还可以帮助 Kaspersky Security Network 的其他用户及时收到有关其组织的 IT 基础架构威胁的信息。

当您参与 Kaspersky Security Network 时，Kaspersky Anti Targeted Attack Platform 会向 Kaspersky Security Network 发送有关文件，网络资源和软件声誉的请求，并会收到包含有关这些对象声誉的数据的响应。

用户的个人信息不会被收集、处理或存储。有关 Kaspersky Anti Targeted Attack Platform 发送到卡巴斯基安全网络的数据的信息，请参阅KSN 声明。

参与 Kaspersky Security Network 是自愿的。参与 Kaspersky Security Network 的决定是在安装 Kaspersky Anti Targeted Attack Platform 期间做出的，该决定可以随时更改。

如果您不想参与 KSN，可以使用卡巴斯基私人安全网络（以下也称为“KPSN”）。KPSN 是一个允许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，而不从他们自己的计算机实际发送数据到卡巴斯基安全网络的解决方案。

如果想购买卡巴斯基私人安全网络应用程序，您可以联系您所在地区的卡巴斯基合作伙伴。

参与 KSN 是在 Central Node 服务器上配置的，并被应用于所有连接的 Sensor 服务器。

如果您使用分布式解决方案和多租户模式，则参与 KSN 在 PCN 服务器上进行配置。配置的 KSN 参与适用于连接到 PCN 的所有 SCN 服务器。

更新功能（包括反病毒签名更新和代码库更新）以及 KSN 功能可能无法在美国境内使用。

查看 KSN 声明并配置参与 KSN

要配置参与卡巴斯基安全网络：

1. 利用管理员账户登录应用程序 Web 界面。
2. 选择**设置** 部分的**KSN/KPSN 和 MDR**子部分。

3. 在**连接类型**参数名称的右侧，单击**KSN**按钮。

4. 仔细阅读卡巴斯基安全网络声明并选择如下选项之一：

   - **我同意参与 KSN**，如果您接受 KSN 声明的条款并希望参与 KSN。
   - **我不同意参与 KSN**，如果您不接受 KSN 声明的条款并且不想参与 KSN。

     如果您不同意声明条款，将不会启用卡巴斯基安全网络。

5. 单击**应用**。

   将不会配置参与卡巴斯基安全网络。

配置使用 KPSN

要正确连接到 KPSN，您必须使用在*作为服务器部署的 Central Node 的服务所使用的端口*部分中列出的 ksn_proxy 服务的端口。当 KPSN 集成与其他端口配置时，连接尝试失败。

要启用 KPSN:

1. 利用管理员账户登录应用程序 Web 界面。

2. 选择**设置**部分的**KSN/KPSN 和 MDR**子部分。

3. 在**连接类型**参数名称的右侧，单击**KPSN**按钮。

4. 在**KPSN 配置文件**部分，通过单击**浏览**上传 client_config.xms、helper_config.xms 和 keystore.dat 文件。

5. 单击**应用**。

   将启用 Kaspersky Private Security Network。

配置与 KPSN 本地信誉数据库的连接

应用程序可以将有关 Sandbox 组件警报的信息保存到 KPSN 的本地信誉数据库。在这种情况下，*不信任*状态将分配给对象。本地信誉数据库的数据仅适用于企业局域网计算机。

如果您使用分布式解决方案和多租户模式，请使用要为其配置参数的 PCN 或 SCN 服务器的 Web 界面。

配置 Kaspersky Anti Targeted Attack Platform 与本地 KPSN 信誉数据库的连接:

1. 利用管理员账户登录应用程序 Web 界面。

2. 选择**设置**部分的**KPSN 信誉数据库**子部分。

3. 在**主机**字段中，指定存储 KPSN 本地信誉数据库的 KPSN 服务器的 IP 地址。

4. 单击**TLS 证书**字段右侧的**浏览**。
   这将打开文件选择窗口。

5. 在 KPSN 中选择用于用户身份验证的证书文件，然后单击**打开**按钮。

6. 在**TLS 加密密钥**字段的右侧，单击**浏览**。
   这将打开文件选择窗口。

7. 选择包含私有加密密钥的文件，然后单击**打开**按钮。

与 KPSN 本地信誉数据库的连接将得到配置。

配置要保存到 KPSN 本地信誉数据库的信息

应用程序可以将 Sandbox 组件检测到的对象的 MD5 和SHA256 哈希值保存在KPSN 的本地信誉数据库中。在这种情况下，*不信任*状态将分配给对象。本地信誉数据库的数据仅适用于企业局域网计算机。

要配置将 Sandbox 组件检测到的对象保存到 KPSN 的本地信誉数据库：

1. 在高级安全人员账户下登录应用程序 Web 界面。

2. 选择**设置**部分的**KPSN 信誉数据库**子部分。

3. 执行以下操作之一：

   - 如果您希望应用程序将对象状态设置为“*不受信任*”并将有关它们的信息保存在 KPSN 的本地信誉数据库中，请打开“**将“不受信任”状态分配给对象**”开关。
   - 如果您不想在 KPSN 的本地信誉数据库中保存有关检测到的对象的信息，请关闭“**将“不受信任”状态分配给对象**”开关。

4. 单击**保存**。

将信息保存到 KPSN 的本地信誉数据库得到配置。

KSN 参与度和 KPSN 使用量下降

要拒绝参与卡巴斯基安全网络和使用 KPSN：

1. 利用管理员账户登录应用程序 Web 界面。

2. 选择**设置**部分的**KSN/KPSN 和 MDR**子部分。

3. 在**连接类型**参数名称的右侧，单击**未连接**按钮。

4. 单击**应用**。

您将不参与 KSN 也不会使用 KPSN。

通过 Web 界面管理 Sandbox 组件

Sandbox Web 界面位于托管 Sandbox 组件的服务器上。

保护 Sandbox Web 界面免受 **CSRF 攻击**，并且仅当 Web 界面用户的浏览器提供 HTTP POST 请求的 Referrer 头信息时才运行。确保用于 Sandbox Web 界面的浏览器不会修改 HTTP POST 请求的 Referrer 头信息。如果与 Web 界面的连接是通过您组织的代理服务器建立的，请检查设置并确保代理服务器不会修改 HTTP POST 请求的 Referrer 头信息。

跨站请求伪造（也称为“XSRF 攻击”）。利用 HTTP 协议的漏洞攻击网站用户。这种攻击使得黑客能够打着授权用户的幌子在易受攻击的网站中执行操作。例如，在易受攻击的网站中，黑客可以打着授权用户的幌子秘密地向外部支付系统的服务器发送请求，以便将资金转移到黑客的账户。

要开始使用 Sandbox 应用程序的 Web 界面：

1. 在允许访问具有 Sandbox 组件的服务器的任何一台计算机的浏览器上，输入具有 Sandbox 组件的服务器的 IP 地址。

   这将打开 Sandbox 组件管理员凭证输入窗口。

2. 输入您在安装 Sandbox 组件期间指定的 Sandbox 组件管理员用户名和密码。

现在可以开始在 Sandbox Web 界面工作。

如果您使用多个具有 Sandbox 组件的服务器，请从此服务器的 Sandbox Web 界面为每个 Sandbox 组件配置设置。

更新 Sandbox 组件数据库

Sandbox 组件数据库是具有记录的文件，通过这些记录可以检测已扫描对象中的恶意代码和可疑行为的迹象。

卡巴斯基的病毒分析师每天检测成百上千种新威胁，并创建记录来识别它们，将它们加入到*数据库升级包*（或升级包）中。升级包由一个或多个包含记录的文件组成，这些记录可用于识别自上次升级包发布以来检测到的威胁。我们建议您定期接收升级包。

在授权许可有效期内，您可以每小时自动获取一次更新包，或手动更新数据库。

如果您在隔离网络或互联网带宽有限的网络中部署了 Kaspersky Anti Targeted Attack Platform，则可以使用卡巴斯基更新实用程序配置组件数据库更新。如果选择此 Central Node 作为更新源，Sandbox 还可以从其连接的 Central Node 接收数据库更新。

手动更新数据库

要开始手动更新数据库：

1. 在 Sandbox Web 界面窗口中选择**数据库更新**部分。

   最后更新设置组将显示 Sandbox 数据库最近一次更新的时间和状态。

2. 单击**开始**。

选择数据库更新源

选择数据库更新源：

1. 在 Sandbox Web 界面窗口中选择**数据库更新**部分。
2. 在**更新源**设置组中，选择想要接收升级包的源：

   - **卡巴斯基更新服务器**。

     该应用程序通过 HTTP 连接到卡巴斯基更新服务器并下载最新的数据库。

   - **卡巴斯基更新服务器 (安全连接)**。

     该应用程序通过 HTTPS 连接到卡巴斯基更新服务器并下载最新的数据库。建议使用 HTTPS 进行数据库更新。

   - **自定义服务器**。

     应用程序连接到您的 FTP 或 HTTP 服务器或计算机上包含应用程序数据库的目录，以下载最新数据库。您还可以选择 Sandbox 连接到的 Central Node 作为更新源。

     HTTP 必须用于 HTTP 服务器和 Sandbox 之间的通信。在这种情况下，不支持 HTTPS。

3. 如果您选择了**自定义服务器**：

   - 如果要指定 FTP 或 HTTP 服务器作为更新源，请在此设置下方的字段中指定应用程序数据库更新包目录的完整路径。
   - 如果要将 Sandbox 连接到的 Central Node 指定为更新源，请在字段下左键单击要使用的 Central Node 服务器的 IP 地址。该字段以 HTTP://<Central Node IP 地址>/retranslation 格式显示 Central Node 服务器的地址。

4. 单击窗口下部的**应用**。

数据库更新源被选中。

使用卡巴斯基更新实用程序进行更新数据库

如果您已将 Kaspersky Anti Targeted Attack Platform 部署在隔离网络或互联网带宽有限的网络中，则可以使用卡巴斯基更新实用程序配置组件数据库更新。在这种情况下，该实用程序会将更新包下载到组织本地网络之外的计算机，然后将其复制到您的 FTP 或 HTTP 服务器。Sandbox 将从此服务器接收更新包。

使用该实用程序配置组件数据库更新涉及以下步骤：

1. 使用卡巴斯基更新实用程序下载更新包。

   首先，您需要联系卡巴斯基技术支持，并索取该实用程序的分发包以及您可以从中下载更新的服务器列表。

2. 将更新包上传到您的 FTP 或 HTTP 服务器。

   HTTP 必须用于 HTTP 服务器和 Sandbox 之间的通信。在这种情况下不支持 HTTPS。

3. 选择此 FTP 或 HTTP 服务器作为数据库更新源。

使用卡巴斯基更新实用程序下载更新包

要按照这些步骤操作，您需要该实用程序的分发包以及可以从中下载更新的服务器列表。您可以向卡巴斯基技术支持索取这些信息。

要使用卡巴斯基更新实用程序下载更新包：

1. 将包含实用程序分发包的文件夹下载到您的计算机。
2. 运行 UpdateUtility-Gui.exe 文件。
3. 在打开的窗口中，点击“**应用程序**”按钮，然后选中 **7.0-7.1** 选项左侧的复选框。
4. 点击“**确定**”和“**应用**”。
5. 在实用程序的主窗口中，点击“**设置**”按钮，然后选择“**下载**”。
6. 在“**更新源**”下，选择“**其他**”，然后输入用于下载更新的服务器地址。
7. 点击“**确定**”和“**应用**”。
8. 单击“**启动**”。

更新包被下载到运行该实用程序的计算机上。

启用和禁用更新数据库的代理服务器

要启用或禁用代理服务器来更新 Sandbox 组件数据库：

1. 在 Sandbox Web 界面窗口中选择**数据库更新**部分。
2. 在工作区中，执行以下操作之一：
   - 如果您想将代理服务器用于 Sandbox 组件数据库更新，请启用**代理服务器的**设置组名称旁边的开关。
   - 如果您不想将代理服务器用于 Sandbox 组件数据库更新，请禁用**代理服务器的**设置组名称旁边的开关。

配置数据库更新的代理服务器连接设置

配置代理服务器连接以更新 Sandbox 组件数据库：

1. 在 Sandbox Web 界面窗口中选择**数据库更新**部分。
2. 启用**代理服务器**设置组名称旁边的开关。
3. 在**地址** 字段中，输入代理服务器地址。
4. 在 **端口** 字段中，输入代理服务器端口号。
5. 在**用户名称**字段中，输入代理服务器用户名。
6. 在**密码**字段中，输入密码以获取与代理服务器的连接。
7. 执行以下操作之一：
   - 选择**跳过本地地址的代理服务器**复选框， 如果您不想将代理服务器用于您组织的内部 IP 地址。
   - 清除**跳过本地地址的代理服务器**复选框， 如果您想使用代理服务器，而不管您组织的 IP 地址隶属关系如何。
8. 单击窗口下部的**应用**。

配置 Sandbox 和 Central Node 组件间的连接

以下步骤用于配置 Sandbox 组件和 Central Node 组件间的连接：

1. 在应用程序 Web 界面中创建连接到 Sandbox 组件的请求。
2. Sandbox Web 界面显示连接请求。
   您可以接受或拒绝请求。

> 配置连接后，Sandbox 服务器需要 5 到 10 分钟才能准备好运行。在此期间，**系统健康**应用程序 Web 界面的窗口显示警告：*标准配置出现问题*。当服务器准备好运行时，警告就会消失。

在 Sandbox Web 界面处理来自 Central Node 服务器的连接请求

您可以在Sandbox Web 界面中接受、拒绝或撤销先前接受的来自 Central Node 服务器的连接请求。

要接受、拒绝或撤销来自 Central Node 服务器的连接请求：

1. 在 Sandbox Web 界面窗口中，选择 **授权**部分。
   中央节点连接请求部分将显示来自 Central Node 组件的连接请求列表。
   每个连接请求都包含以下信息：
   - **IP** — Central Node 服务器的 IP 地址。
   - **证书指纹** — 用于在服务器之间建立加密连接的 Central Node TLS 证书的指纹。
   - **状态** — 连接请求的状态。
     可能具有**待办的**或**已接受**值。
2. 确保 Central Node 证书指纹与为 Central Node 配置的证书指纹相匹配。
   您可以从**管理服务器证书**部分的 Central Node 服务器管理员菜单中检查 Central Node 证书指纹。
3. 单击包含来自 Central Node 组件的连接请求的行中的以下按钮之一：
   - **接受**，如果您想接受连接请求。
   - **拒绝**，如果您想拒绝连接请求。
   - **撤销**，如果您想撤销先前接受的连接请求。
4. 单击窗口下部的**应用**。

配置 Sandbox 组件网络接口

本节介绍 Sandbox 组件网络接口的配置。

配置 DNS 设置

要配置 DNS：

1. 在 Sandbox Web 界面的窗口中，选择**网络接口**部分。
2. 在**主机名称**字段中，输入以 FQDN 格式（例如，Sandbox）安装 Sandbox 组件的服务器的名称。
3. 在 **DNS 服务器**参数名称的右侧，单击**添加**按钮。
   这将添加一个用于输入 DNS 服务器 IP 地址的空白字段。
4. 以 IPv4 格式输入主 DNS 服务器的 IP 地址。
5. 单击输入字段右侧的✓按钮。
   这将添加一个 DNS 服务器。
6. 如果您想添加其他 DNS 服务器，请重复步骤 2-5。
7. 如果您想移除一个先前添加的 DNS 服务器，请单击包含 DNS 服务器 IP 地址的行右侧的🗑按钮。

> 您只能移除其他 DNS 服务器。您不能移除主 DNS 服务器。如果您添加了 2 个或更多 DNS 服务器，那么您可以移除它们中的任何一个，剩下的 DNS 服务器将被用作主服务器。

配置管理网络接口的设置

管理网络接口旨在通过 SSH 协议提供对具有 Sandbox 组件的服务器的访问权限，并且 Sandbox 组件也会通过这一接口接收来自 Central Node 组件的对象。

您可以在Sandbox 组件安装期间配置管理网络接口。

您也可以从 Sandbox Web 界面配置一个管理网络接口。

要从 Sandbox Web 界面配置一个管理网络接口：

1. 在 Sandbox Web 界面的窗口中，选择**网络接口**部分。
2. 在**接口**下拉列表里的**管理界面**设置组中，选择您要将其用作管理接口的网络接口。
3. 在 **IP** 字段中，如果未分配 IP 地址，请输入您想要分配给此网络接口的 IP 地址。

4. 在**掩码**字段中，输入想要使用此网络接口的网络掩码。

5. 单击窗口下部的**应用**。

配置用于对已处理对象进行 Internet 访问的网络接口的设置

由 Sandbox 组件处理的对象可能会尝试通过用于被处理对象的 Internet 访问的网络接口来尝试在 Internet 上活动。Sandbox 组件可以对这些对象的行为进行分析。

如果阻止因特网访问，则 Sandbox 组件无法分析因特网上对象的行为，因此将只分析无因特网访问对象的行为。

用于对已处理对象进行 Internet 访问的网络接口必须与组织的本地网络隔离。

如果组织的安全策略拒绝来自本地网络用户的计算机访问 Internet，并且您已经为已处理对象配置用于访问 Internet 的 Sandbox 网络接口，则存在以下情形的风险：

黑客可以将恶意应用程序附加到随机文件，并从本地网络用户的计算机启动对该文件的 Sandbox 扫描。在通过 Sandbox 组件扫描文件的过程中，该文件将通过用于对已处理对象进行 Internet 访问的网络接口在本地网络以外被接管。

用于对已处理对象进行 Internet 访问的 Sandbox 网络接口不可用，这消除了此类数据传输的任何风险，但降低了警报质量。

要配置用于对已处理对象进行 Internet 访问的网络接口：

1. 在 Sandbox Web 界面的窗口中，选择**网络接口**部分。

2. 在**接口**列表的 **互联网接口**设置组中，选择您要将其用于对已处理对象进行因特网访问的网络接口。

   在此网络接口列表中，不可以选择您先前配置的管理网络接口。

3. 在 **IP** 字段中，输入您想要分配给此网络接口的 IP 地址。

4. 在**掩码**字段中，输入想要使用此网络接口的网络掩码。

5. 在**默认网关**字段中，输入您想要使用此网络接口的网络的网关地址。

6. 单击窗口下部的**应用**。

添加、更改和移除静态网络路由

在Sandbox 组件安装期间，您可以配置静态网络路由。

您还可以从 Sandbox Web 界面添加、移除或更改静态网络路由。

要添加静态网络路由：

1. 在 Sandbox Web 界面的窗口中，选择**网络接口**部分。
2. 在**静态路由**设置组中，单击**添加**按钮。
   具有空白字段的行将添加到静态网络路由列表中。
3. 在 **IP** 字段中，输入您想要为其配置静态网络路由的服务器的 IP 地址。
4. 在**掩码**字段中，输入子网掩码。
5. 在**网关**字段中，输入网关的 IP 地址。
6. 从**接口**列表中，选择一个您想要为其添加静态网络路由的网络接口。
7. 单击✓。
8. 单击窗口下部的**应用**。

要移除静态网络路由，请执行以下操作：

1. 在 Sandbox Web 界面的窗口中，选择**网络接口**部分。
2. 在包含有您想要移除的静态网络路由的行中的**静态路由**设置组中，单击🗑按钮。
3. 单击窗口下部的**应用**。

要修改静态网络路由：

1. 在 Sandbox Web 界面的窗口中，选择**网络接口**部分。
2. 在包含有您想要修改的静态网络路由的行中的**静态路由**设置组中，单击✎按钮。
   此静态网络路由行将变为可编辑状态。您可以更改静态网络路由的一个或多个参数。
3. 在**IP**字段中，更改您想要为其配置静态路由的服务器的 IP 地址。
4. 在**掩码**字段中，更改子网掩码。
5. 在**网关**字段中，更改网关的 IP 地址。
6. 从**接口**列表中，选择您正在编辑其网络路由的网络接口。
7. 单击✓。
8. 单击窗口下部的**应用**。

设置 Sandbox 系统的日期和时间

要在托管 Sandbox 组件的服务器上设置日期和时间：

1. 在 Sandbox Web 界面窗口中，选择**日期和时间**。
2. 在**国家**下拉列表中，选择相关国家。
3. 在**时区**下拉列表中，选择相关时区。
4. 如果您希望与 NTP 服务器的时间同步，请选择**与 NTP 服务器同步**。
5. 如果您希望手动设置日期和时间，请不要启用**与 NTP 服务器同步**参数名称右侧的开关，并执行以下操作：
   a. 在**日期**字段中，输入当前日期，或单击按钮并在日历中选择一个日期。
   b. 在**时间**字段中，输入当前时间。
6. 单击窗口下部的**应用**。

准备虚拟机以供使用

Sandbox 使用虚拟机在各种操作系统上运行对象，以便分析对象的行为并检测其恶意活动。

您可以安装两种类型的虚拟机：

- 预配置。预配置虚拟机基于分发包中的操作系统镜像（ISO 文件）。您无法修改这些镜像或其中安装的应用程序。

  > 默认操作系统和应用程序可能需要激活。激活是使用您的授权许可进行的。

- 自定义。默认虚拟机基于您选择的操作系统。您可以在这些操作系统上安装任何应用程序来模拟真实的工作环境。

  自定义操作系统必须按照“*配置操作系统和软件*”*部分中的说明进行配置*。要扫描此类操作系统中的对象，您需要创建用户定义的 Sandbox 规则。

您可以同时使用自定义和预设的操作系统镜像。

> 我们强烈建议您在每个 Sandbox 服务器上使用分发工具包中的所有可用预设操作系统镜像。如果仅使用分发包中的部分镜像或仅使用自定义镜像，则扫描对象的质量可能会降低。

基于分发工具包中的操作系统镜像创建预设虚拟机

基于分发工具包中的操作系统镜像创建虚拟机的过程包括以下步骤：

1. 导入模板
2. 创建虚拟机
3. 安装虚拟机

基于您自己的操作系统镜像创建自定义虚拟机

基于您自己的操作系统镜像创建虚拟机涉及以下步骤：

1. 将操作系统镜像以及要安装在操作系统上的应用程序上传到 Sandbox 存储。
   您可以跳过此步骤并在创建和编辑模板时上传镜像。
2. 创建或导入用户自定义模板。
3. 如果操作系统之前未配置过，则必须按照“*配置操作系统和软件*”部分中的说明进行配置。配置操作在编辑模板时执行。
4. 创建虚拟机
5. 安装虚拟机

如果您在安装的虚拟机上遇到问题，可以参考卡巴斯基客户服务知识库。

如果操作系统或应用程序激活出现问题， Sandbox 组件的 Web 界面会显示错误消息。如果发生这种情况，请联系卡巴斯基技术支持。

管理 Sandbox 存储中的操作系统和应用程序镜像

您想要在这些操作系统上安装的操作系统和应用程序的自定义镜像放置在 Sandbox 存储中。

您可以将以下自定义操作系统镜像上传到存储：

- Windows XP SP3 或更高版本
- Windows 7

- Windows 8.1 64 位
- Windows 10 64 位（最高版本 1909）

> 上传的文件必须具有 .ISO 扩展名。

不支持上传 Linux 操作系统的自定义镜像。

如果要在模板中使用自定义操作系统镜像，您必须配置这些操作系统。

查看 Sandbox 存储中的操作系统和应用程序镜像表

要查看 Sandbox 存储中的操作系统和应用程序镜像表：

1. 在 Sandbox Web 界面窗口中，选择**模板和存储**部分。
2. 前往**存储**部分。

   Sandbox 存储中的操作系统和应用程序镜像表得到显示。

表包含以下信息：

- **已上传**是镜像上传时间。
- **名称**是镜像的名称。
- **大小**是镜像的大小。
- **操作**是可对镜像进行的操作。可能的值：**创建 VM**、**导出**、**删除**。

将操作系统和应用程序镜像上传到存储

要将您想要在这些操作系统上安装的操作系统和应用程序的自定义镜像上传到存储：

1. 在 Sandbox Web 界面窗口中，选择**模板和存储**部分。
2. 前往**存储**部分。
3. 单击**上传**。
4. 这将打开文件上传窗口。
5. 选择您想上传到存储的 .ISO 文件。
6. 单击**打开**。

   如果要上传多个镜像，请为每个镜像重复步骤 1 至 6。

镜像将被上传到存储并显示在对象表中。

激活 Sandbox 存储中的操作系统和应用程序镜像

您可以使用 Windows 7（64 位）、Windows 10（64 位）以及 Sandbox 组件所需的应用程序的未激活镜像创建虚拟机，并在安装虚拟机后使用您自己的授权许可代码激活它们。

Windows 镜像和 Microsoft Office 套件可以使用 kata_images.py 文件激活。该文件是分发包的一部分。

正确激活 Windows 镜像和 Microsoft Office 套件需要访问 Internet。确保Internet 访问配置正确。

在“**控制板**”部分的激活过程中，Central Node 会提醒您 Sandbox 的自诊断错误。成功激活后，Sandbox 自我诊断错误不再显示。激活期间，对象不会被发送到 Sandbox 进行扫描。

要激活 Windows 镜像和 Microsoft Office 套件：

1. 确保创建并安装了带有 Windows 7（64 位）、Windows 10（64 位）和 Microsoft Office 套件的未激活镜像的虚拟机。
2. 使用 SSH 将 kata_images.py 文件放置在 Sandbox 服务器上：

   `scp ./kata_images.py admin@<Sandbox 服务器的 IP 地址>:`
3. 通过 SSH 协议或终端登录到 Sandbox 组件服务器的管理控制台。
4. 系统提示时，请输入管理员用户名和安装应用程序期间设置的密码。

   显示 Sandbox 服务器的管理员菜单。
5. 在应用程序管理员菜单中，选择**技术支持模式**。
6. 按 **ENTER** 键。

   这将打开技术支持模式确认窗口。
7. 选择**是**，然后按 **ENTER** 键。
8. 通过运行以下命令序列激活 Windows 镜像和 Microsoft Office 套件：

   a. `cd /var/opt/kaspersky/apt/files`

   b. `sudo -s`

   c. `./kata_images.py activate --vm_id Win7_x64 --component Win7 --key <Windows 7 64 位激活码>`

   d. `./kata_images.py activate --vm_id Win7_x64 --component Office2010 --key <Microsoft Office 2010 激活码>`

e. `./kata_images.py activate --vm_id Win10_x64 --component Win10 --key <Windows 10 64 位激活码>`

f. `./kata_images.py activate --vm_id Win10_x64 --component Office2016 --key <Microsoft Office 2016 激活码>`

> 激活码的格式如下：XXXXX-XXXXX-XXXXX-XXXXX-XXXXX。

9. 为添加了授权许可密钥的虚拟机创建恢复点：

   `./kata_images.py snapshot --vm_ids Win7_x64,Win10_x64`

   该过程可能需要一些时间。

10. 确保应用程序 Web 界面的**控制板**部分不显示有关不工作 Sandbox 组件的警告。

    Windows 镜像和 Microsoft Office 套件已激活。您必须在所有 Sandbox 服务器上激活 Windows 操作系统和 Microsoft Office 应用程序套件的镜像。

从 Sandbox 存储中删除操作系统和应用程序镜像

要从 Sandbox 存储中删除操作系统或应用程序镜像：

1. 在 Sandbox Web 界面窗口中，选择**模板和存储**部分。
2. 前往**存储**部分。
3. 在相关镜像旁边的**操作**列中，单击**删除**。

   这将打开操作确认窗口。

4. 单击**是**。

镜像被删除。

管理虚拟机模板

虚拟机根据模板创建。要创建虚拟机，您必须首先为其导入或创建模板。可以基于同一模板创建多个虚拟机。

您可以对模板执行以下操作：查看模板表、启用或禁用模板、编辑、导出或删除模板。

> 如果正在从该模板创建或安装具有自定义操作系统镜像的虚拟机，则无法使用该模板进行操作。虚拟机创建和安装过程完成后，您可以再次使用模板进行操作。

创建虚拟机模板

要使用所选操作系统创建虚拟机，必须首先为其创建模板。

要为虚拟机创建模板：

1. 在 Sandbox Web 界面窗口中，选择**模板和存储**部分。
2. 前往**模板**部分。
3. 从**添加**下拉列表中选择**创建模板**。
   这将打开模板创建窗口。
4. 在**准备镜像**步骤：
   a. 在**名称**字段中，输入模板的名称。
   b. 在**描述**字段中，输入模板描述。该字段是可选的。
   c. 在**操作系统镜像**下拉列表中，执行以下操作之一：
      - 从可用镜像列表中选择要用于模板的操作系统镜像。
        要在列表中显示镜像，您必须首先将其上传到存储。
      - 要上传操作系统镜像，请单击**上传**链接，选择相关文件，然后单击**"打开"**。
        上传的文件必须具有 ISO 扩展名。
5. 单击**继续**。
6. 在**自定义模板**步骤，执行以下操作之一：
   a. 在**挂载 ISO**下拉列表中，选择要在操作系统中安装的应用程序的镜像。
   对于要在列表中显示的镜像，请执行以下操作之一：
      - 将镜像上传到存储。
      - 在**挂载 ISO**下拉列表中，单击**上传**链接，选择相关文件，然后单击**"打开"**。
        上传的文件必须具有 ISO 扩展名。
   b. 如果要卸载已安装的镜像，请在**挂载 ISO**下拉列表中，单击该镜像旁边的 ⏏ 图标。
   c. 配置操作系统和安装的软件。
   d. 在**关机**下拉列表中，执行以下操作之一：
      - **关机**，如果您想关闭系统同时保存正在运行的应用程序的结果。
      - **关闭电源**，如果您想关闭系统而不保存结果。

      > 如果启用了模板，您将无法使用该模板创建虚拟机，也无法导出该模板。如果您想继续配置模板，请将其启用。

虚拟机模板已创建。您可以基于它创建虚拟机。

查看模板表格

要查看模板表：

1. 在 Sandbox Web 界面窗口中，选择**模板和存储**部分。
2. 前往**模板**部分。

   模板表将显示。

表包含以下信息：

- **已创建**是模板创建时间。
- **类型**是操作系统的类型：自定义或预设。
- **名称**是模板的名称。
- **状态**是模板的状态，例如，**开机**或者**已关闭电源**
- **大小**是模板的大小。
- **操作系统**是用于模板的操作系统版本。
- **VM**是根据这个模板创建的虚拟机。
- **操作**是可以对模板进行的操作。可以进行以下操作：**创建 VM**，**导出**（  ），**删除**（  ）。
- **描述**是创建模板时指定的描述。

打开或关闭模板

如果模板已关闭，您可以使用模板执行以下操作：基于模板创建虚拟机、导出或删除它。如果模板已打开，您可以对其进行编辑。

要打开或关闭模板：

1. 在 Sandbox Web 界面窗口中，选择**模板和存储**部分。
2. 前往**模板**部分。
3. 选择相关模板。

4. 在**自定义模板**部分中，执行以下操作之一：
   - 如果您想开启模板，请在模板管理控制台中单击**开机**。
   - 如果您想关闭模板，请在模板管理控制台的**关机**下拉列表中选择选项之一：
     - **关机**，如果您想关闭系统同时保存正在运行的应用程序的结果。
     - **关闭电源**，如果您想关闭系统而不保存结果。

模板已打开或关闭。

编辑模板

编辑模板：

1. 在 Sandbox Web 界面窗口中，选择**模板和存储**部分。
2. 前往**模板**部分。
3. 选择相关模板。
4. 如果模板已关闭，请单击**开机**将其打开。
5. 如果要在用于模板的操作系统上安装应用程序，请从**挂载 ISO**下拉列表中选择相关的应用程序镜像。要在列表中显示镜像，您必须首先将镜像上传到存储。
6. 如果要卸载已安装的镜像，请在**挂载 ISO**下拉列表中，单击该镜像旁边的**卸载** ⏏ 图标。
7. 配置操作系统和已安装的软件。

模板已编辑。

配置操作系统和软件

准备操作系统以供使用

安装 Windows 7、8.1 或 10 操作系统时，必须满足以下要求：

- 禁用屏幕保护程序。
- 选择*始终开启*电源计划。
- 禁用自动更新。
- 禁用 Windows 防火墙。

如果您使用的是 Windows 7，则需要支持 SHA-2 哈希算法。要确保此哈希算法受支持，请安装适用于 x64 系统的 Windows 7 安全更新 (KB3033929)。对于 32 位 Windows 7 操作系统，还必须安装更新 KB3033929。

> 不要安装更新 KB4474419。此更新可能会导致虚拟机部署期间崩溃。

要使用 Windows 7，您必须在操作系统设置中启用 TLS 1.1 和 TLS 1.2。为此，在 Windows 7 中的“**控制面板**” → “**Internet 选项**” → “**高级**”部分中，选中“**使用 TLS 1.1**”和“**使用 TLS 1.2**”复选框。

使用 Windows 8.1 和 10 操作系统时，必须禁用快速启动并启用自动登录。

操作系统的本地化

您可以在安装系统时选择本地化语言，也可以安装带有英语本地化的系统，并在该系统中额外安装本地化包。您可以选择以下语言之一：俄语、英语、中文（简体）、阿拉伯语、西班牙语（墨西哥）。如果选择不同的本地化，对象扫描的质量会降低。

> 对于 Windows XP 操作系统，仅支持俄语和英语。

配置操作系统

安装操作系统时：

- 确保配置了默认命令 shell。
- 激活操作系统和其他许可软件。

> 使用 Windows 10 操作系统时，需要缓解 Spectre 和 Meltdown 漏洞并禁用 Windows Defender。

您可以使用已安装的操作系统执行以下操作：

- 为计算机分配静态名称。
- 创建用户账户。

  > 此时，您需要配置自动登录。

- 安装软件。
  软件安装限制：
  - 一次只能将一张镜像连接到一个模板。保存模板后，您可以断开一个镜像并安装另一个镜像。
  - 2016 年之后的 Microsoft Office 版本不受支持。

- 强烈建议不要安装以下类型的软件：
  - 将其代码注入另一个正在运行的进程的软件
  - 保护驱动程序
  - 防病毒应用程序，包括 Windows Defender
- 无法保证检测到依赖高度专业化软件运行的文件的恶意活动。

Kaspersky Anti Targeted Attack Platform 不会通知操作系统上安装的软件出现的问题。

缓解 Spectre 和 Meltdown 漏洞。

要正确安装基于 Windows 10 操作系统的自定义虚拟机，需要缓解 Spectre 和 Meltdown 漏洞。

要缓解 Spectre 和 Meltdown 漏洞：

1. 在访客操作系统的命令行中，运行以下命令序列：

   ```
   reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" /v FeatureSettingsOverride /t REG_DWORD /d 3 /f
   ```

   ```
   reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" /v FeatureSettingsOverrideMask /t REG_DWORD /d 3 /f
   ```

2. 重启虚拟机。

漏洞得到缓解。

禁用 Windows Defender

要正确安装基于 Windows 10 操作系统的自定义虚拟机，必须禁用 Windows Defender。

所有操作均在访客操作系统中执行。

要禁用 Windows Defender：

1. 在“HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender”注册表键中创建一个 DWORD32 值。
2. 将以下数据添加到步骤 1 中创建的 DWORD32 值中：
   - AllowFastServiceStartup = 0.
   - ServiceKeepAlive = 0.
   - DisableAntiSpyware = 1.
3. 在“HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender”注册表键下创建“Real-Time Protection”键。

4. 在此键中创建一个 DWORD32 值。
5. 将以下数据添加到步骤 4 中创建的 DWORD32 值中：
   - DisableIOAVProtection = 1.
   - DisableRealtimeMonitoring = 1.
6. 在“HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender”注册表键下创建 Spynet 键。
7. 在此键中创建一个 DWORD32 值。
8. 将以下数据添加到步骤 6 中创建的 DWORD32 值中：
   - DisableBlockAtFirstSeen = 1.
   - LocalSettingOverrideSpynetReporting = 1.
   - SubmitSamplesConsent = 1.
9. 使用组策略禁用 Windows Defender。为此，请在**“运行”**对话框的**“打开”**字段中输入 gpedit.msc → **计算机配置 → 管理模板 → Windows 组件 → Microsoft Defender 反病毒 → 关闭 Microsoft Defender 反病毒 → 编辑策略设置 → 已禁用**。
10. 进入安全模式：
    a. 在**“运行”**对话框的**“打开”**字段中，输入 msconfig → 选择**“引导”**选项卡。
    b. 选中**“安全启动”**复选框。
    c. 选择**“最小”**。
    d. 点击**“应用”**，然后点击**“确定”**。
    e. 在显示的窗口中，选择**“重启”**。
11. 重启后，从注册表中删除 WinDefend 键。
    a. 在“**运行”**对话框的“**打开**”字段中，输入 regedit。
    b. 删除“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services”注册表键下的“WinDefend”键。
12. 禁用安全模式：
    a. 在**“运行”**对话框的**“打开”**字段中，输入 msconfig → 选择**“引导”**选项卡。
    b. 取消选中**“安全启动”**复选框。
    c. 点击“**应用**”，然后点击“**确定**”。
    d. 在显示的窗口中，选择“**重启**”。

Windows Defender 被禁用。

导出模板

您可以通过以下方式之一导出模板：

- 在模板表中。
- 查看模板时。

> 必须关闭该模板。

要导出模板表中的模板：

1. 在 Sandbox Web 界面窗口中，选择**模板和存储**部分。
2. 前往**模板**部分。
3. 在相关镜像旁边的**操作**列中，单击。

   模板已导出。文件下载自动开始。

查看模板时导出模板：

1. 在 Sandbox Web 界面窗口中，选择**模板和存储**部分。
2. 前往**模板**部分。
3. 选择相关模板。
4. 在**操作**下拉列表中，选择**导出**。

   文件下载自动开始。文件下载自动开始。

导入模板

您可以导入以前创建的模板。

要导入模板：

1. 在 Sandbox Web 界面窗口中，选择**模板和存储**部分。
2. 前往**模板**部分。
3. 在**添加**下拉列表中，选择**导入模板**。
4. 这将打开文件上传窗口。

5. 选择您想导入的文件。
6. 单击**打开**。

   该模板出现在模板列表中。

您可以编辑模板、根据模板创建虚拟机、导出或删除模板。

删除模板

删除模板时，所有基于该模板创建的虚拟机都将被删除。

您可以通过以下方式之一删除模板：

- 在模板表中。
- 查看模板时。

必须关闭该模板。

要删除模板表中的模板：

1. 在 Sandbox Web 界面窗口中，选择**模板和存储**部分。
2. 前往**模板**部分。
3. 在相关镜像旁边的**操作**列中，单击。
   这将打开操作确认窗口。
4. 单击**是**。

   模板被删除。

查看模板时删除模板：

1. 在 Sandbox Web 界面窗口中，选择**模板和存储**部分。
2. 前往**模板**部分。
3. 选择相关模板。
4. 在**操作**下拉列表中，选择**删除**。
   这将打开操作确认窗口。
5. 单击**是**。

   模板被删除。

管理虚拟机

您可以创建、安装或删除已安装的虚拟机和待安装的虚拟机。您还可以查看具有预设和自定义操作系统的虚拟机列表。

创建虚拟机

您可以通过以下方式之一创建虚拟机：

- 在**虚拟机**部分。
- 在模板表中。
- 在模板视图中。

虚拟机模板必须关闭。创建虚拟机后，必须安装它。

> 创建具有自定义操作系统镜像的虚拟机需要访问 Internet。

在“虚拟机”部分创建虚拟机

*在**虚拟机**部分中使用预设操作系统镜像创建虚拟机：*

1. 在 Sandbox Web 界面窗口中，选择**模板和存储**部分。
2. 前往**虚拟机**部分。
3. 单击**创建 VM**。
   这将打开虚拟机创建窗口。
4. 在**模板**下拉列表中，选择虚拟机的模板。
   如果列表中没有合适的模板，您可以在 Sandbox Web 界面窗口的**模板**部分中导入或创建模板。
5. 在**名称**字段中，键入虚拟机的名称。
6. 在**描述**字段中，输入虚拟机的描述。该字段是可选的。
7. 单击**保存**。
8. 分发包中的某些操作系统要求接受相关最终用户授权许可协议的条款。阅读最终用户授权许可协议的文本并单击**接受**。

具有预设操作系统镜像的虚拟机已创建。

*在**虚拟机**部分中使用自定义操作系统镜像创建虚拟机：*

1. 在 Sandbox Web 界面窗口中，选择**模板和存储**部分。
2. 前往**虚拟机**部分。
3. 单击**创建 VM**。
   这将打开虚拟机创建窗口。
4. 在**模板**下拉列表中，选择虚拟机的模板。
   如果列表中没有合适的模板，您可以在 Sandbox Web 界面窗口的**模板**部分中导入或创建模板。
5. 在**名称**字段中，键入虚拟机的名称。

   > 该名称必须由拉丁字符组成。

6. 在**描述**字段中，输入虚拟机的描述。该字段是可选的。
7. 单击**保存**。
8. 如果没有为在其上创建虚拟机的服务器配置 Internet 访问，则*无 Internet 访问*错误消息将显示在**模板**窗口。要完成虚拟机创建过程，您必须下载调试符号。

具有自定义操作系统镜像的虚拟机被创建。

在模板表中创建虚拟机

要使用模板表中预设的操作系统镜像创建虚拟机：

1. 在 Sandbox Web 界面窗口中，选择**模板和存储**部分。
   前往**模板**部分。
2. 在模板旁边的**操作**列中，单击**创建 VM**。
   这将打开虚拟机创建窗口。
3. 在**模板**下拉列表中，选择虚拟机的模板。
   如果列表中没有合适的模板，您可以在 Sandbox Web 界面窗口的**模板**部分中导入或创建模板。
4. 在**名称**字段中，键入虚拟机的名称。
5. 在**描述**字段中，输入虚拟机的描述。该字段是可选的。
6. 单击**保存**。
7. 分发包中的某些操作系统要求接受相关最终用户授权许可协议的条款。阅读最终用户授权许可协议的文本并单击**接受**。

具有预设操作系统镜像的虚拟机已创建。

要使用模板表中的自定义操作系统镜像创建虚拟机：

1. 在 Sandbox Web 界面窗口中，选择**模板和存储**部分。
   前往**模板**部分。
2. 在模板旁边的**操作**列中，单击**创建 VM**。
   这将打开虚拟机创建窗口。
3. 在**模板**下拉列表中，选择虚拟机的模板。
   如果列表中没有合适的模板，您可以在 Sandbox Web 界面窗口的**模板**部分中导入或创建模板。
4. 在**名称**字段中，键入虚拟机的名称。

   > 该名称必须由拉丁字符组成。

5. 在**描述**字段中，输入虚拟机的描述。该字段是可选的。
6. 单击**保存**。
7. 如果没有为在其上创建虚拟机的服务器配置 Internet 访问，则*无 Internet 访问*错误消息将显示在**模板**窗口。要完成虚拟机创建过程，您必须下载调试符号。

具有自定义操作系统镜像的虚拟机被创建。

在模板视图中创建虚拟机

要使用模板视图中预设的操作系统镜像创建虚拟机：

1. 在 Sandbox Web 界面窗口中，选择**模板和存储**部分。
2. 前往**模板**部分。
3. 选择相关模板。
4. 单击**创建 VM**。
   这将打开虚拟机创建窗口。
5. 在**模板**下拉列表中，选择虚拟机的模板。
   如果列表中没有合适的模板，您可以在 Sandbox Web 界面窗口的**模板**部分中导入或创建模板。
6. 在**名称**字段中，键入虚拟机的名称。
7. 在**描述**字段中，输入虚拟机的描述。该字段是可选的。
8. 单击**保存**。
9. 分发包中的某些操作系统要求接受相关最终用户授权许可协议的条款。阅读最终用户授权许可协议的文本并单击**接受**。

具有预设操作系统镜像的虚拟机已创建。

要使用模板视图中的自定义操作系统镜像创建虚拟机：

1. 在 Sandbox Web 界面窗口中，选择**模板和存储**部分。
2. 前往**模板**部分。
3. 选择相关模板。
4. 单击**创建 VM**。
   这将打开虚拟机创建窗口。
5. 在**模板**下拉列表中，选择虚拟机的模板。
   如果列表中没有合适的模板，您可以在 Sandbox Web 界面窗口的**模板**部分中导入或创建模板。
6. 在**名称**字段中，键入虚拟机的名称。

   > 该名称必须由拉丁字符组成。

7. 在**描述**字段中，输入虚拟机的描述。该字段是可选的。
8. 单击**保存**。
9. 如果没有为在其上创建虚拟机的服务器配置 Internet 访问，则*无 Internet 访问*错误消息将显示在**模板**窗口。要完成虚拟机创建过程，您必须下载调试符号。

具有自定义操作系统镜像的虚拟机被创建。

查看具有预设操作系统的虚拟机表

要查看具有预设操作系统的虚拟机列表：

1. 在 Sandbox Web 界面的窗口中，选择**虚拟机**部分。
2. 选择**预配置**选项卡。

具有预设操作系统的虚拟机表被显示。

表包含以下信息：

- **名称**是虚拟机的名称。
- **状态**是虚拟机的状态，例如，**已启用**或者**已禁用**。
- **操作**是可以对虚拟机进行的操作。可以进行以下操作：**删除**。

未安装虚拟机部分显示已准备好安装但尚未安装的虚拟机。

查看具有自定义操作系统的虚拟机表

要查看具有自定义操作系统的虚拟机列表：

1. 在 Sandbox Web 界面的窗口中，选择**虚拟机**部分。
2. 单击**自定义**选项卡。

   具有自定义操作系统的虚拟机表被显示。

表包含以下信息：

- **已创建**是虚拟机创建的时间。
- **名称**是虚拟机的名称。
- **状态**是虚拟机的状态，例如，**已启用**或者**已禁用**。
- **操作**是可以对虚拟机进行的操作。可以进行以下操作：**删除**。
- **描述**是创建虚拟机时指定的描述。

安装虚拟机

创建虚拟机后，必须安装它。

要安装具有预设操作系统镜像的虚拟机：

1. 在 Sandbox Web 界面的窗口中，选择**虚拟机**部分。
2. 选择**预配置**选项卡。
3. 在**未安装虚拟机**部分，单击**安装准备好的 VM**。

   所有待安装的虚拟机均已安装。

要安装具有自定义操作系统镜像的虚拟机：

1. 在 Sandbox Web 界面的窗口中，选择**虚拟机**部分。
2. 单击**自定义**选项卡。
3. 在相关虚拟机旁边的**操作**列中，单击**安装**链接。
4. 安装虚拟机后，在**操作**列中，单击**启用**链接。

   虚拟机已安装并可供使用。

删除虚拟机

要删除已安装的虚拟机：

1. 在 Sandbox Web 界面的窗口中，选择**虚拟机**部分。
2. 选择**预配置**或者**自定义**选项卡。
3. 在相关虚拟机旁边的**操作**列中，单击**删除**。

   虚拟机已删除。

要删除具有预设操作系统镜像的未安装虚拟机：

1. 在 Sandbox Web 界面的窗口中，选择**虚拟机**部分。
2. 在**未安装虚拟机**部分，单击**删除所有挂起的 VM**。

   所有具有待安装的预设操作系统镜像的虚拟机都将被删除。

要删除具有自定义操作系统镜像的未安装虚拟机：

1. 在 Sandbox Web 界面的窗口中，选择**虚拟机**部分。
2. 单击**自定义**选项卡。
3. 在相关虚拟机旁边的**操作**列中，单击**删除**链接。

   具有等待安装的自定义操作系统镜像的虚拟机将被删除。

下载调试符号

如果在其上安装具有自定义镜像的虚拟机的服务器未配置 Internet 访问，则必须下载 Microsoft 调试符号才能正确完成虚拟机安装。

您可以在虚拟机安装过程中在**模板**窗口中下载调试符号，或在虚拟机收到虚拟机列表中的**已失败**状态后下载调试符号。

> 为了正确下载调试符号，用于虚拟机模板的操作系统必须安装 Windows 调试工具，并且连接到网络的主机的名称（hostname）必须仅包含拉丁字母、数字和特殊字符。

*在虚拟机安装期间在**模板**窗口中下载调试符号：*

1. 在 Sandbox Web 界面窗口中，选择**模板和存储**部分。
2. 前往**模板**部分。
3. 选择相关模板。

4. 在包含*无互联网访问*错误的窗口中，单击**下载声明**。

   > **下载声明**直到虚拟机获得**已失败**状态后才可用。

   存档将下载到您的计算机上。

5. 解压下载的存档。

6. 使用 Windows PowerShell 运行 sbsymtool.ps1。
   带有调试符号的存档将被下载到该文件所在的文件夹中。

7. 在 Sandbox Web 界面窗口中，选择**模板和存储**部分。

8. 前往**模板**部分。

9. 选择您已为其下载调试符号的模板。

10. 在**操作**下拉列表中，选择**上传符号**。

11. 这会打开一个窗口；在该窗口中，选择带有调试符号的存档，然后单击**打开**。

    调试符号被下载。虚拟机被安装并显示在运行自定义操作系统的虚拟机列表中。

*在虚拟机收到虚拟机列表中的**已失败**状态后下载调试符号：*

1. 在 Sandbox Web 界面窗口中，选择**模板和存储**部分。

2. 前往**模板**部分。

3. 选择相关模板。

4. 在**操作**下拉列表中，选择**下载声明**。
   存档将下载到您的计算机上。

5. 解压下载的存档。

6. 使用 Windows PowerShell 运行 sbsymtool.ps1。
   带有调试符号的存档将被下载到该文件所在的文件夹中。

7. 在**模板**窗口中，展开**操作**列表并选择**上传符号**。

8. 这会打开一个窗口；在该窗口中，选择带有调试符号的存档，然后单击**打开**。

   调试符号被下载。虚拟机被安装并显示在运行自定义操作系统的虚拟机列表中。

设置同时运行的虚拟机的最大数量

设置同时运行、并且具有 Sandbox 组件在其中处理对象的操作系统的虚拟机的数量限制。我们建议使用“*Sandbox 组件计算*”部分中给出的值。如果要使用其他值，请确保安装 Sandbox 的服务器有足够的硬件资源。

您可以使用以下公式计算同时运行的具有操作系统镜像的虚拟机的数量：<逻辑核心数> * 1.5。

同时运行的虚拟机的最大数量不能超过 200。

要设置同时运行的虚拟机的最大数量：

1. 在 Sandbox Web 界面窗口中，选择**管理**部分。
2. 在**来宾虚拟机**设置组的**最大同时运行的 VM**字段中，输入同时运行的虚拟机数量。
   您可以输入一个 1 到 200 之间的数字。
3. 单击**保存**。

更改具有自定义操作系统镜像的虚拟机的授权许可密钥数量

创建具有自定义操作系统镜像的虚拟机时，Kaspersky Anti Targeted Attack Platform 会指定该虚拟机内使用的软件的授权许可密钥数量。默认情况下，授权许可密钥的数量等于同时运行的虚拟机的数量。您的授权许可必须涵盖此数量。如有必要，您可以更改虚拟机的授权许可密钥数量。

如果为虚拟机配置的授权许可密钥数量少于同时运行的虚拟机数量，Sandbox 服务器的整体性能可能会下降。

不建议更改同时运行的虚拟机的指定数量。

要更改具有自定义操作系统镜像的虚拟机的授权许可密钥数量：

1. 通过 SSH 协议或者通过终端进入 Sandbox 服务器的管理控制台。
2. 通过运行`sb-custom-images list-vm`命令获取服务器列表。
   虚拟机表将显示，其中`id`是虚拟机的 ID， `name`是虚拟机的名称， `licenses`是授权许可密钥的数量。
3. 通过运行 `sb-custom-images licenses -id <虚拟机 ID> -ln <授权许可数量>` 命令设置所选虚拟机的授权许可密钥数量。

   授权许可密钥的数量已更改。

要获取脚本的帮助，请运行`sb-custom-images --help`命令。

将 Sandbox 系统日志下载到硬盘驱动器

Sandbox 系统的日志数据以开放且未加密的形式储存。储存的数据涵盖了过去 7 天。

将 Sandbox 系统日志下载到硬盘驱动器：

1. 在 Sandbox Web 界面窗口中，选择**管理**部分。
2. 在**系统日志**设置组中，单击**下载**按钮。
3. 将 Sandbox 系统日志下载到您计算机的硬盘驱动器的文件夹中，该文件夹设置为用于使用该应用程序的浏览器设置中的文件下载文件夹。

导出 Sandbox 设置

导出 Sandbox 系统的设置：

1. 在 Sandbox Web 界面窗口中，选择**管理**部分。
2. 在**设置**设置组中，单击**导出**按钮。
   这将打开**警告**窗口，其中包含关于导出系统参数的警告详情。

   Sandbox 系统参数取决于安装 Sandbox 组件的服务器的硬件和软件参数。Sandbox 系统导出的参数旨在导入到配置严格相同的相同服务器或其他服务器。任意使用保存在其他 Sandbox 系统的参数值来恢复 Sandbox 系统配置的尝试都可能会破坏 Sandbox 系统。

3. 单击**节省**。

将 tar.gz 文件下载到您计算机的硬盘驱动器的文件夹中，该文件夹设置为用于使用该应用程序的浏览器设置中的文件下载文件夹。文件包含了所有 Sandbox 系统当前参数。

带系统参数备份副本的存档可以包含机密信息，例如密码和隐私密钥。Kaspersky Anti Targeted Attack Platform 的管理员必须自行确保此数据的安全。

导入 Sandbox 设置

导入 Sandbox 设置：

1. 在 Sandbox Web 界面窗口中，选择**管理**部分。
2. 在**设置**设置组中，单击**导入**按钮。
   这将打开**警告**窗口，其中包含关于导入系统参数的警告详情。

   Sandbox 组件参数取决于安装 Sandbox 的服务器的硬件和软件参数。Sandbox 导出的参数旨在导入到配置严格相同的相同服务器或其他服务器。任意使用保存在其他 Sandbox 系统的参数设置来恢复 Sandbox 系统配置的尝试都可能会破坏 Sandbox 系统。

3. 单击**恢复**。

   这将打开文件选择窗口。

4. 选择一个 tar.gz 文件，其中包含要下载的 Sandbox 参数，然后单击**打开**按钮。

   这将关闭文件选择窗口。

   如果 Sandbox 参数导入成功，则 Sandbox 服务器将重新启动。几分钟后，您需要刷新浏览器窗口并重新登录。

带系统配置备份副本的存档可以包含机密信息，例如密码和隐私密钥。Kaspersky Anti Targeted Attack Platform 的管理员必须自行确保此数据的储存安全。

重新启动 Sandbox 服务器

重新启动 Sandbox 服务器：

1. 在 Sandbox Web 界面窗口中，选择**管理**部分。
2. 在**电源**设置组中，单击**重新启动**按钮。

   这将打开 Sandbox 服务器重新启动确认窗口。

3. 单击**是**。

Sandbox 服务器将重新启动。几分钟后，您将可以登录系统。

关闭 Sandbox 服务器电源

关闭 Sandbox 服务器电源：

1. 在 Sandbox Web 界面窗口中，选择**管理**部分。
2. 在**电源**设置组中，单击**关闭电源**按钮。

   这将打开 Sandbox 服务器关闭确认窗口。

3. 单击**是**。

Sandbox 服务器电源关闭。

更改 Sandbox 管理员账户密码

更改 Sandbox 管理员账户密码：

1. 在 Sandbox Web 界面窗口中，选择**管理**部分。
2. **更改密码**设置组将显示您在 Sandbox 安装期间设置的 Sandbox 管理员账户名以及修改密码的字段。
3. 在**当前密码**字段中，输入 Sandbox 管理员账户的当前密码。
4. 在**新密码**字段中，输入 Sandbox 管理员账户的新密码。
5. 在**确认密码**字段中，再次输入 Sandbox 管理员账户的新密码。
6. 单击**更改密码**。
   Sandbox 管理员账户密码将被更改。

对于管理员：应用程序 Web 界面使用入门

本节的目标受众是安装和管理 Kaspersky Anti Targeted Attack Platform 以及以分布式解决方案和多租户模式管理 PCN 和 SCN 服务器和租户的人员。

Kaspersky Anti Targeted Attack Platform 界面

该应用程序通过 Web 界面进行管理。应用程序 Web 界面的各个部分因用户的角色不同而有所不同：管理员或高级安全官（**高级安全官**、**安全官**、**安全审计员**）。

应用程序 Web 界面窗口包含如下内容：

- 应用程序 Web 界面窗口左侧和下侧的部分。
- 在应用程序 Web 界面窗口上部用于应用程序某些部分的选项卡。
- 应用程序 Web 界面窗口下侧的工作区。

应用程序 Web 界面窗口的部分

管理员角色的应用程序 Web 界面包含以下几个部分：

- **控制板**。包含 Kaspersky Anti Targeted Attack Platform 监控数据。
- **操作模式**。包含有关 PCN 和 SCN 服务器以及分布式解决方案和多租户模式中租户的信息。
- **资产**。包含有关具有 Kaspersky Endpoint Agent 组件的联机计算机及其设置的信息。
- **日志**：**用户活动**、**应用程序消息**、**审计**。包含有关应用程序性能的信息以及 Web 界面中用户活动的审计记录。
- **设置**。包含具有 Central Node 组件的服务器的设置。
- **Sensor 服务器**。包含有关已连接的 Sensor 组件及其设置的信息。
- **Sandbox 服务器**。包含有关 Central Node 组件与 Sandbox 组件的连接的信息。
- **外部系统**。包含有关应用程序与邮件传感器集成的信息。
- **服务器配置**。包含有关应用程序的尺寸参数的信息。

应用程序 Web 界面窗口的工作区

工作区显示了您选择在应用程序 Web 界面窗口的各个部分和选项卡上查看的信息。它还包含了可用于配置信息显示方式的控制元素。

具有**安全审计员**角色的用户还可以查看应用程序 Web 界面的这些部分。

监控应用程序的性能

您可以使用应用程序 Web 界面窗口的**控制板**部分中的小组件来监控应用程序运行。您可以添加、删除和移动小组件，配置小组件的显示比例，以及选择数据显示时段。

关于小组件和布局

您可以使用小组件来监控应用程序运行。

*布局*是**控制板**部分中应用程序 Web 界面窗口工作区的外观。您可以添加、删除和移动布局中的小组件。

应用程序中有如下小组件：

- **管理**：
  - **Sandbox 处理时间**。显示 Sandbox 扫描对象的平均时间。
  - **已处理**。显示从 Sensor 和 Endpoint Agent 到 Central Node 的流量的处理状态。
  - **队列**。显示有关应用程序模块和组件要扫描的对象的数量信息。

  如果您使用分布式解决方案和多租户模式，该部分将显示有关您选择的租户和服务器的的信息。
- NDR：
  - **自定义小部件**。具有任意静态内容的小部件。例如，您可以使用自定义小组件在“**控制板**”部分中以逻辑方式分隔小组件组。
  - **流量**。传入流量的速率。该小部件可以显示已安装应用程序组件的所有节点的所有监控点的信息，也可以显示选定节点的监控点的信息，或者显示单个监控点的信息。
  - **CPU 使用率**。安装了应用程序组件的选定节点上的 CPU 负载。
  - **内存使用情况**。安装了应用程序组件的选定节点上正在使用的物理 RAM 数量。

- **NDR 健康**。有关应用程序性能当前状态的信息。此小组件可以显示以下值：
  - **正常** – 没有关于性能问题的消息，或者所有性能问题已解决。
  - **非严重故障** – 报告了非严重故障。该值会一直显示，直到性能问题得到解决。
  - **操作中断** – 报告了应用程序中断。该值会一直显示，直到性能问题得到解决。
  - **维护模式** – 应用程序正在维护模式下运行。
- **存储** – 有关安装了应用程序组件的选定节点上的本地文件系统中的驱动器的信息。在此小组件中，您可以选择显示以下信息：
  - **磁盘使用情况** – 处理数据读/写操作所花费的时间百分比。
  - **磁盘占用** – 磁盘空间已满。
  - **从磁盘读取** – 从磁盘读取数据的速率。
  - **写入磁盘** – 将数据写入磁盘的速率。
- **流量处理延迟**。处理流量时的当前延迟，从流量到达节点的监控点开始计算。显示所有启用的监控点中的最大延迟。该小部件可以显示已安装应用程序组件的所有节点的所有监控点的信息，以及选定节点的监控点的信息。
- **保护功能状态**。有关应用程序中保护功能当前状态的一般信息。此小组件可以显示以下值：
  - **全部启用** – 所有用于持续使用的技术和方法都已启用，所有创建的监控点都已启用。
  - **并非全部启用** – 某些保护功能被禁用或在学习模式下启用，或者并非所有监控点都启用。
- **运行时间**。Kaspersky Anti Targeted Attack Platform 的运行时间。在此小组件中，您可以选择显示以下信息：
  - 有效运行时间 – 自最近一次启动到当前时刻，应用程序正常运行（无故障）的持续时间。
  - 总运行时间 – 从应用程序首次启动到当前时刻的时间。包括应用程序正常运行期间和故障期间。
  - 自应用程序首次启动以来 – 从应用程序首次启动到当前时刻经过的总时间。包括正常运行期、故障期和无法运行期。

根据传入的信息，小部件采用各种方式来吸引注意力。例如，如果信息需要引起注意（特别是，当硬件资源上的负载接近临界负载时），包含有关应用程序和硬件资源信息的小组件可以自动改变颜色。

小部件仅显示动态变化的基本信息。如果您需要查看详细信息，可以从“**控制板**”部分导航到应用程序 Web 界面的其他部分。您可以通过单击小部件来导航 Web 界面。

为了在 NDR 小部件中显示正确的信息，您必须配置 Central Node 和 Sensor 组件之间的日期和时间同步。

在“仪表板”部分选择要管理的租户和服务器

如果您使用的是分布式解决方案和多租户模式，在使用**控制板**部分之前，您必须选择要查看其数据的租户和服务器。NDR 功能的小部件将显示当前节点或在小部件设置中选择的节点的信息。

*要选择要在“**控制板**”部分的小部件中显示其数据的租户和服务器：*

1. 在应用程序 Web 界面窗口的右上方，单击服务器名称旁边的箭头。
2. 在下拉列表中，从列表中选择租户和服务器。

所选服务器的数据将予以显示。如果要选择不同的租户和服务器，请重复选择租户和服务器的步骤。

添加小组件到当前布局

要添加小组件到当前布局：

1. 在应用程序 Web 界面窗口中选择**控制板**部分。
2. 在窗口的上部，单击 ☰ 按钮。
3. 在下拉列表中，选择**定制**。
4. 单击**小部件**。
5. 在打开的**管理小部件**窗口中：
   - 如果您想添加**Sandbox 处理时间**小组件，打开该小组件名称旁边的切换开关。
   - 如果您想添加不同的小组件，单击小部件名称旁边的 + 。
6. 关闭“**管理小部件**”窗口并单击“**应用**”。

所选小组件将被添加到当前布局。

在当前布局中移动小组件

要在当前布局中移动小组件：

1. 在应用程序 Web 界面窗口中选择**控制板**部分。
2. 在窗口的上部，单击 ☰ 按钮。
3. 在下拉列表中，选择**定制**。
4. 在布局中选择要移动的小组件。

5. 单击并按住小组件的上部可将小组件拖放到布局中的不同位置。

6. 单击**应用**。

   当前布局已保存。

更改 NDR 小部件中信息的显示

添加 NDR 小部件后，它将根据默认设置显示信息。如果需要，您可以编辑显示设置。

要编辑 NDR 小部件显示设置：

1. 在应用程序 Web 界面窗口中选择**控制板**部分。

2. 在窗口的上部，单击 ☰ 按钮。

3. 在下拉列表中，选择**定制**。

4. 在要配置的 NDR 小部件的右上角，单击 ⚙ 按钮。

   这将打开显示设置窗口。

5. 管理 NDR 小部件的显示设置。

   根据所选的 NDR 小组件，窗口可能包含以下设置：

   - **更改名称** – 如果选中“**更改名称**”复选框，您可以在“**小组件名称**”字段中为小组件定义任何名称（不同于默认名称）。自定义小组件中没有“**更改名称**”设置。
   - **小组件名称** – 用于输入与默认名称不同的小组件名称的字段。
   - **编辑描述** – 如果选中“**编辑描述**”复选框，您可以在“**小组件描述**”字段中为小组件提供任何描述（不同于默认描述）。自定义小组件中缺少“**编辑描述**”设置。
   - **小部件描述** – 用于输入与默认名称不同的小组件名称的字段。
   - **刷新周期** – 显示的信息更新的时间（以秒为单位）。
   - **显示** – 定义显示数据的类型（对于允许您选择显示哪些数据的小组件）。
   - **数据源** – 安装了应用程序组件且小部件显示其信息的主机。如果选择了“**整个应用程序**”，小组件将显示来自所有节点的数据。
   - **根据状态改变颜色** – 如果选中此复选框，小组件的背景颜色将根据传入数据的严重性自动改变。关键（最大）重要级别以红色背景表示。如果清除此复选框，则背景颜色被禁用。
   - **定义的背景** – 定义自定义小组件的背景颜色。您可以选择与严重性级别 (**信息**、**警告**或**严重**) 相对应的背景颜色，或选择**中性**以禁用背景颜色。

6. 单击**应用**。

从当前布局移除小组件

要从当前布局移除小组件：

1. 在应用程序 Web 界面窗口中选择**控制板**部分。
2. 在窗口的上部，单击 ☰ 按钮。
3. 在下拉列表中，选择**定制**。
4. 单击要从当前布局移除的小组件右上角的 × 图标。
   小组件被从应用程序 Web 界面窗口的工作区移除。
5. 单击**应用**。

小组件被从当前布局移除。

保存布局为 PDF

布局中的 NDR 小部件未保存到 PDF。

要保存布局为 PDF：

1. 在应用程序 Web 界面窗口中选择**控制板**部分。
2. 在窗口的上部，单击 ☰ 按钮。
3. 在下拉列表中，选择**保存为 PDF**。
   这将打开**另存为 PDF**窗口。
4. 在窗口下部的**布局**下拉列表中，选择页面方向。
5. 单击**下载**。
   PDF 格式的布局被保存到您的计算机硬盘驱动器上的浏览器下载文件夹中。
6. 单击**关闭**。

配置小部件中的数据显示周期

您可以配置在小组件中显示数据的以下时段：

- **天**。
- **周**。
- **月份**。

对于 NDR 小部件，您可以使用以下时间段：

- **1 小时**
- **12 小时**
- **24 小时**
- **7 天**

您可以为每个单独的 NDR 小部件配置一个数据显示周期。

更改小部件中信息的显示

要配置小组件中一天的数据显示（从早上 00:00 到晚上 11:59）：

1. 在应用程序 Web 界面窗口中选择**控制板**部分。
2. 在应用程序 Web 界面窗口右上角的数据显示时段下拉列表中，选择**天**。
3. 在**天**时段名称右侧的日历中，选择要在小组件中显示数据的日期。

   控制板页上的所有小组件都会显示选定时段的数据。

要在小组件上配置一周（周一到周日）的数据显示：

1. 在应用程序 Web 界面窗口中选择**控制板**部分。
2. 在应用程序 Web 界面窗口右上角的数据显示时段下拉列表中，选择**周**。
3. 在**周**时段名称右侧的日历中，选择要在小组件上显示数据的周。

   控制板页上的所有小组件都会显示选定时段的数据。

要在小组件中显示一个月（日历月）的数据显示：

1. 在应用程序 Web 界面窗口中选择**控制板**部分。
2. 在应用程序 Web 界面窗口右上角的数据显示时段下拉列表中，选择**月份**。
3. 在**月份**时段名称右侧的日历中，选择要在小组件中显示数据的月份。

控制板页上的所有小组件都会显示选定时段的数据。

更改小部件中信息的显示

要配置 NDR 小部件中的信息显示：

1. 在应用程序 Web 界面窗口中选择**控制板**部分。
2. 在您要配置的 NDR 小部件的右上角，单击代表您需要的时间间隔的按钮。

NDR 小部件显示选定时间段的信息。

监控传入数据的接收和处理

在“**已处理**”小组件中，您可以访问从 Sensor 和 Endpoint Agent 到 Central Node 的数据的处理状态，并跟踪数据处理错误。

要选择为其评估传入数据的组件（Sensor 或 Endpoint Agent），请使用**已处理**小组件名称右侧的下拉列表。

您可以在组件名称（Sensor 或 Endpoint Agent）右侧的下拉列表中选择数据显示类型：

- **当前负载** — 最近 5 分钟。
- **所选期间**。在这种情况下，您还可以配置小组件中的数据显示时段。

每个小组件的左侧部分显示小组件本身使用的颜色的图例。

如果选择**当前负载**数据显示类型，那么在过去 5 分钟内的平均数据处理速率将显示在键的右侧。

例如：
选择了**(SPAN)**或**(ICAP)** Sensor 类型和“**当前负载**”数据显示类型的“**已处理**”小组件显示特定时间段内从 Sensor 到 Central Node 的 SPAN 和 ICAP 流量的数据处理速率。
将显示以下信息：

- **流量** – 传入 Central Node 服务器的流量速率，以绿色表示 (Mbps)。

  如果流量速率低于 1 Mbps，则小部件上不会显示有关它的信息。

- **文件** – 文件处理速率以灰色表示（每秒对象数）。
- **URL** – URL 处理率，以蓝色表示（每秒对象数）。
- **未处理** – 由垂直红线表示的未处理对象的数量。
  将鼠标光标移到小组件上时，您会看到一个弹出窗口，上面显示了特定时段的数据处理速率。
  选择了**(SMTP)** Sensor 类型和“**当前负载**”数据显示类型的“**已处理**”小组件显示特定时间段内从邮件传感器到 Central Node 服务器的邮件流量的 SPAN 和 ICAP 流量数据处理速率。
  将显示以下数据：
- **流量** – 传入具有 Sensor 组件的服务器的流量速率，以绿色表示（每秒消息数）。
- **文件** – 文件处理速率以灰色表示（每秒对象数）。
- **URL** – URL 处理率，以蓝色表示（每秒对象数）。
- **未处理** – 由垂直红线表示的未处理对象的数量。
  将鼠标光标移到小组件上时，您会看到一个弹出窗口，上面显示了特定时段的数据处理速率。
  已处理小组件选择了**(LOAD) Endpoint Agent** Sensor 类型和**当前负载**数据显示类型，并显示特定时间段内从 Endpoint Agent 组件到具有 Central Node 组件的服务器的事件的处理速率（每秒事件数）。
  将鼠标光标移到小组件上时，您会看到一个弹出窗口，上面显示了特定时段的数据处理速率。

如果选择了“**所选期间**”数据显示类型，那么在图例的右侧，您将看到至 Central Node 服务器的传入流量的平均速率以及选定时段内处理的对象数量。

例如：
选择了**(SPAN)**或**(ICAP)** Sensor、“**所选期间**”数据显示类型以及“**月份**”数据显示时段的“**已处理**”小组件显示传入 Central Node 服务器的 SPAN 和 ICAP 流量的速率，以及选定月份内从邮件流量中提取的文件和 URL 的数量。
将显示以下信息：

- **平均流量** – 到具有 Central Node 组件的服务器的传入流量速率，以绿色表示（每秒对象数）。
- **文件** – 提取的文件数量，以灰色表示。
- **URL** – 提取的 URL 数量，以蓝色表示。
- **未处理** – 由垂直红线表示的未处理对象的数量。
  当您将鼠标悬停在小部件上时，会显示一个弹出窗口，其中显示传入 Central Node 的流量速率和特定时间内处理的对象数量。
  选择了**(SMTP)** Sensor、“**所选期间**”数据显示类型和“**月份**”数据显示时段的“**已处理**”小组件显示从邮件服务器到 Central Node 的邮件流量的数据处理速率，以及选定月份内从邮件流量中提取的文件和 URL 的数量。
  将显示以下信息：
- **平均流量**– 到达 Central Node 服务器的流量速率，以绿色表示（对象/秒）。
- **文件** – 提取的文件数量，以灰色表示。
- **URL** – 提取的 URL 数量，以蓝色表示。
- **未处理** – 由垂直红线表示的未处理对象的数量。
  当您将鼠标悬停在小部件上时，会显示一个弹出窗口，其中显示传入 Central Node 的流量速率和特定时间内处理的对象数量。

选择了“**(LOAD) Endpoint Agent**” Sensor 类型、“**所选期间**”数据显示类型和“**月份**”数据显示时段的“**已处理**”小组件显示所选月份内从 Endpoint Agent 主机传入到 Central Node 服务器的事件数。

将鼠标光标移到小组件上时，您会看到一个弹出窗口，上面显示了特定时段的事件数。

监控由应用程序模块和组件对数据进行处理的队列

您可以使用**队列**小组件来评估YARA和AM Engine应用程序模块以及Sandbox 组件的数据处理状态，并监控未处理的数据量。

队列中的数据传输以消息数来衡量。

您可以在**队列**小组件名称右侧的下拉列表中选择数据显示类型：

- **当前负载** — 最近 5 分钟。
- **所选期间**。在这种情况下，您还可以配置小组件上的数据显示时段。

小组件的左侧部分显示小组件中使用的颜色的图例。

队列小组件显示了以下数据：

- 应用程序模块和组件处理的**消息数量**和**数据量**：
  - YARA — 蓝色。
  - Sandbox — 紫色。
  - AM **引擎** — 绿色。
- **未处理的**– 由垂直红线指示的未处理数据量。

将鼠标光标移到小组件上时，会看到一个弹出窗口，上面显示了**YARA** 和 **AM Engine**应用程序模块和**Sandbox 组件**的数据处理状态，以及特定时段内的未处理数据数量。

监控 Sandbox 组件对数据的处理

Sandbox 处理时间小组件显示所选期间从数据被发送到一个或多个 Sandbox 组件服务器（包括发送之前在队列中花费的时间）到 Sandbox 处理结果显示在 Kaspersky Anti Targeted Attack Platform 的 Web 界面中所经过的平均时间。

例如：
如果**月份**配置为小组件中数据显示的周期，则**Sandbox 处理时间**小组件显示当月每一天的橙色条。
将鼠标光标移动到每列上时，您会看到一个弹出窗口，显示了在选定天内从数据发送到一个或多个具有 Sandbox 组件的服务器的时刻开始，直到 Sandbox 组件的数据处理结果显示在 Kaspersky Anti Targeted Attack Platform 的 Web 界面中的平均时间。

通过增加具有 Sandbox 组件的服务器数量以及在这些服务器之间分配要处理的数据，可以提高 Sandbox 组件处理数据的速率以及 Sandbox 组件的吞吐量。

查看应用程序模块和组件的工作状况

如果应用程序的模块或组件遇到建议管理员查看的错误，则一个黄色警告框会显示在应用程序 Web 界面的**控制板**部分。

具有“**管理员**”或者“**安全审计员**”角色的用户可以访问有关用户当前管理的 Central Node、PCN 或 SCN 服务器的工作状况信息。

具有“**高级安全官**”、“**安全官**”或者“**安全审计员**”角色的用户可以访问有关工作状况的以下信息：

- 如果您使用的是独立的 Central Node 服务器，用户可以访问有关用户当前管理的 Central Node 服务器的工作状况的信息。
- 如果您使用分布式解决方案和多租户模式，并且用户正在管理 SCN 服务器，则用户可以访问该 SCN 服务器的工作状况信息，以获取其有权访问数据的租户的信息。
- 如果您使用分布式解决方案和多租户模式，并且用户正在管理 PCN 服务器，则用户可以访问该 PCN 服务器和所有连接到该服务器的 SCN 服务器的工作状况信息，以获取其有权访问数据的租户的信息。

若要详细了解应用程序模块及组件的工作情况，

单击**查看详情**打开**系统健康**窗口。

在**系统健康**窗口中，根据应用程序模块和组件的工作状况会显示以下图标之一：

- OK 如果应用程序的模块和组件正常工作。
- 带有问题数量的图标（例如，1），如果发现建议管理员注意的问题。在这种情况下，详细的问题信息会显示在**系统健康**窗口的右侧。

系统健康窗口包含以下部分：

- **组件健康**包含有关应用程序在其上运行的所有服务器上的应用程序模块和组件的运行状态、隔离以及数据库更新的信息。

  例如：
  如果一个或多个应用程序组件的数据库在 24 小时内未更新，则图标显示在安装应用程序模块和组件的服务器的名称旁边。
  要解决该问题，请确保可以访问更新服务器。如果您使用代理服务器连接到更新服务器，请确保代理服务器没有与 Kaspersky Anti Targeted Attack Platform 服务器连接相关的错误。

- **已处理** – 传入数据接收和处理状态。状态根据以下条件生成：
  - 从带有 Sensor 组件的服务器、带有邮件传感器的服务器或虚拟机、带有 Endpoint Agent 组件的主机接收数据的状态。
  - 有关超出对象在队列中等待应用程序模块和组件扫描的最长允许时间的信息。
- **与服务器的连接** – PCN 服务器和连接的 SCN 服务器之间的连接状态（如果您使用分布式解决方案和多租户模式，则会显示）。

如果检测到应用程序模块或组件的性能问题，您无法自行解决这些问题，请联系卡巴斯基技术支持。

管理 Central Node 或 Sensor 服务器信息

有关带有 Central Node 或 Sensor 组件的服务器的信息显示在应用程序 Web 界面窗口的“**Sensor 服务器**”区域。

此部分显示组件的卡（左侧）和在这些组件上检测到的网络接口卡（每个组件的右侧）。

Sensor 组件卡片上方是该 Sensor 所连接的 Central Node 组件卡片。如果 Central Node 组件部署了嵌入式 Sensor，则该 Sensor 组件的名称将在卡上显示为嵌入式 Sensor。

您可以查看组件卡和网络接口卡。

查看有关 Central Node 或 Sensor 服务器的信息

要查看有关 Central Node 或 Sensor 组件的信息：

1. 在应用程序 Web 界面窗口中选择**Sensor 服务器**部分。
2. 单击相关组件的卡片。
   这将打开一个窗口，其中包含有关组件的信息。

Central Node 和 Sensor 组件的**“设置”**选项卡显示以下信息：

- “**状态**”是通过图标和文本描述指示的组件的当前状态。
- **节点类型**表示应用程序组件：**Server**（Central Node 组件）或者**Sensor**（Sensor组件）。
- **应用程序当前使用的磁盘空间**是应用程序文件占用的磁盘空间。包括已安装的文件和应用程序在运行过程中创建的文件。
- **应用程序可使用的最大磁盘空间**就是应用程序文件可占用的磁盘空间。包括已安装的文件和数据存储规则中配置的所有空间限制的总和。该值不得超过可用磁盘空间量。
- “**磁盘占用**”是所有文件使用的磁盘空间。包括应用程序文件、操作系统文件和其他应用程序的文件。该空间是根据包含组件文件系统中 /var 目录的磁盘来计算的。
- “**可用磁盘空间**”是未被文件使用的磁盘空间。该空间是根据包含组件文件系统中 /var 目录的磁盘来计算的。
- “**总磁盘空间**”是包含组件文件系统中 /var 目录的驱动器上的磁盘空间总量。
- “**BPF 过滤**”指示是否启用或禁用使用基于网络数据包中的地址参数的 Berkley Packet Filter (BPF) 技术进行过滤。
- **流量转储文件的外部存储**指示外部存储的连接状态。可能显示以下状态：**已连接**、**未连接**。
- “**保留规则**”指示应用程序数据的大小、项目数量和存储期限的当前值和最大值。

对于 Sensor 组件，除了“**设置**”选项卡之外，还会显示“**外部存储**”、“**其他**”、“**ICAP 集成**”、“**POP3 集成**”和“**SMTP 集成**”选项卡。

- “**外部存储**”选项卡显示有关镜像 SPAN 流量的外部存储配置的信息。
- 在“**其他**”选项卡上，显示以下信息：
  - 扫描文件的最大大小是组件当前能够扫描的文件大小的限制。
  - 转储 HTTP 正文指示是否启用或禁用 HTTP 正文内容转储。
- “**ICAP 集成**”选项卡显示通过 ICAP 与代理服务器集成的设置。

  Host字段显示“icap://<Sensor 连接到的 Central Node 服务器的 IP 地址>:1344/av/<respmod or reqmod>”格式的响应修改(RESPMOD)和请求修改(REQMOD)服务的 URL。

  要配置与 Kaspersky Anti Targeted Attack Platform 的集成，请复制相关的 URL，将 Central Node 服务器的 IP 地址替换为您要配置 ICAP 集成的 Sensor 服务器的 IP 地址，然后在您组织的代理服务器的设置中指定生成的 URL。
- “**POP3 集成**”选项卡显示 POP3 邮件服务器集成设置。
- “**SMTP 集成**”选项卡显示 SMTP 邮件服务器集成设置。

查看网络接口信息

应用程序 Web 界面的**Sensor 服务器**部分中的网络接口卡显示以下信息：

- 网络接口名称
- 网络接口的 MAC 地址
- 网络接口的 IP 地址
- 网络接口频宽
- 闪烁。此链接可让您识别与网络接口关联的以太网端口

如果网络接口已经添加了监控点，则网络接口的卡片中将显示该监控点的以下信息：

- 监控点名称。
- **技术模式**是技术继承功能的状态。它可以是**已启用**或者**已禁用**。

您可以查看网络接口详细信息。

要查看网络接口详细信息：

1. 在应用程序 Web 界面窗口中选择**Sensor 服务器**部分。
2. 单击相关网络接口的卡。

   这将打开一个窗口，其中包含有关网络接口的信息。

网络接口卡显示以下信息：

- “**网络接口**”是操作系统中网络接口的名称。
- “**连接**”是表示网线已连接到网络接口的以太网端口的图标：
  - – 网线已连接。
  - – 网线已断开连接。
    启用以太网端口指示模式时，图标闪烁。
  - **MAC 地址**是网络接口的 MAC 地址。
  - **IP 地址**是网络接口的 IP 地址。
    如果网络接口上发现多个 IP 地址，则详细信息区域中最多显示 16 个 IP 地址。

如果网络接口上已经添加了监控点，则网络接口的卡片中会显示以下信息：

- “**状态**”是监控点当前的状态，用图标和文字描述表示：
  - *正常*。监测点可用。
  - *切换*。监控点运行模式正在改变。
  - *错误*。切换监控点操作模式时检测到错误。
- “**连接**”是表示网线已连接到网络接口的以太网端口的图标：
  - – 网线已连接。
  - – 网线已断开连接。

  启用以太网端口指示模式时，图标闪烁。
- “**网络接口**”是操作系统中网络接口的名称。
- “**模式**”是监控点当前的模式：
  - *已启用*。
  - *已禁用*。
- 在**“设置”**选项卡上：
  - “**技术继承**”指示是否为服务器启用或禁用技术继承。
  - **MAC 地址**是网络接口的 MAC 地址。
  - **IP 地址**是网络接口的 IP 地址。

识别与网络接口关联的以太网端口

安装应用程序组件的服务器可以有多个以太网端口用于连接本地网络。您可以使用该应用程序为网络接口启用闪烁模式，并找出与该接口关联的以太网端口。在闪烁模式下，以太网端口旁边的 LED 会闪烁 15 秒。

如果网络接口不支持 LED 指示（例如，如果以太网端口没有配备 LED，或者网络接口是逻辑绑定接口），则尝试启用闪烁模式时会显示错误。

要识别与网络接口关联的以太网端口：

1. 在应用程序 Web 界面窗口中选择**Sensor 服务器**部分。
2. 在相关网络接口的卡上，点击“**闪烁**”按钮。

   如果网络接口支持 LED 指示，网线连接图标在网络接口卡上开始闪烁。同时，计算机相应网络适配器上以太网端口旁边的 LED 开始闪烁。

当网络接口处于闪烁模式时，您无法为同一服务器上的任何其他网络接口打开闪烁模式。

使用应用程序 Web 界面管理 Central Node、PCN 或 SCN 服务器

您可以使用应用程序 Web 界面利用安装有 Central Node 组件的服务器执行以下操作：

- 更改服务器的 FQDN 名称
- 配置服务器上的日期和时间。
- 关闭并重启服务器。
- 管理服务器的证书
- 管理流量保存设置
- 管理保存流量转储文件的设置
- 管理服务器的网络设置

如果您使用分布式解决方案和多租户模式，请使用要为其配置参数的 PCN 或 SCN 服务器的 Web 界面。

配置服务器上的日期和时间

如果您使用分布式解决方案和多租户模式，请使用要为其配置参数的 PCN 或 SCN 服务器的 Web 界面。

要配置服务器上的日期和时间。

1. 在应用程序 Web 界面窗口中，选择**设置**部分的**日期和时间**子部分。
2. 在“**时区**”下拉列表中，选择 Central Node 服务器的物理位置时区。
3. 在“**NTP 服务器**”下，指定“**最大数据包传输时间**”设置的值，限制从 Central Node 服务器向 NTP 服务器传送数据包所需的最大时间。

   默认设置为 5 秒。
4. 在**NTP 服务器** 部分:
   - 如果您要添加一个新的 NTP 服务器:
     a. 单击**添加**。
     b. 在打开的字段中，输入 NTP 服务器的 IP 地址或域名。
     c. 单击字段右侧的按钮。
   - 如果您想要编辑 NTP 服务器的 IP 地址或域名，请单击包含服务器的行中的按钮。
   - 如果您想要删除一个 NTP 服务器，请单击包含服务器的行中的按钮。
5. 单击**应用**。

将配置服务器上的日期和时间。

生成或上传服务器的 TLS 证书

如果您已在使用服务器 TLS 证书，则生成或上传新证书会导致当前使用的证书被删除并替换为新证书。

在使用旧证书的所有地方都必须输入新证书的数据。

如果您替换 TLS 证书，您将需要:

- 重新授权 Central Node 上的邮件 Sensor (KSMG、KLMS)。
- 重新配置 Central Node、PCN、SCN 与 Sandbox 的连接。
- 重新配置从 Endpoint Agent 到 Sensor 的流量转发以及与 Endpoint Agent 的受信任连接。

请确保删除所有 Endpoint Agent 主机隔离规则。与隔离主机的连接将丢失，您将无法管理它们。

您可以在 Central Node 服务器的 Web 界面中生成新证书或上传您独立创建的证书。

如果您使用分布式解决方案和多租户模式，请使用要为其配置参数的 PCN 或 SCN 服务器的 Web 界面。

要为 Central Node 服务器生成 TLS 证书：

1. 使用管理员凭据登录 Kaspersky Anti Targeted Attack Platform Web 界面。
2. 在应用程序 Web 界面窗口中，选择**设置**部分的**证书**子部分。
3. 在**服务器证书**部分，单击**生成和导出**。
   这将打开操作确认窗口。
4. 单击**是**。

Kaspersky Anti Targeted Attack Platform 生成新的 TLS 证书。页面会自动刷新。

与邮件传感器、Sandbox 组件和 Kaspersky Endpoint Agent 应用程序的通信将被中断，直到重新授权。

您可以选择自行准备 TLS 证书并使用 Kaspersky Anti Targeted Attack Platform Web 界面上传。

准备上传的 TLS 证书文件必须满足以下要求：

- 文件必须包含证书本身和用于连接的私人加密密钥。
- 文件必须是 PEM 格式。

  该应用程序不支持其他格式的证书。

  如果您准备了其他格式的证书，则必须将其转换为 PEM 格式。
- 私钥长度必须为 2048 位或更长。

要获取准备 TLS 证书进行导入的更多详细信息，请参阅 Open SSL 文档。

在要将证书上传到的 PCN 或 SCN 服务器的 Web 界面中上传 TLS 证书。

要使用 Kaspersky Anti Targeted Attack Platform Web 界面上传独立准备的 TLS 证书：

1. 使用管理员凭据登录 Kaspersky Anti Targeted Attack Platform Web 界面。
2. 在应用程序 Web 界面窗口中，选择**设置**部分的**证书**子部分。
3. 在**服务器证书**部分，单击**上传**。
   这将打开文件选择窗口。
4. 选择要下载的 TLS 证书文件，然后单击**打开**按钮。
   这将关闭文件选择窗口。

TLS 证书已添加到 Kaspersky Anti Targeted Attack Platform。

与邮件传感器、Sandbox 组件和 Kaspersky Endpoint Agent 应用程序的通信将被中断，直到重新授权。

下载服务器的 TLS 证书

如果您使用分布式解决方案和多租户模式，请使用要为其配置参数的 PCN 或 SCN 服务器的 Web 界面。

要下载服务器的 TLS 证书：

1. 在应用程序 Web 界面窗口中，选择**设置**部分的**证书**子部分。
2. 在**服务器证书**部分，单击**下载**。

   服务器证书文件将被保存在浏览器下载文件夹中。

服务器的 FQDN 设置

如果您使用分布式解决方案和多租户模式，请使用要为其配置参数的 PCN 或 SCN 服务器的 Web 界面。

若要设置服务器的 FQDN：

1. 在程序 Web 界面窗口中，选择**设置**部分的**网络设置**子部分。
2. 在**服务器名称 (FQDN)**字段中，输入服务器的完整域名。
   以 FQDN 格式指定服务器名称（例如：`host.domain.com` 或 `host.domain.subdomain.com`）。
3. 单击**应用**。

   将分配服务器名称。

配置 DNS 设置

如果您使用分布式解决方案和多租户模式，请使用要为其配置参数的 PCN 或 SCN 服务器的 Web 界面。

要配置 DNS：

1. 在程序 Web 界面窗口中，选择**设置**部分的**网络设置**子部分。
2. 在**DNS 设置**组中，在**DNS 服务器**字段中输入 DNS 服务器的 IP 地址。
3. 单击**应用**。

   这将配置 DNS 设置。

配置网络接口的设置

如果您使用分布式解决方案和多租户模式，请使用要为其配置参数的 PCN 或 SCN 服务器的 Web 界面。

配置网络接口：

1. 在程序 Web 界面窗口中，选择**设置**部分的**网络设置**子部分。
2. 选择要配置其设置的网络接口。
   这将打开**编辑网络接口**窗口。
3. 在**状态**设置组中，选择以下选项之一：
   - **已禁用**。
   - **已启用，使用 DHCP 服务器**，如果您希望将从 DHCP 服务器接收到的设置用于网络接口。
   - **已启用，手动配置**，如果您希望使用手动配置的网络接口。
4. 如果您选择了**已启用，手动配置**，指定以下参数的值：
   a. 在**IP**字段中，输入网络接口的 IP 地址。
   b. 在**子网掩码**字段中，指定网络接口的子网掩码。
   c. 在**网关**文本框中，输入网关的 IP 地址。
5. 单击**保存**。

将配置网络接口的设置。

配置默认网络路由

如果您使用分布式解决方案和多租户模式，请使用要为其配置参数的 PCN 或 SCN 服务器的 Web 界面。

配置默认网络路由：

1. 在程序 Web 界面窗口中，选择**设置**部分的**网络设置**子部分。
2. 在**网络路由**设置组的**网络接口**下拉列表中，选择要为其配置网络路由的网络接口。
3. 在**网关**文本框中，输入网关的 IP 地址。
4. 单击**应用**。

将配置默认网络路由。

配置代理服务器连接设置

如果您使用分布式解决方案和多租户模式，请使用要为其配置参数的 PCN 或 SCN 服务器的 Web 界面。

要配置代理服务器连接：

1. 在应用程序 Web 界面窗口中，选择“**设置**”部分的“**网络设置**”子部分。
2. 在代理服务器设置组中，将切换开关设置为已启用。
3. 在**主机**字段中，指定邮件服务器的 URL 或 IP 地址。
4. 在**端口**字段中，指定用于连接到代理服务器的端口。
5. 在**用户名称**字段中，指定用于代理服务器进行身份验证的用户名。
6. 在**密码**字段中，指定用于在代理服务器上进行身份验证的密码。
7. 在连接到本地地址时，如果您不想使用代理服务器，请选择**跳过本地地址的代理服务器** 复选框。
8. 单击**应用**。

   将配置代理服务器连接设置。

   如果在保存设置时发生错误，请将“**使用代理服务器**”拨动开关设置到“**已禁用**”，然后将其设置回“**已启用**”，然后点击“**应用**”按钮。

配置邮件服务器连接

如果您使用分布式解决方案和多租户模式，请使用要为其配置参数的 PCN 或 SCN 服务器的 Web 界面。

该应用程序可以发送有关警报和系统性能的通知。为此，您必须配置用于发送通知的服务器的设置。

要配置用于发送通知的服务器：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**通知**子部分。
2. 前往**邮件服务器配置**选项卡。
3. 在**主机**字段中，指定邮件服务器的 IP 地址。
4. 在**端口**字段中，指定连接到邮件服务器的端口。
5. 在**电子邮件发件人**字段中，指定发送通知的电子邮件地址。
6. 如果您想要在邮件服务器上启用身份验证，请选择**使用邮件收件人的 SMTP 身份验证**复选框。

7. 在**用户名称**字段中，指定用于在用来发送通知的服务器上进行身份验证的用户名。
8. 在**密码**字段中，指定用于在用来发送通知的服务器上进行身份验证的密码。
9. 发送通知时，如果您想要发送 TLS 加密，请选择**使用 TLS 加密**复选框。
10. 如果您想要验证邮件服务器的证书，请选择**验证 TLS 加密**复选框。
    证书指纹字段显示邮件服务器证书的指纹。

    如果未选择**验证 TLS 加密**复选框，应用程序将考虑信任邮件服务器的任意证书。

11. 单击**应用**。

将配置用于发送通知的服务器的设置。

管理流量节省设置

应用程序可以保存注册事件时收到的流量。在注册启用流量节省的事件时，流量将保存在 Central Node 服务器的数据库中。应用程序还可以根据流量下载请求，使用临时流量转储文件直接将流量保存在服务器数据库中。

应用程序以块的形式存储流量数据。如果某个流量块与多个事件相关联（对于短时间内记录的事件），则该流量块不会在数据库中重复。

要管理在服务器数据库中保存流量的设置：

1. 在应用程序 Web 界面窗口中选择**Sensor 服务器**部分。
2. 单击相关 Central Node 组件的卡片。
   这将打开一个窗口，其中包含有关组件的信息。
3. 单击**"编辑"**。
4. 转到"**常规**"选项卡。
5. 在"**事件的流量**"下，在"**最大流量**"字段中指定要保存的最大流量。
   您可以选择大小限制的计量单位：**MB** 或 **GB**。
   编辑值时，还需要考虑到所有大小限制的总和不得超过为服务器指定的最大存储容量。
6. 单击"**保存**"按钮。

流量节省设置已修改。

管理保存流量转储文件的设置

该应用程序将通过监控点接收的流量保存为流量转储文件。应用程序使用这些文件来分析传入流量。您还可以使用这些文件在应用程序中执行以下操作：

- 管理网络交互图时下载流量
- 下载网络会话流量
- 下载事件的流量（流量转储文件可让您加载事件的流量，即使相关事件类型的流量保存功能被禁用）

流量转储文件保存在具有 Sensor 组件的服务器的内部存储中。如果您使用带有嵌入式 Sensor 的 Central Node 组件，流量转储文件将保存在 Central Node 服务器的内部存储中。

应用程序临时存储流量转储文件。当流量到达时，如果文件的总大小接近存储设置的限制，应用程序会自动从存储中删除最旧的流量转储文件。您可以配置在内部存储中存储流量的设置。

要配置将流量转储文件保存到内部存储：

1. 在应用程序 Web 界面窗口中选择**Sensor 服务器**部分。
2. 单击相关 Central Node 组件的卡片。

   这将打开一个窗口，其中包含有关组件的信息。
3. 单击**"编辑"**。
4. 转到"**常规**"选项卡。
5. 如有必要，在"**过滤存储的流量**"部分，启用过滤并输入基于网络数据包的地址设置使用 Berkeley Packet Filter (BPF) 技术的过滤表达式。

   过滤可以通过丢弃与过滤器不匹配的网络数据包来减少存储的流量的大小。但是，如果您依赖过滤，请考虑过滤后的流量可能无法提供应用程序进行高质量流量分析所需的所有数据。您需要以这样的方式配置过滤，以便应用程序分析流量所需的所有网络数据包都保存在流量转储文件中。
6. 在"**流量转储文件**"下，使用"**最大卷**"设置来设置存储的流量转储文件的大小限制。

   您可以选择大小限制的计量单位：**MB** 或 **GB**。

   在编辑值时，还需要考虑接收的流量总量、接收速率以及所有大小限制的总和不得超过节点指定的最大存储容量这一事实。
7. 单击"**保存**"。

已配置将流量转储保存到内部存储中。

选择扫描 Sandbox 中的对象时要使用的操作系统

您可以选择一组操作系统，它们将被用于生成使用 Sandbox 组件扫描对象的任务。在 Sandbox 服务器上，您必须安装具有与配置集匹配的操作系统的虚拟机。

要选择操作系统集：

1. 在应用程序 Web 界面窗口中选择**Sandbox 服务器**部分。
2. 前往**设置**选项卡。
3. 在**操作系统集合**下面，选择以下选项之一：
   - **Windows 7、Windows 10**。
   - **CentOS 7.8、Windows 7、Windows 10**。
   - **Astra Linux 1.7、Windows 7、Windows 10**。
   - **自定义**。
4. 如果您选择了**自定义**， 在**集合组成**下面，选择要包含在该集合中的操作系统旁边的复选框。

   如果 Sandbox 服务器上安装了具有这些操作系统的虚拟机，则自定义操作系统将显示在列表中。预设操作系统始终显示在列表中，但如果未部署运行这些操作系统的虚拟机，则**未知**状态会显示在操作系统名称旁边。

Kaspersky Anti Targeted Attack Platform 将根据选定的集合创建扫描 Sandbox 中对象的任务。

如果 Sandbox 服务器上安装的操作系统集与 Central Node 服务器上选择的操作系统集不匹配，则该 Sandbox 服务器不会发送对象以进行扫描。如果有多个 Sandbox 服务器连接到 Central Node 服务器，则应用程序会将对象发送到其安装的操作系统与 Central Node 上选择的集合相匹配的 Sandbox 服务器。

您可以在使用应用程序的过程中更改操作系统集。在这种情况下，您需要确保 Sandbox 服务器的配置满足硬件要求。

在分布式解决方案和多租户模式下，PCN 服务器上配置的操作系统集的设置不会被应用于连接到该 PCN 服务器的 SCN 服务器。您可以单独为每个 PCN 和 SCN 服务器选择操作系统集。

密码策略

您可以为 Kaspersky Anti Targeted Attack Platform 的用户配置密码策略：在应用程序 Web 界面中第一次成功身份验证后和/或定期强制更改密码。

这些策略适用于所有“**KATA 用户账户**”账户类型的 Kaspersky Anti Targeted Attack Platform 用户，无论分配了什么角色。

首次身份验证成功后强制更改密码

如果启用此功能，则密码将根据以下情况更改：

1. 管理员创建一个用户账户。
2. Kaspersky Anti Targeted Attack Platform Web 界面中的用户身份验证。
3. 该用户下次登录 Web 界面时，应用程序会提示用户更改账户密码。旧密码将无效。

用户首次登录应用程序主 Web 界面被视为首次身份验证。如果用户返回并登录到尺寸管理的 Web 界面或应用程序的管理员菜单，则不会显示任何密码更改提示。如果用户账户用于将 SCN 连接到 PCN，则不会显示密码更改提示。

定期密码更改

如果启用了定期密码更改，则应用程序会在管理员设置的期限到期后提示用户更改密码。倒计时从更改账户密码的那一刻开始，并针对每个用户单独进行跟踪。

分布式解决方案和多租户模式

在分布式解决方案和多租户模式下，PCN 上指定的密码策略设置应用于 SCN。

首次身份验证成功后强制更改密码

有关此功能的详细信息，请参阅“*密码策略*”部分。

要启用在第一次成功身份验证后强制更改密码：

1. 在应用程序 Web 界面窗口中选择“**设置**”部分。
2. 前往“**身份验证策略**”选项卡。
3. 在“**首次身份验证后更改密码**”部分，设置“**请求密码更改**”切换开关至“**已启用**”。
4. 单击**应用**。

第一次身份验证后强制更改密码被启用。

强制定期更改密码

有关此功能的详细信息，请参阅“*密码策略*”部分。

要启用并配置强制定期更改密码：

1. 在应用程序 Web 界面窗口中选择“**设置**”部分。
2. 前往“**身份验证策略**”选项卡。
3. 在“**定期更改密码**”部分，设置“**请求密码更改**”切换开关至“**已启用**”。
4. 在“**在此时间后更改密码**”字段中，输入您想要在多少天后更改密码。
5. 单击**应用**。

指定期限后强制更改密码被启用并配置。

管理 Sensor 组件

Sensor 组件从网络流量和邮件流量接收数据。

您可以在同一服务器或不同服务器上安装 Sensor 和 Central Node 组件。安装在独立服务器上的 Sensor 组件必须连接到具有 Central Node 组件的服务器。如果您使用分布式解决方案和多租户模式，请按照以下步骤连接要连接组件的 PCN 或 SCN 服务器上的 Sensor 组件。

不支持在分布式解决方案和多租户模式下使用 PCN 对 Sensor 组件进行集中管理。Sensor 组件只能从连接组件的特定 Central Node 服务器进行配置。

将 Sandbox 组件连接到 Central Node

添加 Sensor 组件时，会在 Central Node 上生成一个配置包，其中包含 Sensor 组件的证书和配置数据。添加的组件使用 Sensor 组件的 Web 界面进行连接。该组件的 Web 界面允许您上传配置包并通过以下方式连接组件：

- 使用通信数据包。

  在这种情况下，配置包将保存为证书受密码保护的文件。这个文件被称为*通信数据包*。必须将通信数据包上传至 Sensor 组件的 Web 界面。上传通信数据包后，Sensor 组件自动连接到创建通信数据包的 Central Node。

- 通过网络自动传输。

  在这种情况下，配置包通过网络发送到具有 Sensor 组件的服务器的指定 IP 地址。Sensor 处理配置包，基于它生成证书签名请求 (CSR)，并将此请求发送到 Central Node 组件。收到 CSR 后，CSR 的指纹会以字符序列的形式显示在 Kaspersky Anti Targeted Attack Platform 的 Web 界面上。相同的指纹同时显示在 Sensor 组件的 Web 界面上。终止连接之前必须确保指纹相同。

如果 Central Node 和 Sensor 组件之间的连接是在受信任介质之外建立的，为了保护连接免遭流量拦截，您需要使用支持您所在国家/地区批准的加密算法的外部加密信息保护设施。如果组件通过受信任介质连接，例如，可以阻止第三方访问的服务器机架内的跳线，则无需使用外部加密信息保护设施。

通过网络自动添加和连接 Sensor 组件

要通过网络自动连接 Sensor 组件：

1. 在应用程序 Web 界面窗口中选择**Sensor 服务器**部分。
2. 单击“**添加 Sensor**”。

   这将打开“**添加新 Sensor**”窗口。
3. 转到**“通过网络自动**”选项卡。
4. 在“**Sensor 名称**”字段中，输入要连接的 Sensor 组件的名称。

   与 Central Node 的连接建立后，带有组件的 Web 界面页面的浏览器选项卡的标题将显示您在此步骤配置的名称。
5. 在“**服务器地址**”字段中，输入要连接 Sensor 组件的 Central Node 服务器的 IP 地址。

   如果 Central Node 部署为集群，则需要输入集群中**配置为从 SPAN 端口接收镜像流量的**处理服务器的 IP 地址。

   您可以在安装组件时启用镜像流量的接收。如果您在安装阶段禁用了流量接收：

   1. 通过 SSH 或使用终端进入服务器的任何处理服务器的管理控制台。
   2. 运行以下命令：

      ```
      kata-enable-span
      ```

      将启用从 SPAN 端口接收镜像流量。
6. 在“**Sensor IP 地址**”字段中，输入要连接到 Central Node 组件的 Sensor 组件服务器的 IP 地址。

   应用程序与安装了 Sensor 组件的服务器建立连接，且应用程序的 Web 界面上会显示一个提示，要求您确认收到的证书签名请求的指纹。
7. 在任何允许访问 Sensor 服务器的计算机上，启动命令行解释器。
8. 运行以下命令：

   ```
   ssh -4 -L 9444:localhost:9444 admin@<具有 Sensor 组件的服务器的 IP 地址>
   ```

   如果运行命令后出现“*Corrupted MAC on input. ssh_dispatch_run_fatal: Connection to <Sensor 服务器的 IP 地址> port 22: message authentication code incorrect*”错误，请运行以下命令：

   ```
   ssh -4 -L 9444:localhost:9444 admin@<具有 Sensor 组件的服务器的 IP 地址> -o "MACs hmac-sha2-256"
   ```
9. 在浏览器的地址栏中输入：https://localhost:9444。

   浏览器中显示 Sensor 组件的 Web 界面。Web 界面显示一条消息，其中包含有关发送到 Central Node 组件的证书签名请求的指纹的信息。

10. 确保代表证书请求指纹的字符序列在 Sensor 和 Central Node 组件的 Web 界面中相同。

11. 在应用程序 Web 界面上，点击按钮确认收到的证书签名请求的指纹。

    Sensor 组件与 Central Node 组件相连接，之后在 Sensor 和 Central Node 组件的 Web 界面中就会出现连接信息。

使用通信数据包连接 Sensor 组件

要使用通信数据包连接 Sensor 组件：

1. 在应用程序 Web 界面窗口中选择**Sensor 服务器**部分。

2. 单击“**添加 Sensor**”。

   这将打开“**添加新 Sensor**”窗口。

3. 在“**Sensor 名称**”字段中，输入要连接的 Sensor 组件的名称。

   与 Central Node 的连接建立后，带有组件的 Web 界面页面的浏览器选项卡的标题将显示您在此步骤配置的名称。

4. 在“**服务器地址**”字段中，输入要连接 Sensor 组件的 Central Node 服务器的 IP 地址。

   如果 Central Node 部署为集群，则需要输入集群中**配置为从 SPAN 端口接收镜像流量的**处理服务器的 IP 地址。

   您可以在安装组件时启用镜像流量的接收。如果您在安装阶段禁用了流量接收：

   1. 通过 SSH 或使用终端进入服务器的任何处理服务器的管理控制台。

   2. 运行以下命令：

      ```
      kata-enable-span
      ```

      将启用从 SPAN 端口接收镜像流量。

5. 在“**Sensor IP 地址**”字段中，输入要连接到 Central Node 组件的 Sensor 组件服务器的 IP 地址。

6. 在“**通信数据包中的证书加密**”部分中设置您想要使用的证书保护密码。

   密码必须满足以下要求：

   - 包含 8 到 256 个 ASCII 字符。
   - 包含一个或多个拉丁字母的大写字母。
   - 包含一个或多个拉丁字母的小写字母。
   - 包含一个或多个数字。
   - 不包含连续四个或更多相同的字符。

7. 单击“**创建通信数据包**”。您的浏览器保存了下载的文件。根据您的浏览器的设置，屏幕上可能会显示一个窗口，您可以在其中指定下载文件的路径和名称。

8. 将保存的通信数据包文件放置在任何允许访问 Sensor 服务器的计算机上。

9. 在放置通信数据包文件的计算机上，启动命令行解释器。

10. 运行以下命令：

    ```
    ssh -4 -L 9444:localhost:9444 admin@<具有 Sensor 组件的服务器的 IP 地址>
    ```

    如果运行命令后出现“*Corrupted MAC on input. ssh_dispatch_run_fatal: Connection to <Sensor 服务器的 IP 地址> port 22: message authentication code incorrect*”错误，请运行以下命令：

    ```
    ssh -4 -L 9444:localhost:9444 admin@<具有 Sensor 组件的服务器的 IP 地址> -o "MACs hmac-sha2-256"
    ```

11. 在浏览器的地址栏中输入：https://localhost:9444。

12. 在 Sensor Web 界面页面上，单击“**选择文件**”。

    这将打开用于选择文件的标准浏览器窗口。

13. 指定通信数据包的路径。

14. 单击“打开文件”按钮。

15. 文件上传完成后，输入您在本说明的第 6 步中设置的证书密码。

    Sensor 组件与 Central Node 组件相连接，之后在 Sensor 和 Central Node 组件的 Web 界面中就会出现连接信息。

删除 Sensor 组件

您可以从应用程序中删除该组件。删除组件后，所有为此组件配置的集成设置都将被删除，并且不再接收或处理数据。

如有必要，您可以将已删除的组件重新连接到 Central Node。

要删除组件：

1. 在应用程序 Web 界面窗口中选择**Sensor 服务器**部分。

2. 单击相关组件的卡片。

   这将打开一个窗口，其中包含有关组件的信息。

3. 单击**删除**。

组件已删除。

管理 Sensor 组件的证书

本节介绍如何管理 Sensor 组件的 TLS 证书。

证书可以在应用程序管理员菜单中进行管理。

在 Sensor 服务器的管理员菜单中为 Sensor 服务器生成 TLS 证书

要为具有 Sensor 组件的服务器创建 TLS 证书，请在 Sensor 服务器的管理员菜单中执行以下操作：

1. 在管理员菜单的主窗口中，选择**程序设置**。
2. 按 **ENTER** 键。
   这将打开管理员菜单的下一个窗口。
3. 选择**管理服务器证书**。
4. 按 **ENTER** 键。
   这将打开**证书管理**窗口。
5. 在窗口的下部，选择**新建**。
6. 按 **ENTER** 键。
   这将打开一个窗口，其中包含有关新建证书的信息。
7. 单击**继续**。
   这将打开操作确认窗口。
8. 单击**生成**。
   证书创建开始。
9. 证书创建完成后，按 **ENTER** 键。
   这将打开一个窗口，其中包含已安装证书的信息。
10. 单击**继续**。
    这将打开操作确认窗口。
11. 单击**确定**。

将创建证书。先前安装的证书的数据被覆盖。

在 Sensor 服务器的管理员菜单中上传您自己的 TLS 证书

您可以准备自己的 TLS 证书并使用 SCP 将其上传到 Sensor 服务器。要获取通过 SCP 协议上传文件的方法的更多详细信息，请参阅您要上传其 TLS 证书的计算机上安装的操作系统文档。

准备上传到服务器的 TLS 证书文件必须满足以下要求：

- 文件必须包含证书本身和用于连接的私人加密密钥。
- 文件必须是 PEM 格式。
- 文件名必须为 kata.pem。
- 私人密钥长度必须为 2048 位或更长。

要获取准备 TLS 证书进行导入的更多详细信息，请参阅 Open SSL 文档。

要使用 SCP 将您自己的 TLS 证书上传到 Sensor 服务器，请在计算机的 SCP 界面中执行以下操作（示例中使用 Linux）：

1. 运行以下命令：`scp kata.pem admin@<具有 Sensor 组件的服务器的 IP 地址>:`
2. 在密码提示处，输入用于管理 Sensor 服务器的管理员菜单的管理员密码，此密码是在安装时设置的。

TLS 证书被上传到 Sensor 服务器。

要在 Sensor 服务器上应用上传的 TLS 证书，请在 Sensor 服务器的管理员菜单中执行以下操作：

1. 在管理员菜单的主窗口中，选择**程序设置**。
2. 按 **ENTER** 键。
   这将打开管理员菜单的下一个窗口。
3. 选择**管理服务器证书**。
4. 按 **ENTER** 键。
   这将打开**证书管理**窗口。
5. 在窗口的下部，选择“**从文件安装**”。
6. 按 **ENTER** 键。

将应用证书。先前安装的证书的数据将被覆盖。

将 Sensor 服务器的 TLS 证书下载到您的计算机

您可以将 TLS 证书从 Sensor 服务器下载到任何可以通过 SCP 协议连接到 Sensor 服务器的计算机。要获取通过 SCP 协议上传文件的方法的更多详细信息，请参阅您要将 TLS 证书下载到的计算机上安装的操作系统文档。

要通过 SCP 协议从具有 Sensor 组件的服务器下载 TSL 证书，请在用于处理 SCP 协议的计算机界面中执行以下操作（以 Linux 操作系统为例）：

1. 运行以下命令：`scp admin@<具有 Sensor 组件的服务器的 IP 地址>:ssl/kata.crt.`
2. 在密码提示处，输入用于在具有 Sensor 组件的服务器的管理员菜单中工作的管理员密码，此密码是在安装时设置的。

TLS 证书将从带有 Sensor 组件的服务器下载到当前目录。

登录 Sensor 组件的 Web 界面

Sensor Web 界面位于托管 Sensor 组件的服务器上。

Sensor Web 界面被保护免受 **CSRF 攻击**，并且仅当用户的浏览器提供 HTTP POST 请求的 Referrer 头信息时才运行。确保用于 Sensor Web 界面的浏览器不会修改 HTTP POST 请求的 Referrer 头信息。如果与 Web 界面的连接是通过您组织的代理服务器建立的，请检查设置并确保代理服务器不会修改 HTTP POST 请求的 Referrer 头信息。

跨站请求伪造（也称为“XSRF 攻击”）。利用 HTTP 协议的漏洞攻击网站用户。这种攻击使得黑客能够打着授权用户的幌子在易受攻击的网站中执行操作。例如，在易受攻击的网站中，黑客可以打着授权用户的幌子秘密地向外部支付系统的服务器发送请求，以便将资金转移到黑客的账户。

要开始使用 Sensor 应用程序的 Web 界面：

在任何允许访问 Sensor 服务器的计算机上的浏览器中，在浏览器的地址栏中输入：https://<带有 Sensor 组件的服务器的 IP 地址> :<9443>。

浏览器中显示 Sensor 组件的 Web 界面。带有 Web 界面页面的浏览器选项卡的名称包含 Sensor 组件的名称，该名称是在组件连接到 Central Node 时指定的。

在 Sensor 组件的 Web 界面中，您可以执行以下操作：

- 上传通信数据包，使该组件与 Central Node 组件建立连接。
- 当组件通过网络自动连接到 Central Node 时，查看证书签名请求的指纹，并将其与 Kaspersky Anti Targeted Attack Platform Web 界面中的指纹进行比较。
- 查看组件与 Central Node 的连接状态。

更改服务器名称

要重命名 Central Node 服务器：

1. 在应用程序 Web 界面窗口中选择**Sensor 服务器**部分。
2. 单击相关 Sensor 组件的卡片。
   这将打开一个窗口，其中包含有关组件的信息。
3. 单击**“编辑”**。
4. 转到**“常规”**选项卡。

5. 在“**Sensor 名称**”字段中，输入新名称。

   该名称必须是唯一的（不能与其他组件的名称相同）并且最多可包含 100 个字符。您可以使用英文字母、数字、空格以及特殊字符：_ 和 -（例如，Server_1）。名称必须以空格以外的任何有效字符开始和结束。

6. 单击“**保存**”按钮。

服务器将被重命名。

管理监控点

Kaspersky Anti Targeted Attack Platform 使用监控点接收和处理镜像 SPAN 流量。可以为 Central Node 和 Sensor 组件添加和删除监控点。

每个监控点必须与一个网络接口相关联，该接口接收来自某个网段的流量副本。若要添加监控点，可以使用满足以下条件的网络接口：

- 网络接口类型：以太网。
- MAC 地址：不是 00:00:00:00:00:00。
- 网络接口专门用于接收网络流量的副本，不用于其他目的（例如，连接已安装应用程序组件的服务器）。

可以启用或禁用监控点。您可以禁用监控点以暂时停止监控网络接口上接收流量副本的网段。当需要恢复监控时，重新启用该监控点即可。

禁用或删除监控点后，应用程序可能会在一段时间内记录涉及该监控点的事件。这是因为当 Central Node 组件负载较高时，处理传入流量可能会出现延迟。

监控点详情显示在该监控点所关联的网络接口的卡片中。若有必要，可以重命名监控点。

添加监控点

为了在节点的网络接口上接收和处理来自网络的流量，需要在该网络接口上添加一个监控点。

要向网络接口添加监控点：

1. 在应用程序 Web 界面窗口中选择**Sensor 服务器**部分。
2. 在相关网络接口的卡片中，点击“**添加监控点**”链接。

   这将打开添加监控点的窗口。

3. 在“**监控点名称**”字段中，输入监控点的名称。

   您可以使用拉丁字母的大写和小写字母、数字以及 _ 和 - 字符。

监控点名称必须满足以下要求：

- 是唯一的（未分配给任何其他监测点）。
- 包含 1 至 100 个字符。

4. 单击**“添加监控点”**。

监控点被添加。

重命名监控点

您可以重命名与网络接口关联的监控点。

> 监控点的新名称反映在重命名后记录的事件中。先前记录的事件保留监控点的旧名称。

要重命名监控点：

1. 在应用程序 Web 界面窗口中选择**Sensor 服务器**部分。
2. 单击相关网络接口的卡。
3. 这将打开一个窗口，其中包含有关网络接口的信息。
4. 单击**“编辑”**。
5. 在“**监控点名称**”字段中，输入新名称。
   您可以使用拉丁字母的大写和小写字母、数字以及 _ 和 - 字符。
   监控点名称必须满足以下要求：
   - 是唯一的（未分配给任何其他监测点）。
   - 包含 1 至 100 个字符。
6. 单击“**保存**”。

监控点被重新命名。

启用监控点

如果监控点被禁用，应用程序将不会接收或处理到达其网络接口的流量。如果要恢复接收和处理流量，则必须启用监控点。

您可以为一个组件或所有组件单独或一次性启用监控点。

只有具有管理员角色的用户才能启用监控点。

要启用监控点：

1. 在应用程序 Web 界面窗口中选择**Sensor 服务器**部分。
2. 执行以下操作之一：
   - 如果要启用单个监控点，在相关组件的卡片中，点击“**启用**”按钮。如果监控点被禁用，则此按钮可用。
   - 如果要启用所有监控点，在相关组件的卡片中，点击“**全部启用**”按钮。如果组件具有已禁用监控点的网络接口，则该按钮可用。
   - 如果要启用所有组件的所有监控点，请单击工具栏中的“**在所有节点上启用**”链接。
3. 等待更改应用。

   选定的监控点已启用。

禁用监控点

如果您想暂时停止接收和处理该监控点网络接口上的流量，您可以禁用该监控点。

您可以针对所有组件单独禁用监控点，也可以同时禁用所有监控点。

要禁用监控点：

1. 在应用程序 Web 界面窗口中选择**Sensor 服务器**部分。
2. 执行以下操作之一：
   - 如果要禁用单个监控点，请在相关组件的卡片中点击“**禁用**”按钮。监控点启用后该按钮可用。
   - 若想禁用所有监控点，在相关组件的卡片上，点击“**全部禁用**”按钮。如果组件具有已启用监控点的网络接口，则该按钮可用。
   - 如果要禁用所有组件的所有监控点，请单击工具栏中的“**在所有节点上禁用**”链接。
3. 等待更改得到应用。

   选定的监控点被禁用。

正在删除监控点

您可以删除与网络接口关联的监控点。如果网络接口不再用于接收流量，则可能需要删除监控点。

如果需要暂时停止接收监控点网络接口上的流量（例如在维护调试期间），可以禁用该监控点而不删除它。

> 在监控点删除之前从其接收到的流量不会从数据库中删除。此外，有关此监控点的信息保存在记录事件表中。

要删除监控点：

1. 在应用程序 Web 界面窗口中选择**Sensor 服务器**部分。
2. 单击相关网络接口的卡。
3. 这将打开一个窗口，其中包含有关网络接口的信息。
4. 单击“**删除**”。
   这将打开一个确认提示窗口。如果监控点已启用，应用程序将提示您禁用该监控点。
5. 在提示窗口中确认删除监控点。

该监控点已删除。

配置扫描文件的最大大小

如果您使用分布式解决方案和多租户模式，请使用要为其配置参数的 PCN 或 SCN 服务器的 Web 界面。

要配置扫描文件的最大大小：

1. 在应用程序 Web 界面窗口中选择**Sensor 服务器**部分。
2. 单击相关 Sensor 组件的卡片。
   这将打开一个窗口，其中包含有关组件的信息。
3. 单击**“编辑”**。
4. 转到“**其他**”选项卡。
5. 将**“设置大小限制”**切换开关设置为“**已启用**”。
6. 在“**计量单位**”字段中，选择一个计量单位。
7. 在“**空间**”字段中，输入文件允许的最大大小。
8. 单击**保存**。

将配置扫描文件的最大大小。

如果要将扫描文件的最大大小设置为大于 100 MB 的值：

1. 通过 SSH 协议或终端进入 Sensor 服务器的管理控制台。
2. 系统提示时，请输入管理员用户名和安装组件期间指定的密码。
3. 显示应用程序组件管理员菜单。
4. 选择技术支持模式。
5. 按 ENTER。

6. 这将打开技术支持模式确认窗口。

7. 确认您想要在技术支持模式下管理应用程序。为此，请选择“是”并按 ENTER。

8. 要查看当前扫描文件的大小限制，请运行以下命令：

```
docker exec $(docker ps -q -f name=nta_core) grep body-limit
/var/opt/kaspersky/kics4net/ids/client/templates/suricata.yaml.templ | grep -v '#'
```

9. 当前限制显示在 request-body-limit 和 response-body-limit 字段中。当前限制以字节为单位显示。

10. 要更改当前限制，请运行以下命令：

```
exec $(docker ps -q -f name=nta_core) sed -i 's/<以字节表示的先前值>/<以字节表示的新值>/'
/var/opt/kaspersky/kics4net/ids/client/templates/suricata.yaml.templ
```

11. 完成上述说明中的步骤 1-8。

您可以将扫描文件的最大大小设置为超过 100 MB。

配置 HTTP 数据包正文转储

如果您使用分布式解决方案和多租户模式，请使用要为其配置参数的 PCN 或 SCN 服务器的 Web 界面。

要配置 HTTP 数据包正文转储：

1. 在应用程序 Web 界面窗口中选择**Sensor 服务器**部分。

2. 单击相关 Sensor 组件的卡片。
这将打开一个窗口，其中包含有关组件的信息。

3. 单击**“编辑”**。

4. 转到“**其他**”选项卡。

5. 在“**转储 HTTP 正文**”部分中：

   - 如果要启用 HTTP 数据包正文转储，请将**“启用 http-body”**切换开关设置为“**已启用**”。
   默认情况下，切换开关位于**已禁用**位置。

   - 如果要禁用 HTTP 数据包正文转储，请将**“启用 http-body”**切换开关设置为“**已禁用**”。

6. 单击“**保存**”。

HTTP 数据包正文转储已启用或禁用。

配置通过 SMTP 与邮件服务器集成

如果您使用分布式解决方案和多租户模式，请使用要为其配置参数的 PCN 或 SCN 服务器的 Web 界面。

要配置通过 SMTP 与邮件服务器集成：

1. 在应用程序 Web 界面窗口中选择**Sensor 服务器**部分。
2. 单击相关 Sensor 组件的卡片。
   这将打开一个窗口，其中包含有关组件的信息。
3. 单击**"编辑"**。
4. 转到"**SMTP 集成**"选项卡。
5. 如果要通过 SMTP 启用与邮件服务器的集成，请将**"启用 SMTP 集成"**切换开关设置为"**已启用**"。
6. 在**目标域**字段中，指定邮件域或子域的名称。该应用程序将扫描被发送到指定域的邮箱的电子邮件。
   要禁用域或子域，请将其括在`!domain.tld`表单中。
   如果将邮件域名留为空白，应用程序将接收发送至任何电子邮件地址的邮件。
7. 在**客户端**字段中，指定允许应用程序通过 SMTP 协议进行交互的主机和/或子网掩码（采用 CIDR 表示法）的 IP 地址。
   要禁用主机或子网，请将地址括在`!host`表单中。
   如果将此字段留空，应用程序将收到以下消息：
   - 如果您在**目标域**字段中指定了电子邮件域，请从任何电子邮件地址发送。
   - 如果"**目标域**"字段中未指示域，则从与 Sensor 服务器位于同一子网中的邮件服务器发送。
8. 如果要设置允许接收邮件的最大大小，请将**"设置邮件大小"**切换开关设置为"**已启用**"。
9. 在"**计量单位**"字段中，选择一个计量单位。
10. 在"**空间**"字段中，输入文件允许的最大大小。
11. 如果要配置与邮件服务器的 SMTP 连接的 TLS 加密，请在"**客户端 TLS 安全级别**"下，选择下列选项之一：
    - **禁用 TLS 加密**。
      该应用程序不会使用与邮件服务器的连接的 TLS 加密。
    - **允许对传入消息进行 TLS 加密**。
      该应用程序将支持连接的 TLS 加密，但加密不是强制性的。
    - **要求对传入消息进行 TLS 加密**。
      该应用程序将仅通过加密通道接收消息。
12. 单击**下载 TLS 证书**按钮，将具有 Sensor 组件的服务器的 TLS 证书保存在浏览器下载文件夹中的计算机上。
    邮件服务器上的身份验证需要此证书。
13. 在**请求客户端 TLS 证书**设置组中，选择以下选项之一：
    - **不请求**。
      该应用程序不会验证邮件服务器的 TLS 证书。

- **请求**。
  该应用程序将从邮件服务器请求 TLS 证书（如果有）。
- **要求**。
  该应用程序将仅从具有 TLS 证书的邮件服务器接收消息。

14. 单击**保存**。

将配置通过 SMTP 与邮件服务器集成。该应用程序将根据定义的设置扫描通过SMTP协议接收的电子邮件。

如果您已将 Central Node 和 Sensor 组件部署为集群，则可以配置与邮件服务器的高可用性集成。

要配置与邮件服务器的高可用性集成：

1. 在 Central Node 集群对应域名的 DNS 服务器上配置轮询调度算法。
2. 在邮件服务器设置中指定此域名。

与邮件服务器的集成将根据域名进行配置。邮件服务器将与集群中的随机服务器进行通信。如果该服务器出现故障，邮件服务器将与集群中另一台健康的服务器进行通信。

对于集群配置中的应用程序 7.0 版本，在与邮件服务器集成时，发送电子邮件消息时可能会出现错误：“451 4.3.0 错误：队列文件写入错误”。

要解决该错误，请执行以下操作：

1. 通过 SSH 或使用终端进入任何集群服务器的管理控制台。
2. 系统提示时，输入管理员用户名和安装组件期间指定的密码。
   显示应用程序组件管理员菜单。
3. 在应用程序管理员菜单中，选择技术支持模式。
4. 按 ENTER。
   这将打开技术支持模式确认窗口。
5. 确认您想要在技术支持模式下管理应用程序。为此，请选择“是”并按 ENTER。
6. 运行以下命令：
   `for addr in <群集服务器的 IP 地址（用空格分隔）>; do nc -zv $addr 10025; done`
   服务器列表显示在控制台上。
7. 在应用程序的 Web 界面中，在上述说明的第 7 步中，指定在控制台上显示“`localhost [127.0.0.1] 10025 (?) open`”字符串的服务器的 IP 地址。

错误已解决。

如果您没有为任何集群服务器获取“`localhost [127.0.0.1] 10025 (?) open`”字符串，请联系技术支持。

在服务器上安装 7.0.3 版本的 Central Node 组件时，Kaspersky Anti Targeted Attack Platform 可能会拒绝通过 SMTP 接收的电子邮件。发送者可能会收到“连接被拒绝”错误。

要消除限制：

1. 通过 SSH 或终端登录相关 Central Node 服务器的管理控制台。
2. 系统提示时，输入管理员用户名和安装组件期间指定的密码。
   显示应用程序组件管理员菜单。
3. 在应用程序管理员菜单中，选择技术支持模式。
4. 按 ENTER。
   这将打开技术支持模式确认窗口。
5. 确认您想要在技术支持模式下管理应用程序。为此，请选择“是”并按 ENTER。
6. 运行以下命令：
   ```
   sudo -i
   ```
7. 运行以下命令：
   a. `docker exec $(docker ps -q -f name=preprocessor_span) supervisorctl restart preprocessor`
   b. `docker exec $(docker ps -q -f name=preprocessor_smtp) supervisorctl restart preprocessor`

限制已移除。

配置通过 ICAP 与代理服务器集成

通过 ICAP 与带有反馈的代理服务器集成，您可以防止恶意对象进入公司 LAN 并防止主机用户访问恶意或网络钓鱼网站。Kaspersky Anti Targeted Attack Platform 充当 ICAP 服务器，而您的代理服务器充当 ICAP 客户端。代理服务器将 ICAP 请求发送到 ICAP 服务器。ICAP 服务器运行扫描并将结果返回到代理服务器。如果检测到任何威胁，会向主机上的用户显示通知 HTML 页面。

通过 ICAP 与代理服务器集成时，存在一些限制。

启用和禁用通过 ICAP 与代理服务器集成

如果您使用分布式解决方案和多租户模式，请使用要为其配置参数的 PCN 或 SCN 服务器的 Web 界面。

使用独立代理服务器时，Kaspersky Anti Targeted Attack Platform 默认不提供 ICAP 流量加密或 ICAP 客户端身份验证。应用程序管理员必须采取措施，通过使用流量隧道或 iptables 确保代理服务器和 Kaspersky Anti Targeted Attack Platform 之间的网络连接安全。

要在安装了 Central Node 和 Sensor 组件的服务器上通过 ICAP 启用或禁用与代理服务器的集成：

1. 在应用程序 Web 界面窗口中选择**Sensor 服务器**部分。
2. 单击相关 Sensor 组件的卡片。
   这将打开一个窗口，其中包含有关组件的信息。
3. 单击**"编辑"**。
4. 转到"**ICAP 与代理服务器集成**"选项卡。
5. 执行以下操作：
   - 如果要通过 ICAP 启用与代理服务器的集成，请将**"启用 ICAP 集成"**切换开关设置为"**已启用**"。
   - 如果要通过 ICAP 禁用与代理服务器的集成，请将"**启用 ICAP 整合**"切换开关设置为"**已禁用**"。

通过 ICAP 与代理服务器集成被启用。

要在具有 Sensor 组件的单个服务器上通过 ICAP 启用或禁用与代理服务器的集成：

1. 通过 SSH 协议或终端进入 Sensor 服务器的管理控制台。
2. 系统提示时，请输入管理员用户名和安装应用程序期间设置的密码。
   这将打开 Sensor 组件的设置菜单。如果菜单未打开，请输入 `kata-admin-menu` 命令并按 **ENTER** 键。
3. 转至**程序设置** → **配置 ICAP 集成**部分。
   要选择一行，您可以使用 ↑、↓ 和 **ENTER** 键。所选行以红色突出显示。
4. 这将打开一个窗口，在该窗口中，选择**"已启用"**行并按 **ENTER** 键。
   [x]显示在**已启用**设置的右侧。
5. 在代理服务器的设置中，输入 **RESPMOD** 字段中的 URL。

通过 ICAP 将代理服务器和具有 Sensor 组件的单个服务器的集成得到配置。

如果您已将 Central Node 和 Sensor 组件部署为集群，则可以配置与代理服务器的高可用性集成。

要配置与代理服务器的高可用性集成：

1. 在 Central Node 集群对应域名的 DNS 服务器上配置轮询调度算法。
2. 在代理服务器设置中指定此域名。

与代理服务器的集成将根据域名进行配置。代理服务器将与集群中的随机服务器进行通信。如果该服务器出现故障，代理服务器将与集群中另一台健康的服务器进行通信。

启用或禁用 ICAP 流量实时扫描

如果您使用分布式解决方案和多租户模式，请使用要为其配置参数的 PCN 或 SCN 服务器的 Web 界面。

如果启用了通过 ICAP 与代理服务器的集成，您可以启用或禁用 ICAP 流量实时扫描。

如果启用 ICAP 流量实时扫描，Kaspersky Anti Targeted Attack Platform 会实时向 ICAP 客户端发送有关扫描对象的信息。这有助于防止下载恶意对象和单击不受信任的链接。

要在安装了 Central Node 和 Sensor 组件的服务器上启用或禁用 ICAP 流量实时扫描：

1. 在应用程序 Web 界面窗口中选择**Sensor 服务器**部分。
2. 单击相关 Sensor 组件的卡片。
   这将打开一个窗口，其中包含有关组件的信息。
3. 单击**"编辑"**。
4. 转到"**ICAP 与代理服务器集成**"选项卡。
5. 在**实时扫描**下面，选择以下选项之一：
   - **已禁用。**
     如果选择此选项，ICAP 流量实时扫描将被禁用。默认情况下选择此选项。
   - **已启用，标准 ICAP 流量扫描。**
     启用此类扫描后，将根据卡巴斯基安全网络的知识库检查文件和 URL 的信誉，并由 Sandbox 组件、反恶意软件引擎和 YARA 模块扫描文件。当文件正在被 Sandbox 组件扫描时，它们仍然可用。
   - **已启用，高级 ICAP 流量扫描。**
     启用此类扫描后，将根据卡巴斯基安全网络的知识库检查文件和 URL 的信誉，并由 Sandbox 组件、反恶意软件引擎和 YARA 模块扫描文件。当文件正在被 Sandbox 组件扫描时，它们不可用。
6. 在"**提取用户名**"下：
   如果要从 ICAP 服务器获取用户名，请将**"提取用户名"**切换开关字段设置为**"已启用"**。如果需要使用 Base64 解码，请选择"**使用 Base64 解码**"复选框。
7. 单击"**保存**"。

ICAP 流量的实时扫描被启用或禁用。

要在安装了 Sensor 组件的单个服务器上启用或禁用 ICAP 流量实时扫描：

1. 通过 SSH 协议或终端进入 Sensor 服务器的管理控制台。
2. 系统提示时，请输入管理员用户名和安装应用程序期间设置的密码。
   这将打开 Sensor 组件的设置菜单。如果菜单未打开，请输入 `kata-admin-menu` 命令并按 **ENTER** 键。

3. 转至**程序设置** → **配置 ICAP 集成**部分。

   要选择一行，您可以使用 ↑、↓ 和 **ENTER** 键。所选行以红色突出显示。

4. 这将打开一个窗口；在该窗口中，确保**[x]**显示在**已启用**设置的右侧。

5. 选择以下选项之一：

   - **禁用实时扫描**。

     如果选择此选项，ICAP 流量实时扫描将被禁用。默认情况下选择此选项。

   - **标准 ICAP 扫描**。

     启用此类扫描后，将根据卡巴斯基安全网络的知识库检查文件和 URL 的信誉，并由反恶意软件引擎和 YARA 模块扫描文件。

   - **高级 ICAP 扫描**。

     启用此类扫描后，将根据卡巴斯基安全网络的知识库检查文件和 URL 的信誉，并由 Sandbox 组件、反恶意软件引擎和 YARA 模块扫描文件。

6. 选择一个选项并按 **ENTER** 键。**(O)**显示在所选选项的右侧。

   要选择一行，您可以使用 ↑ 和 ↓ 键。所选行以红色突出显示。

7. 如果您启用了 ICAP 流量实时扫描并启用了高级扫描模式或标准扫描模式，请在代理服务器设置中的 **REQMOD**字段中指定 URL。

在具有 Sensor 组件的单个服务器进行 ICAP 流量实时扫描被启用或禁用。

如果您启用了 ICAP 流量的实时扫描，并且禁用了与代理服务器的集成，则扫描将不起作用。所有 ICAP 流量扫描设置均已保存。当您重新启用与代理服务器的集成时，ICAP 流量扫描也会被启用。

配置 ICAP 流量实时扫描

如果您使用分布式解决方案和多租户模式，请使用要为其配置参数的 PCN 或 SCN 服务器的 Web 界面。

只能在技术支持模式下才能配置在具有 Sensor 组件的独立服务器上进行实时 ICAP 流量扫描。要在技术支持模式下执行操作，我们建议联系技术支持。

您可以在具有 Central Node 和 Sensor 组件的服务器上配置 ICAP 流量实时扫描，以对数据进行防病毒扫描。扫描结果在通知 HTML 页面上向主机用户显示。

要配置 ICAP 流量实时扫描：

1. 在应用程序 Web 界面窗口中，选择**设置**部分的**ICAP 流量扫描**子部分。

   ICAP 流量扫描设置页面将显示。

   默认情况下，在**通知**下面，与以下事件对应的页面将得到加载：

   - 如果在用户请求的地址检测到威胁，则会显示在**链接被阻止**字段中上传的页面。

   - 如果在扫描文件中检测到威胁，则会显示在**文件已阻止**字段中上传的页面。

- 如果文件扫描开始，则会显示在**扫描文件**字段中上传的页面。如果文件安全，用户可以单击链接下载文件。
- 如果文件已扫描，但是该文件的存储时长已过期，则会显示在**文件已过期**字段中上传的页面。

默认情况下，分发包中的 HTML 页面会加载到 Kaspersky Anti Targeted Attack Platform 中。您可以上传自己的通知页面并配置它们的显示方式。通知页面的大小不得超过 1.5 MB。如果上传的通知页面大于1.5 MB，则会显示错误。

2. 在**文件块阈值**下面的**Sandbox 警报重要性**字段中，从下拉列表中选择一个值。根据卡巴斯基的专家意见，这些值对应于警报对计算机或公司网络安全可能产生的影响。

   此设置可以采用以下值之一：

   - **高** 对于高度重要的警报。默认情况下选择此选项。
   - **中** 对于中等重要性的警报。
   - **低** 对于低重要性警报。

3. 在**扫描超时**下面的**超时**字段中，指定在其后扫描文件链接被解除阻止并可以下载扫描文件的时间。

   默认值为 10 分钟。您可以设置任何大于 1 分钟的值。

4. 单击**应用**。

扫描使用指定的设置执行。

配置通知页面的显示

如果您使用分布式解决方案和多租户模式，请使用要为其配置参数的 PCN 或 SCN 服务器的 Web 界面。

在实时扫描 ICAP 流量时，Kaspersky Anti Targeted Attack Platform 可以对扫描的对象执行各种操作：阻止对 URL 的访问、阻止文件下载、阻止文件在扫描时被下载以及提供重新下载文件（如果扫描后文件的存储期限已过期）。当这些操作在进行时，将向尝试进行 URL 访问或文件下载请求的主机上的用户显示 HTML 通知页面。如果您想显示自己的页面而不是默认页面，您可以上传自己的自定义 HTML 页面。

上传通知页面：

1. 在应用程序 Web 界面窗口中，选择**设置**部分的**ICAP 流量扫描**子部分。
2. 在**通知**部分，单击您需要的字段之一旁边的**浏览**。
3. 这将打开一个窗口；在该窗口中，选择您的 HTML 页面。
4. 单击**打开**。

   您的页面已上传。

扫描文件事件的通知页面与其他通知页面不同，因为它包含下载文件的链接。如果想上传**扫描文件**通知页面，您必须在通知页面的源代码中添加已扫描文件下载链接。

示例：

```
<html>
<body>
<p>文件正在被扫描。扫描完成后，您将能够下载它，或者您将收到有关任何检测到的威胁的报告。</p>
<a href="{{ download_url }}">下载链接...</a>
</body>
</html>
```

配置 SPAN 端口镜像流量的记录

借助 Kaspersky Anti Targeted Attack Platform，您可以节省 SPAN 端口镜像流量，以便调查和检测企业 LAN 范围内的恶意活动。通过镜像流量记录，您可以对网络事件进行回顾分析并调查黑客的操作。流量以 PCAP 格式保存为转储。

要保存来自 SPAN 端口的镜像流量，请启用此类流量的记录，并在应用程序的 Web 界面或 Sensor 组件的管理员菜单中进行配置。您还可以选择用于接收流量的网络协议。

选择用于从 SPAN 端口接收镜像流量的网络协议

如果您使用分布式解决方案和多租户模式，请在 Sensor 组件连接到的 PCN 或 SCN 服务器的 Web 界面中执行配置操作。

要选择从 SPAN 端口接收镜像流量的网络协议：

1. 通过 SSH 协议或终端进入 Sensor 服务器的管理控制台。
2. 系统提示时，请输入管理员用户名和安装应用程序期间设置的密码。
   这将打开 Sensor 组件的设置菜单。如果菜单未打开，请输入 `kata-admin-menu` 命令并按 **ENTER** 键。
3. 转到**程序设置** → **配置流量捕获** → **设置捕获协议**部分，使用 ↑、↓ 和 **ENTER** 键。所选行以红色突出显示。
   这将打开一个窗口，您可以在其中启用或禁用从以下网络协议的 SPAN 端口接收镜像流量：
   - **DNS**
   - **FTP**
   - **HTTP**
   - **HTTP2**
   - **SMTP**
   - **SMB**
   - **NFS**

     要分析 NFS 流量，您必须挂载 NFS 分区并指定协议版本。

示例：

对于 NFS v.4：

```
mount -t nfs -o vers=4 -O uid=1000,iocharset=utf-8 <address>:/from/dir /to/dir
```

对于 NFS v.3：

```
mount -t nfs -o vers=3 -O uid=1000,iocharset=utf-8 <address>:/from/dir /to/dir
```

如果启用通过网络协议从 SPAN 端口接收镜像流量，则**[x]**将显示在网络协议名称的右侧。如果针对特定网络协议禁用从 SPAN 端口接收镜像流量，则**[ ]**将显示在协议名称的右侧。

默认情况下，对所有网络协议（**HTTP2** 除外）启用从 SPAN 端口接收镜像流量。

4. 如果要启用或禁用从特定网络协议的 SPAN 端口接收镜像流量，请使用 ↑、↓ 键然后按 **ENTER**。
5. 选择包含**应用并退出**的行，然后按 **ENTER**。

用于从 SPAN 端口接收镜像流量的网络协议被选择。

在与 Central Node 分开安装的 Sensor 组件的服务器上选择网络协议

如果您在将独立 Sensor 连接到 Central Node 之前选择了网络协议以从其 SPAN 端口获取镜像流量，并且想要在连接后更改这些设置，则您需要先执行更改设置之前的准备步骤，然后按照上述说明进行操作。

使用 Web 界面配置 SPAN 端口镜像流量的记录

如果您使用分布式解决方案和多租户模式，请使用要为其配置参数的 PCN 或 SCN 服务器的 Web 界面。

要启用并配置来自 SPAN 端口的镜像流量记录：

1. 连接并配置外部存储。
2. 在应用程序 Web 界面窗口中选择**Sensor 服务器**部分。
3. 单击相关 Sensor 组件的卡片。

   这将打开一个窗口，其中包含有关组件的信息。
4. 单击**“编辑”**。
5. 转到“**外部存储**”选项卡。

   如果未连接外部存储，则不会显示此选项卡。

   在“**外部存储**”部分，“**最旧的数据包**”字段显示外部存储中第一次保存的转储的日期和时间。“**最新数据包**”字段显示最后一次转储保存到外部存储的日期和时间。
6. 如果要使用外部存储，请将“**记录流量**”切换开关设置为“**已启用**”。

   默认情况下，切换开关位于**已禁用**位置。

7. 在“**保存流量的路径**”字段中，指定您希望应用程序保存流量转储的目录的路径。

8. 执行以下操作：

   a. 在“**最大存储大小**”下，指定将存储在存储中的流量转储的最大大小。

   如果存储中的转储大小超过指定值，最早的转储将被删除，其总大小等于新转储的大小。

   > 如果您减小最大转储存储大小，则最早的转储将被删除，其总大小等于设置的更改。

   b. 如果要限制流量中的数据捕获，请在**“捕获时的流量过滤”**下，将“**BPF 过滤**”切换开关设置为“**已启用**”。流量筛选可以减少转储存储中的转储大小并有利于流量分析。

   在“**BPF 过滤规则**”中，过滤规则。BPF 筛选规则以 libpcap 格式编写。有关语法的更多详细信息，请参阅 pcap-filter 手册页。

   筛选表达式示例：

   ```
   tcp port 102 or tcp port 502
   ```

   c. 如需配置流量转储存储时长，请在“**存储时长**”下，将“**启用存储时长**”切换开关设置为“**已启用**”。在“**存储时间（天）**”字段中，输入您要存储流量转储的天数。存储时间超过指定持续时间的流量转储将被从存储中删除。

   d. 单击“**保存**”。

将配置记录从 SPAN 端口接收的镜像流量。

使用 Sensor 组件的管理员菜单配置 SPAN 端口镜像流量的记录

要在 Sensor 组件的管理员菜单中启用镜像 SPAN 流量的记录，请执行以下操作：

1. 连接并配置外部存储。

2. 通过 SSH 协议或终端进入 Sensor 服务器的管理控制台。

3. 系统提示时，请输入管理员用户名和安装应用程序期间设置的密码。

   这将打开 Sensor 组件的设置菜单。如果菜单未打开，请输入`kata-admin-menu`命令然后按**`Enter`**。

4. 转到**程序设置** → **配置流量捕获**部分。

   要选择一行，您可以使用 ↑、↓ 和 **`Enter`** 键。所选行以红色突出显示。

5. 这将打开一个窗口，在该窗口中，选择**启用流量存储**行并按 **`Enter`** 键。

   [x]显示在该行标题的右侧。

   在带有 Sensor 组件的独立服务器上的原始网络流量记录将被启用。

6. 如有必要，编辑原始网络流量记录设置：

   a. 选择**流量存储大小**行然后按 **`Enter`** 键。这会打开一个窗口；在该窗口中，指定存储的原始流量转储的最大总大小（以 TB 为单位）。

   默认情况下，最小值设置为 100 GB。最大值为 1000000 TB。为了应用程序正确运行，连接的驱动器必须至少具有指定量的可用磁盘空间。如果在此字段中输入的数字超过连接的驱动器上的可用空间，则会显示错误。

b. 选择**确定**按钮然后按 **Enter** 键。

c. 选择**流量捕获 BPF 筛选**行然后按 **Enter** 键。这会打开一个窗口；在该窗口中输入筛选规则。BPF 筛选规则以 libpcap 格式编写。有关语法的更多详细信息，请参阅 pcap-filter 手册页。

筛选表达式示例：

```
tcp port 102 or tcp port 502
```

d. 选择**确定**按钮然后按 **Enter** 键。

e. 选择**流量存储持续时间（以天为单位）**行然后按 **Enter** 键。这会打开一个窗口；在该窗口中，输入原始网络流量转储在存储中的存储持续时间（以天为单位）。

f. 选择**确定**按钮然后按 **Enter** 键。

镜像 SPAN 流量的记录在 Sensor 组件的管理员菜单中配置。

配置通过 POP3 与邮件服务器集成

如果您使用分布式解决方案和多租户模式，请使用要为其配置参数的 PCN 或 SCN 服务器的 Web 界面。

要配置通过 POP3 与邮件服务器集成：

1. 在应用程序 Web 界面窗口中选择**Sensor 服务器**部分。
2. 单击相关 Sensor 组件的卡片。
   这将打开一个窗口，其中包含有关组件的信息。
3. 单击**"编辑"**。
4. 转到"**POP3 集成**"选项卡。
5. 将**"启用 POP3 集成"**切换开关设置为"**已启用**"。
6. 在**邮件服务器**字段中，输入需要配置集成的邮件服务器的 IP 地址。
7. 在**端口**字段中，指定连接到邮件服务器的端口。
8. 在**接收频率**字段中，指定邮件服务器连接频率（以秒为单位）。
9. 如果要通过 POP3 使用与邮件服务器的连接的 TLS 加密，请选择**使用 TLS 加密**复选框。
10. 在**用户名称**字段中，指定用于访问邮件服务器的账户名称。
11. 在**密码**字段中，指定用于访问邮件服务器的密码。

邮件服务器必须支持基本身份验证。

12. 在**TLS证书**下拉列表中，选择以下选项之一：

- **接受任何**。
- **接受不受信任的自签名证书**。
- **只接受受信任的**。

> 与外部邮件服务器建立连接时，建议仅配置受信任的 TLS 证书。如果您接受不受信任的 TLS 证书，则无法保证连接免受 MITM 攻击。尽管接受可信赖的 TLS 证书也无法保证连接免受 MITM 攻击，但它是通过 POP3 协议与邮件服务器集成的最安全的受支持方法。

13. 如有必要，在**密码套件**字段中，修改通过POP3与邮件服务器建立连接时使用的 OpenSSL 设置。
    您可以通过单击**帮助**链接查看有关 OpenSSL 的参考信息。
14. 单击**"保存"**。

将配置通过 POP3 与邮件服务器集成。

如果您已将 Central Node 和 Sensor 组件部署为集群，则可以配置与邮件服务器的高可用性集成。

要配置与邮件服务器的高可用性集成：

1. 在 Central Node 集群对应域名的 DNS 服务器上配置轮询调度算法。
2. 在邮件服务器设置中指定此域名。

与邮件服务器的集成将根据域名进行配置。邮件服务器将与集群中的随机服务器进行通信。如果该服务器出现故障，邮件服务器将与集群中另一台健康的服务器进行通信。

管理集群

您可以查看集群服务器表、向集群添加服务器、退役服务器以及启用或禁用集群。如有必要，您可以增加存储服务器上的磁盘空间。

查看集群的服务器表

集群服务器表显示在应用程序 Web 界面的"**集群**"部分。

表包含以下信息：

- **服务器类型** — 服务器类型取决于其在集群中的角色。
  以下值可以显示：
  - **存储**。
  - **处理**。

- **状态** – 服务器状态。
  以下值可以显示：
  - **已连接**。
  - **未连接**。
- **主机名称** – 服务器名称。
- **IP** – 服务器的 IP 地址。
- **内存** – 服务器的 RAM 负载水平。
- **CPU** – 服务器的 CPU 负载水平。
- **操作** – 您可以用服务器执行的操作。
  可以执行以下操作：**删除**。

将服务器添加到集群

要将服务器添加到集群，您需要在此服务器上开始安装 Kaspersky Anti Targeted Attack Platform，并按照步骤安装组件。添加的服务器显示在集群服务器列表中。

增加存储服务器上的磁盘空间

您可以通过安装额外的磁盘来增加运行的存储服务器上的磁盘空间。

如需通过额外磁盘的方式增加存储服务器的磁盘空间，您需要联系技术支持。

服务器配置为技术支持模式。

停用服务器

要停用正在运行的服务器，您需要联系技术支持。

如果服务器出现故障，您可以自行停用它。

要停用无法运行的处理服务器：

1. 将新处理服务器添加到集群中。
2. 从集群中删除服务器。
3. 为新配置配置应用程序的大小。

处理服务器将被停用。

要停用无法运行的存储服务器：

1. 将新的存储服务器添加到集群中。
2. 联系技术支持以从集群中删除无法运行的服务器。

   存储服务器将被停用。

从集群中删除服务器

如果您使用分布式解决方案和多租户模式，请使用要为其配置参数的 PCN 或 SCN 服务器的 Web 界面。

被删除的服务器无法恢复。确保所选服务器不可运行。

要从集群中删除服务器：

1. 在应用程序 Web 界面窗口中，选择“**集群**”部分。
2. 在**操作**列中，单击与您要删除的服务器相对的**删除**链接。
3. 单击**继续**。

   删除过程将开始。删除可能需要大约一天的时间。有关已删除服务器的信息将不会显示在服务器表中。

删除服务器后，您可以重新配置集群中的服务器或添加具有相同角色的服务器，以保持相同水平的应用程序性能。

启动和关闭集群

要关闭或启动集群，我们建议联系技术支持。如果遇到应用程序运行状况问题，请勿关闭或启动集群。

如果要关闭集群中的健康服务器，必须先关闭集群，以免数据丢失。

关闭集群：

1. 在应用程序 Web 界面中，转到“**集群**”部分。
2. 单击**关机**按钮。

   应用程序的主要组件已停止。您现在可以关闭集群服务器的电源。

启动集群服务器：

1. 如果之前未断开服务器的电源，请断开服务器的电源。
2. 打开存储服务器的电源。
3. 启动其余服务器。

   集群服务器将启动。

集群中的所有服务器启动大约需要 90 分钟。在所有集群服务器启动之前，应用程序 Web 界面即可使用。然而，对于“**高级安全官**”、“**安全官**”、“**安全审计员**”角色的用户，应用程序 Web 界面不显示应用程序菜单，并且具有“**管理员**”角色的用户只能管理“**服务器配置**”部分。

我们强烈建议不要在集群中的所有服务器都启动并运行之前管理应用程序的大小设置。

当集群中的所有服务器均正常运行时，应用程序 Web 界面菜单正常显示。

有关 Central Node 和 Sensor 服务器允许的最大 CPU 和 RAM 负载的通知

在 Central Node 和 Sensor 服务器的 CPU 和 RAM 上保持高负载可能会阻止应用程序组件工作。

您可以配置 Central Node 和 Sensor 服务器上 CPU 和 RAM 的最大使用率；如果超过这些值，则为具有“**高级安全官**”、“**安全官**”和“**管理员**”角色的用户提供的应用程序 Web 界面的“**控制板**”部分的上部会显示一个黄色警告框。您还可以配置要发送到一个或多个电子邮件地址的通知，和用于将有关 CPU 和 RAM 负载的信息发送到支持该协议的外部系统的 SNMP 协议连接。

如果您已将 Central Node 和 Sensor 组件部署为集群，则将为集群中的每台服务器单独显示警告。

具有**高级安全官**或者**安全官**角色的用户还可以创建发送通知的规则。在这种情况下，正确发送通知需要配置服务器的 CPU 和 RAM 的最大允许负载值，以及服务器上的通知设置。

在发送有关应用程序组件的通知的现有规则中，如果满足以下条件，则会自动启用 CPU 负载和 RAM 负载通知：当规则被创建时在**组件**下面选择**所有**复选框。

配置 Central Node 和 Sensor 服务器允许的最大 CPU 和 RAM 负载

在分布式解决方案和多租户模式下，您需要为要从其接收通知的每个 Central Node 服务器设置 CPU 和 RAM 负载的最大允许负载值。如果您使用 Central Node 集群，则可以在任何集群服务器上配置这些设置。

要配置 Central Node 和 Sensor 服务器的 CPU 和 RAM 上允许的最大负载：

1. 在应用程序 Web 界面窗口中，选择**设置**部分的**常规设置**子部分。
2. 在**监控**下面：
   - 在**CPU 使用率超出此值时警告N% 持续M分钟**字段中，输入允许的最大 CPU 使用率以及可以维持最大负载的时间段。

     默认情况下，CPU 最大负载为 95%，持续 5 分钟。
   - 在**内存使用率超出此值时警告N% 持续M分钟**字段中，输入允许的最大 RAM 使用率以及可以维持最大使用率的时间段。

     默认情况下，最大 RAM 使用率为 95%，持续 5 分钟。
3. 单击**应用**。

服务器 CPU 和 RAM 的最大允许负载将得到配置。如果其中一个值在 Central Node 和/或 Sensor 服务器上被超出，则在为具有“**高级安全官**”、“**安全官**”和“**管理员**”角色的用户提供的应用程序 Web 界面的“**控制板**”部分的上部会显示一个黄色警告框。

配置 SNMP 协议连接

您可以将有关 Central Node 和 Sensor 服务器上的 CPU 和 RAM 负载的信息发送到支持 SNMP 协议的外部系统。为此，您必须配置协议的连接。

如果 Central Node 组件被部署为集群，则有关集群中每个服务器的 CPU 和 RAM 负载的数据将被发送到外部系统。

要在 Central Node 服务器上配置 SNMP 协议连接：

1. 在应用程序 Web 界面窗口中，选择**设置**部分的**常规设置**子部分。
2. 在**SNMP**下面，选择**使用 SNMP**复选框。
3. 在**协议版本**字段中，选择协议版本：
   - **v2c**
   - **v3**
4. 如果您选择的是**v2c**协议版本，则在**社区字符串**字段中，输入用于连接Kaspersky Anti Targeted Attack Platform 的密码。
5. 如果您选择了**v3**：
   a. 在**身份验证协议**字段中，选择以下选项之一来检查发送到外部系统的数据的准确性和完整性：
      - **MD5**
      - **SHA256**

   b. 在**用户名称**字段中，输入用户名。

c. 在**密码**字段中，输入身份验证密码。

> 在**用户名称**和**密码**字段中配置的用户名和密码必须与在外部系统中创建账户时配置的用户名和密码匹配。如果凭据不匹配，则无法建立连接。

d. 在**隐私协议**字段中，选择加密类型：

- **DES**。
- **AES**。

e. 在**密码**字段中，输入加密密码。

> 在此字段中配置的密码必须与外部系统中配置的密码匹配。

Central Node 服务器上的协议连接已配置。如果数据请求得到成功处理，外部系统的服务器将显示有关 Central Node 服务器的 CPU 和 RAM 负载的信息。

要在 Sensor 服务器上配置 SNMP 协议连接：

1. 通过 SSH 协议或终端进入 Sensor 服务器的管理控制台。
2. 系统提示时，请输入管理员用户名和安装应用程序期间设置的密码。
   显示应用程序组件管理员菜单。
3. 请按照上述说明的步骤 2 至 5 进行操作。

Sensor 服务器上的协议连接已配置。如果请求得到成功处理，外部系统的服务器将显示有关 Sensor 服务器的 CPU 和 RAM 负载的信息。

> 在分布式解决方案和多租户模式下，必须单独配置每个 PCN、SCN 和 Sensor 服务器的 SNMP 连接设置。

Kaspersky Anti Targeted Attack Platform 的 MIB 对象描述

下表提供了有关 Kaspersky Anti Targeted Attack Platform 的MIB对象的信息。

有关 Central Node 和 Sensor 服务器的硬盘驱动器、CPU 和 RAM 负载的信息

有关 Central Node 和 Sensor 服务器的硬盘驱动器、CPU 和 RAM 负载的信息

象征性名称	描述	对象标识符（OID）
`dskTotal`	磁盘或分区的总大小（KB）。	1.3.6.1.4.1.2021.9.1.6
`dskAvail`	磁盘上的可用空间（KB）。	1.3.6.1.4.1.2021.9.1.7

象征性名称	描述	对象标识符（OID）
dskUsed	磁盘上的已用空间（KB）。	1.3.6.1.4.1.2021.9.1.8
dskPercent	磁盘上已使用空间的百分比（%）。	1.3.6.1.4.1.2021.9.1.9
laLoad	1、5 和 15 分钟的系统负载平均值。	1.3.6.1.4.1.2021.10.1.3
memTotalReal	总 RAM 大小（KB）。	1.3.6.1.4.1.2021.4.5
memAvailReal	使用的 RAM 总量（KB）。	1.3.6.1.4.1.2021.4.6
memTotalFree	可用 RAM 总量（KB）。	1.3.6.1.4.1.2021.4.11

管理 Endpoint Agent 主机信息

用作Endpoint Agent 组件的应用程序安装在组织的 IT 基础架构中的各个计算机（以下也称为"主机"）上。应用程序持续监控在这些主机上运行的进程、活动的网络连接和正在被修改的文件。

具有**高级安全官**、**安全官**、**安全审计员**或者**管理员**角色的用户可以在**Endpoint Agent**选项卡上评估从具有 Endpoint Agent 组件的主机接收数据的频率，该选项卡位于用户可以访问其数据的租户的 Central Node 服务器的 Web 界面窗口中。如果您使用分布式解决方案和多租户模式，PCN 服务器的 Web 界面将为 PCN 以及所有连接的 SCN 显示具有 Endpoint Agent 组件的主机列表。

具有**管理员**角色的用户可以为他们有权访问数据的租户配置显示从具有 Endpoint Agent 的主机接收数据的频率。

如果检测到可疑的网络活动，具有**高级安全官**角色的用户可以为有权访问其数据的租户将任何带有 Kaspersky Endpoint Agent 的主机与网络隔离。在这种情况下，服务器与 Central Node 组件和具有 Endpoint Agent 组件的主机之间的连接不会中断。

为了在 Endpoint Agent 组件出现问题时提供支持，技术支持人员可能会要求您执行以下操作以进行调试（包括在技术支持模式下）：

- 激活扩展诊断信息的收集。
- 修改个体应用程序组件的设置。
- 修改用于存储和发送获取的诊断信息的设置。
- 配置要被拦截并保存到文件的网络流量。

技术支持人员会提供执行这些操作所需的所有信息（步骤顺序说明、要修改的设置、配置文件、脚本、附加的命令行功能、调试模块、特定用途的实用程序和其他资源等），并会告知您出于调试目的所获取的数据的范围。检索到的诊断信息保存在用户的计算机上。检索到的数据不会自动发送到卡巴斯基。

以上列出的操作只能在技术支持专家的指导和监督下进行。未按照本手册或技术支持专家的说明更改应用程序设置，将会导致操作系统变慢或崩溃，降低计算机安全，并可能会影响正在处理的数据的可用性和完整性。

在“Endpoint Agent”部分中选择要管理的租户

如果您使用的是分布式解决方案和多租户模式，在使用“**资产** → **Endpoint Agent**”部分之前，您必须选择要查看其数据的租户。

*选择要在“**资产** → **Endpoint Agent**”部分中管理的租户：*

1. 在应用程序 Web 界面菜单的上部，单击租户名称旁边的箭头。
2. 在下拉列表中，选择租户。

所选租户的数据将显示。如果您想选择其他租户，请重复选择租户的步骤。

查看独立 Central Node 服务器上具有 Endpoint Agent 组件的主机表

具有 Endpoint Agent 组件的主机表位于应用程序 Web 界面窗口的**Endpoint Agent**部分。

该表可以显示以下数据：

- Endpoint Agent 组件的活动指示器和主机数量：
  - **严重不活动**是很久以前从其收到最新数据的主机数量。
  - **警告**是长久以前从其收到最新数据的主机数量。
  - **正常活动**是最近从其收到最新数据的主机数量。
- **主机** — 具有 Endpoint Agent 组件的主机的名称。
- **服务器** — 具有 Endpoint Agent 组件的主机所连接的服务器的名称。
  如果您使用分布式解决方案和多租户模式，则此字段会显示。
- IP — 安装 Endpoint Agent 组件的计算机的 IP 地址。
- **操作系统** — 安装在具有 Endpoint Agent 组件的计算机上的操作系统的版本。
- “**授权许可**”是用作 Endpoint Agent 组件的应用程序的授权许可密钥的状态。
- **版本**是充当 Endpoint Agent 组件角色的应用程序的版本。

- **活动** — Endpoint Agent 组件的活动指示器。可能值：
  - **正常活动**用于最近从其收到最新数据的主机。
  - **警告**用于长久以前从其收到最新数据的主机。
  - **严重不活动**用于很久很久以前从其收到最新数据的主机。
- **最后一次连接**用于 Endpoint Agent 组件上次连接到 Central Node 服务器时的日期和时间。

单击表格中列的链接将打开一个列表，您可以从其中选择以下操作之一：

- **按照此值进行过滤**。
- **从过滤器中排除**。
- **复制值到剪贴板**。

查看有关主机的信息

要查看有关具有 Endpoint Agent 组件的主机的信息：

1. 在应用程序 Web 界面窗口中选择"**资产**"部分。
2. 转到"**Endpoint Agent**"选项卡。
3. 选择您想查看信息的主机。

   这将打开一个窗口，其中包含有关主机的信息。

该窗口包含以下信息：

- 在**主机**部分：
  - **名称**是具有 Endpoint Agent 组件的主机的名称。
  - **IP**是安装 Endpoint Agent 组件的主机的 IP 地址。
  - **操作系统**是安装了 Endpoint Agent 组件的主机上操作系统的版本。
  - **服务器** — SCN 或 PCN 服务器的名称。仅在分布式解决方案和多租户模式下显示。
- 在**Endpoint Agent**部分：
  - **版本**是充当 Endpoint Agent 组件角色的应用程序的版本。
  - **活动**是Endpoint Agent 组件的活动指示器。可能值：
    - **正常活动**用于最近从其收到最新数据的主机。
    - **警告**用于长久以前从其收到最新数据的主机。
    - **严重不活动**用于很久很久以前从其收到最新数据的主机。

- **已连接到服务器** – 主机连接到的 Central Node、SCN 或 PCN 服务器的名称。
- **最后一次连接** – 上次连接到 Central Node、SCN 或 PCN 服务器的时间。
- **授权许可密钥状态**是用作 Endpoint Agent 组件的应用程序的授权许可密钥的状态。

单击带有主机名及其 IP 地址的链接可以执行以下操作：**复制值到剪贴板**。

按主机名筛选和搜索具有 Endpoint Agent 组件的主机

要按主机名筛选或搜索具有 Endpoint Agent 组件的主机：

1. 在应用程序 Web 界面窗口中选择“**资产**”部分。
2. 转到“**Endpoint Agent**”选项卡。
   这将打开主机表。
3. 单击**主机**链接以打开筛选配置窗口。
4. 如果您只想显示隔离的主机，请选择**仅显示隔离的 Endpoint Agent**复选框。
5. 在下拉列表中，选择以下筛选运算符之一：
   - **包含**
   - **不包含**
6. 在输入字段中，指定主机名的一个或多个字符。
7. 要使用不同条件添加筛选条件，请单击 + 并指定筛选条件。
8. 如果要删除筛选条件，请单击该字段右侧的 按钮。
9. 单击**应用**。

   筛选配置窗口关闭。

   表格将仅显示与您设置的筛选条件相匹配的主机。

您可以同时使用多个筛选器。

根据已与网络隔离的 Endpoint Agent 组件筛选和搜索主机

要筛选或搜索与网络隔离的具有 Endpoint Agent 组件的主机：

1. 在应用程序 Web 界面窗口中选择“**资产**”部分。
2. 转到“**Endpoint Agent**”选项卡。
   这将打开主机表。
3. 单击**主机**链接以打开筛选配置窗口。
4. 选择**仅显示隔离的 Endpoint Agent**复选框。
5. 单击**应用**。

   筛选配置窗口关闭。

   表格将仅显示与您设置的筛选条件相匹配的主机。

您可以同时使用多个筛选器。

按 PCN 和 SCN 服务器名称筛选和搜索具有 Endpoint Agent 组件的主机

如果使用分布式解决方案和多租户模式，您可以根据主机所连接的 PCN 和 SCN 服务器的名称筛选或查找具有 Kaspersky Endpoint Agent 组件的主机。

要按 PCN 和 SCN 服务器的名称筛选或搜索具有 Endpoint Agent 组件的主机：

1. 在应用程序 Web 界面窗口中选择“**资产**”部分。
2. 转到“**Endpoint Agent**”选项卡。
   这将打开主机表。
3. 单击**服务器**链接以打开筛选配置窗口。
4. 选择想要按其筛选或搜索具有 Endpoint Agent 组件的主机的服务器名称旁边的复选框。
5. 单击**应用**。

   筛选配置窗口关闭。

表格将仅显示与您设置的筛选条件相匹配的主机。

您可以同时使用多个筛选器。

按计算机 IP 地址筛选和搜索具有 Endpoint Agent 组件的主机

要按在其上安装应用程序的计算机的 IP 地址筛选或搜索具有 Endpoint Agent 组件的主机：

1. 在应用程序 Web 界面窗口中选择“**资产**”部分。
2. 转到“**Endpoint Agent**”选项卡。
   这将打开主机表。
3. 单击 **IP** 链接以打开筛选配置窗口。
4. 在下拉列表中，选择以下筛选运算符之一：
   - **包含**
   - **不包含**
5. 在输入字段中，指定计算机 IP 地址的一个或多个字符。您可以输入 IPv4 格式的 IP 地址或子网掩码（例如，`192.0.0.1` 或 `192.0.0.0/16`）。
6. 要使用不同条件添加筛选条件，请单击 + 并指定筛选条件。
7. 如果要删除筛选条件，请单击该字段右侧的 按钮。
8. 单击**应用**。

筛选配置窗口关闭。

表格将仅显示与您设置的筛选条件相匹配的主机。

您可以同时使用多个筛选器。

按计算机上的操作系统版本筛选和搜索具有 Endpoint Agent 组件的主机

要根据安装在计算机上的操作系统版本筛选或搜索具有 Endpoint Agent 组件的主机：

1. 在应用程序 Web 界面窗口中选择“**资产**”部分。
2. 转到“**Endpoint Agent**”选项卡。
   这将打开主机表。
3. 单击**操作系统**链接以打开筛选设置窗口。
4. 在下拉列表中，选择以下筛选运算符之一：
   - **包含**
   - **不包含**
5. 在输入字段中，指定操作系统版本的一个或多个字符。
6. 要使用不同条件添加筛选条件，请单击 + 并指定筛选条件。
7. 如果要删除筛选条件，请单击该字段右侧的 按钮。
8. 单击**应用**。

   筛选配置窗口关闭。

   表格将仅显示与您设置的筛选条件相匹配的主机。

您可以同时使用多个筛选器。

按组件版本筛选和搜索具有 Endpoint Agent 组件的主机

您可以按 Endpoint Agent 组件的角色中使用的应用程序版本筛选主机。

要按组件版本筛选或搜索具有 Endpoint Agent 组件的主机：

1. 在应用程序 Web 界面窗口中选择“**资产**”部分。
2. 转到“**Endpoint Agent**”选项卡。
   这将打开主机表。
3. 单击**版本**链接以打开筛选设置窗口。

4. 在下拉列表中，选择以下筛选运算符之一：

   - **包含**
   - **不包含**

5. 在输入字段中，指定用作 Endpoint Agent 组件的应用程序版本的一个或多个字符。

6. 要使用不同条件添加筛选条件，请单击 + 并指定筛选条件。

7. 如果要删除筛选条件，请单击该字段右侧的 按钮。

8. 单击**应用**。

   筛选配置窗口关闭。

   表格将仅显示与您设置的筛选条件相匹配的主机。

您可以同时使用多个筛选器。

按活动筛选和搜索具有 Endpoint Agent 组件的主机

要按其活动筛选或搜索具有 Endpoint Agent 组件的主机：

1. 在应用程序 Web 界面窗口中选择“**资产**”部分。

2. 转到“**Endpoint Agent**”选项卡。
   这将打开主机表。

3. 单击**活动**链接以打开筛选配置窗口。
   选择一个或多个活动指示器旁边的复选框：

   - **正常活动**，如果您想查找最近从其中接收到最后数据的主机。
   - **警告**，如果您想查找前段时间从其中接收到最后数据的主机。
   - **严重不活动**，如果您想查找很久以前从其中接收到最后数据的主机。

4. 单击**应用**。

   筛选配置窗口关闭。

   表格将仅显示与您设置的筛选条件相匹配的主机。

您可以同时使用多个筛选器。

为具有 Endpoint Agent 组件的主机快速创建筛选器

要为具有 Endpoint Agent 组件的主机快速创建筛选器：

1. 在应用程序 Web 界面窗口中选择“**资产**”部分。
2. 转到“**Endpoint Agent**”选项卡。
   这将打开主机表。
3. 执行以下操作以便将筛选条件快速添加到正在创建的筛选器中：
   a. 将鼠标光标置于包含您希望将其作为筛选条件添加的表列值的链接上。
   b. 左键单击。
      这将打开要对值执行的操作列表。
   c. 在打开的列表中，选择以下操作之一：
      - **按照此值进行过滤**，如果您想将该值包含在筛选条件中。
      - **从过滤器中排除**，如果您想从筛选条件中排除该值。
4. 如果您想添加多个筛选条件到正在创建的筛选器中，请执行操作以将每个筛选条件快速添加到正在创建的筛选器。

表格将仅显示与您设置的筛选条件相匹配的主机。

为具有 Endpoint Agent 组件的主机重置筛选器

要清除一个或多个筛选条件的 Endpoint Agent 主机筛选器：

1. 在应用程序 Web 界面窗口中选择“**资产**”部分。
2. 转到“**Endpoint Agent**”选项卡。
3. 单击您想清除其筛选条件的表列标题右侧的。

> 如果要清除多个筛选条件，请执行必要的操作以清除每个筛选条件。

选定筛选器将被清除。

表格将仅显示与您设置的筛选条件相匹配的主机。

配置 Endpoint Agent 组件的活动指示器

具有**管理员**角色的用户可以定义被用作 Endpoint Agent 组件的应用程序的不活动持续时间如何被视为正常、低或极低，并且可以配置应用程序的活动指示器。具有**安全审计员**角色的用户可以查看组件活动指示器的设置。具有**高级安全官**或者**安全官**角色的用户可以在应用程序 Web 界面的"**Endpoint Agent**"部分中 Endpoint Agent 组件表的"**活动**"字段中查看您为 Endpoint Agent 组件配置的活动指示器。

要配置 Endpoint Agent 组件的活动指示器：

1. 在应用程序 Web 界面的窗口中，选择**设置**部分的**Endpoint Agent**子部分。
2. 在该部分名称下的字段中，输入您想显示为**警告**和**严重不活动**的具有 Endpoint Agent 组件的主机处于非活动状态的天数。

   默认值为 1 和 7。
3. 单击**应用**。

Endpoint Agent 组件的活动指示器得到配置。

删除具有 Endpoint Agent 组件的主机

从**Endpoint Agent**表中删除一台或多台主机：

1. 在应用程序 Web 界面窗口中选择"**资产**"部分。
2. 转到"**Endpoint Agent**"选项卡。
3. 选择要删除的一台或多台主机旁边的复选框。您可以通过选择包含列标题的行中的复选框来选择所有主机。

   控制面板出现在窗口的下部。
4. 单击**删除**。
5. 这将打开操作确认窗口；在该窗口中，单击**是**。

选定的主机将被从**Endpoint Agent**表中移除。

主机被移除后，Kaspersky Anti Targeted Attack Platform 的 Web 界面会发生以下更改：

- 您无法为已移除的主机创建任务、防止规则或网络隔离规则。
- 如果之前为主机创建了防止规则，则其在规则窗口中的名称（**防止于**字段）在主机被移除后隐藏。该规则继续适用。

  如果该主机重新连接到 Central Node 服务器，主机名将在**防止于**字段中被恢复，防护规则将再次对其应用。
- 如果之前为主机创建了网络隔离规则，则该规则将继续应用，直到规则中指定的时间到期。

  当该主机重新连接到 Central Node 时，该规则将被重新应用于该主机。

- 远程主机上被隔离的对象的元数据将被从 Kaspersky Anti Targeted Attack Platform 隔离区中删除。

  当该主机重新连接到 Central Node 服务器时，Kaspersky Anti Targeted Attack Platform 隔离区中对象的元数据**不会**恢复。您可以通过在命令行或 Kaspersky Security Center 中清除主机上的隔离区来避免填满隔离区。有关详细信息，请参阅您在 Endpoint Agent 组件角色中使用的应用程序的帮助。

- 如果对象仅在一台主机上被**隔离文件**任务隔离且该主机已被移除，任务窗口中的**恢复所有**按钮将处于非活动状态，因为文件无法在已移除的主机上恢复。

按被移除主机的名称进行事件搜索仍然可用。

自动删除不活动的主机

您可以启用或禁用从**Endpoint Agent**表中自动移除不活动的主机。非活动主机是指在配置的时间内未连接到 Central Node 服务器的主机。

*要启用或禁用从**Endpoint Agent**表中自动移除不活动的主机：*

1. 在应用程序 Web 界面的窗口中，选择**设置**部分的**Endpoint Agent**子部分。
2. 在**自动删除不活动的主机**下面， 执行下列操作：
   - 如果您想启用此功能，请将**删除主机**切换开关移至**已启用**。
   - 如果您想启用此功能，请将**删除主机**切换开关移至**已禁用**。
3. 如果您启用了此功能，请在**在此之后删除**字段，指定未连接到 Central Node 组件的主机必须被视为不活动的天数。

   最小值为 1，最大值为 365。

自动移除不活动主机被启用或禁用。

如果在**在此之后删除**字段中指定的值小于在**活动指标**下面的**警告**和/或**严重不活动**字段中指定的值，则主机被移除时间早于在**控制板**部分中显示不活动警告。

主机被移除后，Kaspersky Anti Targeted Attack Platform 的 Web 界面会发生以下更改：

- 您无法为已移除的主机创建任务、防止规则或网络隔离规则。
- 如果之前为主机创建了防止规则，则其在规则窗口中的名称（**防止于**字段）在主机被移除后隐藏。该规则继续适用。

  如果该主机重新连接到 Central Node 服务器，主机名将在**防止于**字段中被恢复，防护规则将再次对其应用。

- 如果之前为主机创建了网络隔离规则，则该规则将继续应用，直到规则中指定的时间到期。

  当该主机重新连接到 Central Node 时，该规则将被重新应用于该主机。

- 远程主机上被隔离的对象的元数据将被从 Kaspersky Anti Targeted Attack Platform 隔离区中删除。

  当该主机重新连接到 Central Node 服务器时，Kaspersky Anti Targeted Attack Platform 隔离区中对象的元数据**不会**恢复。您可以通过在命令行或 Kaspersky Security Center 中清除主机上的隔离区来避免填满隔离区。有关详细信息，请参阅您在 Endpoint Agent 组件角色中使用的应用程序的帮助。

- 如果对象仅在一台主机上被**隔离文件**任务隔离且该主机已被移除，任务窗口中的**恢复所有**按钮将处于非活动状态，因为文件无法在已移除的主机上恢复。

按被移除主机的名称进行事件搜索仍然可用。

支持的解释器和进程

Kaspersky Endpoint Agent 应用程序通过以下解释器监控脚本的执行：

- cmd.exe
- reg.exe
- regedit.exe
- regedt32.exe
- cscript.exe
- wscript.exe
- mmc.exe
- msiexec.exe
- mshta.exe
- rundll32.exe
- runlegacycplelevated.exe
- control.exe
- explorer.exe
- regsvr32.exe
- wwahost.exe
- powershell.exe
- java.exe 和 javaw.exe（仅当使用 –jar 选项启动时）
- InstallUtil.exe
- msdt.exe
- python.exe

- ruby.exe
- rubyw.exe

有关被 Kaspersky Endpoint Agent 应用程序监控的进程的信息，请参见下表。

进程及其打开的文件扩展名

进程	文件扩展名
winword.exe	rtf doc dot docm docx dotx dotm docb
excel.exe	xls xlt xlm xlsx xlsm xltx xltm xlsb xla xlam xll xlw
powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm
acrord32.exe	pdf
wordpad.exe	docx pdf
chrome.exe	pdf
MicrosoftEdge.exe	pdf

配置与 Sandbox 组件的集成

您可以将一个 Sandbox 组件连接到多个 Central Node 组件。

以下步骤用于配置 Sandbox 组件和 Central Node 组件间的连接：

1. **创建连接到 Sandbox 组件的请求**

   您可以在管理员账户下的应用程序 Web 界面中创建请求。如果服务器上安装了多个 Central Node 组件，则需要为每个具有要连接到 Sandbox 组件的 Central Node 组件的服务器创建请求。如果 Central Node 组件被部署为集群，您可以从集群中的任何服务器创建连接请求。

2. **在 Sandbox Web 界面中处理连接请求**

   您可以接受或拒绝每个请求。

如果您要将多个 Sandbox 组件连接到单个 Central Node 组件，请确保您连接的 Sandbox 组件具有相同的用于扫描对象的操作系统集，以及同时运行的虚拟机的最大数量。

配置连接后，Sandbox 服务器需要 5 到 10 分钟才能准备好运行。在此期间，**系统健康**应用程序 Web 界面的窗口显示警告：*标准配置出现问题*。当服务器准备好运行时，警告就会消失。

查看具有 Sandbox 组件的服务器表

具有**安全审计员**角色的用户可以查看具有Sandbox 组件的服务器表。

具有 Sandbox 组件的服务器表位于程序 Web 界面窗口的**Sandbox 服务器**部分的**服务器**选项卡上。

证书指纹字段显示 Central Node 服务器的 TLS 证书的指纹。

服务器列表表包含以下信息：

- **IP 和名称** — 具有 Sandbox 组件的服务器的 IP 地址或完全限定域名。
- **证书指纹** — 具有 Sandbox 组件的服务器的证书指纹。
- **授权** — 连接到 Sandbox 组件的请求的状态。
- **状态** — 与 Sandbox 组件的连接状态。

具有**安全官**角色无法查看具有 Sandbox 组件的服务器表。

使用 Sandbox 组件创建连接到服务器的请求

要通过应用程序 Web 界面创建使用 Sandbox 组件连接到服务器的请求：

1. 在应用程序 Web 界面窗口中选择**Sandbox 服务器**部分。
2. 在窗口的右上角，单击**添加**按钮。
   这将打开**Sandbox 服务器连接**窗口。
3. 在**IP**字段中，使用要连接的 Sandbox 组件指定服务器的 IP 地址。

4. 单击**获取证书指纹**。
   工作区显示具有 Sandbox 组件的服务器证书的指纹。
5. 将获得的证书指纹与**证书指纹**字段的**KATA 授权**部分中 Sandbox Web 界面中指示的指纹进行比较。
   如果证书指纹匹配，请执行说明的后续步骤。

   > 如果证书指纹不匹配，确认该连接不是最佳选择。确保您输入的数据正确。

6. 在**名称**字段中，指定将在 Central Node 组件的 Web 界面中显示的 Sandbox 组件名称。
   该名称与安装 Sandbox 的主机名无关。
7. 如果要在连接后立即激活与 Sandbox 的连接，请选中**启用**复选框。
8. 单击**添加**。

连接请求显示在 Sandbox 组件的 Web 界面中。

启用和禁用与 Sandbox 组件的连接

要激活与 Sandbox 组件的连接或禁用它：

1. 在应用程序 Web 界面窗口中选择**Sandbox 服务器**部分。
   将显示具有 Sandbox 组件的服务器表。
2. 在**状态**列中包含相关服务器的行中，执行以下操作之一：
   - 如果要激活与 Sandbox 组件的连接，请将切换开关设置为**已启用**。
   - 如果要禁用与 Sandbox 组件的连接，请将切换开关设置为**已禁用**。
3. 单击**应用**。

与 Sandbox 组件的连接将变为活动状态或将被禁用。

删除与 Sandbox 组件的连接

要删除与 Sandbox 组件的连接：

1. 在应用程序 Web 界面窗口中选择**Sandbox 服务器**部分。
   这将显示安装了 Sandbox 组件的计算机表。
2. 选择包含您想删除的 Sandbox 组件连接的行中的复选框。
3. 在窗口的右上角，单击**删除**按钮。
4. 在确认窗口中，单击**是**。

将删除与 Sandbox 组件的连接。

从 Endpoint Agent 主机手动发送文件以供 Sandbox 扫描

您可以启用和禁用从具有 Endpoint Agent 组件的主机手动发送文件以供 Sandbox 组件扫描。如果启用此功能，具有 Endpoint Agent 组件的主机的用户可以使用 Sandbox 扫描他们认为不安全的任何文件。

如果将 Kaspersky Endpoint Security for Windows 和/或 Kaspersky Endpoint Security for Linux 应用程序用作 Endpoint Agent 组件，并且为这些组件配置了与 Kaspersky Anti Targeted Attack Platform 的集成，则此功能可用。

发送文件进行扫描涉及以下步骤：

1. 在 Kaspersky Anti Targeted Attack Platform Web 界面中允许从具有 Endpoint Agent 组件的主机手动发送文件，以便由 Sandbox 组件进行扫描。
2. 发送文件以供 Kaspersky Endpoint Security for Windows 和 Kaspersky Endpoint Security for Linux 中的 Sandbox 组件扫描。

根据扫描结果，Kaspersky Anti Targeted Attack Platform 可能会在警报数据库中记录警报。这些警报的详细信息显示在“**按攻击向量分类的警报**”小部件中。

在分布式解决方案和多租户模式下，您必须在每个要使用 Sandbox 组件的 Central Node 服务器上启用手动发送文件以供 Sandbox 组件扫描的功能。如果 Central Node 组件被部署为集群，您可以在集群中的任何服务器上启用该功能。

如果您仅使用 KATA 功能（KATA 授权许可密钥），则在 Kaspersky Anti Targeted Attack Platform Web 界面中，“**Endpoint Agent**”部分显示已发送文件以供 Sandbox 组件扫描的主机列表。您可以查看此列表和有关所选主机的信息。

启用和禁用从 Endpoint Agent 主机手动发送文件以供 Sandbox 扫描

要启用或禁用手动发送要由 Sandbox 组件扫描的文件：

1. 在应用程序 Web 界面的窗口中，选择**设置**部分的**Endpoint Agent**子部分。
2. 在“**手动将文件从主机发送到 Sandbox 进行分析**”下，执行以下操作：
   - 设置“**发送文件**”拨动开关至“**已启用**”，如果您想启用手动发送文件以供 Sandbox 组件扫描。
     默认情况下启用此功能。
   - 设置“**发送文件**”拨动开关至“**已禁用**”，如果您想禁用手动发送文件以供 Sandbox 组件扫描。
3. 单击**应用**。

启用或禁用从 Endpoint Agent 主机手动发送文件以供 Sandbox 组件扫描。

配置与外部系统的集成

您可以配置 Kaspersky Anti Targeted Attack Platform 与外部系统的集成，以扫描存储在这些系统中的文件。它们的扫描结果将显示在警报表中。

外部系统的角色的用户可以由邮件传感器提供，例如 Kaspersky Secure Mail Gateway 或 Kaspersky Security for Linux 邮件服务器。邮件传感器将电子邮件发送到 Kaspersky Anti Targeted Attack Platform 进行处理。基于 Kaspersky Anti Targeted Attack Platform 中的电子邮件处理结果，邮件传感器可能会阻止邮件的传输。

Kaspersky Anti Targeted Attack Platform 与外部系统的集成涉及以下过程：

1. **输入集成设置并从外部系统创建集成请求。**

   有关输入邮件传感器集成设置的更多详情，请参阅 Kaspersky Secure Mail Gateway 帮助 或 Kaspersky Security for Linux 邮件服务器帮助。

   要集成其他外部系统，请使用 REST API。

2. **确认 Kaspersky Anti Targeted Attack Platform 的集成**

   外部系统必须使用唯一证书在具有 Central Node 组件的服务器上进行授权。如果是这种情况，将在 Kaspersky Anti Targeted Attack Platform 的界面中显示单个集成请求。要连接具有相同 IP 地址的多个外部系统，您必须为每个外部系统使用唯一证书。

   > 使用一张证书时，您只能配置与一个外部系统的集成。

3. **检查外部系统和 Kaspersky Anti Targeted Attack Platform 之间的连接**

查看外部系统表

外部系统表位于应用程序 Web 界面窗口的**外部系统**部分。表包含以下信息：

- **Sensor** — 外部系统服务器的 IP 地址或域名。
- **类型** — 外部系统的类型（邮件传感器或其他系统）。
- **名称** — 不是邮件传感器的集成外部系统的名称。
  邮件传感器的此列中显示破折号。
- **ID** — 外部系统的 ID。
- **证书指纹** — 服务器的 TLS 证书的指纹，外部系统用于与托管 Central Node 组件的服务器建立加密连接。

  > 具有 Central Node 组件的服务器的证书指纹显示在**证书指纹**字段中窗口的上部。

- **状态** — 集成请求的状态。

处理来自外部系统的请求

要处理来自外部系统的集成请求：

1. 在应用程序 Web 界面窗口中选择**外部系统**部分。

   服务器列表表显示已连接的外部系统，以及从外部系统与 Kaspersky Anti Targeted Attack Platform 集成的请求。

2. 在包含集成请求的行中，执行以下操作之一：

   - 如果要配置与外部系统的集成，请单击**接受**按钮。
   - 如果您不想配置与外部系统的集成，请单击**拒绝**按钮。

3. 在确认窗口中，单击**是**。

将处理来自外部系统的集成请求。

从允许集成的列表中移除外部系统

在接受来自外部系统的集成请求后，可以从允许集成的列表中移除它。如果是这种情况，Kaspersky Anti Targeted Attack Platform 和外部系统之间的连接将被终止。

要从允许集成的系统列表中移除外部系统：

1. 在应用程序 Web 界面窗口中选择**外部系统**部分。

   服务器列表显示已添加的外部系统以及从外部系统与Kaspersky Anti Targeted Attack Platform集成的请求。

2. 在包含来自想移除的外部系统集成请求的行中，单击**删除**按钮。

3. 在确认窗口中，单击**是**。

外部系统将从允许集成的列表中移除。

配置处理来自邮件传感器的流量的优先级

您可以启用或禁用处理来自邮件传感器的流量的最高优先级。

要启用或禁用处理来自邮件传感器的流量的最高优先级：

1. 在应用程序 Web 界面窗口中选择**外部系统**部分。
2. 执行以下操作之一：
   - 如果您想启用处理来自邮件传感器的流量的最高优先级，请打开**最大扫描优先级**参数名称旁边的切换开关。
   - 如果您想禁用处理来自邮件传感器的流量的最高优先级，请关闭**最大扫描优先级**参数名称旁边的切换开关。

将配置处理来自邮件传感器的流量的优先级。

配置与 Kaspersky Managed Detection and Response 的集成

Kaspersky Managed Detection and Response（以下简称"MDR"）可检测并防止客户端基础架构中的欺诈行为。MDR 提供持续的受管理保护，使组织能够自动发现难以检测的威胁，同时让 IT 安全人员能够专注于解决需要他们参与的问题。

Kaspersky Anti Targeted Attack Platform 获取数据并使用卡巴斯基安全网络流将其发送到 Kaspersky Managed Detection and Response。因此，参与 KSN 对于配置与 MDR 的集成很有必要。

仅当至少有一个KATA 或 EDR授权许可处于活动状态时，才能与 MDR 集成。如果仅在应用程序中添加一个授权许可密钥（仅 KATA 或仅 EDR），则统计信息仅限于该授权许可提供的功能。如果两个授权许可密钥都被添加到应用程序中，则会发送完整的统计信息。

在配置 Kaspersky Anti Targeted Attack Platform 与 MDR 应用程序的集成之前，您必须从 MDR 门户下载包含配置文件的存档。

启用 MDR 集成

确保添加了有效的授权许可密钥并在应用程序中配置了参与 KSN。否则 MDR 集成不可用。

要启用与 MDR 的集成：

1. 利用管理员账户登录应用程序 Web 界面。
2. 选择**设置**部分的**KSN/KPSN 和 MDR**子部分。
3. 在**MDR 集成**下面，单击**上传**上传配置文件。
   这将打开文件选择窗口。
4. 选择您在 MDR 门户注册期间下载的存档，然后单击**打开**。

窗口中将显示有关 MDR 授权许可的以下信息：

- **序列号**。
- **到期日期**。
- **剩余天数**。

与 MDR 的集成被启用。在配置文件中配置的集成设置将被应用于所有连接的 Sensor 组件。MDR 开始使用通过 KSN 流发送的警报统计信息。

禁用 MDR 集成

要禁用与 MDR 的集成：

1. 利用管理员账户登录应用程序 Web 界面。
2. 选择**设置**部分的**KSN/KPSN 和 MDR**子部分。
3. 在**MDR 集成**下面，单击**删除文件**。
4. 在确认窗口中，单击**是**。

配置文件将被删除，MDR 集成将被禁用。统计信息仍会被发送到 KSN 服务器，但 MDR 不使用此信息。

替换 MDR 配置文件

替换 MDR 配置文件：

1. 利用管理员账户登录应用程序 Web 界面。
2. 选择**设置**部分的**KSN/KPSN 和 MDR**子部分。
3. 在**MDR 集成**下面，单击**替换文件**。
   这将打开文件选择窗口。
4. 选择包含配置文件的新存档，然后单击**打开**。
   MDR 授权许可信息在应用程序 Web 界面中得到更新。

配置文件被替换。新的集成设置将应用于所有连接的 Sensor 组件。

配置与 SIEM 系统的集成

Kaspersky Anti Targeted Attack Platform 可以在应用程序 Web 界面中发布有关用户操作的信息，并使用 Syslog 协议向组织中的 *SIEM 系统*发出警报。

您可以使用 TLS 加密进行数据传输。

如果您已将 Central Node 和 Sensor 组件部署为集群，则可以使用以下选项之一配置与外部系统的高可用性集成：

- 使用轮询调度算法功能。
- 配置外部系统的设置，以便在发生网络错误时外部系统在集群服务器的 IP 地址之间进行切换。

要使用轮询调度算法功能配置与外部系统的高可用性集成：

1. 在 Central Node 集群对应域名的 DNS 服务器上配置轮询调度算法。
2. 在邮件服务器设置中指定此域名。

与外部系统的集成是基于域名配置的。外部系统将与集群中的随机服务器进行通信。如果该服务器出现故障，外部系统将与集群中另一台健康的服务器进行通信。

启用和禁用事件信息记录到远程日志

您可以配置有关 Web 界面中用户操作的信息的记录以及远程日志中的警报。日志文件被存储在安装了 SIEM 系统的服务器上。要写入远程日志，您必须配置与 SIEM 系统的集成。

要启用或禁用在 Web 界面中记录有关用户操作的信息以及向远程日志发出警报：

1. 在应用程序 Web 界面窗口，选择**设置**部分的**SIEM 系统**子部分。
2. 如果要启用/禁用将 Web 界面中的用户操作信息记录到远程日志，请执行以下操作之一：
   - 如果您想要在 Web 界面中启用有关用户操作的信息记录，请选择**用户活动**复选框。
   - 如果您想要禁用在 Web 界面中记录有关用户操作的信息，请清除**用户活动**复选框。
3. 如果要启用/禁用将有关警报的信息记录到远程日志，请执行以下操作之一：
   - 如果要启用警报信息记录，请选择“**检测**”复选框。
   - 如果您想禁用警报信息记录，请清除“**检测**”复选框。

   您可以同时选择两个复选框。
4. 单击窗口下部的**应用**。

远程日志中的信息记录被启用或禁用。

具有**安全审计员**角色的用户只能查看有关远程日志记录设置的信息。

配置 SIEM 系统集成的主要设置

要配置 SIEM 系统集成的主要设置：

1. 在应用程序 Web 界面窗口，选择**设置**部分的**SIEM 系统**子部分。
2. 选择“**用户活动**”和/或“**检测**”复选框。
   您可以选择一个复选框或同时选择两个复选框。
3. 在**主机/IP**字段中，输入您的 SIEM 系统服务器的 IP 地址或主机名。
4. 在**端口**字段中，输入用于连接到您的 SIEM 系统的端口号。
5. 在**协议**字段中， 选择**TCP**或**UDP**。
6. 在**主机 ID**字段中，输入主机 ID。具有该 ID 的主机被指定为 SIEM 系统日志中的警报源。
7. 在**心跳**字段中，输入向 SIEM 系统发送消息的间隔。
8. 单击窗口下部的**应用**。

将配置与 SIEM 系统集成的主要设置。

具有**安全审计员**角色的用户只能查看有关 SIEM 系统集成设置的信息。

上传 TLS 证书

要加载用来加密与 SIEM 系统的连接的 TLS 证书：

1. 在应用程序 Web 界面窗口，选择**设置**部分的**SIEM 系统**子部分。
2. 在**TLS 加密**部分，单击**上传**按钮。
   这将打开文件选择窗口。
3. 选择要下载的 TLS 证书文件，然后单击**打开**按钮。
   这将关闭文件选择窗口。
   TLS 证书被添加到应用程序中。
4. 单击窗口下部的**应用**。

上传的 TLS 证书将用于加密与 SIEM 系统的连接。

启用和禁用与 SIEM 系统的连接的 TLS 加密

要启用或禁用与 SIEM 系统的连接的 TLS 加密：

1. 在应用程序 Web 界面窗口，选择**设置**部分的**SIEM 系统**子部分。
2. 选择**用户活动**和/或**警报**复选框。
   您可以选择一个复选框或同时选择两个复选框。
3. 在**TLS 加密**部分，请执行以下操作之一：
   - 如果您想启用与 SIEM 系统的连接的 TLS 加密，请打开**TLS 加密**参数名称旁边的切换开关。
   - 如果您想禁用与 SIEM 系统的连接的 TLS 加密，请关闭**TLS 加密**参数名称旁边的切换开关。

   只有在加载了 TLS 证书的情况下，**TLS 加密**设置的名称旁边的切换开关才可用。
4. 单击窗口下部的**应用**。

将启用或禁用与 SIEM 系统的连接 TLS 加密。

有关警报的 syslog 邮件的内容和属性

有关每个警报的信息在单独的 syslog 类别（syslog 工具）中传输，系统未使用该类别来传递来自其他来源的消息。有关每个警报的信息以 CEF 格式作为单独的 syslog 邮件传输。如果警报是由针对性攻击分析器模块生成的，则有关该警报的信息将以 CEF 格式作为多个单独的 syslog 消息传输。

有关警报的 syslog 邮件的默认最大大小为 32 KB。超过最大大小的邮件最后会被截断。

有关警报的每个系统日志消息的标题包含以下信息：

- 格式化版本。
  当前版本号：`0`。当前字段值：`CEF:0`。
- 供应商。
  当前字段值：`AO Kaspersky Lab`。
- 应用程序名称。
  当前字段值：`Kaspersky Anti Targeted Attack Platform`。
- 应用程序版本
  当前字段值：7.0.1-500。
- 检测类型。
  见下表。

- 活动名称。

  见下表。

- 检测重要性。

  允许的字段值：低、中、高 或 `0` (对于心跳 消息)。

- 其他信息。

  例如：
  ```
  CEF:0|AO Kaspersky Lab| Kaspersky Anti Targeted Attack Platform |7.0.1-500|url_web| 来自探测的 web 的 URL |Low|
  ```

有关检测的系统日志消息正文与有关该检测的信息匹配，该信息显示在应用程序 Web 界面中。所有字段均以“<参数>=<值>”格式显示。根据网络流量或邮件流量中是否发生检测，以及根据生成检测的技术，可以在系统日志消息的正文中传输各种密钥。如果该值为空，则不传输参数。

参数以及消息中包含的值显示在下表中。

有关 syslog 消息中的检测的信息

检测类型	检测名称和说明	参数及其值的描述
file_web	检测到来自 Web 的文件 在网络流量中检测到文件。	• dvchost = <具有 Central Node 组件的服务器名称>。 • eventId = <检测 ID>。 • rt = <检测的日期和时间，UTC>。 • dst = <目标 IP 地址>。 • dpt = <目标端口>。 • src = <源 IP 地址>。 • spt = <源端口>。 • shost = <检测到文件的主机的名称>。 • suser = <用户名称>。 • fName = <复合对象内文件的路径>。 • fsize = <复合对象中文件的大小（以字节为单位）>。 • fileType = <复合对象中文件的格式>。 • fileHash = <复合对象中文件的 MD5 哈希>。 • KasperskyLabKATAcompositeFilePath = <复合对象的名称>。 • KasperskyLabKATAcompositeFileSize = <复合对象的总大小（以字节为单位）>。 • KasperskyLabKATAcompositeFileHash = <复合对象的 MD5 哈希>。 • KasperskyLabKATAfileSHA256 = <复合对象的 SHA256 哈希>。 • cs2 = <用于检测文件的技术>。 • cs3Label = <检测到文件的虚拟机的名称（仅限 Sandbox 组件）。 • cs1 = <根据卡巴斯基类别检测到的对象的名称>。 • cs3 = <用于扫描文件的数据库的版本>。 • app = <应用程序层协议名称> (HTTP(S) 或 FTP)。 • requestMethod = <HTTP 请求方法>（仅适用于 HTTP(S) 协议）。 • requestClientApplication = <客户端计算机的用户代理>（仅适用于 HTTP(S) 协议）。 • request = <检测到的对象的 URL> （仅适用于 HTTP(S) 协议）。 • requestContext = <HTTP Referrer 头> （仅适用于 HTTP(S) 协议）。
file_mail	检测到邮件的文件 在邮件流量中检测到文件。	• dvchost = <具有 Central Node 组件的服务器名称>。 • eventId = <检测 ID>。 • rt = <警报的日期和时间，UTC>。 • fName = <复合对象内文件的路径>。 • fsize = <复合对象中文件的大小（以字节为单位）>。 • fileType = <复合对象中文件的格式>。 • fileHash = <复合对象中文件的 MD5 哈希>。 • KasperskyLabKATAcompositeFilePath = <复合对象的名称>。 • KasperskyLabKATAcompositeFileSize = <复合对象的总大小（以字节为单位）>。 • KasperskyLabKATAcompositeFileHash = <复合对象的 MD5 哈希>。 • KasperskyLabKATAfileSHA256 = <复合对象的 SHA256 哈希>。 • KasperskyLabKATAmailEnvelopeFrom = <发件人电子邮件地址>（来自“已接收”标题）。 • KasperskyLabKATAmailFor = <收件人电子邮件地址>（来自“已接收”标题）。 • KasperskyLabKATAmailRecievedFromIp = <邮件传递链中第一台服务器的 IP 地址>（来自“已接收”标题）。 • cs2 = <用于检测文件的技术>。 • cs3Label = <检测到文件的虚拟机的名称（仅限 Sandbox 组件）。 • cs1 = <根据卡巴斯基类别检测到的对象的名称>。 • cs3 = <用于扫描文件的数据库的版本>。 • externalId = <邮件消息 ID>。 • suser = <发件人的电子邮件地址>。 • duser = <收件人的电子邮件地址>。 • msg = <邮件主题>。
ids	检测到的 IDS 事件 检测由入侵检测系统模块生成。	• dvchost = <具有 Central Node 组件的服务器名称>。 • eventId = <检测 ID>。 • requestMethod = <HTTP 请求方法>（仅适用于 HTTP(S) 协议）。 • requestClientApplication = <客户端计算机的用户代理>（仅适用于 HTTP(S) 协议）。 • rt = <警报的日期和时间，UTC>。 • dst = <目标 IP 地址>。 • dpt = <目标端口>。 • src = <源 IP 地址>。 • spt = <源端口>。 • proto = <网络级协议的名称>（TCP 或 UDP）。 • cs1 = <根据卡巴斯基实验室类别检测到的对象的类型>。 • cs2Label = <IDS 规则的名称>。 • cs2 = <IDS 规则的编号>。 • cs3 = <入侵检测系统模块数据库版本>。 • requestMethod = <HTTP 请求方法>（仅适用于 HTTP(S) 协议）。

检测类型	检测名称和说明	参数及其值的描述
		• requestClientApplication = <客户端计算机的用户代理>（仅适用于 HTTP(S) 协议）。 • request = <检测到的对象的 URL>。
url_web	检测到 Web 的 URL 网络流量中的 URL 信誉技术或 Sandbox 生成了一条警报。	• dvchost = <具有 Central Node 组件的服务器名称>。 • eventId = <检测 ID>。 • rt = <检测的日期和时间，UTC>。 • dst = <目标 IP 地址>。 • dpt = <目标端口>。 • src = <源 IP 地址>。 • spt = <源端口>。 • shost = <检测到文件的主机的名称>。 • suser = <用户名称>。 • cs1 = <检测到的对象的 URL 所属的分类列表>。 • requestMethod = <HTTP 请求方法>。 • requestClientApplication = <客户端计算机的用户代理>。 • request = <检测到的对象的 URL>。 • requestContext = <HTTP Referer 标头>。 • reason = <HTTP 响应代码>。
url_mail	检测到邮件的 URL 邮件流量中的 URL 信誉技术或 Sandbox 生成了一条警报。	• dvchost = <具有 Central Node 组件的服务器名称>。 • eventId = <检测 ID>。 • rt = <警报的日期和时间，UTC>。 • externalId = <邮件消息 ID>。 • suser = <发件人的电子邮件地址>。 • duser = <收件人的电子邮件地址>。 • KasperskyLabKATAmailEnvelopeFrom = <发件人电子邮件地址>（来自“已接收”标题）。 • KasperskyLabKATAmailFor = <收件人地址>（来自“已接收”标题）。 • KasperskyLabKATAmailRecievedFromIp = <邮件传递链中第一台服务器的 IP 地址>（来自“已接收”标题）。 • msg = <邮件主题>。 • request = <检测到的对象的 URL>。 • cs2 = <用于生成警报的技术>（Sandbox 或URL信誉）。 • cs3Label = <检测到文件的虚拟机的名称（仅限 Sandbox）。 • cs1 = <根据卡巴斯基分类检测到的对象类型列表>（适用于 Sandbox 组件）或<类别列表>（适用于 URL 信誉）。 • cs3 = <用于扫描文件的数据库的版本>（仅适用于 Sandbox）。
dns	检测到 DNS 请求 DNS 流量中的 URL 信誉技术生成了一条警报。	• dvchost = <具有 Central Node 组件的服务器名称>。 • eventId = <检测 ID>。 • rt = <检测的日期和时间，UTC>。 • dst = <目标 IP 地址>。 • dpt = <目标端口>。 • src = <源 IP 地址>。 • spt = <源端口>。 • shost = <检测到文件的主机的名称>。 • suser = <用户名称>。 • cs2 = <域名所属的URL类别列表>。 • requestMethod = <DNS 信息类型>（请求或响应）。 • flexString1 = <来自 DNS 请求的记录类型>。 • dhost = <来自 DNS 请求的主机名>。 • cs1 = <DNS响应中的域名列表>。

检测类型	检测名称和说明	参数及其值的描述
`file_endpoint`	检测到端点的文件 用户计算机上的 Endpoint Agent 组件生成了一条警报，并且该警报包含文件。	• `dvchost` = <具有 Central Node 组件的服务器名称>。 • `eventId` = <检测 ID>。 • `rt` = <警报的日期和时间，UTC>。 • `src` = <源 IP 地址>。 • `shost` = <检测到文件的主机的名称>。 • `fName` = <复合对象内文件的路径>。 • `fsize` = <复合对象中文件的大小（以字节为单位）>。 • `fileType` = <复合对象中文件的格式>。 • `fileHash` = <复合对象中文件的 MD5 哈希>。 • `KasperskyLabKATAcompositeFilePath` = <复合对象的名称>。 • `KasperskyLabKATAcompositeFileSize` = <复合对象的总大小（以字节为单位）>。 • `KasperskyLabKATAcompositeFileHash` = <复合对象的 MD5 哈希>。 • `KasperskyLabKATAfileSHA256` = <复合对象的 SHA256 哈希>。 • `cs2` = <用于检测文件的技术>。 • `cs3Label` = <检测到文件的虚拟机的名称（仅限 Sandbox 组件）。 • `cs1` = <根据卡巴斯基类别检测到的对象的名称>。 • `cs3` = <用于扫描文件的数据库的版本>。 • `app` = <应用程序级协议>（HTTP(S) 或 FTP）。 • 文件路径 = <Endpoint Agent 计算机上文件的路径>。
`iocScanning`	`IOC` 在端点上绊倒 该警报是在使用 Windows Endpoint Agent 组件对主机执行 IOC 扫描时生成的。 如果您使用 KEDR 功能，则可以使用此类警报。	• `dvchost` = <具有 Central Node 组件的服务器名称>。 • `eventId` = <检测 ID>。 • `rt` = <警报的日期和时间，UTC>。 • `src` = <源 IP 地址>。 • `shost` = <检测到文件的主机的名称>。 • `cs1` = <生成警报的 IOC 文件的名称>。
`taaScanning`	`TAA` 在事件数据库上绊倒 IOA 事件分析产生的检测。 如果您使用 KEDR 功能，则可以使用此类检测。	• `dvchost` = <具有 Central Node 组件的服务器名称>。 • `eventId` = <检测 ID>。 • `rt` = <警报的日期和时间，UTC>。 • `shost` = <生成检测的主机名称>。 • `cs1` = <生成警报的 IOA 规则的名称>。
`yaraScanningEP`	`YARA` 在端点上绊倒 该警报是在使用 Windows Endpoint Agent 组件对主机执行 YARA 扫描时生成的。 如果您使用 KEDR 功能，则可以使用此类警报。	• `dvchost` = <具有 Central Node 组件的服务器名称>。 • `eventId` = <检测 ID>。 • `rt` = <警报的日期和时间，UTC>。 • `src` = <源 IP 地址>。 • `shost` = <生成警报的主机名称>。 • `cs1` = <生成警报的 YARA 规则的名称>。
`heartbeat`	包含组件状态的定期消息。	• `dvchost` = <具有 Central Node 组件的服务器名称>。 • `rt` = <事件的日期和时间，UTC>。 • `KasperskyLabKATAcomponentName` = <组件的名称>。 • `KasperskyLabKATAcomponentState` = <组件的状态>（`0` – OK, `>0` – 错误）。

更新使用 API 连接到 Central Node 的证书

要更新使用 Kaspersky Anti Targeted Attack Platform API 连接到 Central Node 服务器的证书，您需要替换 REST API 服务器使用的证书。您可以在“**设置**”部分，“**连接服务器**”字部份中，“**REST API 服务器**”选项卡上指定 REST API 服务器的新证书。

管理连接器

本节包含有关 Kaspersky Anti Targeted Attack Platform 中的连接器的信息。*连接器*是处理与 Kaspersky Anti Targeted Attack Platform 的通信的特殊软件模块，可以允许在应用程序本身中或在应用程序的帮助下执行管理任务。

连接器扩展了应用程序的功能，使其能够与第三方系统交互。根据其功能目的，连接器可以将数据发送到第三方系统（例如，将事件、应用程序消息和审计记录发送到 SIEM 系统）或从第三方系统获取数据。应用程序还可以使用连接器对设备进行主动轮询。

运行连接器软件模块的计算机称为*连接器部署节点*。您可以在任何可以通过网络访问 Central Node 服务器的计算机上部署连接器（包括安装了应用程序组件的节点，包括 Central Node 服务器本身）。

连接器表和连接器类型表显示在应用程序 Web 界面的“**设置**”部分，“**连接器**”子部份。只有具有管理员角色的用户才能管理连接器和连接器类型。拥有“**安全审计员**”、“**安全官**”和“**高级安全官**”角色的用户可以查看连接器和连接器类型。

连接器的功能取决于所选的*连接器类型*。您可以在将连接器添加到应用程序时选择连接器类型。应用程序内置有以下类型的现成连接器：

- **Syslog**

  此连接器类型支持将数据转发到 Syslog 服务器。

  添加 **Syslog** 连接器或编辑其设置时，配置连接器的常规设置以及**“详细信息”**下的附加设置：

  - Syslog 服务器地址
  - Syslog 服务器端口
  - 数据传输协议

- **SIEM**

  此连接器类型支持将数据转发到 SIEM 系统。

  添加“**SIEM**”连接器或编辑其设置时，配置连接器的常规设置以及**“详细信息”**下的附加设置：

  - SIEM 系统服务器地址
  - SIEM 系统服务器端口
  - 数据传输协议

- **一般**

  此连接器类型允许连接使用 Kaspersky Anti Targeted Attack Platform API NDR 的应用程序。

- **电子邮件**

  此连接器类型提供通过电子邮件转发数据的功能。

  添加“**电子邮件**”连接器或编辑其设置时，配置连接器的常规设置以及**“详细信息”**下的附加设置：

  - 用作电子邮件发件人的地址。
  - 电子邮件的收件人地址。
  - 事件、应用程序消息和审计记录的电子邮件主题行。
  - 事件、应用程序消息、审计记录、网络交互描述以及整个通知电子邮件消息的文本描述模板。您可以在模板中使用变量。
  - 当发送的通知数量达到最大限额时发送的电子邮件的主题和正文。

- 每天发送的最大电子邮件数。
- 每条消息中的最大通知数。指定可放入单个电子邮件消息中的同一类型（事件、应用程序消息或审计记录）的已注册通知的最大数量。如果存在更多已注册的通知，则会生成额外的电子邮件消息（在每日限制内）。

为了使**电子邮件**连接器正常工作，您必须首先配置邮件服务器连接。

- **主动轮询**

  此连接器类型提供了具有配置控制和主动轮询作业的主动设备轮询功能。

  添加"**活动轮询**"连接器或编辑其设置时，配置连接器的常规设置以及**"详细信息"**下的附加设置：

  - 使用连接器时应用程序用户可以使用的主动轮询方法。
  - 允许或拒绝主动轮询的设备的被允许和被拒绝 IP 地址范围。`0.0.0.0` 地址与所有可能的 IP 地址匹配。

    如果某个地址既包含在允许的 IP 地址中，也包含在拒绝的 IP 地址中，Kaspersky Anti Targeted Attack Platform 会将其归类为拒绝的 IP 地址。
  - 其对应设备可用于主动轮询的地址空间的名称。如有必要，在 **L3 地址空间**字段中选择 IP 地址的地址空间，并在 **L2 地址空间**字段中选择 MAC 地址的地址空间。

    > 如果选择的地址空间与**默认**地址空间不同，请为该地址空间添加新规则（或编辑现有规则）。该规则必须指定选择此地址空间的连接器。当地址空间改变时，规则设置就会被配置。

- KUMA

  此连接器类型提供与 Kaspersky Unified Monitoring and Analysis Platform (KUMA) 的集成。此类连接器的软件模块与 Kaspersky Anti Targeted Attack Platform 分开分发。这种类型的连接器允许您将有关设备和风险的信息发送到 KUMA，以及在 KUMA 中运行命令来更改设备状态。添加连接器后，必须在 KUMA 中配置集成（创建与 Kaspersky Anti Targeted Attack Platform 的连接）。KUMA 连接器使用 Kaspersky Anti Targeted Attack Platform API 与 Central Node 服务器交互。

  KUMA 连接器提供的集成涉及发送有关设备和风险的信息，以及应用命令来改变设备状态。要将事件发送到 KUMA，您可以向 Kaspersky Anti Targeted Attack Platform 添加 **Syslog** 或 **SIEM** 连接器，并为此连接器指定与 KUMA 服务器的连接设置。添加连接器后，需要在 KUMA 端配置一个收集器。

- Cisco **交换机**

  此连接器类型通过思科网络交换机为设备提供自动网络访问控制支持。

  添加 **Cisco 交换机**连接器或编辑其设置时，配置连接器的常规设置以及**"详细信息"**下的附加设置：

  - 您想要在应用程序使用连接器执行的操作的事件中指定的开关的名称。
  - 将连接器连接到交换机的寻址信息：IP 地址和 SSH 端口。
  - 通过 SSH 连接到交换机的凭据。
  - 在建立 SSH 连接之前，需要将公钥与从网络交换机收到的公钥进行匹配；这样做是为了防止网络中此设备被欺骗。如果该值为空，则不执行检查。

- 用于限制设备网络访问的方法。应用程序提供了基于 MAC 地址（MAC ACL）、IP 地址（IP ACL）在交换机访问控制列表中创建拒绝规则的方法，以及通过禁用设备连接到的以太网端口的方法。

  要使用禁用以太网端口的方法，请配置交换机连接以防止多个设备连接到一个端口。否则，禁用以太网端口以阻止一个设备也会阻止使用该端口连接到网络的所有设备的网络访问。

- 当更改网络访问限制方法时，此设置将重置拒绝规则。如果启用此设置，更改方法将重置已设置的阻止设备的规则。

- 此设置将网络设备排除在网络访问限制方法之外。如果启用该设置，则该方法不适用于**网络设备**、**防火墙**、**交换机**、**虚拟交换机**、**路由器**、**虚拟路由器**、Wi-Fi 设备。

- 此设置仅应用拒绝规则于新设备。如果启用此设置，该方法仅适用于已注册事件类型代码为 4000005003 的新设备检测事件的未经授权的设备。

- 设备表中“*已授权*”和“*未授权*”设备的轮询间隔。

- 此设置允许您配置连接器重新启动时有关被阻止设备的通知。如果启用此设置，则在启用或重新启动连接器后，先前已应用网络访问限制的设备列表将发送到 Central Node 服务器。

如有必要，您可以添加其他连接器类型，以促进数据交换或在应用程序与其他接收系统交互时提供执行管理任务的功能。

某些端口和协议用于连接器与 Central Node 服务器的连接。

第三方系统代表应用程序用户之一通过连接器进行连接。我们建议为每个连接器使用单独的用户账户。这将帮助您使用审计记录分析通过连接器执行的操作。

应用程序中的最大连接器数量为 20。连接器类型的最大数量为 100。

受管理和不受管理的连接器

应用程序可以使用受管理和不受管理的连接器。

如果连接器的软件模块能够在*添加*该连接器后自动注册并启动，则该连接器是可管理的，并且当启用、禁用或删除该连接器时，这些模块能够得到管理。只有安装了应用程序组件的节点才可以作为受管理的连接器的部署节点。

*不受管理的连接器*不提供受管理的连接器的功能。您必须在部署连接器的节点上手动注册这样的连接器、启动、停止或删除其软件模块。当您启用或禁用不受管理的连接器时，应用程序会通过允许或拒绝与 Central Node 服务器端的连接器的交互来反映这一点。

连接器和 Central Node 服务器之间的连接使用证书进行保护。当连接器添加到应用程序时，会生成连接器证书。对于受管理的连接器的软件模块，应用程序会自动发送生成的证书。添加不受管理的连接器时（或在忽略受管理的连接器模式下添加受管理的连接器时），必须使用通信数据包手动上传连接器软件模块的证书。如果需要为此类连接器更换证书（颁发新证书），则需要创建一个新的通信数据包并使用它来上传新的证书。替换受管理的连接器证书的唯一方法是删除并重新添加连接器。

将事件、应用程序消息和审计记录发送到第三方系统

您可以配置通过连接器将事件、应用程序消息或审计记录（以下也称为"注册通知"）转发到第三方系统。对于名为 Syslog、**SIEM** 和 **Email** 的**连接器类型**，默认启用发送注册通知的功能。对于 KUMA **连接器类型**，如果安装了应用程序模块，则可以转发已注册通知。当使用添加到应用程序的其他连接器类型时，此功能是否可用取决于这些特定连接器类型的设置。

为每个连接器单独配置注册通知。配置事件类型时，您可以选择要通过连接器转发的事件类型。创建连接器或编辑其设置时，您可以启用或禁用通过此连接器转发所有应用程序消息和所有审计记录。

电子邮件类型的连接器允许限制传输的数据量。对于此连接器类型，您可以设置有关新注册的通知的电子邮件消息的最大数量以及每则消息中注册的通知的最大数量。如果已发送的电子邮件数量达到最大数量，则会向收件人发送另一则消息，通知他们已超出限制。此后，直到 Central Node 服务器所在时区的当天结束为止，都不会发送任何新消息。

通过**电子邮件**连接器发送的电子邮件消息针对每种类型的注册通知分别生成。也就是说，针对事件、应用程序消息和审计记录生成不同的电子邮件消息。

通过 **Syslog** 和 **SIEM** 类型的连接器转发的已注册通知的信息的内容和顺序在这些系统中可能与 Kaspersky Anti Targeted Attack Platform Web 界面中显示的信息的内容和顺序不同。

通过 Cisco 交换机连接器自动控制设备的网络访问

您可以通过 **Cisco 交换机**连接器为设备配置自动网络访问控制。这种类型的连接器与交换机交换信息，以发送命令来添加或删除连接到交换机的设备的网络访问拒绝规则（限制）。

设备的网络访问控制由其状态驱动。连接器在交换机上为具有"*未授权*"状态的设备创建拒绝规则，并在为设备分配"*已授权*"状态后删除规则。

每个连接器只能与一个网络交换机交换信息。

Cisco 交换机连接器用于仅限制那些详细信息包含其 MAC 地址的设备的网络访问。而且，这些 MAC 地址必须存储在网络交换机的 ARP 表中。也就是说，具有这些 MAC 地址的设备必须连接到连接器所连接的网络交换机。

连接器可以使用各种方法来限制设备的网络访问。应用程序提供了基于 MAC 地址（MAC ACL）、IP 地址（IP ACL）在交换机访问控制列表中创建拒绝规则的方法，以及通过禁用设备连接到的以太网端口的方法。

要使用禁用以太网端口的方法，请配置交换机连接以防止多个设备连接到一个端口。否则，禁用以太网端口以阻止一个设备也会阻止使用该端口连接到网络的所有设备的网络访问。

为了最大限度地降低连接器影响设备的网络辅助功能的风险，您可以在配置连接器时启用以下设置：

- 此设置将网络设备排除在网络访问限制方法之外。如果启用该设置，则该方法不适用于**网络设备**、**防火墙**、**交换机**、**虚拟交换机**、**路由器**、**虚拟路由器**、**Wi-Fi** 设备。
- 此设置仅应用拒绝规则于新设备。如果启用此设置，该方法仅适用于已注册事件类型代码为 4000005003 的新设备检测事件的未经授权的设备。

连接器通过 SSH 与网络交换机连接。SSH 连接凭证在连接器配置中指定并存储。为了保护这些对于识别和身份验证至关重要的敏感凭证，连接器会根据存储的值验证它收到的交换机公钥，以防止交换机欺骗。在验证收到的公钥与连接器中保存的公钥匹配后，识别和身份验证详细信息将发送到交换机。

连接器根据其操作的结果记录应用程序内的事件。这些事件类型通过外部技术记录。生成以下事件标题：

- 重置<交换机名称>的设备拒绝规则

  当连接器由于网络访问限制方法的改变而重置设备先前定义的拒绝规则时，会记录此类事件。

- 根据来自<交换机名称>的数据，更新了关于<设备名称>的信息，地址为<设备 MAC 地址>

  此类事件表示连接器从交换机接收到某个设备连接到某个端口的信息。

- 在<交换机名称>上为<设备名称>添加了设备拒绝规则

  当连接器限制未经授权的设备的网络访问时，会记录此类事件。

- 删除了<交换机名称>上<设备名称>的拒绝规则

  当连接器成功删除特定设备的网络访问限制时，会记录此类事件。

- <交换机名称>先前已添加拒绝规则

  此类事件表明，连接器在打开或重新启动时发现特定交换机上存在预先存在的拒绝规则。

- 在未验证公钥的情况下与<交换机名称>建立了 SSH 连接

  当连接器成功与交换机建立 SSH 连接但无法验证其公钥时，会记录此类事件。我们建议验证网络上没有欺骗设备，然后在连接器设置中保存新的公钥。

- 检测到<交换机名称>的公钥不匹配

  当连接器检测到交换机存储的公钥和接收的公钥不匹配时，就会记录此类事件。这会阻止与交换机的 SSH 连接。我们建议验证网络上没有欺骗设备，并且交换机公钥确实已更改，然后在连接器设置中保存新的公钥。

- 无法与交换机<交换机名称>建立 SSH 连接：凭据不正确

  当连接器由于连接器设置中指定的凭证（用户名或密码）不正确而无法与交换机建立 SSH 连接时，会记录此事件。

- 未对交换机<交换机名称>执行特权模式操作：密码不正确

  当连接器没有特权模式功能来添加和删除交换机上的设备拒绝规则时，会记录此事件。这种情况下，请在连接器设置中输入正确的特权模式密码。

添加连接器

您可以根据应用程序中可用的连接器类型之一添加连接器。不受管理的连接器仅应基于自定义连接器类型创建。

在添加连接器之前，我们建议创建一个单独的用户账户，第三方系统将使用该账户连接到应用程序。为了使**电子邮件**连接器正常工作，您必须首先配置邮件服务器连接。

要添加连接器：

1. 使用应用程序管理员账户登录 Web 界面。
2. 选择“**设置**”部分，“**连接器**”子部分。

3. 在“**连接器**”选项卡上，单击“**添加连接器**”打开详细信息区域。

4. 配置连接器常规设置：

   a. 选择相关的连接器类型并输入连接器名称。

   b. 如果要添加不可管理的连接器（或配置为忽略可管理连接器功能的连接器），请输入访问连接器证书的密码。

   使用定义的密码，证书将被加密在连接器的通信数据包中。

   c. 指定 Central Node 服务器的 IP 地址。

   连接器使用指定的地址连接到 Central Node。

   d. 指定要部署连接器的节点：

   - 如果要添加受管理的连接器，可以指定其中一个已安装应用程序组件的节点作为连接器部署节点。
   - 如果要添加不受管理的连接器，则必须输入要运行该连接器的软件模块的计算机的 IP 地址。

   e. 选择第三方系统将用于通过连接器连接到应用程序的用户。您必须指定其中一个应用程序用户的名称。

5. 在**“详细信息”**下，根据连接器的类型指定高级设置。如果连接器类型不允许管理高级设置，则“**详细信息**”设置组不会显示在详细信息区域中。

6. 如果连接器的类型允许转发审计记录和应用程序消息，请使用相应的复选框启用或禁用此数据的转发。

7. 如果需要，请输入连接器的描述。

8. 单击“**保存**”。

新的连接器已添加到连接器表中。

如果您添加了不受管理的连接器，Central Node 会为新的连接器生成一个通信数据包，然后您的浏览器会保存下载的文件。根据您的浏览器的设置，屏幕上可能会显示一个窗口，您可以在其中指定下载文件的路径和名称。您需要将新的通信数据包的内容上传到将使用连接器的应用程序。

查看连接器表

连接器表显示在“**设置**”部分，“**连接器**”子部分中，“**连接器**”选项卡上。

连接器设置显示在表格以下列中：

- **名称**。

  为连接器指定的名称。

- **连接器 ID**。

  连接器创建时指定的 ID。

- **已启用**。

  指示 Central Node 是否已准备好与连接器的软件模块交互。如果此设置的值为“**否**”，则 Central Node 服务器将不接受来自连接器应用程序模块的请求。

- **状态**。

  连接器的软件模块的状态。可以有以下状态：

  - **等待注册**：添加不受管理的连接器或为不受管理的连接器创建新的通信数据包后，尚未通过此连接器建立连接。
  - **切换**：连接器的应用程序模块状态从**关**切换到**开**，或从开切换到关。
  - **关**表示 Central Node 服务器不接受来自连接器应用程序模块的请求。如果连接器是可管理的，则会向其应用程序模块发送停止命令。
  - "**开**"表示已使用为此连接器创建的证书通过此连接器成功建立连接。
  - "**错误**"表示尝试使用连接器的应用程序模块执行操作时发生错误。

- **类型**。

  连接器类型的图标和名称。

- **上次连接**。

  上次通过连接器连接的日期和时间。

- **可管理**。

  指示连接器是可管理的。如果设置为"**否**"，则连接器是不受管理的，或者配置为忽略受管理的连接器功能。

- **更改时间**。

  连接器设置的最后修改日期和时间。

- **描述**。

  为连接器指定的描述。

查看连接器表时，您可以使用配置、过滤、搜索和排序功能。

启用或禁用连接器

如果您想暂时阻止连接器的软件模块连接到 Central Node 服务器，您可以禁用该连接器。如果您想恢复连接，请启用连接器。

要启用或禁用连接器：

1. 使用应用程序管理员账户登录 Web 界面。
2. 选择"**设置**"部分，"**连接器**"子部分。
3. 在"**连接器**"选项卡，选择要启用或禁用的连接器。

   详细信息区域显示在 Web 界面窗口的右侧。
4. 根据需要单击"**启用**"或"**禁用**"。

   这将打开一个确认提示窗口。
5. 在提示窗口中，单击"**确定**"。

编辑连接器设置

要编辑连接器设置：

1. 使用应用程序管理员账户登录 Web 界面。
2. 选择“**设置**”部分，“**连接器**”子部分。
3. 在“**连接器**”选项卡，选择相关连接器。
   详细信息区域显示在 Web 界面窗口的右侧。
4. 单击**“编辑”**。
5. 按照与添加连接器相同的方式编辑设置。
   并非所有设置都可编辑。例如，您不能更改连接器的类型。
6. 单击“**保存**”。

更改显示在连接器表的相应列中。如果您更改了连接器的名称，新名称将显示在事件类型表的列标题中。

编辑不受管理的连接器的某些设置会导致 Central Node 服务器为连接器生成新的通信数据包（例如，如果您在忽略受管理的连接器模式下更改 **Syslog** 连接器的服务器地址）。根据您的浏览器设置，可能会显示一个窗口，您可以在其中更改要保存的通信数据包的路径和名称。将新的通信数据包的内容上传到使用连接器的应用程序。否则，该应用程序将无法通过该连接器建立新的连接。

为连接器创建新的通信数据包

添加不受管理的连接器时，会自动为该连接器创建通信数据包。如有必要，您可以为连接器创建一个新的通信数据包（例如，如果来自旧通信数据包的证书已被已泄露）。

创建新的通信数据包后，旧通信数据包中的证书将失效。因此，下次通过此连接器连接第三方系统时，必须使用新的通信数据包。

要为不受管理的连接器创建新的通信数据包：

1. 使用应用程序管理员账户登录 Web 界面。
2. 选择“**设置**”部分，“**连接器**”子部分。
3. 在“**连接器**”选项卡，选择要为其创建新的通信数据包的非可管理连接器。
   详细信息区域显示在 Web 界面窗口的右侧。
4. 单击“**获取新的通信数据包**”。
   这将打开“**生成新的通信数据包**”窗口。

5. 指定创建通信数据包的设置：

   - 第三方系统将用于通过连接器连接到应用程序的用户的名称。您必须指定其中一个应用程序用户的名称。

     我们推荐指定在添加连接器时指定的用户名。如果需要指定不同的用户名，我们推荐选择其他连接器未使用且未用于通过 Web 界面连接到 Central Node 的应用程序用户。

   - 连接器的软件模块正在运行的节点的地址。

   - 连接器证书的密码。指定的密码用于加密连接器通信数据包中的证书。

6. 单击“**创建通信数据包**”。

   服务器为所选的连接器生成新的通信数据包，之后您的浏览器会保存下载的文件。根据您的浏览器的设置，屏幕上可能会显示一个窗口，您可以在其中指定下载文件的路径和名称。将下载的通信数据包的内容上传到使用连接器的应用程序。否则，该应用程序将无法通过连接器建立新的连接。

正在删除连接器

当删除受管理的连接器时，其软件模块会在部署该连接器的节点上自动停止并删除。

如果要删除不受管理的连接器或处于忽略受管理的连接器模式的连接器，则必须在删除连接器之前手动停止并删除连接器的软件模块。

要删除连接器：

1. 使用应用程序管理员账户登录 Web 界面。
2. 选择“**设置**”部分，“**连接器**”子部分。
3. 在“**连接器**”选项卡上，选择要删除的连接器。

   详细信息区域显示在 Web 界面窗口的右侧。
4. 单击“**删除**”。

   这将打开一个确认提示窗口。
5. 在提示窗口中确认删除所选连接器。

添加和删除连接器类型

连接器类型定义了连接器可用的功能以及这些功能中实现了哪些功能。您可以使用应用程序内置的两种连接器类型（其供应商是卡巴斯基），或任何其他供应商提供的其他类型的连接器。

要向应用程序添加连接器类型，您必须从供应商处获取以下文件：

- 用于安装连接器软件模块的文件
- 连接器类型描述文件

> 如果第三方供应商的连接器类型允许您在连接器中存储访问第三方系统的用户凭证，我们建议采取措施保护此类凭证免遭泄漏。为了最大限度地降低凭证被泄漏的风险，我们建议向此类账户授予必要的最低权限（仅足以通过连接器建立连接）。

连接器类型表显示在“**设置**”部分，“**连接器**”子部分中，“**连接器类型**”选项卡上。

查看连接器类型表

连接器类型表显示在“**设置**”部分，“**连接器**”子部分中，“**连接器类型**”选项卡上。

连接器设置显示在表格以下列中：

- **名称**。
  供应商指定的连接器类型的名称。
- **供应商**。
  连接器类型的供应商名称。
- **版本**。
  连接器类型的版本号。
- **代码**。
  连接器类型的唯一编号。
- **能力**。
  此类型的连接器必须具备的功能列表。

查看连接器类型表时，您可以使用配置、过滤、搜索和排序功能。

添加连接器类型

您可以使用连接器类型供应商提供的描述文件将连接器类型添加到应用程序。连接器类型描述文件必须打包到 ZIP 档案中。

您必须使用连接器类型供应商提供的文件，手动安装您要添加的连接器类型的连接器软件模块。在您想要在添加连接器时指定为连接器部署节点的计算机上安装软件模块。

要添加连接器类型：

1. 使用应用程序管理员账户登录 Web 界面。
2. 选择“**设置**”部分，“**连接器**”子部分。

3. 在“**连接器类型**”选项卡上，单击“**添加连接器类型**”打开详细信息区域。

4. 单击**“浏览”**选择连接器类型描述文件。

5. 单击“**保存**”。

新的连接器类型被添加到连接器表中。

删除连接器类型

删除连接器类型时，应用程序将删除有关该连接器类型的信息，以及使用此类型添加的所有连接器。

要删除连接器类型：

1. 使用应用程序管理员账户登录 Web 界面。

2. 选择“**设置**”部分，“**连接器**”子部分。

3. 在“**连接器类型**”选项卡上，选择要删除的连接器类型。
详细信息区域显示在 Web 界面窗口的右侧。

4. 点击“**删除**”。
这将打开一个确认提示窗口。

5. 在提示窗口中确认删除所选连接器类型。

6. 如果应用程序具有此类型的连接器，请确认也删除这些连接器。

管理远程连接的账户凭据 Secret

Kaspersky Anti Targeted Attack Platform 实现了 Secret 存储。*Secret* 使您能够安全地存储和使用应用程序自动远程连接到设备所需的标识和身份验证信息。Secret 用于主动轮询作业。

应用程序支持各种类型的 Secret。根据 Secret 的用途，您可以在添加或编辑 Secret 设置时选择相关类型并输入适当的数据。

将使用远程连接协议进行设备远程连接所需的凭据保存在 Secret。根据所选的轮询方法，主动轮询作业可以使用各种协议进行远程连接。

为了确保安全地使用存储在 Secret 中的身份和身份验证详细信息，该应用程序实施了在连接到远程设备时防止 Secret 泄漏的保护。在应用程序中保存从设备收到的公钥后，它会监控到这些设备的所有后续远程连接，并且在网络上发生设备欺骗时不会发送来自 Secret 的信息。

Secret 的关键信息（密码或证书私钥），只有在创建 Secret 时输入这些信息时才能以纯文本形式提供一次。保存 Secret 后，其关键信息将无法再查看。您只能在编辑 Secret 时用新的关键信息替换 Secret 的关键信息（例如，您可以输入不同的密码）。

您可以在“**设置**”部分，“**Secret**”子部分中管理 Secret。不能向应用程序添加超过 500 个 Secret。

只有具有管理员角色的用户才能管理 Secret。

添加 Secret

您可以将 Secret 添加到应用程序 Secret 存储中。

要添加 Secret：

1. 使用应用程序管理员账户登录 Web 界面。
2. 选择“**设置**”部分，“**Secret**”子部分。
3. 单击“**添加 Secret**”。

   这将打开详细信息区域。
4. 输入 Secret 的名称。

   Secret 名称必须是唯一的（不得与其他 Secret 的名称匹配）并且必须包含最多 256 个字符。您可以使用字母、数字、空格和以下特殊字符：`! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . - _`。Secret 名称必须以空格以外的任何有效字符开始和结束。
5. 选择 Secret 类型并配置其设置。

   您可以选择以下类型的 Secret：

   - **仅密码**：如果仅需要具有相关权限的用户的密码即可访问设备配置数据，则使用此类 Secret。
   - **用户名和密码**：如果需要用户名和密码才能从设备接收数据，则使用此类 Secret。
   - **用户名和密码，root 密码**：如果需要用户名和密码才能从设备接收数据，而对于具有管理员（root）权限的连接，还需要 root 密码或以管理员权限处理请求的账户的密码，则使用此类 Secret。
   - **用户名和密码，加密密码**：如果需要用户名和密码才能从设备接收数据，并且还需要加密密码才能建立加密连接，则使用此类 Secret。
   - **混合** Secret 类型用于设备轮询的**远程连接**方法。您可以为此类 Secret 指定以下设置：

     - 用于远程连接设备的用户名。

       用户名可以包含拉丁字母、数字、句点以及特殊字符：`_` 和 `-`。名称必须以字母开头，并以除句点之外的任何受支持的字符结尾。
     - **用户密码**：是否使用用户密码进行身份验证。

       密码可以包含最多 256 个 ASCII 字符。
     - **私钥**：是否使用证书的私钥进行身份验证。

       您可以手动输入组成密钥的字符序列，或者通过单击“**从文件复制**”从证书文件上传密钥。您可以上传 CRT、PEM 和 CER 格式的私钥。如果私钥文件受密码短语保护，请在上传密钥之前在“**密码短语**”字段中输入密码短语。

要使用证书的私钥，您需要将此证书的公钥复制到将使用 Secret 进行远程连接的所有设备上。将公钥复制到设备的步骤无需 Kaspersky Anti Targeted Attack Platform 的参与。

- **Root 用户密码**：如果以管理员 (root) 权限连接网络部件时需要额外的密码。在这种情况下，将以 root 身份或在网络设备上配置为以管理员权限处理请求的用户身份请求访问。

6. 单击“**保存**”。

查看 Secret 表

远程连接 Secret 表显示在应用程序 Web 界面的“**设置**”→“**Secret**”部分。

有关 Secret 的信息显示在表的以下列中：

- **Secret 名称**。
  应用程序对 Secret 使用的名称。
- **创建日期**。
  将 Secret 添加到应用程序的日期和时间。
- **更改时间**。
  应用程序中 Secret 最后修改的日期和时间。

查看 Secret 表时，您可以使用配置、过滤、搜索和排序功能。

连接到远程设备时防止 Secret 泄漏

Secret 中的识别和身份验证详细信息仅应用于与选定用于主动轮询作业的设备的远程连接。为了保护这些信息在设备欺骗的情况下免遭可能的泄漏，应用程序会在发送信息之前验证从设备收到的公钥。设备使用公钥建立 SSH 连接。公钥可帮助应用程序验证是否与正确的设备建立了 SSH 连接。验证收到的公钥与应用程序中保存的公钥匹配后，识别和身份验证详细信息将被发送到设备。

保存的设备公钥显示在“**常规**”选项卡上所选设备的详细信息区域中。

在应用程序中接收并保存设备公钥

默认情况下，Kaspersky Anti Targeted Attack Platform 中未配置任何设备的公钥。首次与该设备建立 SSH 连接时，将接收并保存设备的公钥，以便作为使用**主动轮询**类型的连接器的主动轮询任务的一部分进行扫描。所选秘密的识别和身份验证详细信息将发送到设备，而无需检查收到的公钥。因此，在首次对选定的设备启动主动轮询作业并与其建立 SSH 连接之前，请确保网络上没有被欺骗的设备。为此，您可以运行 `ifconfig` 来检查应用程序中配置的设备的 IP 地址是否与实际设备网络接口上的 IP 地址匹配。

重置已保存的设备公钥

设备上的 SSH 连接密钥可能会随着时间而改变。当设备用户当前的私钥面临泄漏风险时，他们可能会生成新密钥。

当设备上的私钥发生变化时，相应的公钥也会发生变化。更改公钥后，应用程序将停止将 Secret 信息发送到该设备，因为新的公钥不再与应用程序中保存的指纹匹配。因此，作为主动轮询作业一部分的任何后续设备扫描都会以错误结束。

更改设备上的公钥后，您必须重置应用程序中存储的该设备当前保存的公钥。这将允许在远程连接设备时再次使用这些 Secret。

重置保存的公钥后，应用程序将在下次与设备建立 SSH 连接时保存新收到的公钥。检查网络上没有欺骗设备，类似于最初接收和存储公钥时。

只有具有“**高级安全官**”角色的用户可以重置设备保存的公钥。

要重设保存的设备公钥：

1. 使用 Web 界面以“**高级安全官**”角色连接到 Central Node。
2. 选择“**资产**”部分。
3. 在“**设备**”选项卡上，选择要重置已保存的公钥的设备。
4. 右键单击其中一个选定的设备以打开上下文菜单。
5. 在上下文菜单中，选择“**重置公钥**”。
   这将打开一个确认提示窗口。
6. 在提示窗口中，单击“**确定**”。

编辑 Secret 的设置

编辑 Secret 设置时，您可以更改其类型或设置不同的凭据。

修改 Secret 设置（包括 Secret 名称）后，新设置将应用于之前指定过 Secret 的主动轮询作业。如果您更改 Secret 的类型，则当 Secret 的新类型与连接器设置不匹配时，下次启动这些作业时可能会出现错误。

要编辑 Secret 的设置：

1. 使用应用程序管理员账户登录 Web 界面。
2. 选择“**设置**”部分，“**Secret**”子部分。
3. 选择您想要编辑的 Secret。
   详细信息区域显示在 Web 界面窗口的右侧。
4. 单击**“编辑”**。

5. 根据需要编辑设置。您可以按照与添加 Secret 时相同的方式编辑设置。

   Secret 的关键信息（密码和证书的私钥）不会公开显示。您只能使用带有凭证的字段上方的链接将 Secret 的关键信息替换为新的关键信息。

删除 Secret

您可以从 Kaspersky Anti Targeted Attack Platform Secret 存储中删除 Secret。

在删除 Secret 之前，我们建议在使用该 Secret 的主动轮询作业中指定不同的 Secret 或不同的轮询方法。如果在主动轮询作业中指定了已删除的 Secret，则下次运行作业时会出现错误。

若要删除 Secret：

1. 使用应用程序管理员账户登录 Web 界面。
2. 选择“**设置**”部分，“**Secret**”子部分。
3. 选择您想删除的 Secret。
4. 单击“**删除**”。

   这将打开一个确认提示窗口。
5. 在确认提示窗口中，确认删除 Secret。

更新应用程序数据库

应用程序数据库（以下也称为“数据库”）是包含记录的文件，这些记录由应用程序组件和模块用于检测在组织的 IT 基础架构中发生的事件的记录的文件。

卡巴斯基的病毒分析师每天检测到成百上千种新威胁（包括“零日”漏洞），并创建记录来识别它们，将它们加入到数据库更新包（或“更新包”）中。*更新包*由一个或多个包含记录的文件组成，这些记录可用于识别自上次更新包发布以来检测到的威胁。我们建议您定期接收更新包。安装应用程序时，数据库发布日期与应用程序发布日期相同，因此在安装应用程序后必须立即更新数据库。

应用程序会每 30 分钟一次自动寻找卡巴斯基更新服务器上的新更新包。默认情况下，如果由于某些原因应用程序数据库在 24 小时内未更新，Kaspersky Anti Targeted Attack Platform 会在应用程序 Web 界面窗口的**控制板**部分显示此信息。

如果不支持 Kaspersky Anti Targeted Attack Platform 的版本，则不会更新应用程序数据库，并且应用程序 Web 界面的“**系统健康**”窗口的“**控制板**”部分，显示“*不再支持此版本的 Kaspersky Anti Targeted Attack Platform。请将应用程序升级为支持的版本。*”警告。

您可以在应用程序生命周期页面查看当前支持哪些应用程序版本。

更新功能（包括反病毒签名更新和代码库更新）以及 KSN 功能可能无法在美国境内使用。

在分布式解决方案和多租户模式下，应用程序数据库在每个 PCN 和 SCN 服务器上独立更新。

如果您在隔离网络或互联网带宽有限的网络中部署了 Kaspersky Anti Targeted Attack Platform，则可以使用卡巴斯基更新实用程序配置应用程序数据库更新。

选择数据库更新源

如果您使用分布式解决方案和多租户模式，请使用要为其配置参数的 PCN 或 SCN 服务器的 Web 界面。

您可以选择应用程序将下载数据库更新的来源。更新源可以是卡巴斯基服务器、一个网络文件夹或组织的计算机上的本地文件夹。

选择数据库更新源：

1. 在应用程序 Web 界面窗口中，选择**设置**部分的**常规设置**子部分。
2. 在**数据库更新**部分，在**更新源**下拉列表中，选择下列值之一：
   - **卡巴斯基更新服务器**。

     该应用程序通过 HTTP 连接到卡巴斯基更新服务器并下载最新的数据库。
   - **卡巴斯基更新服务器 (安全连接)**。

     该应用程序通过 HTTPS 连接到卡巴斯基更新服务器并下载最新的数据库。建议使用 HTTPS 进行数据库更新。
   - **自定义服务器**。

     该应用程序可连接到您的 FTP 或 HTTP 服务器或计算机上包含应用程序数据库的文件夹以下载最新的数据库。

     HTTP 必须用于 HTTP 服务器和 Central Node 之间的通信。在这种情况下不支持 HTTPS。
3. 如果选择了**自定义服务器**，请在该设置名称下的字段中，输入 HTTP 服务器上更新包的 URL，或计算机上包含应用程序数据库更新包的文件夹的完整路径。
4. 单击**应用**。

应用程序数据库更新源已应用。

手动更新数据库

要开始手动更新数据库：

1. 在应用程序 Web 界面窗口中，选择**设置**部分的**常规设置**子部分。
2. 在**数据库更新**部分，单击**开始**按钮。
3. 单击**应用**。

应用程序数据库更新开始。更新进度将显示在按钮右侧。

使用卡巴斯基更新实用程序进行更新数据库

如果您已将 Kaspersky Anti Targeted Attack Platform 部署在隔离网络或互联网带宽有限的网络中，则可以使用卡巴斯基更新实用程序配置应用程序数据库更新。在这种情况下，该实用程序会将更新包下载到组织本地网络之外的计算机，然后将其复制到您的 FTP 或 HTTP 服务器。Kaspersky Anti Targeted Attack Platform 随后会从此服务器获取更新包。

使用该实用程序配置应用程序数据库更新涉及以下步骤：

1. 使用卡巴斯基更新实用程序下载更新包。
   首先，您需要联系卡巴斯基技术支持，并索取该实用程序的分发包以及您可以从中下载更新的服务器列表。
2. 将更新包上传到您的 FTP 或 HTTP 服务器。
3. 选择此 FTP 或 HTTP 服务器作为数据库更新源。

使用卡巴斯基更新实用程序下载更新包

要按照这些步骤操作，您需要该实用程序的分发包以及可以从中下载更新的服务器列表。您可以向卡巴斯基技术支持索取这些信息。

要使用卡巴斯基更新实用程序下载更新包：

1. 将包含实用程序分发包的文件夹下载到您的计算机。
2. 运行 UpdateUtility-Gui.exe 文件。
3. 在打开的窗口中，点击“**应用程序**”按钮，然后选中 **7.0-7.1** 选项左侧的复选框。
4. 点击“**确定**”和“**应用**”。
5. 在实用程序的主窗口中，点击“**设置**”按钮，然后选择“**下载**”。
6. 在“**更新源**”下，选择“**其他**”，然后输入用于下载更新的服务器地址。
7. 点击“**确定**”和“**应用**”。
8. 单击“**启动**”。

   更新包被下载到运行该实用程序的计算机上。

创建存档的密码列表

该应用程序不扫描受密码保护的存档。您可以为在组织内交换文件时使用的存档创建最常遇到的密码列表。如果这样做，应用程序将在扫描存档时尝试列表中的密码。如果其中一个密码匹配，则将解锁并扫描存档。

应用程序设置中设置的密码列表也会传输到具有 Sandbox 组件的服务器。

要创建存档密码列表：

1. 在应用程序 Web 界面窗口中，选择**设置**部分的**存档密码**子部分。
2. 在**存档密码**字段中，输入应用程序用于密码保护存档的密码。

   在新行上输入每个密码。您最多可以输入50个密码。
3. 单击**应用**。

将创建存档的密码列表。扫描受密码保护的 PDF 文件以及 Microsoft Word、Excel® 和 PowerPoint® 文件时，应用程序将使用定义列表中的密码。

具有**安全审计员**角色的用户可以查看存档的密码列表，但无法编辑它。

与工具集成以解包加密的 SSL/TLS 流量

Kaspersky Anti Targeted Attack Platform 接收来自第三方解密工具到标准网络接口的解密 SSL/TLS 流量，对其进行处理和分析。在 Kaspersky Anti Targeted Attack Platform 中配置解密流量的接收和处理类似于配置镜像 SPAN 流量的接收与处理；您必须在应用程序安装期间启用 SPAN 集成支持。

与未加密流量相比，在应用程序中接收解密流量会使流量处理负载增加 5 倍。关于 Central Node 服务器的硬件要求的详细信息，请参阅*"Central Node 组件的计算"*。

当接收解密流量时，Kaspersky Anti Targeted Attack Platform 可能会处理并保留通过加密协议传输的机密信息。例如，用户名和密码、银行卡号。

对于安全人员：应用程序 Web 界面使用入门

本节适用于在组织内负责数据安全的专家。它包含有关为企业 IT 基础架构的安全性配置资源以及及时检测威胁的信息和说明。

该应用程序允许多个安全人员一起工作。

Kaspersky Anti Targeted Attack Platform 界面

该应用程序通过 Web 界面进行管理。应用程序 Web 界面的各个部分因用户的角色不同而有所不同：管理员或高级安全官（**高级安全官**、**安全官**、**安全审计员**）。

应用程序 Web 界面窗口包含如下内容：

- 应用程序 Web 界面窗口左侧和下侧的部分。
- 在应用程序 Web 界面窗口上部用于应用程序某些部分的选项卡。
- 应用程序 Web 界面窗口下侧的工作区。

应用程序 Web 界面窗口的部分

应用程序 Web 界面为具有**高级安全官**、**安全官** 和**安全审计员**角色的用户提供以下部分：

- **控制板**。包含 Kaspersky Anti Targeted Attack Platform 监控数据。
  对于具有“**安全审计员**”角色的用户，“**控制板**”窗口包含以下部分：**警报**、**系统健康**。
- **警报**。包含有关您有权访问的租户网络中的警报的信息。
- **网络流量事件**。有关网络流量中的事件和聚合事件的信息。
- **威胁搜索**。包含有关在您有权访问的租户的主机上发现的事件的信息。
- **任务**。包含有关可用于管理主机上的文件和应用程序的任务的信息。
- **防止**。包含有关可用于管理在选定主机上文件运行阻止的策略的信息。
- **自定义规则**：TAA、**入侵检测**、IOC、YARA、**Sandbox**。包含用于管理用户定义的规则的信息。
- **存储**：**文件**和**隔离区**。包含用于管理隔离区和存储中的对象的信息。
- **资产**。包含有关具有 Kaspersky Endpoint Agent 组件的计算机及其设置的信息。
- **网络地图**：**网络交互图**、**拓扑图**、**网络会话**。包含不同时间段设备交互的信息、网络中设备物理连接图以及网络会话信息。
- **风险和异常**。包含有关信息系统资源所面临的风险的信息。

- **报告**: **生成的报告** 和 **模板**。包含报告构建器和生成的关于警报的报告列表。
- **日志**：**应用程序消息**。包含有关应用程序性能的信息。
- **设置**：**连接器**、Secret、**IOC 扫描计划**、Endpoint Agent、**KPSN 信誉数据库**、**通知规则**、**VIP 状态**、**排除项**、**允许规则**、Sandbox **服务器**、**存档密码** 和 **授权许可**。包含有关连接器设置的信息、Secret 信息、IOC 扫描计划的信息、Endpoint Agent 组件设置的信息、以及在 KPSN 中发布对象以及根据警报中包含的信息将 VIP 状态分配给警报的设置、允许的对象列表、从扫描中排除的 IDS、TAA (IOA) 和 ICAP 规则、存档密码和添加的密钥。

对于具有"**安全审计员**"角色的用户，应用程序的 Web 界面除了包含上面列出的部分外，还包含以下部分：

- **操作模式**。包含有关 PCN 和 SCN 服务器以及分布式解决方案和多租户模式中租户的信息。
- **Sensor 服务器**。包含有关 Central Node 组件和与其连接的 Sensor 组件的信息。
- **Sandbox 服务器**。包含有关 Central Node 组件与 Sandbox 组件的连接的信息。
- **外部系统**。包含有关应用程序与邮件传感器集成的信息。
- **服务器配置**。包含有关应用程序的尺寸参数的信息。

应用程序 Web 界面窗口的工作区

工作区显示了您选择在应用程序 Web 界面窗口的各个部分和选项卡上查看的信息。它还包含了可用于配置信息显示方式的控制元素。

选择要在应用程序的 Web 界面中管理的租户

如果您用**高级安全官**或者**安全官**账户使用分布式解决方案和多租户模式，在开始使用 Web 界面之前，您必须在应用程序 Web 界面中选择要管理的租户。

要在应用程序的 Web 界面中选择要管理的租户：

1. 在应用程序 Web 界面菜单的上部，单击租户名称旁边的箭头。
2. 在**选择租户**下拉列表中，选择一个租户。
   您还可以开始在搜索框中键入租户的名称，然后从搜索结果列表中选择租户。

应用程序 Web 界面中的所有操作都会应用于所选租户。如果您想选择其他租户，请重复选择租户的步骤。

具有**安全审计员**角色的用户无法在 Web 界面中选择要管理的租户。

监控应用程序的性能

您可以使用应用程序 Web 界面窗口的**控制板**部分中的小组件来监控应用程序运行。您可以添加、删除和移动小组件，配置小组件的显示比例，以及选择数据显示时段。

关于小组件和布局

您可以使用小组件来监控应用程序运行。

*布局*是**控制板**部分中应用程序 Web 界面窗口工作区的外观。您可以在布局中添加、删除和移动小组件，以及配置小组件的比例。

如果您使用分布式解决方案和多租户模式，此部分将显示所选租户的信息。NDR 小部件仅显示当前或选定节点的信息。

默认情况下，此部分仅显示有关用户未处理的警报的信息。若要也显示有关已处理警报的信息，请启用窗口右上角的“**显示已关闭的警报**”切换开关。

控制板部分显示以下小组件：

- 警报:
  - **按状态分类的警报**。显示警报状态，具体取决于处理警报的 Kaspersky Anti Targeted Attack Platform 用户以及是否已处理该警报。
  - **按技术分类的警报**。显示生成警报的应用程序模块或组件的名称。
  - **按攻击向量分类的警报**。根据攻击的矢量显示检测到的对象。
  - **按重要性排列的 VIP 警报**。显示 VIP 身份警报的重要性，具体取决于这些警报可能对基于卡巴斯基经验的计算机或企业局域网安全性产生的影响。
  - **按重要性分类的警报**。显示 Kaspersky Anti Targeted Attack Platform 用户警报的重要性，具体取决于这些警报可能对基于卡巴斯基经验的计算机或企业局域网安全性产生的影响。

  每个小组件的左侧部分显示攻击向量、警报重要性级别、警报状态以及生成警报的扫描技术。每个小组件的右侧部分显示程序在小组件上选定数据显示时段期间警报被触发的次数。

  单击包含攻击媒介名称、警报重要级别、警报状态和生成警报的扫描技术的链接，您将转到应用程序 Web 界面的“**警报**”部分，您可以在其中查看相关警报。警报根据选定内容进行筛选。
- 前 10 个：
  - **域**。警报中最常见的 10 个域名。
  - **IP 地址**。警报中最常见的 10 个 IP 地址。
  - **发件人的电子邮件地址**。警报中最常见的 10 个电子邮件发件人。
  - **收件人电子邮件地址**。警报中最常见的 10 个电子邮件收件人。

- **TAA 主机**。针对性攻击分析器 (TAA) 技术生成的事件和警报中最常出现的 10 台主机。
- **TAA 规则**。在针对性攻击分析器 (TAA) 技术生成的事件和警报中最常出现的 10 个 TAA (IOA) 规则。
- **按 TAA 规则发送到 Sandbox**。最常导致 Kaspersky Anti Targeted Attack Platform 发送文件以供 Sandbox 组件扫描的 10 个 TAA (IOA) 规则。

每个小组件的左侧部分列出了域、收件人的电子邮件地址、邮件发件人的 IP 地址和电子邮件地址、主机名和 TAA (IOA) 规则名称。每个小组件的右侧部分显示程序在小组件上选定数据显示时段期间警报被触发的次数。

单击带有每个域名、收件人地址、IP 地址以及邮件发件人地址的链接，您可以转到应用程序 Web 界面的"**警报**"部分，并查看相关警报。

单击带有主机名和 TAA (IOA) 规则名称的链接，转到应用程序 Web 界面的"**事件**"部分，并查看相关事件。

警报和事件基于所选元素进行过滤。

- NDR：
  - **网络流量事件得分**。选定时间段内事件按得分分布的条形图。条形图对应分数的整数值。您可以将数据显示模式更改为饼图，按严重性级别分布事件。根据分数，事件的严重程度可能为*低*(0.0–3.9)、*中*(4.0–7.9)或*高*(8.0–10.0)。
  - **按技术划分的网络流量事件**。在选定时间段内，通过哪种事件注册技术注册了多少个事件。
  - **设备安全状态**。按设备安全状态进行分布。
  - **网络流量事件中频繁出现的应用程序用户**。根据选定时间段内的 EPP 应用程序信息，在事件中注册最频繁的用户名。
  - **网络流量事件中频繁出现的应用程序**。根据选定时间段内的 EPP 应用程序信息，在事件中注册最频繁的第三方应用程序。
  - **网络流量事件中频繁出现的设备**。选定时间段内事件中注册最频繁的设备。
  - **按风险计数排名靠前的设备**。在选定时间段内检测到的风险的最常注册的设备。
  - **风险分数**。选定期间内风险按分数分布的条形图。条形图对应分数的整数值。您可以将数据显示模式更改为饼图，以按严重程度分布风险。根据分数，风险的严重程度可能为*低*(0.0–3.9)、*中*(4.0–7.9)或*高*(8.0–10.0)。
  - **自定义小部件**。您可以创建具有任意内容的小组件。例如，您可以使用自定义小组件在"**控制板**"部分中以逻辑方式分隔小组件组。
  - **设备**。包含有关网络上的设备的信息（按设备类别排列）。
  - **网络流量事件**。包含有关具有最近的上次可见日期和时间的 NDR 事件和聚合事件的信息。
  - **态势感知**。有关当前已识别的系统安全威胁的通知（例如，检测到 10 次未经授权的网络交互）。此小组件按重要性顺序显示通知。
  - **EPP 应用程序的保护**。受 EPP 应用程序保护的计算机数量与未受 EPP 应用程序保护的计算机数量之比。饼图中央显示受保护和未受保护的计算机的总数。

如果 Kaspersky Anti Targeted Attack Platform 意识到满足以下条件，则认为计算机受到EPP 应用程序的保护：

- 计算机上安装了 EPP 应用程序。
- 正在为 EPP 应用程序运行实时保护任务。
- EPP 应用程序与集成服务器的连接处于*活动*状态。

如果至少有一个条件没有满足，则计算机被认为未受到 EPP 应用程序的保护。将针对 Kaspersky Anti Targeted Attack Platform 中所有包含 Windows 操作系统（任何版本）名称作为所安装操作系统的设备，或设备属于以下类别之一，执行是否缺少 EPP 应用程序保护的检查：

- **服务器**
- **工作站**

为了在 NDR 小部件中显示正确的信息，您必须配置 Central Node 和 Sensor 组件之间的日期和时间同步。

小部件仅显示动态变化的基本信息。如果您需要查看详细信息（例如，有关有问题的设备的信息），您可以从“**控制板**”部分导航到应用程序 Web 界面的其他部分。您可以通过单击小部件来导航 Web 界面。

添加小组件到当前布局

要添加小组件到当前布局：

1. 在应用程序 Web 界面窗口中选择**控制板**部分。
2. 在窗口的上部，单击 ☰ 按钮。
3. 在下拉列表中，选择**定制**。
4. 单击**小部件**。
5. 在打开的**管理小部件**窗口中：
   - 如果要添加与警报或规则关联的小部件，请在“**警报**”或者“**前 10 个**”列表中，选择要添加的小部件旁边的切换开关。
   - 如果要添加与 NDR 功能相关的小部件，请在 **[NDR]** 列表中，单击要添加的小部件名称旁边的 + 按钮。
6. 关闭“**管理小部件**”窗口并单击“**应用**”。

小组件被添加到当前布局。

在当前布局中移动小组件

要在当前布局中移动小组件：

1. 在应用程序 Web 界面窗口中选择**控制板**部分。
2. 在窗口的上部，单击 ☰ 按钮。
3. 在下拉列表中，选择**定制**。
4. 在布局中选择要移动的小组件。
5. 单击并按住小组件的上部可将小组件拖放到布局中的不同位置。
6. 单击**应用**。

   当前布局已保存。

更改 NDR 小部件中信息的显示

添加 NDR 小部件后，它将根据默认设置显示信息。如果需要，您可以编辑显示设置。

要编辑 NDR 小部件显示设置：

1. 在应用程序 Web 界面窗口中选择**控制板**部分。
2. 在窗口的上部，单击 ☰ 按钮。
3. 在下拉列表中，选择**定制**。
4. 在要配置的 NDR 小部件的右上角，单击 ⚙ 按钮。

   这将打开显示设置窗口。
5. 管理小部件的设置。

   根据所选的 NDR 小组件，窗口可能包含以下设置：

   - **更改名称** – 如果选中“**更改名称**”复选框，您可以在“**小组件名称**”字段中为小组件定义任何名称（不同于默认名称）。自定义小组件中没有“**更改名称**”设置。
   - **小组件名称** – 用于输入与默认名称不同的小组件名称的字段。
   - **编辑描述** – 如果选中“**编辑描述**”复选框，您可以在“**小组件描述**”字段中为小组件提供任何描述（不同于默认描述）。自定义小组件中缺少“**编辑描述**”设置。
   - **小部件描述** – 用于输入与默认名称不同的小组件名称的字段。
   - **刷新周期** – 显示的信息更新的时间（以秒为单位）。

- **定义的背景** – 定义自定义小组件的背景颜色。您可以选择与严重性级别 (**信息**、**警告**或**严重**) 相对应的背景颜色，或选择**中性**以禁用背景颜色。
- **显示模式** – 决定数据在小组件中的显示方式。您可以将信息显示配置为条形图或饼图。
- **考虑具有已解决状态的事件** – 如果选择了**考虑具有"已解决"状态的事件**，则小部件会显示所有事件的数据。
- **包括已补救和已接受的风险** – 如果选择"**包括已补救和已接受的风险**"，小组件将显示所有风险的数据。

6. 单击**应用**。

从当前布局移除小组件

要从当前布局移除小组件：

1. 在应用程序 Web 界面窗口中选择**控制板**部分。
2. 在窗口的上部，单击 ☰ 按钮。
3. 在下拉列表中，选择**定制**。
4. 单击要从当前布局移除的小组件右上角的 × 图标。
   小组件被从应用程序 Web 界面窗口的工作区移除。
5. 单击**应用**。

小组件被从当前布局移除。

保存布局为 PDF

布局中的 NDR 小部件未保存到 PDF。

要保存布局为 PDF：

1. 在应用程序 Web 界面窗口中选择**控制板**部分。
2. 在窗口的上部，单击 ☰ 按钮。
3. 在下拉列表中，选择**保存为 PDF**。
   这将打开**另存为 PDF**窗口。
4. 在窗口下部的**布局**下拉列表中，选择页面方向。

5. 单击**下载**。
   PDF 格式的布局被保存到您的计算机硬盘驱动器上的浏览器下载文件夹中。
6. 单击**关闭**。

配置小部件中的数据显示周期

您可以配置在小组件中显示数据的以下时段：

- **天**。
- **周**。
- **月份**。

对于 NDR 小部件，您可以使用以下时间段：

- **1 小时**
- **12 小时**
- **24 小时**
- **7 天**

您可以为每个单独的 NDR 小部件配置一个数据显示周期。

更改小部件中信息的显示

要配置小组件中一天的数据显示（从早上 00:00 到晚上 11:59）：

1. 在应用程序 Web 界面窗口中选择**控制板**部分。
2. 在应用程序 Web 界面窗口右上角的数据显示时段下拉列表中，选择**天**。
3. 在**天**时段名称右侧的日历中，选择要在小组件中显示数据的日期。

   控制板页上的所有小组件都会显示选定时段的数据。

要在小组件上配置一周（周一到周日）的数据显示：

1. 在应用程序 Web 界面窗口中选择**控制板**部分。
2. 在应用程序 Web 界面窗口右上角的数据显示时段下拉列表中，选择**周**。
3. 在**周**时段名称右侧的日历中，选择要在小组件上显示数据的周。

   控制板页上的所有小组件都会显示选定时段的数据。

要在小组件中显示一个月（日历月）的数据显示：

1. 在应用程序 Web 界面窗口中选择**控制板**部分。
2. 在应用程序 Web 界面窗口右上角的数据显示时段下拉列表中，选择**月份**。
3. 在**月份**时段名称右侧的日历中，选择要在小组件中显示数据的月份。

   控制板页上的所有小组件都会显示选定时段的数据。

更改小部件中信息的显示

要配置 NDR 小部件中的信息显示：

1. 在应用程序 Web 界面窗口中选择**控制板**部分。
2. 在您要配置的 NDR 小部件的右上角，单击代表您需要的时间间隔的按钮。

   NDR 小部件显示选定时间段的信息。

配置小组件显示缩放

您可以配置“警报”小组件的显示比例。小组件右上角的☰图标表示您可以配置该小组件的比例。

要配置小组件的显示比例：

1. 在应用程序 Web 界面窗口中选择**控制板**部分。
2. 在窗口的上部，单击 ☰ 按钮。
3. 在下拉列表中，选择**定制**。
4. 单击小组件右上角的☰。
5. 在下拉列表中，选择以下小组件显示大小之一：
   - **1x1**。
   - **2x1**。
   - **3x1**。

   所选小组件的显示比例被修改。
6. 为要设置显示比例的所有小组件重复这些步骤。
7. 单击**保存**。

   小组件的显示比例已配置。

“警报”类型小组件管理基础知识

您可以配置所有“警报”小组件的显示比例。

每个小组件的左侧显示用于小组件的颜色框。

示例：
按重要性分类的警报小组件显示不同重要性的警报的数量。
重要级别 – 根据 Kaspersky 的经验，对于 Kaspersky Anti Targeted Attack Platform 用户而言，警报重要性取决于此警报可能对计算机或企业 LAN 安全造成的影响。
在**按重要性分类的警报**小组件中，以下颜色对应于不同重要性级别：

- 红色 – 警报具有高度重要性。
- 橙色 – 警报具有中度重要性。
- 绿色 – 警报具有较低重要性。

图例的右侧显示了用于在小组件中显示数据的所选时间段内每种类型的警报数量。

单击具有每个警报类型的链接，您可以转到应用程序 Web 界面的**警报**部分，查看所有此类警报。警报将根据指定类型进行筛选。

示例：
按攻击向量分类的警报小组件显示**来自电子邮件的文件**警报，它表示 Kaspersky Anti Targeted Attack Platform 在小组件的选定时段内从邮件流量中检测到的文件的数量。
单击**来自电子邮件的文件**链接可以打开**警报**部分，显示与在小组件选定时段内从邮件流量中检测到的文件相关的所有警报。数据将根据以下参数进行筛选：**对象类型**=文件以及**对象来源**=邮件。

每个小组件的右侧显示数据列。纵轴显示事件数，横轴显示警报的日期和时间。您可以编辑小组件中数据显示的时间段，并选择小组件中显示信息的租户。

将鼠标光标放在每个数据列上，以显示特定列所代表的时段内计数的警报数。默认情况下显示未处理的警报数。您可以通过选择窗口右上角的**已处理**复选框来启用已处理警报的显示。在这种情况下，将显示所有警报的总数量。

事件小组件中的信息

“**控制板**”部分的“**设备**”小部件属于 NDR 功能，并显示有关应用程序已知设备列表中的设备的信息。

该小组件提供以下信息：

- 有关应用程序了解每个类别的多少台设备的信息。该信息以类别图标的形式显示在小部件的上部。每个类别图标下，显示该类别的设备数量。如果应用程序已知的设备列表包含存在问题的设备，则相应类别的图标会带有警告标记。
- 有问题的设备类别列表。如果存在此类设备，则该信息将显示在小部件的中间部分。用于显示图形元素的空间受小部件的大小限制。

存在问题的设备

在下列任何情况下，应用程序确定设备存在问题：

- 设备的状态为“*已授权*”，安全状态不是“*正常*”。
- 设备具有“*未授权*”状态。

如果任何设备出现问题，则为列表中的每个类别显示以下信息：

- 包含类别图标、文本描述以及存在问题的设备数量的链接的行。
- 带有设备图形表示的行。如果小部件有足够的可用空间，则会显示此行。行中的图形的数量取决于 Web 浏览器窗口的当前大小。如果出现问题的设备数量多于行中显示的数量，则隐藏设备的数量将以“+ <设备数量>”的格式显示在右侧。

设备图形

设备的图形表示包括以下信息：

- 设备名称。
- 设备状态。如果设备的状态为“*未授权*”，则显示为图标。
- 设备安全状态。显示为图形左边框上的一条彩色线。线的颜色对应于“*正常*”、“*警告*”或“*严重*”状态。

图形按以下顺序显示：

1. 带有“*未授权*”状态的设备。
2. 带有“*严重*”安全状态的设备。
3. 带有“*警告*”安全状态的设备。

从小组件导航到其他部分

您可以使用“**设备**”小部件界面的元素导航到设备表并显示有关设备的详细信息。可以使用以下选项来实现此目的。

转到设备表并筛选表格

导航到设备表并查看所选类别中的所有设备的信息：

在“**设备**”小组件的上部，单击相关类别的图标。

这将打开包含设备表的“**资产**”部分。根据选定的设备类别对表格进行过滤。

要导航到设备表并查看具有特定类别问题的设备的信息：

在带有问题的设备类别列表中，单击包含相关类别设备数量的链接。此链接显示在行末，带有类别图标和**带有问题**的文本注释。

这将打开包含设备表的“**资产**”部分。表根据存在特定类别问题的设备的 ID 进行过滤。

> 设备表将根据您前往设备表时在“**设备**”小组件中显示的设备的 ID 进行筛选。导航到设备表后，过滤条件不会更新。如果想查看当前有问题的设备数量，您可以再次转到“**控制板**”部分。

要转到设备表并查看有关有问题的设备的信息：

在“**设备**”小组件中，单击代表相关设备的图形元素。

这将打开包含设备表的“**资产**”部分。该表采用按设备 ID 进行过滤的方式。

要转到设备表而不更改当前的表格筛选条件：

单击“**设备**”小组件中的“**显示所有设备**”。

这将打开包含设备表的“**资产**”部分。该表显示符合为设备表配置的过滤条件的设备。

转到设备表并搜索表格

要转到设备表并在表中查找设备：

1. 在“**设备**”小部件中，在“**搜索设备**”字段中输入搜索查询。
2. 单击“**搜索**”。

这将打开包含设备表的“**资产**”部分。表格中显示符合您的搜索条件的设备。

事件小组件中的信息

“**控制板**”部分中的“**网络流量事件**”小部件显示有关 NDR 事件的一般信息以及具有最近上次可见日期和时间的聚合事件。

该小组件显示以下元素：

- 选定时间段内的 NDR 事件和聚合事件的直方图。该信息显示在小部件的上部。直方图按严重级别显示 NDR 事件和聚合事件的分布。
- 有关已注册 NDR 事件和聚合事件的信息列表，按最后可见日期和时间排序。该信息显示在小部件的中间部分。

NDR 事件和聚合事件的统计信息

在 NDR 和聚合事件的分布直方图上，各列对应每个时间间隔的事件总数。条形图中的颜色代表事件的严重级别。以下颜色对应于严重级别：

- 蓝色。此颜色用于*低*严重级别的 NDR 事件和聚合事件。
- 黄色。此颜色用于*中*严重级别的 NDR 事件和聚合事件。
- 红色。此颜色用于*高*严重级别的 NDR 事件和聚合事件。

您可以将鼠标悬停在某个栏上来查看有关它的信息。弹出窗口显示间隔的日期和时间，以及按严重级别划分的 NDR 事件和聚合事件的数量。

时间间隔的长度取决于所选的显示周期。您可以使用以下按钮选择直方图的周期：

- **1 小时**：一小时周期，细分为一分钟间隔。
- **12 小时**：12 小时周期，细分为一小时间隔。
- **24 小时**：24 小时周期，细分为一小时间隔。
- **7 天**：七天周期，细分为一天的间隔。

NDR 事件和聚合事件列表

“**网络流量事件**”小部件中的 NDR 事件和聚合事件列表以在线模式更新。具有最近的上次可见日期和时间的 NDR 事件和聚合事件位于列表顶部。

NDR 事件和聚合事件列表中显示的元素数量受小部件大小的限制。

对于列表中的每个事件，都提供了以下信息：

- NDR 事件或聚合事件的标题。
- 最后可见日期和时间。

- 代表 NDR 事件或聚合事件严重性的图标：
  - – *低*严重级别
  - – *中*严重级别
  - – *高*严重级别

列表中的聚合事件以 标记。

从小组件导航到其他部分

您可以使用“**网络流量事件**”界面的控件转到事件表并显示有关 DNR 事件和聚合事件的详细信息。可以使用以下选项来实现此目的。

导航到网络流量事件表并过滤表格

您可以通过单击“**网络流量事件**”小部件列表中的事件来查看有关 NDR 事件或聚合事件的详细信息。这样做将打开“**网络流量事件**”部分，其中的表格将被根据所选 NDR 事件或聚合事件的 ID 进行过滤。过滤标准还包括从 NDR 事件或聚合事件的注册日期和时间到当前时刻的时间段（不指定时间段的右边界）。

如果想转到网络流量事件表，但不改变“**网络流量事件**”部分中表中当前的过滤条件，点击“**网络流量事件**”小部件中的“**显示所有事件**”链接。

导航至事件表并搜索表格

要转到设备表并在表中查找设备：

1. 在“**网络流量事件**”小部件中，在“**搜索事件**”字段中输入您的搜索查询。
2. 单击“**搜索**”。

   这将打开“**网络流量事件**”部分。事件表显示符合搜索条件的 NDR 事件和聚合事件。

查看应用程序模块和组件的工作状况

如果应用程序的模块或组件遇到建议管理员查看的错误，则一个黄色警告框会显示在应用程序 Web 界面的**控制板**部分。

具有“**管理员**”或者“**安全审计员**”角色的用户可以访问有关用户当前管理的 Central Node、PCN 或 SCN 服务器的工作状况信息。

具有“**高级安全官**”、“**安全官**”或者“**安全审计员**”角色的用户可以访问有关工作状况的以下信息：

- 如果您使用的是独立的 Central Node 服务器，用户可以访问有关用户当前管理的 Central Node 服务器的工作状况的信息。
- 如果您使用分布式解决方案和多租户模式，并且用户正在管理 SCN 服务器，则用户可以访问该 SCN 服务器的工作状况信息，以获取其有权访问数据的租户的信息。
- 如果您使用分布式解决方案和多租户模式，并且用户正在管理 PCN 服务器，则用户可以访问该 PCN 服务器和所有连接到该服务器的 SCN 服务器的工作状况信息，以获取其有权访问数据的租户的信息。

若要详细了解应用程序模块及组件的工作情况，

单击**查看详情**打开**系统健康**窗口。

在**系统健康**窗口中，根据应用程序模块和组件的工作状况会显示以下图标之一：

- OK 如果应用程序的模块和组件正常工作。
- 带有问题数量的图标（例如，1），如果发现建议管理员注意的问题。在这种情况下，详细的问题信息会显示在**系统健康**窗口的右侧。

系统健康窗口包含以下部分：

- **组件健康**包含有关应用程序在其上运行的所有服务器上的应用程序模块和组件的运行状态、隔离以及数据库更新的信息。

  例如：
  如果一个或多个应用程序组件的数据库在 24 小时内未更新，则图标显示在安装应用程序模块和组件的服务器的名称旁边。
  要解决该问题，请确保可以访问更新服务器。如果您使用代理服务器连接到更新服务器，请确保代理服务器没有与 Kaspersky Anti Targeted Attack Platform 服务器连接相关的错误。

- **已处理** — 传入数据接收和处理状态。状态根据以下条件生成：
  - 从带有 Sensor 组件的服务器、带有邮件传感器的服务器或虚拟机、带有 Endpoint Agent 组件的主机接收数据的状态。
  - 有关超出对象在队列中等待应用程序模块和组件扫描的最长允许时间的信息。
- **与服务器的连接** — PCN 服务器和连接的 SCN 服务器之间的连接状态（如果您使用分布式解决方案和多租户模式，则会显示）。

如果检测到应用程序模块或组件的性能问题，您无法自行解决这些问题，请联系卡巴斯基技术支持。

管理技术

Kaspersky Anti Targeted Attack Platform 使用各种技术来分析网络流量。您可以单独启用或禁用技术。对于设备活动检测（AM）技术，您可以选择模式：学习模式或监控模式。

我们建议在预定的时间内启用学习模式，以便应用程序在适当的时间自动将技术切换到监控模式。监控模式是技术的正常模式（与学习模式相反，在学习模式中应用程序仅积累数据以供将来使用）。设置学习模式时，您可以配置希望技术切换到监控模式的时间。

您可以为所有组件和监控点指定相同的技术设置，也可以为某些组件和/或监控点指定特殊设置。技术设置可以自动从父对象继承到子对象。如果为组件或监控点启用了技术继承，则为父对象（Central Node 或 Sensor）指定的技术设置将应用于该对象。如果禁用技术继承，您可以为该组件或监控点上的技术配置特殊设置。

默认情况下，所有技术在应用程序安装后均启用。对于支持模式改变的技术，学习模式是默认启用的。

启用或禁用技术

您可以启用或禁用 Central Node 和 Sensor 组件和监控点的技术。但是，如果在这些对象上禁用技术继承，则可以启用和禁用 Sensor 组件和监控点的技术。

一些技术包括可以单独启用或禁用的方法。如果禁用某种技术或方法，应用程序将不会监控使用该技术或方法的设备交互。但是，您仍然可以管理与禁用的技术或方法相关的应用程序设置（例如，添加或编辑规则）。

以下技术和方法支持启用和禁用：

- 资产管理，以下简称“AM”：
  - 设备活动检测。
  - 设备信息检测。
  - 网络会话检测。
- 入侵检测，以下也称为“IDS”：
  - 基于规则的入侵检测。
  - ARP 欺骗检测。
  - IP 协议异常检测。
  - TCP 协议异常检测。
  - 暴力攻击和扫描检测。

要改变技术和方法的状态：

1. 在应用程序 Web 界面窗口中选择**Sensor 服务器**部分。
2. 点击相关组件或监控点的卡片。
   这将打开一个窗口，其中包含有关组件或监控点的信息。
3. 如果要为 Sensor 组件或监控点更改技术和方法的状态，请将“**继承服务器技术**”技术切换开关设置为“**已禁用**”。
4. 使用窗口左侧的切换开关来启用或禁用技术和/或方法。您可以通过单击**“全部启用”**或**“全部禁用”**来同时启用或禁用所有技术和方法。
5. 启用或禁用某项技术或方法后，请等待更改应用完毕。直到转换至另一状态完成之后，开关才会再次可用。

技术和方法的状态被更改。

配置设备活动检测模式

您可以配置学习模式或启用设备活动检测 (AM) 技术的监控模式。

要更改和配置技术的模式：

1. 在应用程序 Web 界面窗口中选择**Sensor 服务器**部分。
2. 点击相关组件或监控点的卡片。
   这将打开一个窗口，其中包含有关组件或监控点的信息。
3. 如果要为 Sensor 组件或监控点配置技术模式，请将“**继承服务器技术**”技术切换开关设置为“**已禁用**”。
4. 在技术名称右侧的下拉列表中，选择一种模式（**学习**或**监控**）。
5. 选择模式后，等待应用更改。在应用该模式之前，下拉列表中将显示“**更改**”状态。
6. 如果您想指定技术必须从学习模式切换到监控模式的日期和时间，请单击“**设置直到**”链接并选择日期和时间。
   如果之前已配置日期和时间，则日期和时间将显示在模式名称旁边。

技术的模式被配置。

管理技术继承

如果您希望将为父对象配置的技术设置自动应用于 Sensor 组件或监控点，则可以启用技术继承。这意味着 Sensor 组件获取 Central Node 组件的技术设置，而监控点获取添加监控点的组件（Central Node 或 Sensor）的设置。

如有必要，您可以禁用 Sensor 组件或监控点的技术继承。您可能需要这样做来指定特殊的技术设置。

要启用或禁用 Sensor 组件或监控点的技术继承，请执行以下操作：

1. 在应用程序 Web 界面窗口中选择**Sensor 服务器**部分。
2. 点击相关组件或监控点的卡片。
   这将打开一个窗口，其中包含有关组件或监控点的信息。
3. 根据需要设置“**继承服务器技术**”切换开关。

Sensor 组件或监控点的技术继承被启用或禁用。

查看警报表

检测到的针对企业 IT 基础设施的针对性攻击和入侵迹象将显示为警报表。

警报表不会显示至少满足以下条件之一的对象的信息：

- 该对象在 KSN 数据库中具有*受信任*信誉。
- 该对象由以下可信供应商进行数字签名：
  - Kaspersky。
  - Google。
  - Apple。
  - Microsoft。

有关这些警报的信息会保存到应用程序日志中。您可以查看该信息。

当达到允许的最大警报数量时，应用程序日志中的警报信息每晚都会轮换：

- **(IDS) 入侵检测系统**和 **(URL) URL 信誉**组件生成的警报对于每个组件最多有 100000 个警报。
- 所有其他警报对于每个模块或组件最多有 20000 个警报。

如果您使用的是分布式方案和多租户模式，则在所有 SCN 上进行轮转，然后再与 PCN 进行同步。同步后，所有已删除的警报都会被自动从 PCN 中删除。

如果存在有效的 KATA+NDR 授权许可密钥，则会生成 NDR 警报。授权许可密钥过期后，已创建的警报仍然可供查看，但不会创建新的警报。

警报表位于“**警报**”部分。它显示一般的 KATA 警报和 NDR 警报。

> 默认情况下，此部分仅显示有关用户未处理的警报的信息。若要也显示有关已处理警报的信息，请启用窗口右上角的“**显示已关闭的警报**”切换开关。

您可以按**已创建**或者**已更新**、**重要级别**、**源**和**状态**列对表中的警报进行排序。

警报表包含以下信息：

1. **VIP**指定警报是否处于具有特殊访问权限的状态。例如，具有**安全官**角色的用户无法查看 VIP 身份的警报。
2. “**已创建**”是创建警报的时间，“**已更新**”是警报更新的时间。
3. — 根据卡巴斯基的经验，对于 Kaspersky Anti Targeted Attack Platform 用户而言，警报重要性取决于此警报可能对计算机或企业 LAN 安全造成的影响。

   警报可以具有以下重要性级别之一：
   - **高**，以 符号标记 – 此警报具有高度重要性。
   - **中**，以 符号标记 – 此警报具有中度重要性。
   - **低**，以 符号标记 – 此警报重要性较低。
4. **检测到** — 检测到的对象的一个或多个类别。例如，当应用程序检测到感染了 Trojan-Downloader.JS.Cryptoload.ad 病毒的文件时，**检测到**字段就会对此警报显示 Trojan-Downloader.JS.Cryptoload.ad 类别。

5. **详细信息** — 警报摘要。比如：检测到的文件的名称或恶意链接的 URL 地址。

6. **源** — 检测到的对象的源的地址。例如，这可以是发送恶意文件的电子邮件地址，也可以是从中下载恶意文件的 URL。

7. **目标** — 检测到的对象的目标地址。例如，这可以是组织的邮件域（恶意文件发送到该邮件域）的电子邮件地址，也可以是企业 LAN 上的计算机（恶意文件已下载到该计算机）的 IP 地址。

8. "**技术**"是扫描时生成警报的应用程序模块或组件的名称。

   技术列可能表示以下应用程序模块和组件：

   - **(YARA) YARA**。
   - **(SB) Sandbox**。
   - **(URL) URL 信誉**。
   - **(IDS) 入侵检测系统**。
   - **(AM) 反恶意软件引擎**。
   - **(TAA) 针对性攻击分析器**。
   - **(IOC) IOC**。
   - **(NDR: IDS) 入侵检测系统**。
   - **(NDR: EA) 外部分析**。

9. **状态** — 警报状态取决于此警报是否被 Kaspersky Anti Targeted Attack Platform 的用户处理。

   警报可具有以下状态之一：

   - **新的**用于新警报。
   - **进行中**用于 Kaspersky Anti Targeted Attack Platform 用户在处理的警报。
   - **重新扫描**用于重新扫描对象而产生的警报。

- **服务器**是创建警报的服务器名称列表。服务器属于您在应用程序 Web 界面中管理的租户。如果您使用的是分布式解决方案和多租户模式，则会显示此列。
- **分配给**是对其分配了警报的用户的名称。

如果表格列中的信息以链接形式显示，您可以点击该链接打开过滤器菜单，在菜单中选择按此列进行过滤的设置。

警报更新和警报中事件合并涉及的特殊注意事项

如果在处理过程中发现与触发的 TAA（IOA）规则具有相同 ID 的事件，**目标攻击分析器**模块会更新警报中的主机列表和事件数量。更新在当日执行：从当日 00:00 到次日 00:00。如果警报在更新时已关闭，系统会自动重新打开它。

当同时满足以下条件时，**入侵检测系统**模块会在一个警报中合并有关已处理网络事件的信息：

- 触发规则的名称，应用程序数据库的版本以及源都匹配网络事件。
- 活动之间不超过 24 小时。

为满足这些条件的所有网络事件显示一个警报。警报通知仅包含有关第一个网络事件的信息。

配置警报表显示

您可以显示或隐藏列并更改警报表中列的顺序。

要配置警报表显示：

1. 在应用程序 Web 界面窗口中选择**警报**部分。
   这将打开警报表。
2. 在表格的标题部分，单击  。
   这将打开**定制表格**窗口。
3. 如果要在表中显示列，请选择要在表中显示的参数名称旁边的复选框。
   如果要隐藏表中的参数，请清除该复选框。

   > 必须选择至少一个复选框。

4. 如果要更改表格中列的顺序，请将鼠标光标移动到具有相关参数的行，单击  并将该行移动到新位置。
5. 如果要恢复默认表格显示设置，请单击“**恢复默认值**”。
6. 单击**应用**。

   警报表显示已配置。

筛选、排序和搜索警报

您可以筛选要在表格的一个或多个列的警报表中显示的警报，或根据您指定的搜索条件在某些表列中搜索警报。

您可以创建、保存和移除筛选器，并根据保存的筛选器中指定的条件开始筛选和搜索警报。

> 如果您使用分布式解决方案和多租户模式，则无法在 PCN 上保存筛选器。

每个用户的筛选器都保存在创建它们的服务器上。

您还可以按**已创建**或者**已更新**、**重要级别**、**源**和**状态**列对表中的警报进行排序。

默认情况下，此部分仅显示有关用户未处理的警报的信息。若要也显示有关已处理警报的信息，请启用窗口右上角的“**显示已关闭的警报**”切换开关。

按 VIP 身份筛选警报

您可以根据 ☆ 条件在警报表中筛选和搜索警报，该条件表示警报是否属于具有特殊访问权限的警报。例如，具有**安全官**角色的用户无法查看 VIP 身份的警报。

要按 VIP 身份筛选警报：

1. 在应用程序 Web 界面窗口中选择**警报**部分。
   这将打开警报表。
2. 单击**VIP**列的标题以展开筛选器设置列表。
3. 配置警报筛选设置：
   - 如果您希望警报表仅显示具有 VIP 身份的警报，请选择 **VIP**。
   - 如果您希望警报表显示所有警报，请选择**所有**。

   如果两者均未选择，则该表将显示所有警报。

   警报表仅显示与您设置的筛选条件相匹配的警报。

按时间筛选和搜索警报

您可以过滤警报，并根据以下条件在警报表中搜索警报：“**已创建**”值，即警报的创建时间，以及“**已更新**”值，即警报更新的时间。

要按时间筛选或搜索警报：

1. 在应用程序 Web 界面窗口中选择**警报**部分。
   这将打开警报表。
2. 单击“**已创建**”或“**已更新**”链接打开警报显示时段列表。
3. 在下拉列表中，选择以下警报显示周期之一：
   - **所有**，如果您希望应用程序显示表中所有警报。
   - **上一个小时**，如果您希望应用程序显示表中最后一小时内发生的警报。
   - **最后一天**，如果您希望应用程序显示表中最后一天内发生的警报。
   - **自定义范围**，如果您希望应用程序显示表中指定时段内发生的警报。

4. 如果您选择了**自定义范围**事件显示范围，请执行以下操作：

   a. 在打开的日历中，指定警报显示时段的开始和结束日期。

   b. 单击**应用**。

   日历关闭。

警报表仅显示与您设置的筛选条件相匹配的警报。

按重要性级别筛选警报

您可以根据“**重要级别**”条件过滤警报，该条件根据此警报对计算机或公司局域网安全可能产生的影响，为 Kaspersky Anti Targeted Attack Platform 用户指示警报的重要性。

按重要性筛选警报：

1. 在应用程序 Web 界面窗口中选择**警报**部分。
   这将打开警报表。
2. 单击展开筛选器设置列表。
3. 选择一个或多个以下警报重要性级别：
   - **低**，对于低重要性警报。
   - **中**，对于中重要性警报。
   - **高**，对于高重要性警报。

   如果未选择值，表中将显示所有重要性级别的警报。
4. 单击**应用**。

警报表仅显示与您设置的筛选条件相匹配的警报。

按检测到的对象的类别筛选和搜索警报

您可以根据“**检测到**”条件来筛选警报并在警报表中搜索特定警报，该条件表示事件中检测到的对象的一个或多个类别。例如，如果您希望表格显示有关受特定病毒感染的文件的警报，则可以根据此病毒的名称设置筛选器。

要按检测对象的类别筛选或搜索警报：

1. 在应用程序 Web 界面窗口中选择**警报**部分。
   这将打开警报表。
2. 单击**检测到**链接以打开筛选配置窗口。

3. 在下拉列表中，选择以下警报筛选运算符之一：

- **包含**
- **不包含**

4. 在输入字段中，输入类别名称（例如，Trojan）或类别名称中的几个字符。

5. 要使用不同条件添加筛选条件，请单击 + 并指定筛选条件。

6. 单击**应用**。

警报表仅显示与您设置的筛选条件相匹配的警报。

按获取的信息筛选和搜索警报

您可以根据“**详细信息**”条件来筛选警报并在警报表中搜索特定警报，该条件引用了有关警报的简要信息。比如：检测到的文件的名称或恶意链接的 URL 地址。

要按获取的信息筛选和搜索警报：

1. 在应用程序 Web 界面窗口中选择**警报**部分。
   这将打开警报表。

2. 单击**详细信息**链接以打开筛选配置窗口。

3. 在左侧的下拉列表中，选择以下搜索条件之一：

- **详细信息**。搜索将涵盖检测到的对象上的所有数据。
- **ID**。
- **文件名**。
- **文件类型**。
- **MD5**。
- **SHA256**。
- **URL**。
- **域**。
- **用户代理**。
- **主题**。
- **HTTP 状态**。
- **对象来源**。
- **对象类型**。

- **自动发送到 Sandbox**。
- **TAA (IOA) 规则**。
- **事件 ID (NDR)**。
- **资产 ID (NDR)**。

4. 在右侧的下拉列表中，选择以下筛选运算符警报之一：
   - **包含**。
   - **不包含**。
   - **等于**。
   - **不等于**。
5. 在文本框中，输入警报信息的一个或多个字符。
6. 要使用不同条件添加筛选条件，请单击 + 并指定筛选条件。
7. 单击**应用**。

   警报表仅显示与您设置的筛选条件相匹配的警报。

按源地址筛选和搜索警报

您可以根据“**源**”条件来筛选警报并在警报表中搜索特定警报，该条件表示警报的源地址。例如，这可以是从其发送恶意文件的电子邮件地址，也可以是企业 LAN 上的计算机（恶意文件已下载到该计算机）的 IP 地址。

要按源地址筛选或搜索警报：

1. 在应用程序 Web 界面窗口中选择**警报**部分。

   这将打开警报表。
2. 单击**源**链接以打开筛选配置窗口。
3. 在下拉列表中，选择以下警报筛选运算符之一：
   - **包含**
   - **不包含**
   - **匹配**
   - **不匹配**
4. 在文本框中，键入检测到的对象的源地址的一个或多个字符。

5. 要使用不同条件添加筛选条件，请单击 + 并指定筛选条件。

6. 单击**应用**。

警报表仅显示与您设置的筛选条件相匹配的警报。

按目的地址筛选和搜索警报

您可以根据“**目标**”条件来筛选警报并在警报表中搜索特定警报，该条件表示警报的目的地址。例如，这可以是组织的邮件域（恶意文件发送到该邮件域）的电子邮件地址，也可以是企业 LAN 上的计算机（恶意文件已下载到该计算机）的 IP 地址。

要按目标地址筛选或搜索警报：

1. 在应用程序 Web 界面窗口中选择**警报**部分。
   这将打开警报表。

2. 单击**目标**链接以打开筛选配置窗口。

3. 在下拉列表中，选择以下警报筛选运算符之一：

   - **包含**
   - **不包含**
   - **匹配**
   - **不匹配**

4. 在文本框中，键入检测到的对象的目标地址的一个或多个字符。

5. 要使用不同条件添加筛选条件，请单击 + 并指定筛选条件。

6. 单击**应用**。

警报表仅显示与您设置的筛选条件相匹配的警报。

按服务器名称筛选和搜索警报

您可以根据“**服务器**”条件在警报表中筛选和搜索警报，该条件指示创建警报的服务器的名称。

如果您使用分布式解决方案和多租户模式，则服务器属于您在应用程序 Web 界面中管理的租户。筛选仅在 PCN 上可用。

要按服务器名称筛选或搜索警报：

1. 在应用程序 Web 界面窗口中选择**警报**部分。
   这将打开警报表。
2. 单击“**服务器**”展开创建警报的服务器列表。
3. 选择一个或多个服务器名称旁边的复选框。
4. 单击**应用**。

警报表仅显示与您设置的筛选条件相匹配的警报。

按技术名称筛选和搜索警报

您可以根据“**技术**”条件来筛选警报并在警报表中搜索特定警报，该条件指示创建警报的应用程序模块或组件的名称。

要按技术名称筛选警报：

1. 在应用程序 Web 界面窗口中选择**警报**部分。
   这将打开警报表。
2. 单击**技术**链接以打开筛选配置窗口。
3. 在下拉列表中，选择以下警报筛选运算符之一：
   - **包含**，如果您希望应用程序显示由指定应用程序模块或组件生成的警报。
   - **不包含**，如果您希望应用程序隐藏由指定应用程序模块或组件生成的警报。
   - **等于**，如果您希望应用程序显示由指定应用程序模块或组件生成的警报。
   - **不等于**，如果您希望应用程序隐藏由指定应用程序模块或组件生成的警报。
4. 在选定的警报筛选运算符右侧的下拉列表中，选择要用于筛选警报的技术的名称：
   - **(YARA) YARA**。
   - **(SB) Sandbox**。
   - **(URL) URL 信誉**。
   - **(IDS) 入侵检测系统**。
   - **(AM) 反恶意软件引擎**。
   - **(TAA) 针对性攻击分析器**。
   - **(IOC) IOC**。

- **(NDR: IDS) 入侵检测系统**。
- **(NDR: EA) 外部分析**。

例如，如果您希望应用程序显示由 Sandbox 组件作为扫描结果生成的警报，请选择“**包含**”筛选运算符以及 **(SB) Sandbox** 组件的名称。

5. 要使用不同条件添加筛选条件，请单击 + 并指定筛选条件。
6. 单击**应用**。

警报表仅显示与您设置的筛选条件相匹配的警报。

按用户处理状态筛选和搜索警报

您可以根据**状态**条件筛选警报并在警报表中搜索它们 — 警报状态取决于此警报是否由 Kaspersky Anti Targeted Attack Platform 用户处理。

要按 Kaspersky Anti Targeted Attack Platform 用户对其的处理状态来筛选或搜索警报：

1. 在应用程序 Web 界面窗口中选择**警报**部分。

   这将打开警报表。
2. 要将已处理的警报包含在筛选器中，请打开窗口右上角的**已处理**开关。
3. 单击**状态**链接以打开可能的警报选项列表，这取决于 Kaspersky Anti Targeted Attack Platform 用户对其的处理状态。
4. 选择以下值之一：
   - **新的**，如果您希望应用程序显示尚未被任何用户处理的新警报。
   - **进行中**，如果您希望应用程序显示 Kaspersky Anti Targeted Attack Platform 用户正在处理的警报。
   - **重新扫描**，如果您希望应用程序显示重扫描引起的警报。
5. 单击**应用**。

警报表仅显示与您设置的筛选条件相匹配的警报。

按分配了警报的用户的名称过滤和搜索警报

您可以通过“**分配给**”属性在警报表中筛选或查找警报，即分配了警报的用户的名称。

要按分配了警报的用户的名称过滤或查找警报：

1. 在应用程序 Web 界面窗口中选择**警报**部分。

   这将打开警报表。
2. 单击“**分配给**”链接以打开筛选配置窗口。

3. 选择您需要的用户名称旁边的复选框。
   如果您想在列表中查找用户名，请开始在文本框中输入用户名，然后选中找到的用户名旁边的复选框。
   您可以选择多个用户名。

4. 单击**应用**。

警报表中仅显示分配给指定用户的警报。

对表中的警报进行排序

您可以按**已创建**或者**已更新**、**重要级别**、**源**和**状态**列对表中的警报进行排序。

要对警报表中的警报进行排序：

1. 在应用程序 Web 界面窗口中选择**警报**部分。
   这将打开警报表。

2. 如果您想按日期对警报进行排序，请单击**已创建**右侧的图标之一（如果表格显示警报创建日期）或**已更新**（如果表格显示警报更新日期）列标题：

   - ↑ 在表格顶部显示较新的警报。
   - ↓ 在表格顶部显示较旧的警报。

3. 如果您想按重要性级别对警报进行排序，请在≡图标右侧单击以下图标之一：

   - ↑ 在表格顶部显示重要性高的警报。
   - ↓ 在表格顶部显示重要性低的警报。

4. 如果要按检测到的对象的源地址对警报进行排序，请单击**源**列标题右侧的图标之一：

   - ↑ 按字母顺序排序，A-Z。
   - ↓ 按字母顺序排序，Z–A。

5. 如果您想按用户处理状态对警报进行排序，请单击**状态**列标题右侧的图标之一：

   - ↑ 按处理顺序**新的** - **重新扫描** - **进行中** - **已关闭**对警报进行排序。
   - ↓ 按处理顺序**已关闭** - **进行中** - **重新扫描** - **新的**对警报进行排序。

快速创建警报筛选器

要快速创建警报筛选器：

1. 在应用程序 Web 界面窗口中选择**警报**部分。
   这将打开警报表。

2. 执行以下操作以便将筛选条件快速添加到正在创建的筛选器中：

   a. 将鼠标光标置于包含您希望将其作为筛选条件添加的表列值的链接上。

   b. 左键单击。
   这将打开要对值执行的操作列表。

   c. 在打开的列表中，选择以下操作之一：

   - **按照此值进行过滤**，如果您想将该值包含在筛选条件中。
   - **从过滤器中排除**，如果您想从筛选条件中排除该值。

3. 如果您想添加多个筛选条件到正在创建的筛选器中，请执行操作以将每个筛选条件快速添加到正在创建的筛选器。

警报表仅显示与您设置的筛选条件相匹配的警报。

保存筛选器

您可以将过滤器集保存到警报表中。

要保存应用的过滤器：

1. 在应用程序 Web 界面窗口中选择**警报**部分。
   这将打开警报表。

2. 为表的一个或多个列配置过滤设置。

3. 点击“**保存的过滤器**”并选择“**保存当前的过滤器**”。
   过滤器将使用包含所选过滤设置的默认名称进行保存。

4. 如果您想重命名已保存的过滤器：

   a. 点击“**保存的过滤器**”。
   显示已保存的过滤器的列表。

   b. 将鼠标悬停在过滤器上并点击 。

   c. 重命名过滤器并单击 。

过滤器已保存。

重置警报筛选器

要清除一个或多个筛选条件的警报筛选器：

1. 在应用程序 Web 界面窗口中选择**警报**部分。
   这将打开警报表。

2. 单击您想清除其筛选条件的警报表列标题右侧的 。

如果要清除多个筛选条件，请执行必要的操作以清除每个筛选条件。

选定筛选器将被清除。

警报表仅显示与您设置的筛选条件相匹配的警报。

警报处理建议

有关 AM（反恶意软件引擎）、SB（Sandbox）、YARA、IOC、IDS（入侵检测系统）、NDR: IDS 和 NDR: EA 技术产生的警报的信息显示在窗口右侧，包括有关处理这些警报的建议。

要查看警报详细信息：

1. 在应用程序 Web 界面窗口中选择**警报**部分。
   这将打开警报表。
2. 单击包含想查看其信息的警报的行。

这将打开一个窗口，其中包含有关警报的信息。

AM 警报处理建议

在窗口的右侧部分，“**建议**”部分显示您可以遵循的建议，以及与您正在处理的警报具有共同属性的警报或事件的数量。

您可以遵循以下建议：

- 在**分类**下面，展开**查找类似警报**列表。
  一个可用于查找类似警报的属性列表、以及每个属性的类似警报的数量将显示。
  选择以下属性之一：
  - **通过 MD5**。单击链接即可在新的浏览器选项卡中显示**警报**警报表。警报按**详细信息**列、MD5 哈希值筛选。您正在处理的警报中的文件的 MD5 哈希值以黄色突出显示。
  - **通过 SHA256**。单击链接即可在新的浏览器选项卡中显示**警报**警报表。警报按**详细信息**列、SHA256 哈希值筛选。您正在处理的警报中的文件的 SHA256 哈希值以黄色突出显示。
  - **通过主机名**。单击链接即可在新的浏览器选项卡中显示**警报**警报表。警报按**源**列筛选。您正在处理的警报中的主机名以黄色突出显示。
  - **通过发件人地址**。单击链接即可在新的浏览器选项卡中显示**警报**警报表。警报按**源**列筛选。您正在处理的警报中的电子邮件的发件人地址以黄色突出显示。

- **通过收件人地址**。单击链接即可在新的浏览器选项卡中显示**警报**警报表。警报按**目标**列筛选。您正在处理的警报中的电子邮件的收件人地址以黄色突出显示。

- **通过 URL**。单击链接即可在新的浏览器选项卡中显示**警报**警报表。警报按**详细信息**列、您正在处理的警报的 URL 筛选。

- 在**分类**下面，选择**查找类似事件**。单击链接在新浏览器选项卡中显示**威胁搜索**事件表。在搜索条件中，由**RemoteIP**、**MD5**、**SHA256**、**URI**等选择**检测处理结果**事件类型和配置搜索筛选器。筛选值由您正在处理的警报的属性填充。例如，警报中文件的 MD5 哈希值。

  仅当您使用 KEDR 功能并且已添加 KEDR 授权许可密钥时，该操作才可用。

- 在**调查**下面，选择**查找类似事件**。单击链接在新浏览器选项卡中显示**威胁搜索**事件表。在搜索条件中，搜索筛选器由**RemoteIP**、**MD5**、**SHA256**、**URI**等配置。筛选值由您正在处理的警报的属性填充。例如，警报中文件的 MD5 哈希值。

  仅当您使用 KEDR 功能并且已添加 KEDR 授权许可密钥时，该操作才可用。

TAA 警报处理建议

在窗口的右侧部分，“**建议**”部分显示您可以遵循的建议，以及与您正在处理的警报具有共同属性的警报或事件的数量。

您可以遵循以下建议：

- 在**分类**下面，展开**查找类似警报**列表。

  一个可用于查找类似警报的属性列表、以及每个属性的类似警报的数量将显示。

  选择以下属性之一：

  - **按规则名称 (TAA 警报)**。单击链接将在新的浏览器选项卡中打开**警报**警报表；警报按**检测到**和**技术**列筛选，即用于创建警报的 TAA (IOA) 规则的名称以及**(TAA) 针对性攻击分析器**技术的名称。

  - **按规则名称 (SB 警报)**。单击链接将在新的浏览器选项卡中打开**警报**警报表；警报按**检测到**和**技术**列筛选，即用于创建警报的 TAA (IOA) 规则的名称以及**(SB) Sandbox**技术的名称。

- 在**调查**下面，选择**查找类似事件**。单击链接在新浏览器选项卡中显示**威胁搜索**事件表。在搜索条件中，搜索筛选器由**RemoteIP**、**MD5**、**SHA256**、**URI**等配置。筛选值由您正在处理的警报的属性填充。例如，警报中文件的 MD5 哈希值。

  仅当您使用 KEDR 功能并且已添加 KEDR 授权许可密钥时，该操作才可用。

SB 警报处理建议

在窗口的右侧部分，“**建议**”部分显示您可以遵循的建议，以及与您正在处理的警报具有共同属性的警报或事件的数量。

您可以遵循以下建议：

- 在**分类**下面，展开**查找类似警报**列表。

  一个可用于查找类似警报的属性列表、以及每个属性的类似警报的数量将显示。

  选择以下属性之一：

  - **通过 MD5**。单击链接即可在新的浏览器选项卡中显示**警报**警报表。警报按**详细信息**列、MD5 哈希值筛选。您正在处理的警报中的文件的 MD5 哈希值以黄色突出显示。
  - **通过 SHA256**。单击链接即可在新的浏览器选项卡中显示**警报**警报表。警报按**详细信息**列、SHA256 哈希值筛选。您正在处理的警报中的文件的 SHA256 哈希值以黄色突出显示。
  - **通过主机名**。单击链接即可在新的浏览器选项卡中显示**警报**警报表。警报按**源**列筛选。您正在处理的警报中的主机名以黄色突出显示。
  - **通过发件人地址**。单击链接即可在新的浏览器选项卡中显示**警报**警报表。警报按**源**列筛选。您正在处理的警报中的电子邮件的发件人地址以黄色突出显示。
  - **通过收件人地址**。单击链接即可在新的浏览器选项卡中显示**警报**警报表。警报按**目标**列筛选。您正在处理的警报中的电子邮件的收件人地址以黄色突出显示。
  - **通过 URL**。单击链接即可在新的浏览器选项卡中显示**警报**警报表。警报按**详细信息**列、您正在处理的警报的 URL 筛选。
  - **通过 Sandbox 中的 URL**。单击链接即可在新的浏览器选项卡中显示**警报**表。警报按**详细信息**列、即您正在处理的警报的 URL 地址以及处理警报时Sandbox 组件发现的相关所有 URL 筛选。

- 在**分类**下面，选择**查找类似的 EPP 事件**。单击链接在新浏览器选项卡中显示**威胁搜索**事件表。在搜索条件中，由**RemoteIP**、**MD5**、**SHA256**、**URI**等选择**检测处理结果**事件类型和配置搜索筛选器。筛选值由您正在处理的警报的属性填充。例如，警报中文件的 MD5 哈希值。

  仅当您使用 KEDR 功能并且已添加 KEDR 授权许可密钥时，该操作才可用。

- 在**调查**下面，选择**查找类似事件**。单击链接在新浏览器选项卡中显示**威胁搜索**事件表。在搜索条件中，搜索筛选器由**RemoteIP**、**MD5**、**SHA256**、**URI**等配置。筛选值由您正在处理的警报的属性填充。例如，警报中文件的 MD5 哈希值。

  仅当您使用 KEDR 功能并且已添加 KEDR 授权许可密钥时，该操作才可用。

处理 IOC 警报的建议

在窗口的右侧部分，**建议**部分显示您可以遵循的建议，以及与您正在处理的警报具有共同属性的警报的数量。

您可以遵循以下建议：

- 在**分类**下面，选择**通过主机名查找类似警报**。单击链接即可在新的浏览器选项卡中显示**警报**警报表。警报按**源**列筛选。您正在处理的警报中的主机名以黄色突出显示。
- 在**分类**下面，选择**通过 IOC 查找类似警报**。单击链接即可在新的浏览器选项卡中显示**警报**警报表。警报按**检测到**列、您正在处理的警报中的 IOC 文件的名称筛选。
- 在**快速响应**部分，选择**隔离<主机名>**。这将打开网络隔离规则创建窗口。

YARA 警报处理建议

在窗口的右侧部分，“**建议**”部分显示您可以遵循的建议，以及与您正在处理的警报具有共同属性的警报或事件的数量。

您可以遵循以下建议：

- 在**分类**下面，展开**查找类似警报**列表。

  一个可用于查找类似警报的属性列表、以及每个属性的类似警报的数量将显示。

  选择以下属性之一：

  - **通过 MD5**。单击链接即可在新的浏览器选项卡中显示**警报**警报表。警报按**详细信息**列、MD5 哈希值筛选。您正在处理的警报中的文件的 MD5 哈希值以黄色突出显示。
  - **通过 SHA256**。单击链接即可在新的浏览器选项卡中显示**警报**警报表。警报按**详细信息**列、SHA256 哈希值筛选。您正在处理的警报中的文件的 SHA256 哈希值以黄色突出显示。
  - **通过主机名**。单击链接即可在新的浏览器选项卡中显示**警报**警报表。警报按**源**列筛选。您正在处理的警报中的主机名以黄色突出显示。
  - **通过发件人地址**。单击链接即可在新的浏览器选项卡中显示**警报**警报表。警报按**源**列筛选。您正在处理的警报中的电子邮件的发件人地址以黄色突出显示。
  - **通过收件人地址**。单击链接即可在新的浏览器选项卡中显示**警报**警报表。警报按**目标**列筛选。您正在处理的警报中的电子邮件的收件人地址以黄色突出显示。
  - **通过 URL**。单击链接即可在新的浏览器选项卡中显示**警报**警报表。警报按**详细信息**列、您正在处理的警报的 URL 筛选。
- 在**分类**下面，选择**通过主机名查找类似警报**。单击链接在新浏览器选项卡中显示**威胁搜索**事件表。在搜索条件中，由RemoteIP、MD5、SHA256、URI等选择**检测处理结果**事件类型和配置搜索筛选器。筛选值由您正在处理的警报的属性填充。例如，警报中文件的 MD5 哈希值。

仅当您使用 KEDR 功能并且已添加 KEDR 授权许可密钥时，该操作才可用。

- 在**调查**下面，选择**查找类似事件**。单击链接在新浏览器选项卡中显示**威胁搜索**事件表。在搜索条件中，搜索筛选器由**RemoteIP**、**MD5**、**SHA256**、**URI**等配置。筛选值由您正在处理的警报的属性填充。例如，警报中文件的 MD5 哈希值。

  仅当您使用KEDR 功能并且已添加KEDR 授权许可密钥时，该操作才可用。

- 在**快速响应**部分，选择**隔离<主机名>**。这将打开网络隔离规则创建窗口。

IDS 警报处理建议

在窗口的右侧部分，“**建议**”部分显示您可以遵循的建议，以及与您正在处理的警报具有共同属性的警报或事件的数量。

您可以遵循以下建议：

- 在**分类**下面，选择**通过 IP 地址查找类似警报**。单击链接即可在新的浏览器选项卡中显示**警报**警报表。警报按**源**列筛选。您正在处理的警报中的主机名或 IP 地址以黄色突出显示。

- 在**分类**下面，选择**通过 URL 查找类似警报**。单击链接即可在新的浏览器选项卡中显示**警报**警报表。警报按**详细信息**列、URL 筛选。您正在处理的警报的 URL 以黄色突出显示。

- 在**分类**下面，选择**添加到排除项**。

  这将打开**将 IDS 规则添加到排除项**窗口。如果要添加用于创建排除项警报的 IDS 规则，请在**描述**字段中输入注释并单击**添加**。

  IDS 规则将被添加到排除项中，并显示在应用程序 Web 界面中排除项列表的**设置**部分、**排除项**子部分、**IDS**选项卡上。

- 在**调查**下面，选择**通过 URL 查找类似事件**。单击链接在新浏览器选项卡中显示**威胁搜索**事件表。在搜索条件中，搜索筛选器被配置为使用您正在处理的警报中的**URI**。

- 在**调查**下面，选择**通过 IP 地址查找类似事件**。单击链接在新浏览器选项卡中显示**威胁搜索**事件表。在搜索条件中，搜索筛选器被配置为使用您正在处理的警报中的**RemoteIP**。

- 在**调查**部分，单击**下载 IDS 工件**下载包含警报数据的文件。

- 在**调查**部分，单击**下载 PCAP 文件**下载包含截获的流量数据的文件。

处理 NDR:IDS 和 NDR:EA 警报的建议

在窗口的右侧部分，“**建议**”部分显示您可以遵循的建议，以及与您正在处理的警报具有共同属性的警报或事件的数量。

您可以遵循以下建议：

- 在“**分类**”下面，选择“**通过源 IP 查找类似警报**”。单击链接即可在新的浏览器选项卡中显示**警报**警报表。警报按**源**列筛选。您正在处理的警报中的主机名或 IP 地址以黄色突出显示。

- 在“**分类**”下，选择“**通过目标 IP 查找类似警报**”。单击链接即可在新的浏览器选项卡中显示**警报**警报表。警报按**目标**列筛选。您正在处理的警报中的主机名或 IP 地址以黄色突出显示。

- 在“**分类**”下，选择“**通过 URL 查找类似事件**”。单击链接即可在新的浏览器选项卡中显示**警报**警报表。警报按“**详细信息**”列筛选。您正在处理的警报的 URL 以黄色突出显示。
- 在“**分类**”下，选择“**通过入侵检测规则查找类似警报**”。单击链接即可在新的浏览器选项卡中显示**警报**警报表。警报按“**详细信息**”列筛选。您正在处理的警报的扫描结果以黄色突出显示。
- 在“**下载**”部分，单击“**下载 PCAP 文件**”下载包含截获的流量数据的文件。

查看警报

Kaspersky Anti Targeted Attack Platform 的 Web 界面显示用户应该跟踪的以下类型的警报：

- 文件已下载，或试图将文件下载到企业 LAN 计算机。应用程序在组织的本地网络的镜像流量，或 HTTP 流量、FTP 流量以及 HTTPS 流量（如果管理员在代理服务器上配置了 SSL 证书更换）的 ICAP 数据里检测到此文件。
- 文件已发送到企业 LAN 上的用户的电子邮件地址。应用程序在通过 POP3 或 SMTP 协议接收或者从具有 Kaspersky Secure Mail Gateway 的虚拟机或服务器（如果有在组织中使用）接收的电子邮件信息副本中检测到此文件。
- 网站链接在企业 LAN 计算机上打开。应用程序在组织的本地网络的镜像流量，或 HTTP 流量、FTP 流量以及 HTTPS 流量（如果管理员在代理服务器上配置了 SSL 证书更换）的 ICAP 数据里检测到此网络链接。
- 检测到在企业 LAN 计算机的 IP 地址或域名上有网络活动发生。应用程序在组织的本地网络的镜像流量中检测到此网络活动。
- 在企业 LAN 计算机上的进程已启动。应用程序检测到使用安装在属于公司 IT 基础架构的计算机上的 Endpoint Agent 组件的进程。

如果检测到文件，则在应用程序 Web 界面上将显示以下信息，具体取决于生成警报的应用程序模块或组件：

- 有关警报和检测到的文件的常规信息（例如，在其上检测到文件的计算机的 IP 地址，以及检测到的文件的名称）。
- 由 AM 引擎执行的文件病毒扫描结果。
- 由 Yara 模块执行的扫描文件以检查是否有入侵企业 IT 基础构架的迹象的结果。
- Sandbox 组件执行的文件行为分析的结果。
- 使用机器学习技术对云基础架构中的 APK 可执行文件进行分析的结果。

如果检测到网站链接，应用程序 Web 界面中将显示以下信息，具体取决于生成警报的应用程序模块或组件：

- 有关警报和检测到的网站链接的常规信息（例如，在其上检测到网站链接的计算机的 IP 地址，以及网站链接的地址）。
- 由 URL 信誉模块执行的链接扫描结果，旨在检测恶意软件迹象，钓鱼 URL 地址以及黑客之前用于对企业 IT 基础构架进行针对性攻击的 URL 地址。

如果应用程序在企业 LAN 上检测到计算机的 IP 地址或域名的网络活动，则应用程序 Web 界面可能显示以下信息：

- 警报和检测到的网络活动的详细信息。
- 由入侵检测系统模块 (IDS) 执行的 Web 流量扫描结果，该扫描旨在根据预设规则检测入侵企业 IT 基础构架的迹象。
- 使用 Kaspersky TAA (IOA) 规则执行的网络活动扫描的结果。
- 使用 TAA (IOA)、IDS、IOC 用户规则执行网络活动扫描的结果。

如果应用程序在安装了 Endpoint Agent 组件的企业 LAN 计算机上检测到运行的进程，那么应用程序 Web 界面可显示以下信息：

- 有关警报和计算机上运行进程的常规信息。
- 使用 Kaspersky TAA (IOA) 规则对计算机执行网络活动扫描的结果。
- 使用 TAA (IOA)、IOC 用户规则对计算机执行网络活动扫描的结果。

警报可以由具有以下角色的用户管理："**安全官**"和"**高级安全官**"。具有"**安全审计员**"角色的用户可以查看警报。

查看警报详细信息

要查看警报详细信息：

1. 在应用程序 Web 界面窗口中选择**警报**部分。
   这将打开警报表。
2. 单击包含想查看其信息的警报的行。
   这将打开一个窗口，其中包含有关警报的信息。

有关任何类型警报的一般信息

警报详情窗口的标题显示警报 ID。☆或者★图标将显示在状态旁边，具体取决于警报是否具有 VIP 身份。

包含警报信息的窗口的上部可能会显示有关警报的以下常规信息：

- **状态** — 警报状态取决于此警报是否被 Kaspersky Anti Targeted Attack Platform 的用户处理。
- **重要级别** — 根据 Kaspersky 的经验，对于 Kaspersky Anti Targeted Attack Platform 用户而言，警报重要性取决于此警报可能对计算机或企业 LAN 安全造成的影响。
- **服务器**是生成检测的服务器的名称。服务器属于您在应用程序 Web 界面中管理的组织。如果您使用的是分布式解决方案和多租户模式，则会显示此列。
- **主机** — 发生警报的计算机的域名。
- **数据源** — 数据来源。例如，SMTP Sensor 或 SPAN Sensor。

- “**创建时间**”是警报创建的时间。
- **更新时间**是更新警报详情的时间。

您可以配置有关新警报的电子邮件通知。

对象信息部分中的信息

对象信息部分可显示有关检测到的对象的以下事件信息：

- 文件名。

  为了扩大**复制值到剪贴板**操作，请单击带有文件名的链接。

- 文件类型。例如，ExecutableWin32。

  在 Kaspersky TIP 上查找按钮允许在 Kaspersky Threat Intelligence Portal 上查找文件。

  单击**创建防止规则**以防止文件运行。

  单击**下载**将文件下载到计算机的硬盘上。

  该文件以用密码“infected”加密的 ZIP 存档的形式下载。存档内的文件的名称被文件的 MD5 哈希所替换。不显示存档内文件的文件扩展名。

- 文件大小（以千字节为单位）。
- **MD5** — 文件的 MD5 哈希。

  单击具有“**MD5**”的链接将打开一个列表，您可以从其中选择以下操作之一：

  - **在 Kaspersky TIP 上查找**。
  - **查找事件**。
  - **查找警报**。
  - **创建防止规则**。
  - **复制值到剪贴板**。

- **SHA256** — 文件的 SHA256 哈希。

  单击 **SHA256** 链接将打开一个列表，您可以从其中选择以下操作之一：

  - **在 Kaspersky TIP 上查找**。
  - **在 virustotal.com 上查找**。
  - **查找事件**。
  - **查找警报**。
  - **创建防止规则**。
  - **复制值到剪贴板**。

- **发件人的电子邮件地址** — 从中发送包含文件的邮件的电子邮件地址。

- **收件人电子邮件地址** – 包含文件的邮件发送到的一个或多个电子邮件地址。
- **原始发件人电子邮件地址** – 从中发送包含文件的邮件的源电子邮件地址。
  该字段由"已接收"标题中的数据填充。
- **原始收件人电子邮件地址** – 包含文件的消息发送到的源电子邮件地址。
  该字段由"已接收"标题中的数据填充。
- **主题** – 邮件主题。
- **发件人服务器 IP** – 消息传递链中第一个邮件服务器的 IP 地址。
  单击**发件人服务器 IP**链接将打开一个列表，您可以从其中选择以下操作之一：
  - **查找事件**。
  - **查找警报**。
  - **复制值到剪贴板**。
- **标头** – 邮件消息标题的扩展集合。例如，它可以包含有关邮件发件人和收件人的电子邮件地址，有关邮件中继的邮件服务器以及电子邮件中的内容类型的信息。

"警报详情"部分中的信息

警报详细信息部分可以显示有关警报的以下信息：

- , 或 – 根据 Kaspersky 的经验，对于 Kaspersky Anti Targeted Attack Platform 用户而言，警报重要性取决于此警报可能对计算机或企业 LAN 安全造成的影响。
- "**时间**"是警报创建的时间。
- **检测到** – 检测到的对象的一个或多个类别。例如，当应用程序检测到感染了 Trojan-Downloader.JS.Cryptoload.ad 病毒的文件时，**检测到**字段就会对此警报显示 Trojan-Downloader.JS.Cryptoload.ad 类别。
- **方法** – HTTP 请求方法。例如，Get、Post 或 Connect。
- **URL** – 检测到的 URL。它还可能包含响应代码。
  单击具有 **URL** 的链接将打开一个列表，您可以从其中选择以下操作之一：
  - 通过 URL 在 Kaspersky TIP 上查找。
  - **通过域名在 Kaspersky TIP 上查找**。
  - **查找事件**。
  - **查找警报**。
  - **复制值到剪贴板**。
- **Referer** – 用户是通过此 URL 重定向到需要关注的网站链接。在 HTTP 协议中，它是包含了请求源 URL 的客户端请求头之一。

- **目标 IP** — 用户或应用程序请求的资源的 IP 地址。
  单击具有**目标 IP**的链接将打开一个列表，您可以在其中选择以下操作之一：
  - **在 Kaspersky TIP 上查找**。
  - **查找事件**。
  - **查找警报**。
  - **复制值到剪贴板**。
- **用户名称** — 其操作导致事件的用户账户的名称。
- **请求/响应** — 请求和响应的长度。

“有关使用 NDR 技术进行扫描的信息”部分中的信息

“**关于使用 NDR 技术进行扫描的信息**”部分可以显示以下结果：

- **监控点**：导致注册网络流量事件和创建警报的流量的监控点的名称。
- **网络接口 ID**：导致注册网络流量事件和创建警报的流量的监控点的 ID。

扫描结果部分中的信息

“**扫描结果**”部分可以显示以下结果：

- 生成警报的应用程序模块或组件的名称。
- 检测到的对象的一个或多个类别。例如，可以显示病毒名称：Virus.Win32.Chiton.i。
- 生成警报的 Kaspersky Anti Targeted Attack Platform 模块和组件的数据库版本。
- 应用程序模块或组件执行的警报扫描结果：
  - **YARA** — 对 Central Node 接收的文件和对象进行流式扫描的结果，或扫描带有 Endpoint Agent 组件的主机的结果。可能值:
    - 在 YARA 规则下检测到的文件的类别（例如：可能会显示 susp_fake_Microsoft_signer 类别名称）。
      对于流式扫描显示。
      单击**创建防止规则**以防止文件运行。
      在 Kaspersky TIP 上查找按钮允许在 Kaspersky Threat Intelligence Portal 上查找文件。
    - 文件路径和/或内存转储的名称。
      使用 Kaspersky Endpoint Agent 组件扫描主机时显示。

单击具有文件路径的链接将打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **复制值到剪贴板**。

您可以单击**创建任务**创建以下任务：

- 获取数据 → 文件，磁盘镜像，内存转储。
- **删除文件**。
- **隔离文件**。

单击**创建防止规则**以防止文件运行。

- **在 Kaspersky TIP 上查找**按钮允许在 Kaspersky Threat Intelligence Portal 上查找文件。
  您可以单击**在隔离区查看**以显示隔离对象的详细信息。
- **SB** （Sandbox） — Sandbox 组件执行的文件行为分析的结果。
  您可以单击**Sandbox 检测**打开一个窗口，其中包含有关文件行为分析结果的详细信息。

  只有当 Sandbox 检测该文件时，才会显示文件行为分析结果。如果文件上传到系统，然后在 Sandbox 中扫描，但组件没有检测到威胁，则不会显示结果。

  在 Kaspersky TIP 上查找按钮允许在 Kaspersky Threat Intelligence Portal 上查找文件。
  单击**创建防止规则**以防止文件运行。
  您可以通过单击**下载调试信息**下载所有操作系统中文件行为分析的详细日志。
  该文件以用密码“infected”加密的 ZIP 存档的形式下载。存档内的已扫描文件的名称被文件的 MD5 哈希所替换。不显示存档内文件的文件扩展名。

  默认状态下，用于存储文件行为扫描日志的最大硬盘空间在所有操作系统上均为 300 GB。达到这一限制后，应用程序将删除旧的文件行为扫描日志，并用新日志替换。

- **URL** （URL 信誉）是恶意、网络钓鱼 URL 或攻击者先前用于对企业 IT 基础架构进行针对性攻击的 URL 的类别。
- **IDS** （入侵检测系统）是基于入侵检测系统数据库或用于创建警报的 IDS 用户规则名称的检测对象的类别。例如，显示的类别可以是 Trojan-Clicker.Win32.Cycler.a。
  单击该链接可显示卡巴斯基威胁数据库中对象的类别。
- **AM** （反恶意软件引擎） — 根据反病毒数据库检测到的对象的类别。例如，可以显示病毒名称：Virus.Win32.Chiton.i。
  单击该链接可显示卡巴斯基威胁数据库中对象的类别。
  在 Kaspersky TIP 上查找按钮允许在 Kaspersky Threat Intelligence Portal 上查找文件。
  单击**创建防止规则**以防止文件运行。
  单击**下载**将文件下载到计算机的硬盘上。

- **TAA** （针对性攻击分析器） – 有关使用针对性攻击分析器技术进行文件分析的结果的信息：用于创建警报的 TAA (IOA) 规则的名称。

  单击链接可显示有关 TAA (IOA) 规则的信息。如果规则是由卡巴斯基专家提供的，则它包含有关触发的 MITRE 技术的信息以及对事件进行反应的建议。

- **IOC** – 用于创建警报的 IOC 文件的名称。

  选择 IOC 文件以打开包含IOC 扫描结果的窗口。

  单击**与警报相关的所有事件**在新浏览器选项卡中显示**威胁搜索**事件表。在搜索条件中配置搜索筛选器，例如按**MD5** 、 **FileFullName**。筛选值由您正在处理的警报的属性填充。例如，警报中文件的 MD5 哈希值。

- **NDR: IDS** 是警报的原因。对应于导致创建警报的网络流量事件的名称。此类 NDR 事件是使用 IDS 技术注册的，并且与检测流量中的攻击指标异常（例如，基于 ARP 欺骗指标检测的事件）相关联。

- **NDR: EA**（外部分析）是创建警报的原因。使用 Kaspersky Anti Targeted Attack Platform API NDR 从外部系统接收的事件。当注册事件时，标题和描述由外部系统确定。该事件是使用 EXT 技术注册的。

IDS 规则部分中的信息

IDS 规则部分以十六进制编辑器矩阵的形式显示有关 IDS（入侵检测系统）技术发出的警报的信息。

*十六进制编辑器*是用于编辑数据的应用程序，其中数据表示为字节序列。

矩阵的上半部分显示 IDS 规则的长度。

矩阵的左侧部分以文本格式显示规则的数据。

IDS 规则部分的**规则详情**子部分以 Suricata 格式显示 IDS 规则的标题和 IDS 警报的数据。例如，它可以显示有关流量方向的信息 (`flow`)、HTTP 请求方法 (`http_method`)、HTTP 标头 (`http_header`)、安全 ID (`sid`)。

URL 部分中的信息

在“**URL**”下，将显示触发警报的 URL。

单击“**URL**”链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **通过 URL 在 Kaspersky TIP 上查找**。
- **通过域名在 Kaspersky TIP 上查找**。
- **复制值到剪贴板**。

“检测相关设备的 IP 地址”部分中的信息

在“**警报相关设备的 IP 地址**”下，显示与警报相关的设备信息：

- **协议**。
- **源 IP**。
- **源 MAC**。
- **目标 IP**。
- **目的地 MAC**。

网络事件部分中的信息

网络事件部分可以显示有关计算机上打开的网站链接的以下信息：

- **日期**和**时间** — 网络事件的日期和时间。
- **方法** — HTTP 请求的类型，例如，GET 或 POST。
- **源 IP** — 在其上打开网站链接的计算机的 IP 地址。
- **目标 IP** — 在其上打开网站链接的计算机的 IP 地址。
- **URL** — HTTP 请求的类型，例如 GET 或 POST，以及网站的 URL。

  如果针对从流量中提取的文件创建警报，则 URL 会指定用于传输从中提取文件的流量的协议。可能的协议：HTTP、HTTPS、FTP、SMTP、POP3、SMB、NFS。

  单击具有 URL 的链接将打开一个列表，您可以从其中选择以下操作之一：

  - **通过 URL 在 Kaspersky TIP 上查找**。
  - **通过域名在 Kaspersky TIP 上查找**。
  - **查找事件**。
  - **查找警报**。
  - **复制值到剪贴板**。
- **用户代理** — 有关曾用于下载文件、试图下载文件或打开网站链接的浏览器的信息。它是 HTTP 请求中包含的文本字符串，通常包含浏览器的名称和版本以及用户计算机上安装的操作系统的名称和版本。

Sandbox 扫描结果

只有当 Sandbox 检测该文件时，才会显示文件行为分析结果。如果文件上传到系统，然后在 Sandbox 中扫描，但组件没有检测到威胁，则不会显示结果。

Sandbox 中的对象扫描结果窗口可以显示以下详细信息：

- **文件** — 扫描文件的全名和路径。
- **文件大小** — 文件的大小。
- **MD5** — 文件的 MD5 哈希。
- **单击具有 MD5 的链接将打开一个列表，您可以从其中选择以下操作之一：**
- **在 Kaspersky TIP 上查找。**
- **查找事件。**
- **查找警报。**
- **创建防止规则。**
- **复制值到剪贴板。**
- **检测到** — 检测到的对象的一个或多个类别。例如，当应用程序检测到感染了 Trojan-Downloader.JS.Cryptoload.ad 病毒的文件时，**检测到**字段就会对此警报显示 Trojan-Downloader.JS.Cryptoload.ad 类别。
- **处理时间** — 扫描文件的时间。
- **数据库版本** — 创建警报的 Kaspersky Anti Targeted Attack Platform 模块和组件数据库的版本。

您可以单击窗口右上角的 **新的防止规则**以防止文件运行。

为 Sandbox 组件执行扫描的每个操作系统提供有关文件行为分析结果的信息。对于 Windows 7 操作系统（64 位），您可以查看两种 Sandbox 组件扫描模式的文件活动日志：**快速扫描模式**和**完整日志模式**。

以下活动日志可用于每种扫描模式：

- **活动列表** — 操作系统中的文件操作。
- **活动树** — 文件分析过程的图形表示。
- **HTTP 活动日志** — 文件的 HTTP 活动日志。它包含以下信息：
  - **目标 IP** — 此文件试图从操作系统转到的 IP 地址。
  - **方法** — HTTP 请求方法，例如 GET 或 POST。
  - **URL** — 文件试图从操作系统打开的网站链接的 URL。

单击**目标 IP**列中的链接将打开一个列表，您可以从其中选择以下操作之一：

- **在 Kaspersky TIP 上查找**。
- **查找事件**。
- **查找警报**。
- **复制值到剪贴板**。

单击**URL**列中的链接将打开一个列表，您可以从其中选择以下操作之一：

- **通过 URL 在 Kaspersky TIP 上查找**。
- **通过域名在 Kaspersky TIP 上查找**。
- **查找事件**。
- **查找警报**。
- **复制值到剪贴板**。

- **IDS 活动日志** — 文件的网络活动日志。它包含以下信息：
  - **源 IP** — 在其中保存文件的主机的 IP 地址。
  - **目标 IP** — 此文件试图从操作系统转到的 IP 地址。
  - **方法** — HTTP 请求方法，例如 GET 或 POST。
  - **URL** — 文件试图从操作系统打开的网站链接的 URL。

  单击**目标 IP**列中的链接将打开一个列表，您可以从其中选择以下操作之一：
  - **在 Kaspersky TIP 上查找**。
  - **查找事件**。
  - **查找警报**。
  - **复制值到剪贴板**。

  单击**URL**列中的链接将打开一个列表，您可以从其中选择以下操作之一：
  - **通过 URL 在 Kaspersky TIP 上查找**。
  - **通过域名在 Kaspersky TIP 上查找**。
  - **查找事件**。
  - **查找警报**。
  - **复制值到剪贴板**。

- **DNS 活动日志** – 文件的 DNS 活动日志。它包含以下信息：
  - 请求类型（请求或响应）。
  - **DNS 名称** – 服务器的域名。
  - **类型** – DNS 请求的类型，例如 A 或 CNAME。
  - **主机** – 与之交互的主机名或 IP 地址。

  单击**DNS 名称**或**主机**列中的链接将打开一个列表，您可以从其中选择以下操作之一：
  - **在 Kaspersky TIP 上查找**。
  - **查找事件**。
  - **查找警报**。
  - **复制值到剪贴板**。
- **屏幕截图** – 包含文件执行期间拍摄的屏幕截图。
  您可以在应用程序 Web 界面中查看屏幕截图，或者下载包含屏幕截图的 Zip 存档。

您可以单击每个扫描模式（**快速扫描模式**和**完整日志模式**）下方的**下载完整日志**将各操作系统中的文件行为分析日志下载到您的计算机上

IOC 扫描结果

根据处理对象的类型，入侵指标搜索结果窗口指示器可能显示以下信息：

- **ARP 协议**：
  - ARP 表中的 IP 地址。
  - ARP 表中的物理地址。
- **DNS 记录**：
  - DNS 记录的类型和名称。
  - 受保护计算机的 IP 地址。
- **Windows 日志事件**：
  - 事件日志中的条目 ID。
  - 日志中的数据源名称。
  - 日志名称。
  - 用户账户。
  - 事件时间。

- **文件**:
  - 文件的 MD5 哈希。
  - 文件的 SHA256 哈希。
  - 文件全名（包括路径）。
  - 文件大小。
- **端口**:
  - 扫描时与其建立连接的远程 IP 地址。
  - 扫描时与其建立连接的远程端口。
  - 本地适配器的 IP 地址。
  - 本地适配器上打开的端口。
  - 作为数字的协议（根据 IANA 标准）。
- **进程**:
  - 进程名称。
  - 进程参数。
  - 进程文件路径。
  - 进程的 Windows ID (PID)。
  - 父进程的 Windows ID (PID)。
  - 启动进程的用户账户名称。
  - 进程开始的日期和时间。
- **服务**:
  - 服务名称。
  - 服务说明。
  - DLL 服务的路径和名称（对于 svchost）。
  - 服务的可执行文件的路径和名称。
  - 服务的 Windows ID (PID)。
  - 服务类型（例如，内核驱动程序或适配器）。
  - 服务状态。
  - 服务运行模式。

- **用户**:
  - 用户账户名称。
- **卷**:
  - 卷名。
  - 卷符。
  - 卷类型。
- **注册表**:
  - Windows 注册表值。
  - 注册表配置单元值。
  - 注册表项的路径（没有配置单元或值名称）。
  - 注册表参数。
- **环境变量**:
  - 受保护计算机的物理（MAC）地址。
  - 系统（环境）。
  - 操作系统名称和版本。
  - 受保护设备的网络名称。
  - 受保护计算机所属的域和组。

IOC部分显示 IOC 文件的结构。如果处理的对象与 IOC 规则的条件匹配，则该条件会突出显示。如果处理的对象匹配多个条件，则整个分支的文本会突出显示。

主机部分中的信息

主机部分显示有关在其上触发了 TAA (IOA) 规则的主机的以下信息:

- **主机名称** – 事件在其中发生的计算机的 IP 地址或域名。单击链接将打开**威胁搜索**部分，其中有包含所选规则的 ID 和所选主机的搜索条件。
- **IP** – 事件在其中发生的计算机的 IP 地址。

  如果您使用动态 IP 地址，该字段将显示创建或更新警报时分配给计算机的 IP 地址。

  该应用程序不支持 IPv6。如果您使用的是 IPv6，则不会显示计算机的 IP 地址。

- **事件数量** – 主机上发生的事件数。
- **查找事件**。单击链接将打开**威胁搜索**部分，其中有包含所选规则的 ID 的搜索条件。

“更改日志”部分中的信息

更改日志部分可以显示以下检测信息：

- 警报修改的日期和时间。
- 修改的作者。
  例如，**系统**或应用程序用户名。
- 警报发生的修改。
  例如，警报可能被分配给 VIP 组，或被标记为已处理。

发送警报数据

您可以向卡巴斯基提供有关警报的数据（URL 信誉和“IOC”技术除外）进行进一步分析。

为此，您必须将警报数据复制到剪贴板，然后通过电子邮件将其发送至卡巴斯基。

警报数据可能包含被视为机密的组织信息。您必须咨询组织的安全部门并获得批准，才能将此数据发送到卡巴斯基以供进一步分析。

要将警报详情复制到剪贴板：

1. 在应用程序 Web 界面窗口中选择**警报**部分。
   这将打开警报表。
2. 单击包含想查看其信息的警报的行。
   这将打开一个窗口，其中包含有关警报的信息。
3. 单击包含警报信息的窗口下部的**向卡巴斯基提供警报详细信息**链接。
   这将打开**显示更多**窗口。
4. 查看要发送至卡巴斯基的警报数据。
5. 如果您想复制此数据，请单击**复制到剪贴板**按钮。
   警报数据将被复制到剪贴板。您将可以将其发送到卡巴斯基进行进一步分析。

查看警报关系

从警报卡中，您可以转到与此警报相关的事件、资产或网络会话表。

要查看警报的关系：

1. 在应用程序 Web 界面窗口中选择**警报**部分。
   这将打开警报表。
2. 打开您想要查看其关系的警报。
3. 在警报卡中，点击“**显示相关**”按钮旁边的箭头。
4. 从列表中选择警报关系：
   - **事件**。
   - **资产**。
   - **网络会话**。

这将打开 Web 界面中带有关系表的相应部分。

在警报上执行的用户操作

使用**高级安全官**或者**安全官**账户管理应用程序 Web 界面时，您可以对警报采取以下操作：

- 为自己或应用程序 Web 界面其他用户分配警报。
  您可以通过根据用户处理状态筛选警报来查看分配给特定用户的所有警报。
- 将警报标记为已处理。
  您可以通过根据用户处理状态筛选警报来查看所有由特定用户处理过的警报。
- 为警报添加注释。
  您可以根据收到的信息筛选警报，评论中的关键字找到评论警报。
- 将警报标记为 VIP。
  此操作仅适用于具有**高级安全官**角色的用户。具有此角色的用户可以通过按 VIP 身份筛选警报来查看具有 VIP 身份的所有警报。

具有**安全审计员**角色的用户可以查看有关警报的信息，但无法编辑此信息。

将警报分配给特定用户

具有“**高级安全官**”角色的用户可以向自己或具有“**高级安全官**”或“**安全官**”角色的应用程序 Web 界面的其他用户分配一个警报或多个警报。

要为自己或应用程序 Web 界面其他用户分配警报：

1. 在应用程序 Web 界面窗口中选择**警报**部分。
   这将打开警报表。
2. 选择您想要分配给自己或其他用户的一个或多个警报旁边的复选框。
   您可以通过选择表标题中的复选框来选择所有警报。
3. 在窗口下部显示的窗格中，通过单击“**分配给**”按钮右侧的箭头展开用户列表。
4. 选择您要为其分配警报的用户。
   这将打开操作确认窗口。您还可以留下评论，该评论将显示在警报更改历史记录中。
5. 单击**继续**。

该警报将被分配给选定用户。

您可以通过根据用户处理状态筛选警报来查看分配给特定用户的所有警报。

> 具有**安全审计员**角色的用户无法向自己或应用程序 Web 界面的其他用户分配警报。具有**高级安全官**和**安全官**角色的用户也无法将警报分配给具有**安全审计员**角色的用户。

具有“**高级安全官**”和“**安全官**”角色的用户在管理警报时可以向自己或具有“**高级安全官**”或“**安全官**”角色的应用程序 Web 界面的其他用户分配该警报。

要在管理警报时将警报分配给您自己或其他用户：

1. 在应用程序 Web 界面窗口中选择**警报**部分。
   这将打开警报表。
2. 打开您想要分配给您自己或应用程序的其他用户的警报。
   这将打开警报卡。
3. 如果您要将警报分配给自己，请点击“**分配给 @我**”。
4. 如果要将警报分配给应用程序的另一个用户，请单击“**分配给**”按钮右侧的箭头并选择您想要分配警报的用户。

此警报被分配给选定用户。

标记单个警报处理的完成

> 具有**安全审计员**角色的用户无法分配和处理警报。

要关闭警报表中的单个警报：

1. 在应用程序 Web 界面窗口中选择**警报**部分。
   这将打开警报表。

2. 在要关闭的警报的“**状态**”列中，单击警报的状态。

3. 在操作列表中，选择“**关闭警报**”。

警报已关闭。

要在管理警报时关闭警报：

1. 在应用程序 Web 界面窗口中选择**警报**部分。
   这将打开警报表。

2. 打开您想关闭的警报。

3. 在窗口的右上角，单击“**关闭警报**”。

警报已关闭。如果警报已被分配给其他用户，它被标记为已由您处理。

您可以通过根据用户处理状态筛选警报或通过使用“**显示已关闭的警报**”切换开关来查看所有由特定用户处理过的警报。

如果在一天内（早 00:00 到晚 11:59）收到基于使用 TAA (IOA)、IDS 或 URL 技术的扫描的类似于已处理警报的警报，则应用程序创建新警报或更新状态为“**新的**”或者“**进行中**”的相同警报的信息。

关闭 NDR 警报时，与该警报关联的聚合事件和嵌套 NDR 事件将被标记为已解决，并且与这些事件关联的其他警报也将被关闭。如果重新打开已关闭的 NDR 警报，则不会重新打开相关的已关闭的 NDR 事件。

标记警报处理的完成

拥有“**安全官**”角色的用户无法对警报执行批量操作。具有**安全审计员**角色的用户无法分配和处理警报。

要关闭一个或多个警报：

1. 在应用程序 Web 界面窗口中选择**警报**部分。
   这将打开警报表。

2. 选择要关闭的警报对面的复选框。
   您可以通过选择表标题中的复选框来选择所有警报。

3. 在窗口下部显示的窗格中，单击**关闭警报**按钮。
   这将打开操作确认窗口。
   您还可以留下评论，该评论将显示在警报更改历史记录中。

4. 单击**继续**。

选定的警报被关闭。如果警报已被分配给其他用户，它们被标记为已由您关闭。

您可以通过根据用户处理状态筛选警报或通过使用“**显示已关闭的警报**”切换开关来查看所有关闭的警报。

如果在一天内（早 00:00 到晚 11:59）收到基于使用 TAA (IOA)、IDS 或 URL 技术的扫描的类似于已处理警报的警报，则应用程序创建新警报或更新状态为“**新的**”或者“**进行中**”的相同警报的信息。

关闭 NDR 警报时，与该警报关联的聚合事件和嵌套 NDR 事件将被标记为已解决，并且与这些事件关联的其他警报也将被关闭。如果重新打开已关闭的 NDR 警报，则不会重新打开相关的已关闭的 NDR 事件。

修改 VIP 警报的状态

具有**高级安全官**角色的用户可以为警报分配 VIP 身份或清除警报的 VIP 身份。

要切换警报的 VIP 身份：

1. 在应用程序 Web 界面窗口中选择**警报**部分。
   这将打开警报表。
2. 选择要为其更改 VIP 身份的警报的复选框。
   您可以通过选择表标题中的复选框来选择所有警报。
3. 执行以下操作之一：
   - 如果您想将警报标记为 VIP，请单击窗口下部出现的窗格中的**标记为 VIP**按钮。
   - 如果要从警报中删除 VIP 状态，请在窗口下部显示的窗格中的“**标记为 VIP**”下拉列表中选择“**标记为非 VIP**”。

   这将打开操作确认窗口。
   您还可以留下评论，该评论将显示在警报更改历史记录中。
4. 单击**继续**。

警报的 VIP 身份已更改。

具有**高级安全官**和**安全审计员**角色的用户可以通过按 VIP 身份筛选警报来查看具有 VIP 身份的所有事件。

为警报添加注释

具有**高级安全官**和**安全官**角色的用户可以向警报添加注释。

要为警报添加注释：

1. 在应用程序 Web 界面窗口中选择**警报**部分。
   这将打开警报表。
2. 选择您要添加注释的警报。
   这将打开一个窗口，其中包含有关警报的信息。

3. 在 **更改日志**部分下的注释输入字段中，为警报输入注释。

4. 单击**添加**。

该注释将添加到警报中，并显示在该警报的**更改日志**部分。

您可以根据收到的信息筛选警报，注释中的关键字找到注释警报。

具有**安全审计员**角色的用户可以查看警报的注释，但无法编辑注释。

监控网络流量事件

该应用程序在分析网络流量时会注册事件。网络流量分析是 NDR 功能的一部分。

网络流量事件（也称为 *NDR 事件*）是包含有关检测网络流量中需要信息安全专业人员注意的某些变化或条件的信息的记录。NDR 事件被注册并发送到 Central Node。服务器会处理收到的事件并将其存储在数据库中。

*聚合事件*是一种特殊类型的事件，在收到特定序列的 NDR 事件时会被注册。聚合事件将具有一些共同特征或与同一进程相关的 NDR 事件分组。

应用程序根据事件关联规则注册聚合事件。*事件关联规则*描述了扫描事件序列的条件。当检测到符合规则条件的一系列 NDR 事件时，应用程序会注册一个提及触发规则名称的聚合事件。聚合事件注册的系统事件类型代码为 8000000001。

事件关联规则内置在应用程序中，无论安全策略如何都会应用。

应用程序安装后，使用原有的事件关联规则。为了提高规则的有效性，卡巴斯基定期使用规则集更新数据库。您可以通过安装更新来更新关联规则。

Kaspersky Anti Targeted Attack Platform 服务器根据为注册事件类型指定的设置来注册 NDR 事件。您可以在“配置事件类型”部分配置这些设置。

为了减少不需要用户注意的频繁重复 NDR 事件的数量，您可以创建事件允许规则。满足允许规则的 NDR 事件不会被注册。例如，您可以使用允许规则暂时禁用来自特定监控点的所有事件的注册。您可以在“**设置**”部分，“**允许规则**”子部分中查看事件的允许规则。为此类规则指明了 EVT 类型。

该应用程序将 NDR 事件和聚合事件存储在 Central Node 的数据库中。存储记录的总量不能超出配置的限制。如果数量超出限制，应用程序会自动删除最旧的记录。但是，如果配置了最短存储期限，则删除时间小于最短期限的记录时，相应的消息将记录在应用程序消息日志中。您可以配置事件和事故存储设置。

您可以在“**网络流量事件**”部分查看有关 NDR 事件和聚合事件的信息。此部分显示有关 NDR 事件和聚合事件的详细信息，并允许从服务器数据库加载任何时期的信息。

具有以下角色的用户可以使用网络流量事件操作：“**安全官**”或者“**高级安全官**”角色。具有“**安全审计员**”角色的用户可以查看事件。

如果存在有效的 KATA+NDR 授权许可密钥，则会生成 NDR 事件。授权许可密钥过期后，创建的事件仍然可供查看，但不会创建相关警报。

NDR 事件分数和严重程度

Kaspersky Anti Targeted Attack Platform 中的 NDR 事件的评分范围是 0.0 到 10.0。

如果 NDR 事件与设备相关联，则应用程序在计算分数时会考虑有关该设备的可用信息。该设备的重要级别以及与该设备相关的风险都被考虑在内。

*事件类型表*中为 NDR 事件类型指定的基本分数被用作计算分数的基准。

如果 NDR 事件未与设备关联，则该事件的分数等于基础分数。

该分数决定了 NDR 事件的严重级别。根据分数的数值，NDR 事件可能具有以下严重级别之一：

- *低*（分数 0.0–3.9）

  低严重级别的 NDR 事件通常不需要立即响应。

- *中*（分数 4.0–7.9）

  中严重级别的 NDR 事件包含必须查看的信息。这些事件可能需要作出响应。

- *高*（分数 8.0–10.0）

  高严重级别的 NDR 事件包含可能产生严重影响的信息。这些事件需要立即作出响应。

NDR 事件注册技术

Kaspersky Anti Targeted Attack Platform 使用以下技术之一来记录 NDR 事件：

- *入侵检测* (IDS)

  该技术会记录与检测流量异常相关的 NDR 事件，这些异常是攻击的指标（例如，NDR 事件可以记录检测到 ARP 欺骗的指标）。

- *外部* (EXT)

  该技术注册 Kaspersky Anti Targeted Attack Platform 使用 Kaspersky Anti Targeted Attack Platform API 的方法从第三方系统接收的聚合和嵌套 NDR 事件。

- *资产管理* (AM)

  该技术会注册涉及检测流量中或从 EPP 应用程序接收的数据中的设备信息的 NDR 事件（例如，当发现设备具有新的 IP 地址时，可以注册 NDR 事件）。

- *端点保护平台* (EPP)

  该技术会为保护工作站和服务器的卡巴斯基应用程序检测到的威胁注册 NDR 事件（例如，恶意软件检测事件）。

NDR 事件状态

NDR 事件状态允许应用程序显示安全官处理收到的信息的过程。

可以为 NDR 事件和聚合事件分配以下状态：

- *新的*。

  当所有 NDR 和聚合事件在 Kaspersky Anti Targeted Attack Platform 中注册时，都会分配到此状态。

- *正在进行中*。

  您可以将此状态分配给 NDR 事件和正在处理的聚合事件（例如，在调查注册这些事件或事故的原因期间）。

- *已解决*。

  您可以将此状态分配给 NDR 事件和已处理的聚合事件（例如，对其注册原因的调查已结束）。

  分配 *"已解决"* 状态后，应用程序在确定设备表和网络交互图中显示的设备的安全状态时，将忽略具有此状态的 NDR 事件和聚合事件。

必须手动更改 NDR 事件和聚合事件的状态。您可以按照从 *"新的"* 到 *"已解决"* 的顺序依次分配状态。但是，您可以跳过 *"进行中"* 状态。更改 NDR 事件或聚合事件的状态后，您无法重新分配先前的状态之一。

如果将 *"已解决"* 状态分配给聚合事件，则所有嵌套 NDR 事件的状态将自动更改为 *"已解决"*，并且相关警报也会关闭。

如果为 NDR 事件分配了 *"已解决"* 状态，则嵌套此 NDR 事件的聚合事件和相关警报不被关闭。

已注册 NDR 事件表

您可以在以下位置查看已注册的 NDR 事件和聚合事件的表格："**网络流量事件**"部分。

默认情况下，已注册的 NDR 事件和聚合事件表会实时更新。表格顶部显示具有最近的上次可见日期和时间值的事件。

NDR 或聚合事件的最后可见日期和时间可能与其注册的日期和时间不同。对于 NDR 事件，最后可见日期和时间可能会在该事件类型的再生期间更新。对于聚合事件，上次可见日期和时间会更新以匹配嵌套 NDR 事件的上次可见日期和时间。

NDR 事件和聚合事件的参数显示在表格的以下列中：

- **开始**。

  对于 NDR 事件，这是注册事件的日期和时间。对于聚合事件，这是第一个嵌套事件的注册日期和时间。您可以同时查看日期和时间，或者仅查看日期或时间。要选择显示的信息，请选中**日期**和**时间**设置对面的复选框。

- **最后可见日期**

  对于 NDR 事件，这是 NDR 事件的最后可见的日期和时间。可能包含事件注册的日期和时间，或者如果事件注册条件在再生期间重复出现，则包含事件重复计数器递增的日期和时间。重新生成计数器的值显示在**出现总数**列中。对于聚合事件，聚合事件中包含的事件中最新的最后可见日期和时间。就像"**开始**"列一样，您可以一起查看日期和时间，或者仅查看日期或时间。

- **标题**。

  为 NDR 事件类型配置的标题。

- **分数**。

  NDR 事件的计算分数。该数值决定了 NDR 事件的严重级别。根据严重级别，分数可以用以下颜色之一显示：

  - 红色表示*高*严重级别事件。
  - 黄色表示*中*严重级别事件。
  - 蓝色表示*低*严重级别事件。

- **来源**。

  网络数据包的源地址。您可以通过以下设置来启用或禁用显示地址信息的地址和端口（表格列中显示的缩写名称在括号中指明）：**IP 地址**、**端口号 (P)**、**MAC 地址**、**VLAN ID (VID)** 和**应用程序级地址**。如果向应用程序添加了额外的地址空间，则可以在配置设备表时使用“**显示地址空间**”设置来启用或禁用地址空间名称的显示。

- **目的地**。

  网络数据包的目标地址。地址信息的显示可以按照与“**资源**”列相同的方式配置。

- **协议**。

  注册事件的应用层协议。

- **技术**。

  与用于注册 NDR 事件的技术相对应的图标。

- **总出现次数**。

  对于 NDR 事件，再生期间内注册 NDR 事件后的重复计数器的值。大于 1 的值表示注册 NDR 事件的条件重复发生了 N – 1 次。对于聚合事件，此列显示值 1。

- **ID**。

  已注册的 NDR 或聚合事件的唯一标识符。

- **应用程序**。

  有关导致注册 NDR 事件的条件的应用程序的信息。NDR 事件存储从 EPP 应用程序收到的应用程序的相关信息。

- **应用程序用户**。

  有关启动“**应用程序**”列中指定的应用程序的用户账户的信息。

- **状态**。

  与 NDR 事件或聚合事件的状态相对应的图标。

- **描述**。

  为 NDR 事件类型指定的描述。

- **结束**。

  对于 NDR 事件，分配“*已解决*”状态的日期和时间或 NDR 事件的再生期。对于聚合事件，嵌套 NDR 事件的最新解决日期和时间。就像“**开始**”列一样，您可以一起查看日期和时间，或者仅查看日期或时间。

- **触发的规则**。

  对于 NDR 事件，触发时导致注册 NDR 事件的进程控制规则或入侵检测规则的名称。对于聚合事件，触发时导致注册聚合事件的关联规则的名称。

- **监控点**。

  其流量触发了 NDR 事件注册的监控点。

- **事件类型**。

  分配给 NDR 事件类型的数字代码。

- **标记**。

  您可以将一组图标分配给任何 NDR 或聚合事件，以便根据表中不存在的条件轻松找到 NDR 或聚合事件。

查看网络流量事件表时，您可以配置、过滤、搜索和排序记录，以及导航到相关项目。

配置已注册事件表

您可以按如下方式配置事件表的显示：

- 显示或隐藏信息面板。
- 显示或隐藏事故中包含的事件。
- 显示或隐藏表格的列并重新排列列。

要配置事件表显示：

1. 在“**网络流量事件**”部分，点击 图标。

   这将打开表格显示配置窗口。

2. 如果要显示显示*“新”*或*“处理中”*状态的事件数量的信息面板，请选中**“显示信息面板”**复选框。

3. 在“**显示嵌入式列表**”下，选择嵌套在聚合事件中的 NDR 事件的显示模式：

   - **扁平**。在此模式下，事件表显示所有 NDR 事件，而不考虑事件嵌套。
   - **树形**。在这种模式下，聚合事件显示为嵌套事件和其他聚合事件的树。如果您希望无论当前的过滤和搜索设置如何都显示嵌套项，请选中“**过滤时显示嵌入事件**”复选框。

4. 在“**显示的列**”下，选中要在表中查看的参数旁边的复选框。您必须至少选择一个参数。

5. 如果要以不同的顺序显示列，请选择要在表中向左或向右移动的列的名称，然后单击带有向上和向下箭头的按钮。

   对于“**开始**”、**“上次看到”**和**“结束”**列，您还可以更改日期和时间值的显示顺序；对于**“源”**和**“目标”**列，您可以更改网络数据包的源地址和目标地址的显示顺序。为此，请选择要在表中向左或向右移动的值，然后单击带有向上和向下箭头的按钮。

选定的列将按新顺序显示在“**网络流量事件**”部分。

查看嵌套在聚合事件内的事件

您可以使用以下模式在网络流量事件表中查看嵌套在聚合事件中的 NDR 事件：

- 扁平模式。在此模式下，NDR 事件表显示所有事件，而不考虑事件嵌套。
- 树模式。在此模式下，聚合事件显示为树，可以使用聚合事件标题旁边的 和 按钮进行折叠和展开。

您可以在配置事件表时更改显示模式。

查看 NDR 事件的详细信息

NDR 和聚合事件的详细信息显示在应用程序 Web 界面的“**网络流量事件**”部分的详细信息区域。

要查看 NDR 或聚合事件的详细信息：

在“**网络流量事件**”部分中，选择一个事件。

详细信息区域显示在 Web 界面窗口的右侧，显示有关所选 NDR 或聚合事件的详细信息。

更改 NDR 事件的状态

您可以更改以下 NDR 事件和聚合事件的状态：

- *新的*。此状态可更改为“*进行中*”或“*已解决*”。
- *正在进行中*。此状态可更改为“*已解决*”。

“*已解决*”状态无法更改。

如果 NDR 事件与风险相关，则在为该事件分配“*已解决*”状态时，您还可以将风险状态更改为“*已接受*”。

要在管理事件表时更改 NDR 事件和聚合事件的状态：

1. 在事件表的“**网络流量事件**”部分中，选择要更改其状态的 NDR 事件或聚合事件。
2. 打开工具栏中的“**更改状态**”下拉列表。
3. 在下拉列表中，选择您想要分配的状态的命令。
   下列情况下，下拉列表的某些项不可用：
   - 如果选定的项目不包含 NDR 事件或具有“**新**”状态的聚合事件，则“*正在进行*”项目不可用。
   - 如果选定的项目不包含 NDR 事件或具有“**新**”或“*处理中*”状态的聚合事件，“*已解决*”项目不可用。

如果选择了所有满足当前过滤和搜索条件的 NDR 事件和聚合事件，且选定项目的数量超过 1000 条，则应用程序不会检查它们的状态。在这种情况下，“**进行中**”和“**已解决**”项目均可用。但是，“**进行中**”项目仅可用于为状态为“*新的*”的事件和事故分配“*进行中*”状态。

这将打开一个确认提示窗口。

4. 如果选定的 NDR 事件与风险相关，并且您想要同时为所有这些风险分配“*已接受*”状态，请选择“**分配与该事件相关的所有风险的已接受状态**”（如果选择了单个事件）或“**分配与该事件相关的所有风险的接受状态**”（如果选择了多个事件）。

   当使用资产管理技术注册某些类型的 NDR 事件时，风险可能会与事件相关。

5. 在提示窗口中，单击“**确定**”。

添加标记

拥有“**高级安全官**”角色的用户可以为 NDR 事件分配标记，并在应用程序 Web 界面的“**网络流量事件**”部分聚合事件。

*标记*是一个图标，可帮助您根据表中不存在的条件查找 NDR 事件和聚合事件。

要为 NDR 或聚合事件分配标记：

1. 在“**网络流量事件**”部分中，在包含 NDR 事件或聚合事件的行中，单击 ☆ 列。
2. 在显示的菜单中，选择要分配给此 NDR 事件或聚合事件的标记。

   您可以从应用程序提供的七个标记中选择一个。每个标记的含义由您决定。
3. 如果需要删除标记，请在菜单中选择“**无标记**”。

拥有“**高级安全官**”和“**安全审计员**”角色的用户可以查看 NDR 事件或使用标记聚合事件。

将 NDR 事件复制到文本编辑器

您可以将有关 NDR 事件和聚合事件的信息从网络流量事件表复制到任何文本编辑器。信息从表中当前显示的列中复制。

如果选择的 NDR 事件和聚合事件不超过 200 个，则可以复制事件。

要将 NDR 和聚合事件复制到文本编辑器中：

1. 在“**网络流量事件**”部分中，选择要复制到文本编辑器的 NDR 事件和聚合事件。
2. 右键单击以打开所选事件之一的上下文菜单。
3. 在上下文菜单中，选择以下命令之一：

   - 如果选择了单个 NDR 或聚合事件，则**复制事件的详细信息**。
   - 如果选择了多个 NDR 事件和聚合事件，则**复制所选事件的详细信息**。

4. 打开任意文本编辑器。

5. 在文本编辑器窗口中，粘贴事件（例如，按 **Ctrl** + **v**）。

可在文本编辑器中编辑复制的事件信息。有关多个事件的信息以空行分隔。

下载事件流量

查看事件表时，您可以下载与已注册的 NDR 事件和聚合事件相关的流量。流量被下载为 PCAP 文件（如果选择一个事件）或包含 PCAP 文件的 ZIP 存档中（如果选择多个事件）。

如果在事件表中选择的事件不超过 200 个（也计算嵌套在聚合事件内的事件），则可以下载流量。

事件的流量从应用程序数据库下载。如果为这些事件启用了流量保存，则可以将流量存储在已注册的 NDR 事件的数据库中。应用程序还可以在请求下载流量时，使用流量转储文件直接将流量保存在数据库中。这些文件用于临时存储，并随着新流量的到来自动删除（轮换周期取决于流量量和应用程序存储配置）。为了保证流量的下载，我们建议为相关事件类型启用流量保存功能，并根据流量积累率和事件注册率在数据库中配置流量存储。

要下载 NDR 事件或聚合事件的流量文件：

1. 在“**网络流量事件**”部分中，选择您想要下载流量的 NDR 事件和聚合事件。

2. 单击“**下载流量**”。

3. 如果文件生成需要很长时间（超过 15 秒），则文件生成操作将成为后台操作。在这种情况下，请按照以下步骤下载文件：

   a. 点击应用程序 Web 界面菜单中的 按钮。

   这将打开后台操作列表。

   b. 等待文件生成操作完成。

   c. 单击“**下载文件**”按钮。

您的浏览器保存了下载的文件。根据您的浏览器的设置，屏幕上可能会显示一个窗口，您可以在其中指定下载文件的路径和名称。

创建用于将事件导出至网络共享的目录

您可以导出事件并将包含导出事件的文件保存在服务器计算机的网络共享上。对于网络共享，您可以使用网络文件系统 (NFS) 协议，该协议允许您在服务器计算机的本地文件系统中挂载另一台计算机的共享（例如， NFS 服务器导出点）。使用操作系统的标准工具创建目录并安装网络共享。

当使用 NFS 协议时，rpcbind 软件包会被在操作系统中激活。请记住，攻击者可能会尝试使用此软件包进行某些类型的 DDoS 攻击。为了消除入侵威胁，必须配置防火墙。在 CentOS Stream 中，我们建议使用 firewalld 实用程序来配置防火墙。

手动创建目录并挂载网络共享

要创建用于保存文件到网络共享的目录：

1. 打开操作系统的控制台。
2. 创建一个本地目录，在其中挂载网络共享。为此，请输入以下命令：
   `mkdir <本地目录的完整路径>`
   例如：
   `mkdir ~/nfsshare`
3. 创建目录后，输入挂载网络共享的命令：
   `sudo mount -t nfs <远程计算机的名称或 IP 地址>:\`
   `<网络共享的完整路径>\`
   `<本地目录的完整路径>`
   例如：
   `sudo mount -t nfs nfs-server.example:/nfsshare ~/nfsshare`
4. 确认挂载成功：
   `mount | grep <本地目录的完整路径>`
   例如：
   `mount | grep ~/nfsshare`
   如果挂载成功，显示的信息包含远程计算机的名称或 IP 地址、网络共享的名称以及父目录的名称。

自动挂载网络共享

要在 CentOS 操作系统中配置网络共享的自动挂载：

以 root 身份打开 /etc/fstab 文件进行编辑，并在文件中添加以下行：

`<远程计算机的名称或 IP 地址>:<网络共享的完整路径> <本地目录的完整路径> nfs defaults 0 0`

例如：

`nfs-server.example:/nfsshare /home/user1/nfsshare nfs defaults 0 0`

事件数据库威胁追踪

当管理应用程序 Web 界面时，您可以生成搜索查询并使用 IOC 和 YAML 文件在事件数据库中搜索威胁以及您有权访问其数据的租户。

要通过事件数据库形成搜索查询，您可以使用*构建器模式*或*源代码模式*。

在构建器模式下，您可以使用包含字段值类型和运算符选项的下拉列表创建和修改搜索查询。

在源代码模式下，您可以使用文本命令创建和修改搜索查询。

您可以上传一个带有 Sigma 规则的 IOC 文件或 YAML 文件，并根据该文件中指定的条件搜索事件。

具有**高级安全官**，**安全官**角色的用户还可以根据事件搜索条件创建 TAA (IOA) 规则。

在构建器模式下搜索事件

一个搜索查询最多可以包含 25 个条件。不支持在单个查询中使用更多条件。

要在构建器模式下定义事件搜索条件：

1. 选择程序 Web 界面窗口中**威胁搜索**部分的**生成器**选项卡。
   这将打开事件搜索表单。
2. 在下拉列表中，选择事件搜索条件。
   您可以在"*事件搜索条件*"部分查看事件搜索条件描述。
3. 在下拉列表中，选择运算符。
   有关可用运算符的列表，请参阅"*运算符*"部分。
   每种类型的字段值都有其自己相关的一组运算符。例如，当选择 **EventType** 字段值类型时，**=** 和 **!=** 运算符将可用。
4. 根据选定的字段值类型，执行以下操作之一：
   - 在该字段中，指定您想用于执行事件搜索的一个或多个字符。
   - 在下拉列表中，选择您想要执行事件搜索的字段值选项。

   例如，要根据用户名搜索完整匹配，请输入用户名。
5. 如果您想添加新条件，请使用 **AND** 或 **OR** 逻辑运算符并重复添加条件的必要操作。
6. 如果您想添加一组条件，请单击**组**按钮并重复添加条件所必需的操作。
7. 如果您想删除一组条件，请单击**移除组**按钮。
8. 如果您想搜索在特定时段内发生的事件，请在"**最后一天**"下拉列表中选择以下事件搜索时段之一：
   - **最后一天**，如果您希望表格显示在最后一天内找到的事件。
   - **上一个小时**，如果您希望表格显示在最后一个小时内找到的事件。
   - **上星期**，如果您希望表格显示在最后一星期内找到的事件。
   - **自定义范围**，如果您希望表格显示在指定时段内找到的事件。

9. 如果您选择了**自定义范围**:

   a. 在打开的日历中，指定事件显示范围的开始和结束日期。

   b. 单击**应用**。

   日历关闭。

10. 单击**搜索**。
    满足搜索条件的事件表将显示。
    如果您使用分布式解决方案和多租户模式，找到的事件将按层分组：服务器 – 租户名称 – 服务器名称。

11. 单击要查看其事件的服务器的名称。

    所选服务器的主机表将显示。事件分组级别显示在表格上方。

    您可以将构建器中创建的查询转换为源代码模式下的事件搜索查询。

在源代码模式下搜索事件

一个搜索查询最多可以包含 25 个条件。不支持在单个查询中使用更多条件。

在源代码模式下定义事件搜索条件：

1. 在应用程序 Web 界面窗口中，选择**威胁搜索**部分，**源代码**选项卡。
   这将打开一个表单，其中包含用于在源代码模式下输入事件搜索条件的字段。

2. 使用条件、运算符、逻辑运算符 OR 和 AND 以及分组条件的括号输入事件搜索条件。
   搜索条件必须符合以下语法：<条件> <运算符> <条件值>。

   ```
   示例:
   EventType == 'filechange' AND
   (
   (
   FileName == '*example*' OR
   DllName == '*example*' OR
   DroppedName == '*example*' OR
   BlockedName == '*example*' OR
   InterpretedFileName == '*example*' OR
   InterpretedFiles.FileName == '*example*' OR
   TargetName == '*example*' OR
   HandleSourceName == '*example*' OR
   HandleTargetName == '*example*'
   ) OR
   UserName == '*example*'
   )
   ```

   您可以使用自动完成功能。为此，将光标放在查询行中，然后按 **Ctrl + Space**。

3. 如果您想搜索在特定时段内发生的事件，请单击**任何时候**按钮并选择以下某个事件搜索时段：

   - **任何时候**，如果您希望表显示最早发现的记录的事件。
   - **上一个小时**，如果您希望表格显示在最后一个小时内找到的事件。

- **最后一天**，如果您希望表格显示在最后一天内找到的事件。
- **自定义范围**，如果您希望表格显示在指定时段内找到的事件。

4. 如果您选择了**自定义范围**:

   a. 在打开的日历中，指定事件显示范围的开始和结束日期。

   b. 单击**应用**。

   日历关闭。

5. 单击**搜索**。
   满足搜索条件的事件表将显示。
   如果您使用分布式解决方案和多租户模式，找到的事件将按层分组：**服务器** – 租户名称 – 服务器名称。

6. 单击要查看其事件的服务器的名称。
   所选服务器的主机表将显示。事件分组级别显示在表格上方。

转换生成器查询以在源代码模式下搜索事件

您可以将构建器中创建的查询转换为源模式下的事件搜索查询。

> 当查询被转换时，其语法将适应在源代码模式下搜索事件。

要转换查询:

1. 选择程序 Web 界面窗口中**威胁搜索**部分的**生成器**选项卡。
   这将打开事件搜索表单。

2. 在下拉列表中，选择事件搜索条件。
   您可以在“*事件搜索条件*”部分查看事件搜索条件描述。

3. 在下拉列表中，选择运算符。
   有关可用运算符的列表，请参阅“*运算符*”部分。
   每种类型的字段值都有其自己相关的一组运算符。例如，当选择 **EventType** 字段值类型时，**=** 和 **!=** 运算符将可用。

4. 根据选定的字段值类型，执行以下操作之一:

   - 在该字段中，指定您想用于执行事件搜索的一个或多个字符。
   - 在下拉列表中，选择您想要执行事件搜索的字段值选项。

   例如，要根据用户名搜索完整匹配，请输入用户名。

5. 如果您想添加新条件，请使用 **AND** 或 **OR** 逻辑运算符并重复添加条件的必要操作。

6. 如果您想添加一组条件，请单击**组**按钮并重复添加条件所必需的操作。

7. 如果您想删除一组条件，请单击**移除组**按钮。

8. 如果您想搜索在特定时段内发生的事件，请在**任何时候**下拉列表中选择以下某个事件搜索时段：

   - **任何时候**，如果您希望表显示最早发现的记录的事件。
   - **上一个小时**，如果您希望表格显示在最后一个小时内找到的事件。
   - **最后一天**，如果您希望表格显示在最后一天内找到的事件。
   - **自定义范围**，如果您希望表格显示在指定时段内找到的事件。

9. 如果您选择了**自定义范围**：

   a. 在打开的日历中，指定事件显示范围的开始和结束日期。

   b. 单击**应用**。

   日历关闭。

10. 转到"**源代码**"选项卡。
    将显示一条警告，告知您转换不可逆。

11. 点击"**转换**"。

    该查询被转换为以源代码模式搜索事件的查询。

事件搜索条件

您可以使用以下条件在构建器模式下搜索事件：

- **常规信息**：
  - Host 是主机名。
  - HostIP 是主机的 IP 地址。
  - EventType 是事件的类型。
  - UserName 是用户的名称。
  - OsFamily 是操作系统家族。
  - OsVersion 是主机上使用的操作系统的版本。
- **TAA 属性**：
  - IOAId 是 TAA (IOA) 规则 ID。
  - IOATag 是有关使用 Targeted Attack Analyzer 技术进行文件分析的结果的信息：用于创建警报的 TAA (IOA) 规则的名称。
  - IOATechnique 是 MITRE 技术。

- IOATactics 是 MITRE 策略。
- IOAImportance 是分配给使用此 TAA (IOA) 规则生成的事件的重要性级别。
- IOAConfidence 是置信度，取决于规则引起误报的可能性。

- **文件属性**:
  - CreationTime 是事件创建时间。
  - FileName 是文件的名称。
  - FilePath 是文件所在目录的路径。
  - FileFullName 是文件的完整路径。包括目录路径和文件名。
  - ModificationTime 是文件修改时间。
  - FileSize 是文件的大小。
  - MD5 是文件的 MD5 哈希值。
  - SHA256 是文件的 SHA256 哈希值。
  - SimilarDLLPath 是放置在标准搜索路径上的目录中的恶意 DLL，使操作系统在原始 DLL 之前加载它。
- Linux **进程**:
  - LogonRemoteHost 是发起远程访问的主机的 IP 地址。
  - RealUserName 是用户在系统中注册时分配的用户名。
  - EffectiveUserName 是用于登录系统的用户名。
  - FileOwnerUserName 是文件所有者的名称。
  - RealGroupName 是用户组的名称。
  - EffectiveGroupName 是用于操作的用户组的名称。
  - Environment 是系统环境变量。
  - ProcessType 是进程类型。
  - OperationResult 是操作结果。
- **进程已启动**:
  - PID 是进程 ID。
  - ParentFileFullName 是父进程文件的路径。
  - ParentMD5 是父进程文件的 MD5 哈希值。
  - ParentSHA256 是父进程文件的 SHA256 哈希值。

- StartupParameters 是进程启动时使用的选项。
- ParentPID 是父进程 ID。
- ParentStartupParameters 是父进程的启动设置。

- **远程连接**:
  - HTTPMethod 是HTTP 请求方法。例如，Get、Post 或 Connect。
  - ConnectionDirection 是连接的方向（入站或出站）。
  - LocalIP 是从其进行远程连接尝试的本地计算机的 IP 地址。
  - LocalPort 是从其进行远程连接尝试的本地计算机的 IP 地址。
  - RemoteHostName 是远程连接尝试目标的计算机的名称。
  - RemoteIP 是远程连接尝试目标的计算机的 IP 地址。
  - RemotePort 是远程连接尝试目标的计算机的端口。
  - UR1 是向其发出 HTTP 请求的资源的地址。
  - TlsVersion 是协议的版本。
  - TlsSni 是服务器名称指示，即正在建立连接的资源的名称。
  - TlsCertificateMd5 是 TLS 证书的 MD5 哈希值。
  - TlsCertificateSha1 是 TLS 证书的 SHA1 哈希。
  - TlsCertificateSubjectNames 是主要和次要 DNS 名称。
  - TlsCertificateIssuerName 是证书所有者的组织名称。
  - TlsCertificateSerialNumber 是证书的序列号。
  - TlsCertificateCheckResult 是证书验证结果。
  - TlsCipherSuite 是证书的密码套件。
  - TlsCertificateValidFrom 是计算证书到期日期的日期。
  - TlsCertificateValidTo 是证书到期的日期。
- **DNS**:
  - DnsServerIpAddress 是 DNS 服务器的 IP 地址。
  - DnsQueryDomainName 是来自请求的域名。
  - DnsAnswerData 是响应数据。
  - DnsQueryTypeId 是记录类型 ID。

- **LDAP**:
  - LDAPSearchFilter 是搜索过滤器。
  - LDAPSearchDistinguishedName 是专有名称。
  - LDAPSearchAttributeList 是搜索属性的列表。
  - LDAPSearchScope 是搜索范围。
- **命名管道**:
  - PipeName 是命名管道。
  - PipeOperationType 是命名管道操作的类型。
- **WMI**:
  - WmiOperationType 是 WMI 操作类型："*WMI 活动*"或者"*WMI 事件使用者名称*"。
  - WmiHostName 是机器的名称。
  - WmiUserName 是用户名。
  - WmiNamespaceName 是命名空间。
  - WmiQuery 是查询的文本。
  - WmiFilterName 是事件过滤器。
  - WmiConsumerName 是事件使用者的名称。
  - WmiConsumerText 是事件使用者的源代码。
- **注册表已修改**:
  - RegistryKey 是注册表项。
  - RegistryValueName 是注册表值的名称。
  - RegistrationValue 是注册表值的数据。
  - RegistryOperationType 是注册表操作的类型。
  - RegistryPreviousKey 是上一个注册表项。
  - RegistryPreviousValue 是注册表值的先前名称。
- **系统事件日志**:
  - WinLogEventID 是 Windows 日志中安全事件的类型 ID。
  - LinuxEventType 是事件的类型。此条件用于 Linux 和 macOS 操作系统。
  - WinLogName 是日志的名称。

- WinLogEventRecordID 是日志条目 ID。
- WinLogProviderName 是记录事件的系统的 ID。
- WinLogTargetDomainName 是远程计算机的域名。
- WinLogObjectName 是发起事件的对象的名称。
- WinlogPackageName 是启动事件的软件包的名称。
- WinLogProcessName 是启动事件的进程的名称。

- **检测和处理结果**:
  - DetectName 是检测到的对象的名称。
  - RecordID 是触发规则的ID。
  - ProcessingMode 是扫描模式。
  - ObjectName 是对象的名称。
  - ObjectType 是对象的类型。
  - ThreatStatus 是检测模式。
  - UntreatedReason 是事件处理状态。
  - ObjectContent（也适用于 AMSI 事件）是被发送进行扫描的脚本的内容。
  - ObjectContentType（也适用于 AMSI 事件）是脚本内容的类型。
- **控制台交互输入**:
  - InteractiveInputText 是在命令行中输入的文本。
  - InteractiveInputType 是输入类型（控制台或管道）。
- **文件已修改**:
  - FileOperationType 是文件操作类型。
  - FilePreviousPath 是文件先前所在目录的路径。
  - FilePreviousName 是文件以前的名称。
  - FilePreviousFullName 是文件的全名，包括文件先前所在目录的路径和/或先前的文件名。
  - DroppedFileType 是修改后的文件的类型。
- **代码注入和进程访问**:
  - AccessMethod 是访问方法。
  - InjectAddress 是接收者进程的地址空间。

- InjectedDllName 是注入的 DLL 的名称。
- ModifiedStartupParameters 是修改后的启动参数。
- InjectedDllPath 是注入的 DLL 的路径。
- CallTrace 是调用跟踪。
- TargetStartupParameters 是用于启动接收方进程的命令。

- **进程访问**：
  - AccessOperationType 是操作类型："*进程访问已打开*"或者"*复制句柄*"。
  - ProccessAccessRights 是请求的进程访问权限。
  - HandleSourceStartupParameters 是启动源句柄的命令。
  - HandletargetStartupParameters 是启动目标句柄的命令。
- **其他**：
  - File type 是文件的类型。
  - TlsJa3Md5 包含客户端 hello 数据包中以下字段的十进制字节值：TLS 版本、密码套件、TLS 协议扩展列表、椭圆曲线和椭圆曲线格式。
  - TlsJa3sMd5 包含服务器 hello 数据包中以下字段的十进制字节值：TLS 版本、密码套件和 TLS 协议扩展列表。
  - DotNetAssemblyName 是 .NET 程序集的名称。
  - DotNetAssemblyFlags 包含 .NET 程序集标志。

要以源代码模式查看事件搜索字段列表，您可以下载此文件。

运算符

下表列出了在构建器模式和源代码模式下可用于搜索的运算符。

可用于在构建器模式和源代码模式下搜索的运算符

构建器模式	源代码模式
=	==
!=	NOT (example)
CONTAINS	==*example*
!CONTAINS	NOT (example=='*example*')
STARTS	=='example*'
!STARTS	NOT (example=='example*')
ENDS	==*example'
!ENDS	NOT (example==*example')

对表中的事件进行排序

您可以按**事件时间**、**事件类型**、**主机**和**用户名称**列对表中的事件进行排序。

对事件表中的事件进行排序：

1. 选择程序 Web 界面窗口中的**威胁搜索**部分。
   这将打开**威胁搜索**窗口。
2. 定义在构建器模式或源代码模式下搜索事件的条件。
   满足搜索条件的事件表将显示。
3. 如果您想按时间对事件进行排序，请单击**事件时间**栏目名称右侧的图标之一：
   - ↑ 在表格顶部显示较新的事件。
   - ↓ 在表格顶部显示较早的事件。
4. 如果要按事件类型名称对事件进行排序，请单击**事件类型**列标题右侧的图标之一：
   - ↑ 按字母顺序排序，A-Z。
   - ↓ 按字母顺序排序，Z–A。
5. 如果要根据在其上生成警报的主机名称对事件进行排序，请单击**主机**栏目名称右侧的图标之一：
   - ↑ 按字母顺序排序，A-Z。
   - ↓ 按字母顺序排序，Z–A。
6. 如果要根据主机的用户名对事件进行排序，请单击**用户名称**栏目名称右侧的图标之一：
   - ↑ 按字母顺序排序，A-Z。
   - ↓ 按字母顺序排序，Z–A。
7. 如果要根据主机名称或事件类型名称对事件进行分组，请单击**分组**下拉列表中的某个值：
   - **按主机名分组**，如果您想按主机名称对事件进行分组。
   - **按事件类型分组**，如果您想按事件类型的名称对事件进行分组。

如果事件按**主机**或者**事件类型**字段排序，当事件按相似属性分组时，排序结果将被清除。要返回排序结果，请从**分组**下拉列表选择**分组**值。

默认情况下，表中的事件按时间排序，最新的事件位于表的顶部。

您可以仅根据一种属性对事件进行排序。

当用外语按事件类型排序时，事件将根据英语事件类型的内部名称进行排序。

更改事件搜索条件

*要更改事件搜索条件，请在应用程序 Web 界面窗口的**威胁搜索**部分执行以下操作：*

1. 单击窗口上部包含事件搜索条件的表单。
2. 选择以下选项卡之一：
   - **生成器**，如果您想在构建器模式下更改事件搜索条件。
   - **源代码**，如果您想在源代码模式下更改事件搜索条件。
3. 进行相关更改。
4. 单击以下按钮之一：
   - **刷新**，如果您想使用新条件刷新当前事件搜索。
   - **新搜索**，如果您想执行新的事件搜索。

满足搜索条件的事件表将显示。

按 EPP 应用程序中的处理结果搜索事件

要在构建器模式下按照EPP 应用程序中的处理结果来搜索事件：

1. 选择程序 Web 界面窗口中**威胁搜索**部分的**生成器**选项卡。
   这将打开事件搜索表单。

2. 要按处理状态搜索事件：

a. 在**检测和处理结果**组中丢失的搜索条件下拉菜单中，选择**ThreatStatus**。

b. 在比较运算符下拉列表中，选择以下选项之一：

- **=**（等于）
- **!=**（不等于）

c. 在事件处理状态下拉列表中，选择以下选项之一：

- **清洁对象**。
- **物体已清除**。
- **误报**。
- **用户添加的对象**。
- **对象已添加到排除列表中**。
- **对象已删除**。
- **对象被隔离**。
- **未找到对象**。
- **对象已回滚**。
- **无法处理对象**。
- **对象未处理**。
- **处理已终止**。
- **未知**。

3. 要按事件未被处理的原因搜索事件：

a. 在**检测和处理结果**组中丢失的搜索条件下拉菜单中，选择**UntreatedReason**。

b. 在比较运算符下拉列表中，选择以下选项之一：

- **=**（等于）
- **!=**（不等于）

c. 在事件未被处理的原因下拉列表中，选择以下选项之一：

- **已处理对象**。
- **应用程序正在仅报告模式下运行**。
- **备份对象失败**。

- **复制对象失败**。
- **设备未准备好**。
- **对象被阻止**。
- **无权执行操作**。
- **无法清除的对象**。
- **对象不可覆写**。
- **未找到对象**。
- **磁盘上没有可用空间**。
- **处理已取消**。
- **处理已推迟**。
- **处理任务已停止**。
- **读取数据时出错**。
- **原因不明**。
- **这是一个关键的系统对象**。
- **数据写入错误**。
- **不支持数据写入**。
- **对象写保护**。

4. 如果您想添加新条件，请使用 AND 或 OR 逻辑运算符并重复添加条件的必要操作。

5. 如果您想添加一组条件，请单击**组**按钮并重复添加条件所必需的操作。

6. 如果您想删除一组条件，请单击**移除组**按钮。

7. 如果您想搜索在特定时段内发生的事件，请在**任何时候**下拉列表中选择以下某个事件搜索时段：

   - **任何时候**，如果您希望表显示最早发现的记录的事件。
   - **上一个小时**，如果您希望表格显示在最后一个小时内找到的事件。
   - **最后一天**，如果您希望表格显示在最后一天内找到的事件。
   - **自定义范围**，如果您希望表格显示在指定时段内找到的事件。

8. 如果您为找到的事件选择了**自定义范围**显示时段：

   a. 在打开的日历中，指定事件显示范围的开始和结束日期。

   b. 单击**应用**。

日历关闭。

9. 单击**搜索**。

满足搜索条件的事件表将显示。

使用 IOC 或 YAML 文件中指定的条件搜索事件

创建 IOC 文件时，请在“**威胁搜索**”部分查看可用于搜索事件的 IOC 术语列表。您可以通过从下面的链接下载文件来查看受支持的 IOC 术语列表。

在“**威胁搜索**”部分搜索事件的 IOC 术语

要使用 IOC 或 YAML 文件中指定的条件搜索事件：

1. 选择程序 Web 界面窗口中的**威胁搜索**部分。
   这将打开事件搜索表单。
2. 单击**导入**。
   这将打开文件选择窗口。
3. 选择您想上传的文件，然后单击**打开**。
   文件已上传。
   在“**源代码**”选项卡上，包含事件搜索条件的表单将显示上传的文件中定义的条件。

   > 您可以搜索符合这些条件的事件。您还可以更改上传的文件中定义的条件，或在源代码模式下添加事件搜索条件。

4. 如果您想搜索在特定时段内发生的事件，请单击**任何时候**按钮并选择以下某个事件搜索时段：
   - **任何时候**，如果您希望表显示最早发现的记录的事件。
   - **上一个小时**，如果您希望表格显示在最后一个小时内找到的事件。
   - **最后一天**，如果您希望表格显示在最后一天内找到的事件。
   - **自定义范围**，如果您希望表格显示在指定时段内找到的事件。
5. 如果您为找到的事件选择了**自定义范围**显示时段：
   a. 在打开的日历中，指定事件显示范围的开始和结束日期。
   b. 单击**应用**。
   日历关闭。
6. 单击**搜索**。

一个与上传的文件中指定的条件相对应的事件表将显示。

根据事件搜索条件创建 TAA (IOA) 规则

根据事件搜索条件创建 TAA (IOA) 规则：

1. 选择程序 Web 界面窗口中的**威胁搜索**部分。
   这将打开事件搜索表单。
2. 使用构建器模式或源代码模式执行事件搜索。
3. 单击**另存为 TAA (IOA) 规则**。
   这将打开**新 TAA (IOA) 规则**窗口。
4. 在**名称**字段中，输入规则的名称。
5. 单击**保存**。

事件搜索条件将被保存。在**自定义规则**部分的 TAA（IOA）规则表中，在 Web 界面的**TAA**子部分中，新规则将以指定名称显示。

如果要将事件搜索条件保存为用户定义的 TAA (IOA) 规则，请避免使用以下字段：

- IOAd。
- IOATag。
- IOATechnique。
- IOATactics。
- IOAImportance。
- IOAConfidence。

保存用户定义的 TAA (IOA) 规则时，应用程序可能没有任何包含这些字段数据的事件。当出现具有此数据的事件时，您之前创建的用户定义字段将无法按这些字段标记事件。

具有**安全审计员**和**安全官**角色的用户无法根据事件搜索条件创建 TAA (IOA) 规则。

事件信息

如果您使用分布式解决方案和多租户模式，则在使用 Web 界面管理应用程序时，您可以查看您有权访问其数据的租户的事件信息。

事件信息显示检测到事件的 Endpoint Agent 计算机的本地时间戳。应用程序管理员必须确保具有 Endpoint Agent 组件的计算机上的时间最新。

要启用所有租户的事件显示：

1. 选择程序 Web 界面窗口中的**威胁搜索**部分。
2. 打开**在所有租户中搜索**切换开关。

事件表显示所有租户的事件。

事件处理建议

事件窗口在事件树和具有“**高级安全官**”角色的用户的信息文本之间的框中显示按钮，其中包含可用于处理此事件的操作。

您可以执行以下操作：

- **隔离<主机名>** –将在其中检测到事件的具有 Endpoint Agent 组件的主机从网络隔离。适用于所有事件类型。
- **创建防止规则**–禁止执行在事件中检测到的文件。适用于所有事件类型，除了**系统事件日志**。
- **创建任务** – 创建一个任务。适用于所有事件类型，除了**系统事件日志**。

此外，您可以通过单击包含文件名称、路径、MD5 或 SHA256 哈希值以及主机名的链接来处理事件，同时在窗口下部查看有关事件的文本信息。

单击具有文件名称或文件路径的链接将打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - **杀死进程**。
  - **使用唯一的 PID 杀死进程**。
  - **删除文件**。
  - **获取文件**。
  - **进行取证**。
  - **隔离文件**。
- **复制值到剪贴板**。

单击 **MD5** 链接将打开一个列表，您可以从其中选择以下操作之一：

- **按照此值进行过滤**。
- **从过滤器中排除**。
- **在 Kaspersky TIP 上查找**。

- **查找事件**。
- **查找警报**。
- **复制值到剪贴板**。

单击 **SHA256** 链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **在 Kaspersky TIP 上查找**。
- **在 virustotal.com 上查找**。
- **在存储中查找**。
- **创建防止规则**。
- **复制值到剪贴板**。

单击具有主机名的链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - **杀死进程**。
  - **删除文件**。
  - **获取文件**。
  - **进行取证**。
  - **隔离文件**。
  - **运行应用程序**。
- **复制值到剪贴板**。

> 具有**安全审计员**和**安全官**角色的用户不会被显示事件处理建议。

遵循建议隔离主机

要遵循建议将主机与网络隔离：

1. 在建议框中选择**隔离<主机名>**。
   这将打开您正在处理的事件中的主机的主机隔离设置窗口。

2. 在**此时间后禁用隔离**字段中，输入以小时为单位的时间（1到9999），在此期间主机的网络隔离将处于活动状态。

3. 在**主机隔离规则排除项**设置组中的**流量方向**列表中，选择必须放行的网络流量方向：

   - **传入/传出**。
   - **传入**。
   - **传出**。

4. 在**IP**字段，输入必须放行的网络流量的 IP 地址。

   如果您使用 Kaspersky Endpoint Agent 充当 Endpoint Agent 组件，则可以使用代理服务器将 Kaspersky Endpoint Agent for Windows 与 Kaspersky Anti Targeted Attack Platform 进行连接。当您将此代理服务器添加到排除项时，可通过代理服务器访问的网络资源也被添加到排除项。如果通过代理服务器访问的网络资源已被添加到排除项，但代理服务器本身未被添加到排除项，则此类排除项不起作用。

5. 如果您选择了**传入**或**传出**，请在**端口**字段中输入连接端口。

6. 如果您想添加多个排除项，请单击**添加**并重复上述步骤填写**流量方向**、IP和**端口**字段。

7. 单击**保存**。

主机隔离信息显示在**Endpoint AgentWeb 界面**部分中。

您还可以通过单击警报信息中的隔离<主机名>链接和 Web 界面的**Endpoint Agent**部分创建网络隔离规则。

具有**安全审计员**和**安全官**角色的用户不能将主机与网络隔离。

遵循建议防止文件运行

要遵循建议防止文件运行：

1. 在建议框中，选择**创建防止规则**。
   这将打开防护规则创建窗口，其中包含您正在处理的事件的文件的 MD5 或 SHA256 哈希值。

2. 配置以下设置：

   a. **状态**是防护规则的状态：

      - 如果要启用防护规则，请将切换开关设置为**开启**。
      - 如果要禁用防护规则，请将切换开关设置为**关闭**。

   b. **名称**是防护规则的名称。

   c. 如果您希望应用程序向应用防御的计算机用户显示防护规则触发通知，请选择**通知用户阻止文件执行**复选框。

d. 如果要更改防护规则的范围，请配置**防止于**设置：

- 如果您想在所有服务器的所有主机上应用防御，请选择**所有主机**。
- 如果要在选定的服务器上应用防防护规则，请选择**指定服务器**选项并在**服务器**参数名称的右侧选择要在其上应用防护规则的服务器名称旁边的复选框。

  仅当启用分布式解决方案和多租户模式时，此选项才可用。
- 如果您想在选定主机上应用防护规则，请选择**指定主机**选项并在**主机**字段中列出这些主机。

3. 单击**添加**。

文件运行防御已创建。

创建的防御信息显示在 Web 界面的**防止**部分。

如果您选择了**通知用户阻止文件执行**复选框并尝试执行被阻止运行的文件，则用户会被通知该文件触发了执行阻止规则。

具有**安全审计员**和**安全官**角色的用户无法阻止文件执行。

遵循建议创建任务

要遵循建议创建任务：

1. 单击**创建任务**，然后在建议框中展开任务类型列表。
2. 选择任务类型：

- **杀死进程**。
- **进行取证**。
- **启动 YARA 扫描**。
- **管理服务**。
- **获取进程内存转储**。
- **获取 NTFS 图元文件**。
- **运行应用程序**。
- **获取文件**。
- **删除文件**。
- **隔离文件**。
- **从隔离区恢复文件**。

这将打开任务创建窗口，其中包含您正在处理的事件的预设值（例如主机名、文件路径、文件的 MD5 或 SHA256 哈希值）。

3. 如果您想修改事件的预设值，请编辑相应的字段。
4. 如果您想为任务添加注释，请在**描述**框中输入。
5. 如果您正在创建一个**杀死进程**、**删除文件**、**启动 YARA 扫描**或者**管理服务**任务并且想要修改任务范围，请更改**任务所有者**设置的值：
   - 如果您想运行所有服务器上的任务，请选择**所有主机**选项。
   - 如果要在选定的服务器上运行任务，请选择**指定服务器**选项并在**服务器**参数名称的右侧选择要在其上运行任务的服务器名称旁边的复选框。

     仅当启用分布式解决方案和多租户模式时，此选项才可用。
   - 如果您想运行选定主机上的任务，请选择**指定主机**选项并在**主机**字段中列出这些主机。
6. 单击**添加**。

任务已创建。

已创建任务的信息显示在 Web 界面的**任务**部分。

具有**安全审计员**和**安全官**角色的用户不能创建任务。

有关事件树中事件的信息

事件树显示在事件信息窗口的上部。

事件树包含以下信息：

- 您正在查看其信息的事件。

  您正在查看的事件显示在右侧。
- 父进程。

  父进程显示在您正在查看的事件的左侧。如果您正在查看的事件没有父进程，则会显示在其中注册该事件的主机名。

单击左侧父进程的名称将显示启动相关进程的进程，启动进程是该进程的父进程。如果没有父进程，则显示主机名。

每个父进程名称的右侧显示该进程生成的事件总数。您可以查看事件列表以及有关所选事件的信息。

查看事件树中的父进程信息

要显示正在查看的事件的父进程信息：

1. 使用构建器模式或源代码模式执行事件搜索。
   事件表将显示。
2. 选择您想查看其信息的事件。
   这将打开一个窗口，其中包含有关事件的信息。窗口上部将显示事件树。
3. 单击父进程的名称。
   在窗口的底部，**详细信息**选项卡会显示进程信息，就正在被查看的事件而言该进程是父进程。

查看事件树中有关父进程发起的事件的信息

查看父进程发起的所有事件的表：

1. 使用构建器模式或源代码模式执行事件搜索。
   事件表将显示。
2. 选择您想查看其信息的事件。
   这将打开一个窗口，其中包含有关事件的信息。事件信息窗口的上部将显示事件树。
3. 单击事件树中父进程的名称。
   在窗口的底部，**详细信息**选项卡会显示事件信息，就正在被查看的事件而言该进程是父事件。
4. 前往**事件**选项卡。
   由父进程启动的所有事件的表将显示。默认情况下，表中的事件按时间排序，最新的事件位于表的顶部。
   您可以通过单击相关事件所在行来查看事件信息。事件节点显示在事件树中。

要显示按类型分组的事件表：

1. 使用构建器模式或源代码模式执行事件搜索。
   事件表将显示。
2. 选择您想查看其信息的事件。
   这将打开一个窗口，其中包含有关事件的信息。事件信息窗口的上部将显示事件树。
3. 单击事件树中父进程名称右侧的下拉列表。
   由父进程启动的所有事件的列表将显示。默认情况下，列表中的事件按类型分组。
4. 在事件树中，在父进程名称右侧的下拉列表中，选择以下选项之一：
   - 如果要显示父进程发起的所有事件，请单击**所有事件**。
     由父进程启动的所有事件的表将显示。默认情况下，表中的事件按时间排序，最新的事件位于表的顶部。

- 如果要查看由父进程发起的特定类型的所有事件，请选择相关事件类型的名称。
  由父进程启动的所有事件的表将显示，按类型分组。

您可以通过单击相关事件所在行来查看事件信息。事件显示在事件树中。

查看事件树中的主机信息

如果您正在查看的事件或父进程没有启动它的进程，则事件树中的进程节点将被替换为注册事件或运行父进程的主机的节点。

要查看注册事件或启动父进程的主机的信息：

1. 使用构建器模式或源代码模式执行事件搜索。
   事件表将显示。
2. 选择您想查看其信息的事件。
   这将打开一个窗口，其中包含有关事件的信息。窗口上部将显示事件树。
3. 单击事件树中的主机名。
   窗口的底部将显示有关注册事件的主机或正在运行的父进程的信息。

查看事件表

事件表在**事件数据库中的威胁搜寻**完成后显示在应用程序 Web 界面窗口的威胁搜索部分。您可以按**事件时间**、**事件类型**、**主机**和**用户名称**列对表中的事件进行排序。

如果您使用分布式解决方案和多租户模式，表中的事件将按所选服务器和租户的主机进行分组。

事件表包含以下信息：

1. **事件时间** — 检测到事件的日期和时间。
2. **事件类型**，例如，**进程已启动**。
3. **主机名称** — 生成警报的主机名称。
4. **详细信息** — 有关事件的信息。
5. **用户名称** — 具有 Endpoint Agent 组件的计算机上的用户名称，其用户账户被用于检测事件。

在事件表中，**详细信息**列在**事件类型**列中显示每种类型事件的数据集（见下表）。

事件类型列中每个事件类型的**详细信息**列中的数据集

事件类型	详细信息
进程已启动	已启动的进程文件的名称。SHA256 和 MD5 哈希。
模块已加载	已加载的动态库的名称。SHA256 和 MD5 哈希。
到远程主机的连接	进行远程连接尝试的 URL。尝试建立远程连接的文件的名称。
阻止的应用程序 (防止规则)	阻止启动的应用程序文件的名称。SHA256 和 MD5 哈希。

事件类型	详细信息
文件已阻止	阻止启动的文档的名称。SHA256 和 MD5 哈希。
文件已更改	创建的文件的名称。SHA256 和 MD5 哈希。
系统事件日志	用于在系统日志中记录事件的通道。事件类型 ID。
注册表已修改	注册表中键的名称。 <键中变量的名称>=<变量值>。
监听的端口	服务器地址和端口。监听端口的进程文件的名称。
驱动程序已加载	加载的驱动程序的文件名。SHA256 和 MD5 哈希。
检测	检测到对象的文件的名称。检测到的对象的名称。SHA256 和 MD5 哈希。
检测处理结果	检测到对象的文件的名称。检测到的对象的名称。SHA256 和 MD5 哈希。
AMSI 扫描	扫描对象的名称。脚本的类型。被发送以进行扫描的脚本文本。
进程: 解释文件运行	运行的文件的名称。SHA256 和 MD5 哈希。
进程: 控制台交互式输入	命令文本。
进程已终止	已停止进程的文件名。SHA256 和 MD5 哈希。
DNS	正在查找的域名。资源记录类型 ID。
LDAP	搜索范围和过滤器。
命名管道	管道名称。管道操作类型。
WMI	WMI 操作类型。事件消费者源代码。
代码注入	包含钩子过程的目标进程的文件名或动态链接库的名称以及注入后传递控制权的函数的名称。访问目标进程文件的方法。目标进程文件的 SHA256 和 MD5 哈希。
进程访问	接收者进程文件的名称。事件的重要性。对流程文件执行的操作类型。进程访问权限。

如果您使用 Kaspersky Endpoint Agent 作为 Endpoint Agent 组件，当 Kaspersky Anti Targeted Attack Platform 与 Kaspersky Endpoint Agent for Windows 3.10 或更高版本集成时以及当 Kaspersky Endpoint Agent 与 Kaspersky Endpoint Security for Windows 11.5 或更高版本集成时，有关**AMSI 扫描**事件的信息可用。如果计算机上未安装 Kaspersky Endpoint Security for Windows 且未与 Kaspersky Endpoint Agent 集成，则有关**AMSI 扫描**事件的信息不会记录在事件数据库中，也不会显示在 Kaspersky Anti Targeted Attack Platform Web 界面中。

如果 Kaspersky Endpoint Agent 被用作 Endpoint Agent 组件，则 Central Node 服务器会基于从 EPP 应用程序接收的数据的事件生成**检测**和**检测处理结果**。如果计算机上未安装 EPP 应用程序且未与 Kaspersky Endpoint Agent 集成，则有关这些事件的信息不会记录在事件数据库中，也不会显示在 Kaspersky Anti Targeted Attack Platform Web 界面中。

单击包含事件类型名称、数据、其他信息和用户名的链接将打开一个列表，您可以从其中选择要在对象上执行的操作。根据单元格中的值，您可以执行以下操作之一：

- 对于单元格中的所有值：
  - **按照此值进行过滤**。
  - **从过滤器中排除**。
  - **复制值到剪贴板**。

- 主机名称：
  - **查找事件**。
  - **查找警报**。
  - **从网络隔离**。
- 文件名：
  - **杀死进程**。
  - **使用唯一的 PID 杀死进程**。
  - **删除文件**。
  - **获取文件**。
  - **进行取证**。
  - **隔离文件**。
- MD5 哈希：
  - **查找事件**。
  - **查找警报**。
  - **在 Kaspersky TIP 上查找**。
  - **创建防止规则**。
  - **在存储中查找**。
- SHA256 哈希值：
  - **查找事件**。
  - **查找警报**。
  - **在 Kaspersky TIP 上查找**。
  - **在 virustotal.com 上查找**。
  - **创建防止规则**。
  - **在存储中查找**。

配置事件表显示

您可以显示或隐藏列并更改事件表中列的顺序。

要配置事件表显示：

1. 使用构建器模式或源代码模式执行事件搜索。
   事件表将显示。
2. 在表格的标题部分，单击 。
   这将打开**定制表格**窗口。
3. 如果要在表中显示列，请选择要在表中显示的参数名称旁边的复选框。
   如果要隐藏表中的参数，请清除该复选框。

   > 必须选择至少一个复选框。

4. 如果要更改表格中列的顺序，请将鼠标光标移动到具有相关参数的行，单击 并将该行移动到新位置。
5. 如果要恢复默认表格显示设置，请单击**默认**。
6. 单击**应用**。

事件表的显示已配置。

查看有关事件的信息

查看活动详情：

1. 在应用程序 Web 界面窗口中，选择**威胁搜索**部分，**生成器**或者**源代码**选项卡。
   这将打开事件搜索表单。
2. 如果您使用的是分布式解决方案和多租户模式，并且希望为所有租户启用事件显示，请开启**在所有租户中搜索**切换开关。
3. 使用构建器模式或源代码模式执行事件搜索。
   事件表将显示。
4. 选择您想查看其信息的事件。

这将打开一个窗口，其中包含有关事件的信息。

有关“进程已启动”事件的信息

显示**进程已启动**事件信息的窗口包含以下详情：

- 事件树。
- 处理事件时可以执行的操作。

- **进程已启动**部分：
  - **IOA 标记**– 有关使用 Targeted Attack Analyzer 技术进行文件分析的结果的信息：用于创建警报的 TAA (IOA) 规则的名称。

    单击链接可显示有关 TAA (IOA) 规则的信息。如果规则是由卡巴斯基专家提供的，则它包含有关触发的 MITRE 技术的信息以及对事件进行反应的建议。

    如果在创建事件时触发了 TAA (IOA) 规则，则会显示该字段。
  - **文件** – 进程文件名。
  - **进程 ID** – 进程标识符。
  - **启动参数** – 进程启动设置。

    如果事件由 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Mac记录在事件数据库中而不是**启动参数**字段中，则显示**命令**字段，即用于运行进程的命令。
  - **当前目录** – 进程的当前目录
  - **MD5** – 进程文件的 MD5 哈希。
  - **SHA256** – 进程文件的 MD5 哈希。
  - **大小** – 进程文件的大小。
  - **文件类型** – 进程文件的类型。
  - **事件时间** – 进程启动时间。
  - **属性修改时间** – 进程文件属性发生改变的时间。
  - **创建时间** – 进程文件的创建时间。
  - **修改时间** – 进程文件的上次修改时间。
- **详细信息**部分：
  - **应用程序名称** – 例如，操作系统的名称。
  - **供应商** – 例如，操作系统的供应商。
  - **文件描述** – 例如，示例文件。
  - **原始文件名** – 例如，ExampleFile.exe。
  - **签名主题** – 颁发文件数字证书的组织。
  - **签名验证结果** – 例如，“无效”或“正常”。
  - **属性** – 根据 Windows 分类的文件属性。例如，A（存档）、D（目录）或 S（系统文件）。

如果事件由 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Mac记录在事件数据库中，则**详细信息**部分还包括以下字段：

- **属性** — 进程文件的属性。
- **进程类型** — 例如，exec。
- **环境变量** — 进程的环境变量。
- **真实用户名** — 在系统中注册时指定的用户名称。
- **真实组名称** — 用户所属的组。
- **有效用户名** — 用于登录系统的用户名。
- **有效组名称** — 名称被用于登录系统的用户组。
- **所有者用户名** — 创建了进程文件的用户的名称。
- **所有者组名** — 其用户可以修改或删除进程文件的组的名称。
- **文件允许的功能** — 可用于访问进程文件的权限。如果事件由 Kaspersky Endpoint Security for Mac 记录，则此字段不会显示。
- **文件可继承功能** — 用户组对进程文件的父目录执行操作的权限。如果事件由 Kaspersky Endpoint Security for Mac 记录，则此字段不会显示。
- **文件有效能力** — 当前与流程文件相关的权限。如果事件由 Kaspersky Endpoint Security for Mac 记录，则此字段不会显示。
- **从 URL 下载** — 下载进程文件的 URL。
- **源** — 获取进程文件的消息的元数据。
- **账户属性** — 运行进程的用户账户的标志。
- **进程创建标志** — 进程创建标志。
- **符号链接** — 符号链接的路径。
- **调用跟踪** — 调用堆栈。

- **事件发起者**部分：
  - **文件** — 父进程文件的路径。
  - **进程 ID** — 父进程的标识符。
  - **启动参数** — 父进程启动设置。

    如果事件由 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Mac记录在事件数据库中而不是**启动参数**字段中，则显示**命令**字段，即用于运行父进程的命令。
  - **MD5** — 父进程文件的 MD5 哈希。
  - **SHA256** — 父进程文件的 SHA256 哈希。

- **系统信息**部分：
  - **主机名称** — 启动了进程的主机的名称。
  - **主机 IP** — 启动了进程的主机的 IP 地址。

    如果您使用动态 IP 地址，该字段将显示创建事件时分配给主机的 IP 地址。

    该应用程序不支持 IPv6。如果您使用 IPv6，则不会显示主机的 IP 地址。
  - **用户账户类型** — 运行进程的账户的类型。例如，管理员。
  - **登录类型** — 例如，使用正在运行的服务。
  - **用户名称** — 启动该进程的用户的名称。
  - **操作系统版本** — 主机上正在使用的操作系统的版本。

    如果事件由 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Mac记录在事件数据库中，则**系统信息**部分还显示从其执行远程登录的主机名称的**从远程主机登录**字段。

单击具有文件名称或文件路径的链接将打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - **杀死进程**。
  - **使用唯一的 PID 杀死进程**。
  - **删除文件**。
  - **获取文件**。
  - **进行取证**。
  - **隔离文件**。
- **复制值到剪贴板**。

在 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Mac 在事件数据库中记录的事件信息中，您可以单击包含文件名或文件路径的链接以打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行**获取文件**任务。
- **复制值到剪贴板**。

单击具有主机名的链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - 获取数据→文件、取证、磁盘镜像、内存转储。
  - **杀死进程**。
  - **删除文件**。
  - **隔离文件**。
  - **运行应用程序**。
- **复制值到剪贴板**。

在事件数据库中记录的 Kaspersky Endpoint Security for Linux事件信息中，您可以单击主机名链接打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - **杀死进程**。
  - **删除文件**。
  - **获取文件**。
  - **隔离文件**。
  - **运行应用程序**。
- **复制值到剪贴板**。

在事件数据库中记录的 Kaspersky Endpoint Security for Mac 事件信息中，您可以单击带有文件名或文件路径的链接来打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行**获取文件**任务。
- **复制值到剪贴板**。

单击 **MD5** 链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **在 Kaspersky TIP 上查找**。
- **在存储中查找**。
- **创建防止规则**。
- **复制值到剪贴板**。

单击 **SHA256** 链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **在 Kaspersky TIP 上查找**。
- **在 virustotal.com 上查找**。
- **在存储中查找**。
- **创建防止规则**。
- **复制值到剪贴板**。

有关“进程已终止”事件的信息

显示**进程已终止**事件信息的窗口包含以下详情：

- 事件树。
- 处理事件时可以执行的操作。
- **进程已终止**部分：
  - **IOA 标记** — 有关使用 Targeted Attack Analyzer 技术进行文件分析的结果的信息：用于创建警报的 TAA (IOA) 规则的名称。

    单击链接可显示有关 TAA (IOA) 规则的信息。如果规则是由卡巴斯基专家提供的，则它包含有关触发的 MITRE 技术的信息以及对事件进行反应的建议。

    如果在创建事件时触发了 TAA (IOA) 规则，则会显示该字段。
  - **文件** — 进程文件名。
  - **进程 ID** — 进程标识符。

- **启动参数** — 进程启动设置。

  如果事件由 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Mac记录在事件数据库中而不是**启动参数**字段中，则显示**命令**字段，即用于运行进程的命令。

- **MD5** — 进程文件的 MD5 哈希。
- **SHA256** — 进程文件的 MD5 哈希。
- **大小** — 进程文件的大小。
- **事件时间** — 进程终止时间。

- **事件发起者**部分：
  - **文件** — 父进程文件的路径。
  - **进程 ID** — 父进程的标识符。
  - **启动参数** — 父进程启动设置。

    如果事件由 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Mac记录在事件数据库中而不是**启动参数**字段中，则显示**命令**字段，即用于运行父进程的命令。

  - **MD5** — 父进程文件的 MD5 哈希。
  - **SHA256** — 父进程文件的 SHA256 哈希。
- **系统信息**部分：
  - **主机名称** — 启动了进程的主机的名称。
  - **主机 IP** — 启动了进程的主机的 IP 地址。

    如果您使用动态 IP 地址，该字段将显示创建事件时分配给主机的 IP 地址。

    该应用程序不支持 IPv6。如果您使用 IPv6，则不会显示主机的 IP 地址。

  - **用户账户类型** — 终止进程的账户类型。例如，管理员。
  - **用户名称** — 启动该进程的用户的名称。
  - **操作系统版本** — 主机上正在使用的操作系统的版本。

  如果事件由 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Mac记录在事件数据库中，则**系统信息**部分还显示从其执行远程登录的主机名称的**从远程主机登录**字段。

单击具有文件名称或文件路径的链接将打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。

- 运行以下任务：
  - **删除文件**。
  - **获取文件**。
  - **进行取证**。
  - **隔离文件**。
- **复制值到剪贴板**。

在 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Mac 在事件数据库中记录的事件信息中，您可以单击包含文件名或文件路径的链接以打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行**获取文件**任务。
- **复制值到剪贴板**。

单击具有主机名的链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - 获取数据→文件、取证、磁盘镜像、内存转储。
  - **杀死进程**。
  - **删除文件**。
  - **隔离文件**。
  - **运行应用程序**。
- **复制值到剪贴板**。

在事件数据库中记录的 Kaspersky Endpoint Security for Linux事件信息中，您可以单击主机名链接打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - **杀死进程**。
  - **删除文件**。

- **获取文件**。
- **隔离文件**。
- **运行应用程序**。

- **复制值到剪贴板**。

在事件数据库中记录的 Kaspersky Endpoint Security for Mac 事件信息中，您可以单击带有文件名或文件路径的链接来打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行**获取文件**任务。
- **复制值到剪贴板**。

单击 **MD5** 链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **在 Kaspersky TIP 上查找**。
- **在存储中查找**。
- **创建防止规则**。
- **复制值到剪贴板**。

单击 **SHA256** 链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **在 Kaspersky TIP 上查找**。
- **在 virustotal.com 上查找**。
- **在存储中查找**。
- **创建防止规则**。
- **复制值到剪贴板**。

有关“模块已加载”事件的信息

显示**模块已加载**事件信息的窗口包含以下详细信息：

- 事件树。
- 处理事件时可以执行的操作。
- **模块已加载**部分：
  - **IOA 标记** — 有关使用 Targeted Attack Analyzer 技术进行文件分析的结果的信息：用于创建警报的 TAA (IOA) 规则的名称。

    单击链接可显示有关 TAA (IOA) 规则的信息。如果规则是由卡巴斯基专家提供的，则它包含有关触发的 MITRE 技术的信息以及对事件进行反应的建议。

    如果在创建事件时触发了 TAA (IOA) 规则，则会显示该字段。
  - **文件** — 加载的模块文件的名称。
  - **MD5** — 加载的模块文件的 MD5 哈希。
  - **SHA256** — 加载的模块文件的 SHA256 哈希。
  - **DLL 文件类型** — 已加载模块的类型。
  - **大小** — 加载的模块的大小。
  - **事件时间** — 加载模块的时间。
- **详细信息**部分：
  - **应用程序名称** — 例如，操作系统的名称。
  - **供应商** — 例如，操作系统的供应商。
  - **文件描述** — 例如，示例文件。
  - **原始文件名** — 例如，示例文件。
  - **区域 ID** —
  - **签名主题** — 颁发已加载模块数字证书的组织。
  - **签名验证结果** — 例如，“签名无效”或“签名正常”。
  - **数字签名时间** — 已加载模块的签名时间。
  - **文件属性已修改** — 已加载模块的属性修改时间。
  - **创建时间** — 加载的模块的创建时间。
  - **修改时间** — 加载的模块的上次修改日期。

- **.NET 程序集名称** – 已加载模块的 .NET 程序集的名称。
- **.NET 程序集标志** – 已加载模块的 .NET 程序集的标志。
- **.NET 模块标志** – 已加载模块的标志。
- **旁路路径中的下一个 DLL** – 该字段包含可以加载的 DLL 库的路径，而不是现有库的路径。
  如果满足以下条件，则显示该字段：
  - 加载的 DLL 的来源不受信任。
  - 标准搜索路径中的文件夹包含具有相同名称但不同哈希值的库。

  如果您使用 Kaspersky Endpoint Agent 作为 Endpoint Agent 组件，则仅当 Kaspersky Anti Targeted Attack Platform 与 Kaspersky Endpoint Agent 3.10 for Windows 集成时，Kaspersky Anti Targeted Attack Platform 才会收到填充**旁路路径中的下一个 DLL**字段所需的数据。当应用程序与旧版本的 Kaspersky Endpoint Agent 应用程序集成时，该字段不会显示在事件信息中。

- **事件发起者**部分：
  - **文件** – 父进程文件的路径。
  - **MD5** – 父进程文件的 MD5 哈希。
  - **SHA256** – 父进程文件的 SHA256 哈希。
- **系统信息**部分：
  - **主机名称** – 加载了模块的主机的名称。
  - **主机 IP** – 加载了模块的主机的 IP 地址。

    如果您使用动态 IP 地址，该字段将显示创建事件时分配给主机的 IP 地址。

    该应用程序不支持 IPv6。如果您使用 IPv6，则不会显示主机的 IP 地址。

  - **用户名称** – 加载了模块的用户的名称。
  - **操作系统版本**– 主机上使用的操作系统版本。

单击**模块已加载**部分中包含文件名或文件路径的链接将打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - **删除文件**。
  - **获取文件**。

- **进行取证**。
- **隔离文件**。

- **复制值到剪贴板**。

单击**事件发起者**部分中包含文件名或文件路径的链接将打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - **杀死进程**。
  - **使用唯一的 PID 杀死进程**。
  - **删除文件**。
  - **获取文件**。
  - **进行取证**。
  - **隔离文件**。
- **复制值到剪贴板**。

单击具有主机名的链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - 获取数据→文件、取证、磁盘镜像、内存转储。
  - **杀死进程**。
  - **删除文件**。
  - **隔离文件**。
  - **运行应用程序**。
- **复制值到剪贴板**。

单击 MD5 链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **在 Kaspersky TIP 上查找**。

- **在存储中查找**。
- **创建防止规则**。
- **复制值到剪贴板**。

单击 **SHA256** 链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **在 Kaspersky TIP 上查找**。
- **在 virustotal.com 上查找**。
- **在存储中查找**。
- **创建防止规则**。
- **复制值到剪贴板**。

有关“远程连接”事件的信息

显示**到远程主机的连接**事件信息的窗口包含以下详细信息：

- 事件树。
- 处理事件时可以执行的操作。
- **到远程主机的连接**部分：
  - **IOA 标记** — 有关使用 Targeted Attack Analyzer 技术进行文件分析的结果的信息：用于创建警报的 TAA (IOA) 规则的名称。

    单击链接可显示有关 TAA (IOA) 规则的信息。如果规则是由卡巴斯基专家提供的，则它包含有关触发的 MITRE 技术的信息以及对事件进行反应的建议。

    如果在创建事件时触发了 TAA (IOA) 规则，则会显示该字段。
  - **连接方向**是连接方向（入站或出站）。
  - **远程 IP** — 进行远程连接尝试的主机的 IP 地址。
  - **本地 IP** — 进行远程连接尝试的本地计算机的 IP 地址。
  - **事件时间** — 远程连接尝试的时间。
- “**TLS**”部分：
  - **版本** — 协议的版本。
  - **SNI** — 要连接的网站的名称。
  - **加密 SNI** — 网站的加密名称。

- **证书 MD5** — 证书文件的 MD5 哈希。
- **证书 SHA1** — 证书文件的 SHA1 哈希。
- **证书颁发者名称** — 签署证书的组织的名称。
- **序列号** — 证书的唯一号码。
- **证书验证结果** — 证书验证的结果。
- **证书有效期自** — 证书有效的日期。
- **证书有效期至** — 证书过期的日期。
- **JA3** — 客户端 hello 数据包中以下字段的十进制字节值：TLS 版本、密码套件、TLS 协议扩展列表、椭圆曲线和椭圆曲线格式。要分隔字段，请使用“，”字符；要分隔每个字段中的值，请使用“-”字符。
- **JA3S** — 服务器 hello 数据包中以下字段的十进制字节值：TLS 版本、密码套件和 TLS 协议扩展列表。要分隔字段，请使用“，”字符；要分隔每个字段中的值，请使用“-”字符。
- **JA3 MD5** — JA3 指纹。
- **JA3S MD5** — JA3S 指纹。

- **事件发起者**部分：
  - **文件** — 父进程文件的名称。
  - **MD5** — 父进程文件的 MD5 哈希。
  - **SHA256** — 父进程文件的 SHA256 哈希。
- **系统信息**部分：
  - **主机名称** — 进行远程连接尝试的主机名。
  - **主机 IP** — 从其进行远程连接尝试的主机的 IP 地址。

    如果您使用动态 IP 地址，该字段将显示创建事件时分配给主机的 IP 地址。

    该应用程序不支持 IPv6。如果您使用 IPv6，则不会显示主机的 IP 地址。
  - **用户名称** — 尝试建立远程连接的用户名。
  - **操作系统版本** — 主机上使用的操作系统版本。

单击**到远程主机的连接**部分中包含文件名或文件路径的链接将打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。

- 运行以下任务：
  - **删除文件**。
  - **获取文件**。
  - **进行取证**。
  - **隔离文件**。
- **复制值到剪贴板**。

单击**事件发起者**部分中包含文件名或文件路径的链接将打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - **杀死进程**。
  - **使用唯一的 PID 杀死进程**。
  - **删除文件**。
  - **获取文件**。
  - **进行取证**。
  - **隔离文件**。
- **复制值到剪贴板**。

单击具有主机名的链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - 获取数据→文件、取证、磁盘镜像、内存转储。
  - **杀死进程**。
  - **删除文件**。
  - **隔离文件**。
  - **运行应用程序**。
- **复制值到剪贴板**。

单击 **MD5** 链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **在 Kaspersky TIP 上查找**。
- **在存储中查找**。
- **创建防止规则**。
- **复制值到剪贴板**。

单击 **SHA256** 链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **在 Kaspersky TIP 上查找**。
- **在 virustotal.com 上查找**。
- **在存储中查找**。
- **创建防止规则**。
- **复制值到剪贴板**。

“防护规则”事件信息

该窗口包含有关触发防止规则的事件的信息，即**阻止的应用程序 (防止规则)**类型的事件，显示以下详细信息：

- 事件树。
- 处理事件时可以执行的操作。
- **阻止的应用程序 (防止规则)**部分：
  - **IOA 标记** — 有关使用 Targeted Attack Analyzer 技术进行文件分析的结果的信息：用于创建警报的 TAA (IOA) 规则的名称。

    单击链接可显示有关 TAA (IOA) 规则的信息。如果规则是由卡巴斯基专家提供的，则它包含有关触发的 MITRE 技术的信息以及对事件进行反应的建议。

    如果在创建事件时触发了 TAA (IOA) 规则，则会显示该字段。
  - **文件** — 被阻止运行的文件的名称。
  - **启动参数** — 用于尝试运行文件的参数。
  - **MD5** — 被阻止运行的文件的 MD5 哈希。
  - **SHA256** — 被阻止运行的文件的 SHA256 哈希。

- **大小** – 被阻止运行的文件的大小。
- **事件时间** – 触发阻止文件启动的时间。

- **详细信息**部分：
  - **应用程序名称** – 例如，操作系统的名称。
  - **供应商** – 例如，操作系统的供应商。
  - **文件描述** – 例如，示例文件。
  - **原始文件名** – 例如，ExampleFile.exe。
  - **签名主题** – 颁发文件数字证书的组织。
  - **签名验证结果** – 例如，“签名无效”或“签名正常”。
  - **创建时间** – 被阻止运行的文件的创建时间。
  - **修改时间** – 被阻止运行的文件的上次修改日期。
- **事件发起者**部分：
  - **文件** – 父进程文件的名称。
  - **MD5** – 父进程文件的 MD5 哈希。
  - **SHA256** – 父进程文件的 SHA256 哈希。
  - **进程 ID** – 父进程的标识符。
- **系统信息**部分：
  - **主机名称** – 触发了阻止文件启动的主机的名称。
  - **主机 IP** – 触发了阻止文件启动的主机的 IP 地址。

    如果您使用动态 IP 地址，该字段将显示创建事件时分配给主机的 IP 地址。

    该应用程序不支持 IPv6。如果您使用 IPv6，则不会显示主机的 IP 地址。
  - **用户名称** – 账户用于执行文件的用户的名称。
  - **操作系统版本** – 主机上使用的操作系统版本。

单击具有文件名称或文件路径的链接将打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。

- 运行以下任务：
  - **杀死进程**。
  - **使用唯一的 PID 杀死进程**。
  - **删除文件**。
  - **获取文件**。
  - **进行取证**。
  - **隔离文件**。
- **复制值到剪贴板**。

单击具有主机名的链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - 获取数据→文件、取证、磁盘镜像、内存转储。
  - **杀死进程**。
  - **删除文件**。
  - **隔离文件**。
  - **运行应用程序**。
- **复制值到剪贴板**。

在事件数据库中记录的 Kaspersky Endpoint Security for Linux事件信息中，您可以单击主机名链接打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - **杀死进程**。
  - **删除文件**。
  - **获取文件**。
  - **隔离文件**。
  - **运行应用程序**。
- **复制值到剪贴板**。

单击 **MD5** 链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **在 Kaspersky TIP 上查找**。
- **在存储中查找**。
- **创建防止规则**。
- **复制值到剪贴板**。

单击 **SHA256** 链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **在 Kaspersky TIP 上查找**。
- **在 virustotal.com 上查找**。
- **在存储中查找**。
- **创建防止规则**。
- **复制值到剪贴板**。

有关“文档被阻止”事件的信息

显示**文件已阻止**事件信息的窗口包含以下详细信息：

- 事件树。
- 处理事件时可以执行的操作。
- **文件已阻止**部分：
  - **IOA 标记** — 有关使用 Targeted Attack Analyzer 技术进行文件分析的结果的信息：用于创建警报的 TAA (IOA) 规则的名称。

    单击链接可显示有关 TAA (IOA) 规则的信息。如果规则是由卡巴斯基专家提供的，则它包含有关触发的 MITRE 技术的信息以及对事件进行反应的建议。

    如果在创建事件时触发了 TAA (IOA) 规则，则会显示该字段。
  - **文件** — 阻止的文档的名称。
  - **MD5** — 阻止的文档的 MD5 哈希。
  - **SHA256** — 阻止的文档的 SHA256 哈希。
  - **事件时间** — 文档被阻止的时间。

- **进程文件** – 尝试打开文档的进程的文件名称。
- **进程 MD5** – 尝试打开文档的进程的 MD5 哈希。
- **进程 SHA256** – 尝试打开文档的进程的 SHA256 哈希。

- **事件发起者**部分：
  - **文件** – 父进程文件的名称。
  - **MD5** – 父进程文件的 MD5 哈希。
  - **SHA256** – 父进程文件的 SHA256 哈希。
  - **进程 ID** – 父进程的标识符。
- **系统信息**部分：
  - **主机名称** – 文档被阻止的主机的名称。
  - **主机 IP** – 文档被阻止的主机的 IP 地址。

    如果您使用动态 IP 地址，该字段将显示创建事件时分配给主机的 IP 地址。

    该应用程序不支持 IPv6。如果您使用 IPv6，则不会显示主机的 IP 地址。
  - **用户名称** – 尝试打开文档的用户的名称。
  - **操作系统版本** – 主机上使用的操作系统版本。

单击**文件已阻止**部分中包含文件名或文件路径的链接将打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - **删除文件**。
  - **获取文件**。
  - **进行取证**。
  - **隔离文件**。
- **复制值到剪贴板**。

单击**事件发起者**部分中包含文件名或文件路径的链接将打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。

- 运行以下任务：
  - **杀死进程**。
  - **使用唯一的 PID 杀死进程**。
  - **删除文件**。
  - **获取文件**。
  - **进行取证**。
  - **隔离文件**。
- **复制值到剪贴板**。

单击具有主机名的链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - 获取数据→文件、取证、磁盘镜像、内存转储。
  - **杀死进程**。
  - **删除文件**。
  - **隔离文件。**
  - **运行应用程序**。
- **复制值到剪贴板**。

在事件数据库中记录的 Kaspersky Endpoint Security for Linux事件信息中，您可以单击主机名链接打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - **杀死进程**。
  - **删除文件**。
  - **获取文件**。
  - **隔离文件。**
  - **运行应用程序**。
  - **复制值到剪贴板**。

单击 **MD5** 链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **在 Kaspersky TIP 上查找**。
- **在存储中查找**。
- **创建防止规则**。
- **复制值到剪贴板**。

单击 **SHA256** 链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **在 Kaspersky TIP 上查找**。
- **在 virustotal.com 上查找**。
- **在存储中查找**。
- **创建防止规则**。
- **复制值到剪贴板**。

有关“文件已修改”事件的信息

显示**文件已更改**事件信息的窗口包含以下详情：

- 事件树。
- 处理事件时可以执行的操作。
- 根据对文件执行的操作类型，事件信息中会显示以下部分名称之一：
  - **文件已创建**。
  - **文件已修改**。
  - **文件已重命名**。
  - **文件属性已修改**。
  - **文件已删除**。
  - **文件读取**。
  - **已创建硬链接**。

- **符号链接已创建**。
- **文件创建时间已修改**。

此部分可能会显示以下信息：

- **IOA 标记** — 有关使用 Targeted Attack Analyzer 技术进行文件分析的结果的信息：用于创建警报的 TAA (IOA) 规则的名称。

  单击链接可显示有关 TAA (IOA) 规则的信息。如果规则是由卡巴斯基专家提供的，则它包含有关触发的 MITRE 技术的信息以及对事件进行反应的建议。

  如果在创建事件时触发了 TAA (IOA) 规则，则会显示该字段。
- **文件** — 已创建、删除或修改的文件的名称。
- **MD5** — 已创建、删除或修改的文件的 MD5 哈希。
- **链接引用的文件的 MD5** — 创建的链接指向的文件的 MD5 哈希值。
- **SHA256** — 已创建、删除或修改的文件的 SHA256 哈希值。
- **链接引用的文件的 SHA256** — 创建的链接指向的文件的 SHA256 哈希值。
- **符号链接** — 创建的符号链接指向的文件的全名。
- **大小** — 已创建、删除或修改的文件的大小。
- **事件时间** — 检测到事件的时间。
- **创建时间** — 创建文件的时间。
- **修改时间** — 文件的上次修改时间。
- **属性修改时间** — 文件属性被修改的时间。
- **以前的版本** — 先前版本文件的名称。

  > **以前的版本**字段仅为**文件已重命名**类型的操作显示在事件详细信息中。

- **重启后删除文件** — 要删除的文件的状态。

  如果应用了“删除”操作的文件被在任何应用程序中打开或被其他进程使用，则当这些进程在主机重新启动后终止时，该文件将被删除。在这种情况下，**重启后删除文件**显示是。

  如果应用了“删除”操作的文件被立即删除，则**重启后删除文件**字段显示否。

  > **重启后删除文件**字段仅为**文件已删除**类型的操作显示在事件详细信息中。

如果事件由 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Mac记录在事件数据库中，则该部分还包括以下字段：

- **文件类型** — 已创建、删除或修改的文件的扩展名。
- **文件打开标志** — 已创建、删除或修改的文件的打开标志的值。

- **所有者用户名** — 创建了文件的用户的名称。
- **所有者组名** — 其用户可以修改或删除文件的组的名称。
- **文件允许的功能** — 可用于访问已创建、删除或修改的文件的权限。如果事件由 Kaspersky Endpoint Security for Mac 记录，则此字段不会显示。
- **文件可继承功能** — 用户组对已创建、删除或修改的文件的父目录执行操作的权限。如果事件由 Kaspersky Endpoint Security for Mac 记录，则此字段不会显示。
- **文件有效能力** — 当前与已创建、删除或修改的文件相关的权限。如果事件由 Kaspersky Endpoint Security for Mac 记录，则此字段不会显示。

- **事件发起者**部分：
  - **文件** — 父进程文件的路径。
  - **MD5** — 父进程文件的 MD5 哈希。
  - **SHA256** — 父进程文件的 SHA256 哈希。

  如果事件由 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Mac记录在事件数据库中，则**事件发起者**部分还包括以下字段：
  - **环境变量** — 进程的环境变量。
  - **真实用户名** — 在系统中注册时指定的用户名称。
  - **真实组名称** — 用户所属的组。
  - **有效用户名** — 用于登录系统的用户名。
  - **有效组名称**— 名称被用于登录系统的用户组。
- **系统信息**部分：
  - **主机名称** — 创建文件的主机的名称。
  - **主机 IP** — 在其上创建文件的主机的 IP 地址。

    如果您使用动态 IP 地址，该字段将显示创建事件时分配给主机的 IP 地址。

    该应用程序不支持 IPv6。如果您使用 IPv6，则不会显示主机的 IP 地址。
  - **用户名称** — 创建了文件的用户的名称。
  - **操作系统版本**— 主机上正在使用的操作系统的版本。

  如果事件由 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Mac记录在事件数据库中，则**系统信息**部分还显示从其执行远程登录的主机名称的**从远程主机登录**字段。

在包含执行操作的文件信息的部分中单击包含文件名或文件路径的链接将打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - **删除文件**。
  - **获取文件**。
  - **进行取证**。
  - **隔离文件**。
- **复制值到剪贴板**。

单击**事件发起者**部分中包含文件名或文件路径的链接将打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - **杀死进程**。
  - **使用唯一的 PID 杀死进程**。
  - **删除文件**。
  - **获取文件**。
  - **进行取证**。
  - **隔离文件**。
- **复制值到剪贴板**。

在 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Mac 在事件数据库中记录的事件信息中，您可以单击包含文件名或文件路径的链接以打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行**获取文件**任务。
- **复制值到剪贴板**。

单击具有主机名的链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - 获取数据→文件、取证、磁盘镜像、内存转储。
  - **杀死进程**。
  - **删除文件**。
  - **隔离文件**。
  - **运行应用程序**。
- **复制值到剪贴板**。

在事件数据库中记录的 Kaspersky Endpoint Security for Linux事件信息中，您可以单击主机名链接打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - **杀死进程**。
  - **删除文件**。
  - **获取文件**。
  - **隔离文件**。
  - **运行应用程序**。
- **复制值到剪贴板**。

在事件数据库中记录的 Kaspersky Endpoint Security for Mac 事件信息中，您可以单击带有文件名或文件路径的链接来打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行**获取文件**任务。
- **复制值到剪贴板**。

单击 **MD5** 链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **在 Kaspersky TIP 上查找**。
- **在存储中查找**。
- **创建防止规则**。
- **复制值到剪贴板**。

单击 **SHA256** 链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **在 Kaspersky TIP 上查找**。
- **在 virustotal.com 上查找**。
- **在存储中查找**。
- **创建防止规则**。
- **复制值到剪贴板**。

有关“系统事件日志”事件的信息

显示**系统事件日志**事件信息的窗口包含以下详细信息：

- 事件树。
- 处理事件时可以执行的操作。
- **系统事件日志**部分：
  - **IOA 标记** — 有关使用 Targeted Attack Analyzer 技术进行文件分析的结果的信息：用于创建警报的 TAA (IOA) 规则的名称。

    单击链接可显示有关 TAA (IOA) 规则的信息。如果规则是由卡巴斯基专家提供的，则它包含有关触发的 MITRE 技术的信息以及对事件进行反应的建议。

    如果在创建事件时触发了 TAA (IOA) 规则，则会显示该字段。
  - **事件时间** — 检测到事件的时间。
  - **安全事件 ID** — Windows 日志中安全事件类型的标识符。

如果事件由 Kaspersky Endpoint Security for Linux 记录在事件数据库中，则**系统事件日志**部分还包括以下字段：

- **事件类型** — 事件的类型。
- **操作结果**— 例如，**成功**或者**已失败**。

- **事件数据**部分包含系统日志信息。数据范围取决于 Windows 事件的类型。

  事件数据部分不显示在由 Kaspersky Endpoint Agent for Linux 记录到事件数据库的事件的信息中。

- **事件发起者**部分：
  - **文件** — 进程文件名。
  - **进程 ID** — 进程标识符。
  - **命令** — 用于运行父进程的命令。
  - **环境变量** — 进程的环境变量。
  - **真实用户名** — 在系统中注册时指定的用户名称。
  - **真实组名称** — 用户所属的组。

  事件发起者部分不显示在由 Kaspersky Endpoint Agent for Windows 或 Kaspersky Endpoint Security for Windows 记录到事件数据库的事件信息中。

- **系统信息**部分：
  - **主机名称** — 发生事件的主机的名称。
  - **主机 IP** — 在其上事件发生的主机的 IP 地址。

    如果您使用动态 IP 地址，该字段将显示创建事件时分配给主机的 IP 地址。

    该应用程序不支持 IPv6。如果您使用 IPv6，则不会显示主机的 IP 地址。

  - **用户名称** — 启动了进程的用户的名称，该进程启动了系统日志记录。
  - **操作系统版本** — 主机上正在使用的操作系统的版本。

    Kaspersky Endpoint Security for Linux 记录到事件数据库的事件信息还包括**从远程主机登录**字段，即从其执行远程登录的主机的名称。

在事件数据库中记录的 Kaspersky Endpoint Security for Linux 事件信息中，您可以单击带有文件名或文件路径的链接来打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行**获取文件**任务。
- **复制值到剪贴板**。

单击具有主机名的链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - 获取数据→文件、取证、磁盘镜像、内存转储。
  - **杀死进程**。
  - **删除文件**。
  - **隔离文件**。
  - **运行应用程序**。
- **复制值到剪贴板**。

在事件数据库中记录的 Kaspersky Endpoint Security for Linux事件信息中，您可以单击主机名链接打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - **杀死进程**。
  - **删除文件**。
  - **获取文件**。
  - **隔离文件**。
  - **运行应用程序**。
- **复制值到剪贴板**。

有关“注册表更改”事件的信息

显示**注册表已修改**事件信息的窗口包含以下详细信息：

- 事件树。
- 处理事件时可以执行的操作。
- 根据对注册表执行的操作类型，事件信息中会显示以下部分名称之一：
  - **注册表键已创建**
  - **注册表键已删除**
  - **注册表已修改**
  - **查询的注册表项**
  - **注册表键已重命名**
  - **注册表键已保存**

  该部分显示以下信息：
  - **IOA 标记** — 有关使用 Targeted Attack Analyzer 技术进行文件分析的结果的信息：用于创建警报的 TAA (IOA) 规则的名称。

    单击链接可显示有关 TAA (IOA) 规则的信息。如果规则是由卡巴斯基专家提供的，则它包含有关触发的 MITRE 技术的信息以及对事件进行反应的建议。

    如果在创建事件时触发了 TAA (IOA) 规则，则会显示该字段。
  - “**文件**”是保存注册表项的文件的完整路径。

    > 针对“**注册表键已保存**”类型的事件显示此字段。
  - **密钥路径**是被修改的注册表项的路径
  - **值名称**：例如，RegistrySizeLimit
  - **值数据**是注册表项的值
  - **值类型**：例如，REG_DWORD
  - **事件时间**是修改注册表的时间。

    更改注册表项的名称或值时，您可能会看到其他字段，其中包含有关注册表项修改之前的状态的信息：
    - **之前的密钥路径**字段在注册表项名称被修改时显示。
    - **之前的值数据**字段在注册表值被修改时显示。

- **之前的值类型**字段在注册表值的类型被修改时显示。

  如果您使用 Kaspersky Endpoint Agent 作为 Endpoint Agent 组件，则仅当 Kaspersky Anti Targeted Attack Platform 与 Kaspersky Endpoint Agent for Windows 应用程序版本 3.10 及更高版本集成时，Kaspersky Anti Targeted Attack Platform 才会收到填充**之前的密钥路径**、**之前的值数据**、**之前的值类型**字段所需的数据。将应用程序与旧版本的 Kaspersky Endpoint Agent 集成时，这些字段不会显示在事件信息中。

- **事件发起者**部分：
  - **文件** – 父进程文件的路径。
    单击具有文件名称或文件路径的链接将打开一个列表，您可以在其中选择以下操作之一：
    - **查找事件**。
    - **查找警报**。
    - **复制值到剪贴板**。

    运行以下任务：
    - **杀死进程**。
    - **使用唯一的 PID 杀死进程**。
    - **删除文件**。
    - **获取文件**。
    - **进行取证**。
    - **隔离文件**。
  - **MD5** – 父进程文件的 MD5 哈希。
    单击 **MD5** 链接将打开一个列表，您可以从其中选择以下操作之一：
    - **查找事件**。
    - **查找警报**。
    - **在 Kaspersky TIP 上查找**。
    - **在存储中查找**。
    - **创建防止规则**。

    复制值到剪贴板。
  - **SHA256** – 父进程文件的 SHA256 哈希。

单击 **SHA256** 链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **在 Kaspersky TIP 上查找**。
- **在存储中查找**。
- **创建防止规则**。
- **复制值到剪贴板**。

- **系统信息**部分：
  - **主机名称** – 在其上进行了注册表修改的主机的名称。
    单击具有主机名的链接将打开一个列表，您可以从其中选择以下操作之一：
    - **查找事件**。
    - **查找警报**。
    - **复制值到剪贴板**。

    运行以下任务：
    - 获取数据→文件、取证、磁盘镜像、内存转储。
    - **杀死进程**。
    - **删除文件**。
    - **隔离文件**。
    - **运行应用程序**。
  - **主机 IP** – 在其上进行了注册表修改的主机的 IP 地址。

    如果您使用动态 IP 地址，该字段将显示创建事件时分配给主机的 IP 地址。

    该应用程序不支持 IPv6。如果您使用 IPv6，则不会显示主机的 IP 地址。
  - **用户名称** – 在注册表中进行更改的用户的名称。
  - **操作系统版本** – 主机上使用的操作系统版本。

有关“端口被侦听”事件的信息

显示**监听的端口**事件信息的窗口包含以下详细信息：

- 事件树。
- 处理事件时可以执行的操作。
- **监听的端口**部分：
  - **IOA 标记** — 有关使用 Targeted Attack Analyzer 技术进行文件分析的结果的信息：用于创建警报的 TAA (IOA) 规则的名称。

    单击链接可显示有关 TAA (IOA) 规则的信息。如果规则是由卡巴斯基专家提供的，则它包含有关触发的 MITRE 技术的信息以及对事件进行反应的建议。

    如果在创建事件时触发了 TAA (IOA) 规则，则会显示该字段。
  - **本地端口** — 被监听的端口。
  - **本地 IP** — 端口被监听的网络接口的 IP 地址。
  - **事件时间** — 端口监听时间。
- **事件发起者**部分：
  - **文件** — 父进程文件的路径。

    单击具有文件名称或文件路径的链接将打开一个列表，您可以在其中选择以下操作之一：
    - **查找事件**。
    - **查找警报**。
    - **复制值到剪贴板**。

    运行以下任务：
    - **杀死进程**。
    - **使用唯一的 PID 杀死进程**。
    - **删除文件**。
    - **获取文件**。
    - **进行取证**。
    - **隔离文件**。
  - **MD5** — 父进程文件的 MD5 哈希。

单击 **MD5** 链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **在 Kaspersky TIP 上查找**。
- **在存储中查找**。
- **创建防止规则**。
- **复制值到剪贴板**。

- **SHA256** – 父进程文件的 SHA256 哈希。
  单击 **SHA256** 链接将打开一个列表，您可以从其中选择以下操作之一：
  - **查找事件**。
  - **查找警报**。
  - **在 Kaspersky TIP 上查找**。
  - **在存储中查找**。
  - **创建防止规则**。
  - **复制值到剪贴板**。

- **系统信息**部分：
  - **主机名称** – 端口被监听的主机的名称。
    单击具有主机名的链接将打开一个列表，您可以从其中选择以下操作之一：
    - **查找事件**。
    - **查找警报**。
    - **复制值到剪贴板**。

    运行以下任务：
    - 获取数据→文件、取证、磁盘镜像、内存转储。
    - **杀死进程**。
    - **删除文件**。
    - **隔离文件**。
    - **运行应用程序**。
  - **主机 IP**– 端口被监听的主机的 IP 地址。

如果您使用动态 IP 地址，该字段将显示创建事件时分配给主机的 IP 地址。

该应用程序不支持 IPv6。如果您使用 IPv6，则不会显示主机的 IP 地址。

- **用户名称** — 账户用于监听端口的用户的名称。
- **操作系统版本** — 主机上正在使用的操作系统的版本。

有关“驱动程序已加载”事件的信息

显示**驱动程序已加载**事件信息的窗口包含以下详细信息：

- 事件树。
- 处理事件时可以执行的操作。
- **驱动程序已加载**部分：
  - **IOA 标记** — 有关使用 Targeted Attack Analyzer 技术进行文件分析的结果的信息：用于创建警报的 TAA (IOA) 规则的名称。

    单击链接可显示有关 TAA (IOA) 规则的信息。如果规则是由卡巴斯基专家提供的，则它包含有关触发的 MITRE 技术的信息以及对事件进行反应的建议。

    如果在创建事件时触发了 TAA (IOA) 规则，则会显示该字段。
  - **文件** — 加载的驱动文件的名称。
  - **MD5** — 加载的驱动程序文件的 MD5 哈希。
  - **SHA256** — 加载的驱动程序文件的 MD5 哈希。
  - **大小** — 加载的驱动程序的大小。
  - **事件时间** — 加载驱动程序的时间。
- **详细信息**部分：
  - **应用程序名称** — 例如，操作系统的名称。
  - **供应商** — 例如，操作系统的供应商。
  - **文件描述** — 例如，示例文件。
  - **原始文件名** — 例如，ExampleFile.exe。
  - **签名主题** — 颁发文件数字证书的组织。
  - **签名验证结果** — 例如，“签名无效”或“签名正常”。

- **创建时间** – 加载的驱动程序的创建时间。
- **修改时间** – 加载的驱动程序的上次修改时间。

- **系统信息**部分：
  - **主机名称** – 加载了驱动程序的主机的名称。
  - **主机 IP** – 向其加载了驱动程序的主机的 IP 地址。

    如果您使用动态 IP 地址，该字段将显示创建事件时分配给主机的 IP 地址。

    该应用程序不支持 IPv6。如果您使用 IPv6，则不会显示主机的 IP 地址。
  - **用户名称** – 加载了驱动程序的用户的名称。
  - **操作系统版本** – 主机上使用的操作系统版本。

单击具有文件名称或文件路径的链接将打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - **杀死进程**。
  - **使用唯一的 PID 杀死进程**。
  - **删除文件**。
  - **获取文件**。
  - **进行取证**。
  - **隔离文件**。
- **复制值到剪贴板**。

单击具有主机名的链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - 获取数据→文件、取证、磁盘镜像、内存转储。
  - **杀死进程**。
  - **删除文件**。

- **隔离文件**。
- **运行应用程序**。

- **复制值到剪贴板**。

单击 **MD5** 链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **在 Kaspersky TIP 上查找**。
- **在存储中查找**。
- **创建防止规则**。
- **复制值到剪贴板**。

单击 **SHA256** 链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **在 Kaspersky TIP 上查找**。
- **在 virustotal.com 上查找**。
- **在存储中查找**。
- **创建防止规则**。
- **复制值到剪贴板**。

有关“DNS”事件的信息

显示“**DNS**”事件信息的窗口包含以下详情：

- 事件树。
- 处理事件时可以执行的操作。
- “**DNS**”部分：
  - **IOA 标记** — 有关使用 Targeted Attack Analyzer 技术进行文件分析的结果的信息：用于创建警报的 TAA (IOA) 规则的名称。

    单击链接可显示有关 TAA (IOA) 规则的信息。如果规则是由卡巴斯基专家提供的，则它包含有关触发的 MITRE 技术的信息以及对事件进行反应的建议。

    如果在创建事件时触发了 TAA (IOA) 规则，则会显示该字段。

  - **服务器 IP** — DNS 服务器的 IPv4 地址。

- **查询选项** – DNS 查询选项。
- **请求状态** – DNS 查询的状态。
- **域名** – 要解析 DNS 记录的域名。
- **记录类型 ID** – 资源记录的类型。
- **响应数据** – DNS 服务器对查询的响应内容。
- **事件时间** – 发送 DNS 查询的时间。

- **事件发起者**部分：
  - **文件** – 父进程文件的名称。
  - **MD5** – 父进程文件的 MD5 哈希。
  - **SHA256** – 父进程文件的 SHA256 哈希。
  - **进程 ID** – 父进程的标识符。

    如果事件由 Kaspersky Endpoint Agent for Linux 记录在事件数据库中，则“**事件发起者**”部分还包括以下字段：
  - **环境变量** – 进程的环境变量。
  - **真实用户名** – 在系统中注册时指定的用户名称。
  - **真实组名称** – 用户所属的组。
  - **有效用户名** – 用于登录系统的用户名。
  - **有效组名称**– 名称被用于登录系统的用户组。
- **系统信息**部分：
  - **主机名称** – 向 DNS 服务器发出查询的主机的名称。
  - **主机 IP** – 向 DNS 服务器发出查询的主机的 IP 地址。

    如果您使用动态 IP 地址，该字段将显示创建事件时分配给主机的 IP 地址。

    该应用程序不支持 IPv6。如果您使用 IPv6，则不会显示主机的 IP 地址。
  - **从远程主机登录** – 用于远程登录系统的主机名称。
  - **用户名称** – 向 DNS 服务器发出查询的用户的名称。
  - **操作系统版本** – 主机上正在使用的操作系统的版本。

点击带有服务器 IP 地址、记录类型 ID 和用户名的链接将打开一个列表，您可以在其中执行以下操作之一：

- **查找警报**。
- **复制值到剪贴板**。

单击具有域名的链接将打开一个列表，您可以在其中执行以下操作之一：

- **查找事件**。
- **查找警报**。
- **在 Kaspersky TIP 上查找**。
- **复制值到剪贴板**。

单击具有文件名称或文件路径的链接将打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - **杀死进程**。
  - **使用唯一的 PID 杀死进程**。
  - **删除文件**。
  - **获取文件**。
  - **进行取证**。
  - **隔离文件**。
- **复制值到剪贴板**。

单击 **MD5** 链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **在 Kaspersky TIP 上查找**。
- **在存储中查找**。
- **创建防止规则**。
- **复制值到剪贴板**。

单击 **SHA256** 链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **在 Kaspersky TIP 上查找**。
- **在 virustotal.com 上查找**。
- **在存储中查找**。
- **创建防止规则**。
- **复制值到剪贴板**。

单击具有主机名的链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - 获取数据→文件、取证、磁盘镜像、内存转储。
  - **杀死进程**。
  - **删除文件**。
  - **隔离文件**。
  - **运行应用程序**。
- **复制值到剪贴板**。

在事件数据库中记录的 Kaspersky Endpoint Security for Linux事件信息中，您可以单击主机名链接打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - **杀死进程**。
  - **删除文件**。
  - **获取文件**。

- **隔离文件**。
- **运行应用程序**。

- **复制值到剪贴板**。

单击包含主机 IP 地址的链接将打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **复制值到剪贴板**。

有关“LDAP”事件的信息

显示“**LDAP**”事件信息的窗口包含以下详情：

- 事件树。
- 处理事件时可以执行的操作。
- “**LDAP**”部分：
  - **IOA 标记** — 有关使用 Targeted Attack Analyzer 技术进行文件分析的结果的信息：用于创建警报的 TAA (IOA) 规则的名称。

    单击链接可显示有关 TAA (IOA) 规则的信息。如果规则是由卡巴斯基专家提供的，则它包含有关触发的 MITRE 技术的信息以及对事件进行反应的建议。

    如果在创建事件时触发了 TAA (IOA) 规则，则会显示该字段。
  - **搜索范围** — LDAP 搜索范围。可以具有以下值之一：ADS_SCOPE_BASE、ADS_SCOPE_ONELEVEL、ADS_SCOPE_SUBTREE。
  - **搜索过滤器** — LDAP 搜索过滤器。
  - **可分辨名称** — LDAP 目录条目的名称。
  - **搜索属性列表** — 搜索查询中指定为要返回的值的属性。
  - **启动参数** — 进程启动设置。
- **事件发起者**部分：
  - **文件** — 父进程文件的名称。
  - **MD5** — 父进程文件的 MD5 哈希。
  - **SHA256** — 父进程文件的 SHA256 哈希。

- **系统信息**部分：
  - **主机名称** — 在其上执行 LDAP 搜索的主机的名称。
  - **用户名称** — 其账户用于运行 LDAP 搜索的用户的名称。
  - **操作系统版本** — 主机上正在使用的操作系统的版本。

有关“命名管道”事件的信息

显示“**命名管道**”事件信息的窗口包含以下详情：

- 事件树。
- 处理事件时可以执行的操作。

  根据命名管道操作的类型，事件信息中会显示下列部分名称的其中一个：
  - **已创建管道**
  - **管道已连接**

  该部分显示以下信息：
  - **IOA 标记** — 有关使用 Targeted Attack Analyzer 技术进行文件分析的结果的信息：用于创建警报的 TAA (IOA) 规则的名称。

    单击链接可显示有关 TAA (IOA) 规则的信息。如果规则是由卡巴斯基专家提供的，则它包含有关触发的 MITRE 技术的信息以及对事件进行反应的建议。

    如果在创建事件时触发了 TAA (IOA) 规则，则会显示该字段。
  - **文件** — 创建或连接到命名管道的进程的文件名。
  - **事件时间** — 创建或连接命名管道的时间。
- **事件发起者**部分：
  - **文件** — 父进程文件的名称。
  - **MD5** — 父进程文件的 MD5 哈希。
  - **SHA256** — 父进程文件的 SHA256 哈希。
- **系统信息**部分：
  - **主机名称** — 创建或连接到命名管道的主机的名称。
  - **用户名称** — 创建或连接到命名管道的用户的名称。
  - **操作系统版本** — 主机上正在使用的操作系统的版本。

单击具有管道名称的链接将打开一个列表，您可以在其中执行以下操作之一：

- **查找警报**。
- **复制值到剪贴板**。

单击具有文件名称或文件路径的链接将打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - **杀死进程**。
  - **使用唯一的 PID 杀死进程**。
  - **删除文件**。
  - **获取文件**。
  - **进行取证**。
  - **隔离文件**。
- **复制值到剪贴板**。

单击 **MD5** 链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **在 Kaspersky TIP 上查找**。
- **在存储中查找**。
- **创建防止规则**。
- **复制值到剪贴板**。

单击 **SHA256** 链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **在 Kaspersky TIP 上查找**。
- **在 virustotal.com 上查找**。
- **在存储中查找**。
- **创建防止规则**。

- **复制值到剪贴板**。

单击具有主机名的链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - 获取数据→文件、取证、磁盘镜像、内存转储。
  - **杀死进程**。
  - **删除文件**。
  - **隔离文件**。
  - **运行应用程序**。
- **复制值到剪贴板**。

单击包含主机 IP 地址的链接将打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **复制值到剪贴板**。

单击具有用户名称的链接将打开一个列表，您可以在其中执行以下操作之一：

- **查找警报**。
- **复制值到剪贴板**。

有关“WMI”事件的信息

显示“**WMI**”事件信息的窗口包含以下详情：

- 事件树。
- 处理事件时可以执行的操作。
  根据操作的类型，事件信息中会显示下列部分名称的其中一个：
  - **WMI 活动**
  - **WMI 事件使用者名称**

"**WMI 活动**"部分显示以下信息：

- **IOA 标记** — 有关使用 Targeted Attack Analyzer 技术进行文件分析的结果的信息：用于创建警报的 TAA (IOA) 规则的名称。

  单击链接可显示有关 TAA (IOA) 规则的信息。如果规则是由卡巴斯基专家提供的，则它包含有关触发的 MITRE 技术的信息以及对事件进行反应的建议。

  如果在创建事件时触发了 TAA (IOA) 规则，则会显示该字段。

- **到远程主机的连接** — 远程启动 WMI 服务。如果服务是远程启动的，则字段显示"**是**"。
- **机器名称** — 启动了 WMI 服务的主机的名称。
- **用户名称** — 启动了 WMI 服务的用户的名称。
- **名字空间** — WMI 命名空间。
- **查询** — 用于启动 WMI 服务的命令。

"**WMI 活动**"部分显示以下信息：

- **到远程主机的连接** — 远程启动 WMI 服务。如果服务是远程启动的，则字段显示"**是**"。
- **名字空间** — 事件消费者的命名空间。
- **事件过滤器名称** — 事件消费者的过滤器的名称。此字段为**WMI 活动**事件类型显示。
- **事件用户名称** — 创建的事件消费者的名称。
- **事件用户描述** — 创建的事件消费者的描述。此字段为**WMI 事件使用者名称**事件类型显示。

- **事件发起者**部分：
  - **文件** — 父进程文件的名称。
  - **启动参数** — 父进程启动设置。
  - **MD5** — 父进程文件的 MD5 哈希。
  - **SHA256** — 父进程文件的 SHA256 哈希。
- **系统信息**部分：
  - **主机名称** — 启动 WMI 服务或创建事件消费者的主机的名称。
  - **主机 IP** — 启动 WMI 服务或创建事件消费者的主机的 IP 地址。
  - **用户名称** — 启动 WMI 服务或创建事件消费者的用户的名称。
  - **操作系统版本** — 主机上正在使用的操作系统的版本。

有关“警报”事件的信息

显示**检测**类型事件信息的窗口包含以下详细信息：

- 事件树。
- 处理事件时可以执行的操作。
- 在**详细信息**选项卡上，在**检测**部分：
  - **IOA 标记** — 有关使用 Targeted Attack Analyzer 技术进行文件分析的结果的信息：用于创建警报的 TAA (IOA) 规则的名称。

    单击链接可显示有关 TAA (IOA) 规则的信息。如果规则是由卡巴斯基专家提供的，则它包含有关触发的 MITRE 技术的信息以及对事件进行反应的建议。

    如果在创建事件时触发了 TAA (IOA) 规则，则会显示该字段。
  - **检测** — 检测到的对象的名称。

    单击对象链接将打开一个列表，您可以从其中选择以下操作之一：
    - **查找事件**。
    - **对卡巴斯基威胁的看法**。
    - **复制值到剪贴板**。
  - **最后一个操作** — 对检测到的对象采取的最后一个操作。
  - **对象名称** — 检测到对象的文件的全名。
  - **MD5** — 检测到对象的文件的 MD5 哈希。
  - **SHA256** — 检测到对象的文件的 SHA256 哈希。
  - **对象类型** — 对象类型（例如，文件）。
  - **检测模式** — 生成警报的扫描模式。
  - **事件时间** — 事件的日期和时间。
  - **记录 ID** — 数据库中检测记录的 ID。
  - **数据库版本** — 用于生成警报的数据库版本。
  - **内容**— 被发送进行扫描的脚本的内容。

    您可以通过单击**保存到文件**下载此数据。
- 在**详细信息**选项卡上，在**事件发起者**部分：
  - **文件** — 父进程文件的路径。

单击具有文件名称或文件路径的链接将打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **复制值到剪贴板**。

运行以下任务：

- **杀死进程**。
- **使用唯一的 PID 杀死进程**。
- **删除文件**。
- **获取文件**。
- **进行取证**。
- **隔离文件**。

- **进程 ID** – 父进程的标识符。
- **启动参数** – 父进程启动设置。
- **MD5** – 父进程文件的 MD5 哈希。
- **SHA256** – 父进程文件的 SHA256 哈希。

- 在**详细信息**选项卡上，在**系统信息**部分：
  - **主机名称** – 生成警报的主机名称。
    单击具有主机名的链接将打开一个列表，您可以从其中选择以下操作之一：
    - **查找事件**。
    - **查找警报**。
    - **复制值到剪贴板**。

    运行以下任务：
    - 获取数据→文件、取证、磁盘镜像、内存转储。
    - **杀死进程**。
    - **删除文件**。
    - **隔离文件**。
    - **运行应用程序**。

在事件数据库中记录的 Kaspersky Endpoint Security for Linux事件信息中，您可以单击主机名链接打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行任务：**获取文件**、**删除文件**、**隔离文件**、**运行应用程序**。
- **复制值到剪贴板**。

在事件数据库中记录的 Kaspersky Endpoint Security for Mac 事件信息中，您可以单击带有文件名或文件路径的链接来打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行**获取文件**任务。
- **复制值到剪贴板**。

- **主机 IP** — 在其上生成警报的主机的 IP 地址。

  如果您使用动态 IP 地址，该字段将显示创建事件时分配给主机的 IP 地址。

  该应用程序不支持 IPv6。如果您使用 IPv6，则不会显示主机的 IP 地址。

- **用户名称** — 用户账户，用于完成对检测到的对象执行的操作。
- **操作系统版本** — 主机上正在使用的操作系统的版本。

- 在**历史**选项卡上，在表中：
  - **类型** — 事件类型：**检测**或者**检测处理结果**。
  - **描述** — 事件描述。
  - **时间**— 检测和检测处理结果的日期和时间。

单击 **MD5** 链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **在 Kaspersky TIP 上查找**。
- **在存储中查找**。
- **创建防止规则**。
- **复制值到剪贴板**。

单击 **SHA256** 链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **在 Kaspersky TIP 上查找**。
- **在 virustotal.com 上查找**。
- **在存储中查找**。
- **创建防止规则**。
- **复制值到剪贴板**。

有关“检测处理结果”事件的信息

显示**检测处理结果**类型事件信息的窗口包含以下详细信息：

- 事件树。
- 处理事件时可以执行的操作。
- 在**详细信息**选项卡上，在**检测处理结果**下面：
  - **IOA 标记** — 有关使用 Targeted Attack Analyzer 技术进行文件分析的结果的信息：用于创建警报的 TAA (IOA) 规则的名称。

    单击链接可显示有关 TAA (IOA) 规则的信息。如果规则是由卡巴斯基专家提供的，则它包含有关触发的 MITRE 技术的信息以及对事件进行反应的建议。

    如果在创建事件时触发了 TAA (IOA) 规则，则会显示该字段。
  - **检测** — 检测到的对象的名称。

    单击对象链接将打开一个列表，您可以从其中选择以下操作之一：
    - **查找事件**。
    - **对卡巴斯基威胁的看法**。
    - **复制值到剪贴板**。
  - **最后一个操作** — 对检测到的对象采取的最后一个操作。
  - **MD5** — 检测到对象的文件的 MD5 哈希。
  - **SHA256** — 检测到对象的文件的 SHA256 哈希。
  - **对象类型** — 对象类型（例如，文件）。
  - **对象名称** — 检测到对象的文件的全名。
  - **检测模式** — 生成警报的扫描模式。

- **事件时间** – 事件的日期和时间。
- **记录 ID** – 数据库中检测记录的 ID。
- **数据库版本** – 用于生成警报的数据库版本。

- 在**详细信息**选项卡上，在**事件发起者**下面:
  - **文件** – 父进程文件的路径。
    单击具有文件名称或文件路径的链接将打开一个列表，您可以在其中选择以下操作之一:
    - **查找事件**。
    - **查找警报**。
    - **复制值到剪贴板**。

    运行以下任务:
    - **杀死进程**。
    - **使用唯一的 PID 杀死进程**。
    - **删除文件**。
    - **获取文件**。
    - **进行取证**。
    - **隔离文件**。
  - **进程 ID** – 父进程的标识符。
  - **启动参数** – 父进程启动设置。
  - **MD5** – 父进程文件的 MD5 哈希。
  - **SHA256** – 父进程文件的 SHA256 哈希。
- 在**详细信息**选项卡上，在**系统信息**下面:
  - **主机名称** – 生成警报的主机名称。
    单击具有主机名的链接将打开一个列表，您可以从其中选择以下操作之一:
    - **查找事件**。
    - **查找警报**。
    - **复制值到剪贴板**。

    运行以下任务:
    - 获取数据→文件、取证、磁盘镜像、内存转储。
    - **杀死进程**。

- **删除文件**。
- **隔离文件**。

运行应用程序。

- **主机 IP** – 在其上生成警报的主机的 IP 地址。

  如果您使用动态 IP 地址，该字段将显示创建事件时分配给主机的 IP 地址。

  该应用程序不支持 IPv6。如果您使用 IPv6，则不会显示主机的 IP 地址。

- **用户名称** – 用户账户，用于完成对检测到的对象执行的操作。
- **操作系统版本** – 主机上正在使用的操作系统的版本。

- 在**历史**选项卡上，在表中：
  - **类型**是**检测处理结果**事件的类型。
  - **描述** – 事件描述。
  - **时间**是警报处理结果的日期和时间。

单击 **MD5** 链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **在 Kaspersky TIP 上查找**。
- **在存储中查找**。
- **创建防止规则**。
- **复制值到剪贴板**。

单击 **SHA256** 链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **在 Kaspersky TIP 上查找**。
- **在 virustotal.com 上查找**。
- **在存储中查找**。
- **创建防止规则**。
- **复制值到剪贴板**。

有关“被解释文件运行”事件的信息

显示**进程: 解释文件运行**事件信息的窗口包含以下详情：

- 事件树。
- 处理事件时可以执行的操作。
- **进程: 解释文件运行**部分：
  - **IOA 标记** — 有关使用 Targeted Attack Analyzer 技术进行文件分析的结果的信息：用于创建警报的 TAA (IOA) 规则的名称。

    单击链接可显示有关 TAA (IOA) 规则的信息。如果规则是由卡巴斯基专家提供的，则它包含有关触发的 MITRE 技术的信息以及对事件进行反应的建议。

    如果在创建事件时触发了 TAA (IOA) 规则，则会显示该字段。
  - **文件** — 文件的名称。
  - **MD5** — 文件的 MD5 哈希。
  - **SHA256** — 文件的 SHA256 哈希。
  - **大小** — 文件的大小。
  - **创建时间** — 创建文件的时间。
  - **修改时间** — 文件的上次修改时间。
- **事件发起者**部分：
  - **文件** — 父进程文件的路径。
  - **MD5** — 父进程文件的 MD5 哈希。
  - **SHA256** — 父进程文件的 SHA256 哈希。
  - **进程 ID** — 父进程的标识符。
- **系统信息**部分：
  - **主机名称** — 运行文件的主机的名称。
  - **主机 IP** — 在其上运行文件的主机的 IP 地址。

    如果您使用动态 IP 地址，该字段将显示创建事件时分配给主机的 IP 地址。

    该应用程序不支持 IPv6。如果您使用 IPv6，则不会显示主机的 IP 地址。

- **用户名称** – 账户用于执行文件的用户的名称。
- **操作系统版本** – 主机上使用的操作系统版本。

单击**进程: 解释文件运行**部分中包含文件名或文件路径的链接将打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - **删除文件**。
  - **获取文件**。
  - **进行取证**。
  - **隔离文件**。
- **复制值到剪贴板**。

单击**事件发起者**部分中包含文件名或文件路径的链接将打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - **杀死进程**。
  - **使用唯一的 PID 杀死进程**。
  - **删除文件**。
  - **获取文件**。
  - **进行取证**。
  - **隔离文件**。
- **复制值到剪贴板**。

单击具有主机名的链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - 获取数据→文件、取证、磁盘镜像、内存转储。
  - **杀死进程**。

- **删除文件**。
- **隔离文件**。
- **运行应用程序**。

- **复制值到剪贴板**。

单击 **MD5** 链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **在 Kaspersky TIP 上查找**。
- **在存储中查找**。
- **创建防止规则**。
- **复制值到剪贴板**。

单击 **SHA256** 链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **在 Kaspersky TIP 上查找**。
- **在 virustotal.com 上查找**。
- **在存储中查找**。
- **创建防止规则**。
- **复制值到剪贴板**。

有关“AMSI 扫描”事件的信息

显示**AMSI 扫描**事件信息的窗口包含以下详细信息：

- 事件树。
- 处理事件时可以执行的操作。
- 在**AMSI 扫描**部分：
  - **IOA 标记** — 有关使用 Targeted Attack Analyzer 技术进行文件分析的结果的信息：用于创建警报的 TAA (IOA) 规则的名称。

    单击链接可显示有关 TAA (IOA) 规则的信息。如果规则是由卡巴斯基专家提供的，则它包含有关触发的 MITRE 技术的信息以及对事件进行反应的建议。

    如果在创建事件时触发了 TAA (IOA) 规则，则会显示该字段。

- **对象名称** – 扫描对象的名称。
- **MD5** – 扫描对象的 MD5 哈希。
- **SHA256** – 扫描对象的 SHA256 哈希。
- **事件时间** – 事件的日期和时间。
- **内容类型** – 脚本类型。
  应用程序提供两种类型的脚本：
  - 如果脚本以文本形式呈现，则**内容类型**字段显示*文本*脚本类型。
  - 如果脚本以其他格式呈现，则**内容类型**字段显示*二进制*脚本类型。
- **内容**– 被发送进行扫描的脚本的内容。
  如果数据以文本形式呈现，您可以单击**复制到剪贴板**复制此数据；如果数据有不同的格式，单击**保存到文件**下载包含数据的文件。

  > 如果应用程序注意到针对性攻击迹象，则**内容**字段会显示在事件信息中。

- 在**事件发起者**部分：
  - **文件** – 父进程文件的路径。
    单击具有文件名称或文件路径的链接将打开一个列表，您可以在其中选择以下操作之一：
    - **查找事件**。
    - **查找警报**。
    - **复制值到剪贴板**。

    运行以下任务：
    - **杀死进程**。
    - **使用唯一的 PID 杀死进程**。
    - **删除文件**。
    - **获取文件**。
    - **进行取证**。
    - **隔离文件**。
  - **MD5** – 父进程文件的 MD5 哈希。
    单击 **MD5** 链接将打开一个列表，您可以从其中选择以下操作之一：
    - **查找事件**。
    - **查找警报**。

- **在 Kaspersky TIP 上查找**。
- **在存储中查找**。
- **创建防止规则**。
- **复制值到剪贴板**。

- **SHA256** – 父进程文件的 SHA256 哈希。
  单击 **SHA256** 链接将打开一个列表，您可以从其中选择以下操作之一：
  - **查找事件**。
  - **查找警报**。
  - **在 Kaspersky TIP 上查找**。
  - **在存储中查找**。
  - **创建防止规则**。
  - **复制值到剪贴板**。

- 在**系统信息**部分：
  - **主机名称** – 生成检测的主机名称。
    单击具有主机名的链接将打开一个列表，您可以从其中选择以下操作之一：
    - **查找事件**。
    - **查找警报**。
    - **复制值到剪贴板**。

    运行以下任务：
    - 获取数据→文件、取证、磁盘镜像、内存转储。
    - **杀死进程**。
    - **删除文件**。
    - **隔离文件**。
    - **运行应用程序**。
  - **主机 IP** – 在其上创建警报的主机的 IP 地址。

    如果您使用动态 IP 地址，该字段将显示创建事件时分配给主机的 IP 地址。

    该应用程序不支持 IPv6。如果您使用 IPv6，则不会显示主机的 IP 地址。

- **用户名称**– 用于在注册表中做出更改的用户账户。
- **操作系统版本** – 主机上正在使用的操作系统的版本。

有关“在控制台进行交互式命令输入”事件的信息

显示**进程: 控制台交互式输入**事件信息的窗口包含以下详情：

- 事件树。
- 处理事件时可以执行的操作。
- **进程: 控制台交互式输入**部分：
  - **IOA 标记** – 有关使用 Targeted Attack Analyzer 技术进行文件分析的结果的信息：用于创建警报的 TAA (IOA) 规则的名称。

    单击链接可显示有关 TAA (IOA) 规则的信息。如果规则是由卡巴斯基专家提供的，则它包含有关触发的 MITRE 技术的信息以及对事件进行反应的建议。

    如果在创建事件时触发了 TAA (IOA) 规则，则会显示该字段。
  - **输入类型** – 被传递到控制台应用程序的命令输入类型。

    该应用程序提供两种输入命令的方式：
    - 如果用户在控制台应用程序中输入命令，**输入类型**字段将显示*控制台*命令输入类型。
    - 如果命令被通过管道从另一个应用程序传递到控制台应用程序，**输入类型**字段将显示*管道*命令输入类型。

    > 如果您使用 Kaspersky Endpoint Agent 应用程序作为 Endpoint Agent 组件，则仅当 Kaspersky Anti Targeted Attack Platform 与 Kaspersky Endpoint Agent 3.10 for Windows 集成时，Kaspersky Anti Targeted Attack Platform 才会收到填充**输入**字段所需的数据。当应用程序与旧版本的 Kaspersky Endpoint Agent for Windows 应用程序集成时，该字段不会显示在事件信息中。

    - **输入文本** – 使用 Kaspersky Endpoint Agent for Windows 应用程序在主机上的命令行（例如 CMD）中输入的文本。

    您可以通过单击位于**输入文本**字段中的**复制到剪贴板**按钮复制此文本。
  - **事件时间** – 检测到事件的时间。
- **事件发起者**部分：
  - **文件** – 父进程文件的路径。

    单击具有文件名称或文件路径的链接将打开一个列表，您可以在其中选择以下操作之一：
    - **查找事件**。
    - **查找警报**。
    - **复制值到剪贴板**。

运行以下任务：

- **杀死进程**。
- **使用唯一的 PID 杀死进程**。
- **删除文件**。
- **获取文件**。
- **进行取证**。
- **隔离文件**。

- **MD5** – 父进程文件的 MD5 哈希。
  单击 **MD5** 链接将打开一个列表，您可以从其中选择以下操作之一：
  - **查找事件**。
  - **查找警报**。
  - **在 Kaspersky TIP 上查找**。
  - **在存储中查找**。
  - **创建防止规则**。
  - **复制值到剪贴板**。
- **SHA256** – 父进程文件的 SHA256 哈希。
  单击 **SHA256** 链接将打开一个列表，您可以从其中选择以下操作之一：
  - **查找事件**。
  - **查找警报**。
  - **在 Kaspersky TIP 上查找**。
  - **在存储中查找**。
  - **创建防止规则**。
  - **复制值到剪贴板**。

- **系统信息**部分：
  - **主机名称** – 在其上输入命令的主机的名称。
    单击具有主机名的链接将打开一个列表，您可以从其中选择以下操作之一：
    - **查找事件**。
    - **查找警报**。
    - **复制值到剪贴板**。

运行以下任务：

- 获取数据→文件、取证、磁盘镜像、内存转储。
- **杀死进程**。
- **删除文件**。
- **隔离文件**。
- **运行应用程序**。

- **主机 IP** — 在其上输入命令的主机的 IP 地址。

  如果您使用动态 IP 地址，该字段将显示创建事件时分配给主机的 IP 地址。

  该应用程序不支持 IPv6。如果您使用 IPv6，则不会显示主机的 IP 地址。

- **用户名称** — 被用于输入命令的用户账户。
- **操作系统版本** — 主机上正在使用的操作系统的版本。

有关“代码注入”事件的信息

显示“**代码注入**”事件信息的窗口包含以下详情：

- 事件树。
- 处理事件时可以执行的操作。
- “**代码注入**”部分：
  - **IOA 标记** — 有关使用 Targeted Attack Analyzer 技术进行文件分析的结果的信息：用于创建警报的 TAA (IOA) 规则的名称。

    单击链接可显示有关 TAA (IOA) 规则的信息。如果规则是由卡巴斯基专家提供的，则它包含有关触发的 MITRE 技术的信息以及对事件进行反应的建议。

    如果在创建事件时触发了 TAA (IOA) 规则，则会显示该字段。
  - **文件** — 目标进程文件的路径。
  - **进程 ID** — 目标进程的标识符。
  - **启动参数** — 目标进程的命令行选项。
  - **修改的启动选项** — 修改的目标进程的命令行选项。

    如果使用 ARG_SPOOFING 方法注入代码，则会显示此字段。
  - **MD5** — 目标进程文件的 MD5 哈希。

- **SHA256** – 目标进程文件的 SHA256 哈希。
- **访问方法** – 访问目标进程的方法。

  该字段可以具有以下值：WRITE_EXECUTABLE_MEMORY、SET_WINDOWS_HOOK、QUEUE_APC_THREAD、SET_THREAD_CONTEXT – .MAP_VIEW_OF_SECTION、CREATE_REMOTE_THREAD、ARG_SPOOFING。
- **地址空间** – 目标进程地址空间中放置远程执行代码的地址。

  如果使用 SET_WINDOWS_HOOK 或 ARG_SPOOFING 方法注入代码，则不会填充此字段。
- **系统调用参数** – 启动目标进程的命令行。
- **DLL 名称** – 包含钩子过程的 DLL 的名称以及注入后传递控制权的函数的名称。

  如果使用 SET_WINDOWS_HOOK 方法注入代码，则填充此字段。
- **DLL 完整路径** – 包含钩子过程的 DLL 的路径。

  如果使用 SET_WINDOWS_HOOK 方法注入代码，则填充此字段。
- **事件时间** – 代码注入的时间。
- **调用跟踪** – 拦截代码注入相关函数时的 API 调用堆栈。

- **事件发起者**部分：
  - **文件** – 父进程文件的名称。
  - **MD5** – 父进程文件的 MD5 哈希。
  - **SHA256** – 父进程文件的 SHA256 哈希。
- **系统信息**部分：
  - **主机名称** – 发生代码注入的主机的名称。
  - **用户名称** – 用于代码注入的用户账户的名称。
  - **操作系统版本** – 主机上正在使用的操作系统的版本。

有关“进程访问”事件的信息

显示**文件已更改**事件信息的窗口包含以下详情：

- 事件树。
- 处理事件时可以执行的操作。
- 根据对进程文件执行的操作类型，事件信息中会显示以下部分名称之一：
  - **进程访问已打开**
  - **复制句柄**

"**进程访问已打开**"显示以下信息：

- **IOA 标记** — 有关使用 Targeted Attack Analyzer 技术进行文件分析的结果的信息：用于创建警报的 TAA (IOA) 规则的名称。

  单击链接可显示有关 TAA (IOA) 规则的信息。如果规则是由卡巴斯基专家提供的，则它包含有关触发的 MITRE 技术的信息以及对事件进行反应的建议。

  如果在创建事件时触发了 TAA (IOA) 规则，则会显示该字段。

- **文件** — 接收者进程的名称。
- **进程 ID** — 接收者进程的进程 ID。
- **启动参数** — 接收者进程的命令行选项。
- **MD5** — 接收者进程文件的 MD5 哈希。
- **SHA256** — 接收者进程文件的 SHA256 哈希。
- **访问权限** — 请求的进程访问权限。
- **大小** — 接收者进程文件的大小。
- **事件时间** — 检测到事件的时间。
- 创建时间 — 接收者进程文件的创建时间。
- **修改时间** — 接收者进程文件的上次修改时间。
- **属性修改时间** — 接收者进程文件属性发生改变的时间。
- **调用跟踪** — 调用堆栈。

"**复制句柄** "部分显示以下信息：

- **文件** — 复制过程的文件名。
- **MD5** — 复制进程文件的 MD5 哈希。
- **SHA256** — 复制进程文件的 SHA256 哈希。
- **创建时间** — 复制进程文件的创建时间。
- **修改时间** — 复制进程文件的上次修改时间。
- **属性修改时间** — 复制进程文件属性发生改变的时间。
- **大小** — 复制进程文件的大小。
- **进程 ID** — 重复进程的 ID。
- **启动参数** — 复制进程的命令行选项。

对于此类型的事件，事件信息还包括“**有关向其复制句柄的进程的信息**”和“**有关从其复制句柄的进程的信息**”部分。这些部分包含以下信息：

- **文件** – 进程文件名。
- **MD5** – 进程文件的 MD5 哈希。
- **SHA256** – 进程文件的 MD5 哈希。
- **进程 ID** – 进程标识符。
- **启动参数** – 进程启动设置。
- **大小** – 进程文件的大小。
- **创建时间** – 进程文件的创建时间。
- **修改时间** – 文件的上次修改时间。
- **属性修改时间** – 进程文件属性发生改变的时间。

- **事件发起者**部分：
  - **文件** – 父进程文件的路径。
  - **MD5** – 父进程文件的 MD5 哈希。
  - **SHA256** – 父进程文件的 SHA256 哈希。
  - **启动参数** – 父进程启动设置。
- **系统信息**部分：
  - **主机名称** – 创建文件的主机的名称。
  - **用户名称** – 创建了文件的用户的名称。
  - **操作系统版本**– 主机上正在使用的操作系统的版本。

在包含执行操作的文件信息的部分中单击包含文件名或文件路径的链接将打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
  - **删除文件**。
  - **获取文件**。

    - **进行取证**。
    - **隔离文件**。
- **复制值到剪贴板**。

单击**事件发起者**部分中包含文件名或文件路径的链接将打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- 运行以下任务：
    - **杀死进程**。
    - **使用唯一的 PID 杀死进程**。
    - **删除文件**。
    - **获取文件**。
    - **进行取证**。
    - **隔离文件**。
- **复制值到剪贴板**。

单击 **MD5** 链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **在 Kaspersky TIP 上查找**。
- **在存储中查找**。
- **创建防止规则**。
- **复制值到剪贴板**。

单击 **SHA256** 链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **在 Kaspersky TIP 上查找**。
- **在 virustotal.com 上查找**。
- **在存储中查找**。
- **创建防止规则**。

- **复制值到剪贴板**。

根据 Kaspersky TAA (IOA) 规则进行事件链扫描

有些网络攻击只有通过查看特定的事件序列才能检测到。如果启用了事件链扫描功能，Kaspersky Anti Targeted Attack Platform 会根据 Kaspersky TAA (IOA) 规则标记到达 Central Node 服务器的事件，当检测到可疑事件序列时，会在警报表中记录警报。

您可以通过以下方式之一查看由 Kaspersky TAA (IOA) 规则标记的事件：

- 通过使用以下条件对事件数据库创建搜索查询：IOATag、IOAImportance、IOAConfidence。
- 查看事件和警报时。

Kaspersky TAA (IOA) 规则无法编辑。如果您不希望应用程序为作为对您组织来说正常的主机活动的一部分生成的事件创建警报，您可以将 TAA (IOA) 规则添加到排除项。每个 Kaspersky TAA (IOA) 规则只能创建一个排除项。

在分布式解决方案和多租户模式下，您必须在要使用它的每个 Central Node 服务器上启用事件链扫描功能。如果 Central Node 组件被部署为集群，您可以在集群中的任何服务器上启用该功能。

使用扫描事件链的 TAA（IOA）规则会导致更高的系统资源使用率。如果您在使用该应用程序时遇到性能问题，我们建议禁用此功能。

在小部件中显示事件链信息的特殊注意事项

前 10 个小部件仅显示有关触发 TAA（IOA）规则的事件的信息。小部件不会考虑之前发生并参与事件链但未触发规则的事件。因此，小部件报告的事件数可能与您单击带有主机名和 TAA (IOA) 规则名称的链接时显示的事件数不匹配。

启用或禁用根据 Kaspersky TAA (IOA) 规则进行事件链扫描

要启用或禁用根据 Kaspersky TAA (IOA) 规则进行事件链扫描

1. 在应用程序 Web 界面的窗口中，选择**设置**部分的**Endpoint Agent**子部分。
2. 在“**对事件链使用 TAA (IOA) 规则**”下，执行以下操作之一：
   - 如果要启用该功能，请将“**对事件链使用规则**”切换开关设置为“**已启用**”。
   - 如果要禁用该功能，请将“**对事件链使用规则**”切换开关设置为“**已禁用**”。

   默认情况下禁用此功能。

已启用或禁用根据 Kaspersky TAA (IOA) 规则进行事件链扫描。

查看由 Kaspersky TAA (IOA) 规则标记的事件

*要查看由所选 Kaspersky TAA (IOA) 规则标记的所有事件，在"**警报**"部分：*

1. 在应用程序 Web 界面窗口中选择**警报**部分。
   这将打开警报表。
2. 单击**技术**列中的链接打开筛选器配置窗口。
3. 在左侧的下拉列表中，选择**包含**。
4. 在右侧的下拉列表中，选择**（TAA）针对性攻击分析器**技术。
5. 单击**应用**。
   该表显示 TAA 技术根据 TAA (IOA) 规则生成的警报。
6. 选择一个警报，**检测到**列为其显示相关规则的名称。
   这将打开一个窗口，其中包含有关警报的信息。
7. 在**扫描结果**下面，单击带有规则名称的链接以打开规则信息窗口。
8. 这将打开一个窗口；在该窗口中，单击"**事件**"。

将显示与所选 TAA (IOA) 规则匹配的事件表。

*要查看由所选 Kaspersky TAA (IOA) 规则标记的所有事件，在"**威胁搜索**"部分：*

1. 选择程序 Web 界面窗口中的**威胁搜索**部分。
   这将打开事件搜索表单。
2. 定义搜索条件并单击**搜索**按钮。例如，您可以在构建器模式下在**TAA 属性**组中选择事件搜索条件。
   满足搜索条件的事件表将显示。
3. 选择一个事件。
4. 在**IOA 标记**设置右侧，单击规则名称。
   这将打开一个窗口，其中包含有关规则的信息。
5. 这将打开一个窗口；在该窗口中，单击"**事件**"。

将显示与所选 TAA (IOA) 规则匹配的事件表。

管理资产

*资产*是组织本地和内部网络中存在的所有设备。要管理资产，您可以在 Kaspersky Anti Targeted Attack Platform Web 界面的"**资产**"区域查看设备表。您还可以在管理网络交互图和拓扑图时查看有关设备交互的信息，并对设备执行各种操作。

查看设备表

为了管理设备，应用程序会生成一个设备表。应用程序将表中的所有设备视为已知设备。

要查看设备表：

1. 在应用程序 Web 界面窗口中选择“**资产**”部分。
2. 转到“**设备**”选项卡。
   设备表将显示。

该表显示以下信息：

- **名称**是代表应用程序中设备的名称。
- **设备 ID** 是 Kaspersky Anti Targeted Attack Platform 中分配的设备 ID。
- **状态**是设备状态，决定设备是否允许在公司 LAN 上活动。设备可以具有以下状态之一：
  - **已授权**。此状态分配给允许在网络上活动的设备。
  - **未授权**。此状态分配给不允许在网络上活动的设备。
  - **已存档**。如果设备不再使用或不得在网络上使用，或者设备长时间（30 天或更长时间）未处于活动状态并且有关该设备的信息尚未更新，则会为设备分配此状态。
- **地址信息**列出了设备的 MAC 和/或 IP 地址。如果设备有多个网络接口，则每个网络接口可以有不同的 MAC 和/或 IP 地址。
- **类别**是表征设备功能用途的类别名称。Kaspersky Anti Targeted Attack Platform 识别以下设备类别：
  - **服务器**指部署了服务器软件的计算机。
  - **网络设备**指网络设备（例如路由器、交换机）。
  - **工作站**为固定式个人计算机或操作员工作站。
  - **移动设备**为具有计算功能的便携式电子设备。
  - **笔记本电脑**指便携式个人电脑。
  - **打印机**为打印设备。
  - **UPS** 为连接计算机网络的不间断电源。
  - **网络摄像头**为进行视频监控并传输数字图像数据的设备。
  - **网关**是一种通过转换具有异构数据传输介质和不同协议的网络中的各种接口（例如串行以太网）来连接网络的设备。
  - **存储系统**指在记忆系统内存储信息的设备。

    - **防火墙**是指充当防火墙的设备，用于扫描和阻止不需要的流量。
    - **交换机**是物理连接本地网络主机的设备。
    - **虚拟交换机**是指将物理交换机或软件交换机在逻辑上组合起来用于虚拟化系统的设备。
    - **路由器**是一种在计算机网络各段之间转发网络数据包的设备。
    - **虚拟路由器**是指逻辑上组合物理路由器或使用多个独立路由和转发表的路由器的设备。
    - Wi-Fi 是一种接入点，可通过 Wi-Fi 网络为设备提供无线连接。
    - **历史服务器**指具有存档数据的服务器。
    - **其他**指不属于上述任何类别的设备。
- **组**是设备在设备组树中所属组的名称（包含组本身的名称及其所有父组的名称）。
- **安全状态**是设备的安全状态，由设备相关的事件的存在决定。设备可具有以下安全状态之一：
    - **严重**。该设备具有严重程度评分为 8.0 至 10.0 的相关事件。
    - **警告**。该设备具有严重程度评分为 4.0 至 7.9 的相关事件。
    - **正常**。该设备具有严重程度评分为 0.0 至 3.9 的相关事件，或者设备没有关联事件。
- **重要性**是设备的重要性。根据设备的类别为其分配重要性。设备可以具有以下重要性级别之一：
    - **高**。分配给**服务器**类别的设备。
    - **中**。分配给以下类别的设备：**网络设备**、**工作站**、**网关**、**存储系统**、**防火墙**、**交换机**、**虚拟交换机**、**路由器**、**虚拟路由器**、 Wi-Fi、**历史服务器**。
    - **低**。分配给以下类别的设备：**移动设备**、**笔记本电脑**、**打印机**、 UPS、**网络摄像头**或**其他**。
- **上次看到**是设备上次记录为活动的日期和时间。
- **风险**列出了针对设备检测到的风险类别。默认情况下，设备表仅显示当前风险的信息。要显示所有风险的信息，您可以在配置设备表时选中“**显示已修复和已接受的风险**”复选框。
- **上次修改**是上次修改设备信息的日期和时间。
- **已创建**是将设备添加到设备表的日期和时间。
- OS 是设备上安装的操作系统的名称。
- **硬件供应商**是设备硬件供应商的名称。在详细信息区域中，此参数称为**“供应商”**，并显示在**“硬件”**下的**“常规”**选项卡上。
- **硬件型号**是设备型号的名称。在详细信息区域中，此参数称为**“型号”**，显示在**“硬件”**下的**“常规”**选项卡上。
- **硬件版本**是设备硬件的版本号。在详细信息区域中，此参数称为**“版本”**，显示在**“硬件”**下的**“常规”**选项卡上。
- **软件供应商**是设备软件的供应商名称。在详细信息区域中，此参数称为**“供应商”**，并显示在**“软件”**下的**“常规”**选项卡上。

- **软件名称**是设备软件的名称。在详细信息区域中，此参数称为**"名称"**，显示在**"软件"**下的**"常规"**选项卡上。
- **软件版本**是设备软件的版本号。在详细信息区域中，此参数称为**"版本"**，显示在**"软件"**下的**"常规"**选项卡上。
- **网络名称**是代表网络上的设备的名称。
- **标签**列出了分配给设备的标签。
- **EPP 应用程序**是设备上安装的 EPP 应用程序的简称（如果此应用程序已与 Kaspersky Anti Targeted Attack Platform 通信）。
- **EPP 连接**是设备上安装的 Endpoint Agent 组件与集成服务器的连接状态。可以有以下状态：
  - **活动**。自应用程序上次连接到集成服务器以来，已过去不到 24 小时。
  - **不活动**。自应用程序上次连接到集成服务器以来，已过去超过 24 小时。
  - **N/A**。连接状态未知。
- **上次连接到 EPP** 是 Endpoint Agent 组件上次连接到集成服务器的日期。

查看设备信息

要查看设备信息：

1. 在应用程序 Web 界面窗口中选择"**资产**"部分。
2. 转到"**设备**"选项卡。
3. 选择您想查看信息的设备。

   这将打开一个窗口，其中包含有关设备的信息。

该窗口可以包含以下信息：

- 设备信息：
  - **安全状态**是设备的安全状态，由设备相关的事件的存在决定。设备可具有以下安全状态之一：
    - **严重**。该设备具有严重程度评分为 8.0 至 10.0 的相关事件。
    - **警告**。该设备具有严重程度评分为 4.0 至 7.9 的相关事件。
    - **正常**。该设备具有严重程度评分为 0.0 至 3.9 的相关事件，或者设备没有关联事件。
  - **重要性**是该设备对组织的重要性。根据设备的类别为其分配重要性。设备可以具有以下重要性级别之一：
    - **高**。分配给**服务器**类别的设备。
    - **中**。分配给以下类别的设备：**网络设备**、**工作站**、**网关**、**存储系统**、**防火墙**、**交换机**、**虚拟交换机**、**路由器**、**虚拟路由器**、 Wi-Fi、**历史服务器**。
    - **低**。分配给以下类别的设备：**移动设备**、**笔记本电脑**、**打印机**、 UPS、**网络摄像头**或**其他**。

- **状态**是设备状态，决定设备是否允许在公司 LAN 上活动。设备可以具有以下状态之一：
  - **已授权**。此状态分配给允许在网络上活动的设备。
  - **未授权**。此状态分配给不允许在网络上活动的设备。
  - **已存档**。如果设备不再使用或不得在网络上使用，或者设备长时间（30 天或更长时间）未处于活动状态并且有关该设备的信息尚未更新，则会为设备分配此状态。
- **类别**是表征设备功能用途的类别名称。
- **网络名称**是代表网络上的设备的名称。
- **组**是设备在设备组树中所属组的名称（包含组本身的名称及其所有父组的名称）。

- “**主要**”选项卡：
  - **已创建**是将设备添加到设备表的日期和时间。
  - **上次修改**是上次修改设备信息的日期和时间。
  - **上次看到**是设备上次记录为活动的日期和时间。
  - **地址信息**列出了设备的 MAC 和/或 IP 地址。如果设备有多个网络接口，则每个网络接口可以有不同的 MAC 和/或 IP 地址。
  - **硬件**包含有关设备硬件特性的信息。
  - **软件**包含有关设备软件的信息。
  - **Endpoint Agent** 包含有关 Endpoint Agent 组件的信息。如果设备上安装了 Endpoint Agent 组件，则会显示此部分。
  - **EPP 应用程序**包含有关在 Endpoint Agent 组件角色中使用的应用程序的信息。
  - **路由器**是标记设备为路由设备的属性。

    如果应用程序无法自动确定路由设备属性，则必须手动设置该属性。该属性允许应用程序使用附加算法来检测通过路由器相互交互的设备。
  - **公钥**是用于在建立 SSH 连接之前对设备进行身份验证以及作为安全审计任务的一部分对设备进行扫描的公钥。
  - **附加信息**包含应用程序用户指定的有关设备的附加信息（例如，设备物理位置的描述）。
  - **自定义字段**是一组有关设备的非标准信息，由应用程序的用户指定（例如，设备的类别和保护等级）。一台设备最多可以指定 16 个自定义字段。
  - **动态字段**是使用设备信息检测方法在流量中检测到的一组扩展设备信息。如果应用程序检测到扩展信息，则会显示一个字段。

- **地址**选项卡：
  - **DHCP 服务器**是 DHCP 服务器属性。

    如果设备具有 DHCP 服务器属性，则此字段显示**“是”**。

- **DHCP 中继**是 DHCP 中继属性。

  如果设备具有 DHCP 中继属性，则此字段显示**"是"**。

- **网络接口<号码>**包含有关设备网络接口的信息。

- "**拓扑设置**"选项卡包含有关设备最后一次活动轮询的信息，以及有关设备与其他节点的链接的信息。
- "**设备**"选项卡包含有关设备的 BIOS 程序和 CPU、可用 RAM 和可用本地磁盘空间的数量以及正在使用的 USB 设备和光驱的信息。如果使用硬件监控功能获取信息，则会显示信息。
- "**配置**"选项卡包含有关获取的设备配置的信息。如果信息是由配置监控任务获取的，则会显示该信息。

自动添加和更新设备

应用程序可以自动将设备添加到表中并更新设备信息。要在 Kaspersky Anti Targeted Attack Platform 中启用设备自动添加和更新，您必须启用和配置设备活动检测 (AM) 技术。如果启用该技术，应用程序将使用从网络流量获得的数据以及与 Endpoint Agent 组件的集成来添加和更新设备信息。

添加设备时，应用程序使用以下模板设置默认设备名称：**设备<内部设备计数器值>**。设备名称中的这个内部计数器值可能与"**设备 ID**"列中显示的设备 ID 不匹配。

该应用程序可以根据设备的 MAC 地址自动更新网络设备的供应商信息。为了通过 MAC 地址识别供应商，应用程序会在电气电子工程师协会 (IEEE) 的开放数据库中注册的地址范围内查找设备的 MAC 地址。如果通过 MAC 地址识别网络设备的供应商，则应用程序会保留 IEEE 数据库中的名称。

安装应用程序后，将使用 IEEE 数据库的副本，其中包含有关应用程序当前版本发布时的 MAC 地址和供应商的信息。您可以通过安装更新来使 IEEE 数据库的本地副本保持最新。

手动添加设备

本节提供有关如何手动添加设备的说明。您可以手动将新设备添加到设备表中。您必须指定要添加的设备的 MAC 和/或 IP 地址。

添加的设备的 MAC 地址和 IP 地址在这些地址所属的地址空间内必须是唯一的。如果应用程序中添加了额外的地址空间，则可以将具有相同地址的设备添加到不同的地址空间。

只有具有"**高级安全官**"角色的用户才能手动添加设备。

添加设备后，您可以添加该设备的进程监控设置。

在管理设备表时添加设备

要在管理设备表时添加设备：

1. 在应用程序 Web 界面窗口中选择“**资产**”部分。
2. 在设备表中的“**设备**”选项卡上，选择要查看信息的设备。
   这将打开一个窗口，其中包含有关设备的信息。
3. 单击“**添加设备**”。
4. 在**“设置”**选项卡的详细信息区域中，在设备信息字段中指定值。
5. 在“**地址信息**”选项卡的详细信息区域中：
   a. 在“**DHCP 服务器**”下拉列表中，如果设备是 DHCP 服务器，请选择**“是”**。
   b. 在“**DHCP 中继**”下拉列表中，如果设备是 DHCP 中继，请选择**“是”**。
   在学习模式下，对于作为 DHCP 服务器和 DHCP 中继的设备，这些属性是自动分配的。您可以禁用属性的自动更新（请参阅这些说明的第 6 步）。
   在监控模式下，只有具有“**高级安全官**”角色的用户可以编辑属性。
   c. 在“**地址空间**”下拉列表中，选择您希望设备所属的地址空间。
   d. 在“**MAC 地址**”字段中，输入设备的 MAC 地址。
   e. 在“**IP 地址**”下拉列表中选择 IP 地址分配类型（静态或动态），并输入设备的 IP 地址。
   您可以为设备的同一个网络接口指定多个 IP 地址。要创建 IP 地址列表，请执行以下操作之一：
   - 如果要添加 IP 地址，请单击“**添加 IP 地址**”。
   - 如果要删除 IP 地址，请点击 IP 地址字段右侧的 图标。

   如果设备有多个网络接口，请创建网络接口列表：
   - 如果要添加网络接口，请点击最后一个网络接口设置下方的“**添加接口**”。
   - 如果要删除网络接口，请点击网络接口名称右侧的 × 图标（如果设备有两个或更多网络接口）。
   - 如果要为网络接口输入不同的名称，请点击当前名称右侧的 图标，然后在显示的字段中输入新名称。
6. 在**“设置”**和**“地址信息”**选项卡的详细信息区域中，启用或禁用对设备信息某些元素的自动修改。为此，请点击 或者 图标。

   如果禁用设备 IP 地址的自动更新，则 IP 地址类型（静态或动态）和地址空间信息的自动更新也会被禁用。

7. 在“**自定义字段**”选项卡的详细信息区域中，创建自定义字段列表。

8. 单击“**保存**”。

   如果设备设置不包含所有必需的信息或某些指定的设置无效，则此按钮不可用。需要正确值的设置的选项卡标有 . 图标。

设备表中将出现一个“*已授权*”状态的新设备。

在管理拓扑图时添加设备

您可以在管理拓扑图的同时将新设备添加到设备表中。

要在管理拓扑图的同时将新设备添加到设备表：

1. 在应用程序 Web 界面窗口中选择“**网络地图**”部分。
2. 转到“**拓扑图**”选项卡。
3. 单击“**添加设备**”。
4. 在**“设置”**选项卡的详细信息区域中，在设备信息字段中指定值。
5. 在“**地址信息**”选项卡的详细信息区域中：

   a. 在“**DHCP 服务器**”下拉列表中，如果设备是 DHCP 服务器，请选择**“是”**。

   b. 在“**DHCP 中继**”下拉列表中，如果设备是 DHCP 中继，请选择**“是”**。

   在学习模式下，对于作为 DHCP 服务器和 DHCP 中继的设备，这些属性是自动分配的。您可以禁用属性的自动更新（请参阅这些说明的第 6 步）。

   在监控模式下，只有具有“**高级安全官**”角色的用户可以编辑属性。

   c. 在“**地址空间**”下拉列表中，选择您希望设备所属的地址空间。

   d. 在“**MAC 地址**”字段中，输入设备的 MAC 地址。

   e. 在“**IP 地址**”下拉列表中选择 IP 地址分配类型（静态或动态），并输入设备的 IP 地址。

   您可以为设备的同一个网络接口指定多个 IP 地址。要创建 IP 地址列表，请执行以下操作之一：

   - 如果要添加 IP 地址，请单击“**添加 IP 地址**”。
   - 如果要删除 IP 地址，请点击 IP 地址字段右侧的 图标。

   如果设备有多个网络接口，请创建网络接口列表：

   - 如果要添加网络接口，请点击最后一个网络接口设置下方的“**添加接口**”。
   - 如果要删除网络接口，请点击网络接口名称右侧的 × 图标（如果设备有两个或更多网络接口）。
   - 如果要为网络接口输入不同的名称，请点击当前名称右侧的 图标，然后在显示的字段中输入新名称。

6. 在**"设置"**和**"地址信息"**选项卡的详细信息区域中，启用或禁用对设备信息某些元素的自动修改。为此，请点击 或者 图标。

   如果禁用设备 IP 地址的自动更新，则 IP 地址类型（静态或动态）和地址空间信息的自动更新也会被禁用。

7. 在"**自定义字段**"选项卡的详细信息区域中，创建自定义字段列表。

8. 单击"**保存**"。

   如果设备设置不包含所有必需的信息或某些指定的设置无效，则此按钮不可用。需要正确值的设置的选项卡标有 . 图标。

设备表中将出现一个"*已授权*"状态的新设备。

根据网络交互图上的未知设备节点添加设备

在管理网络交互图时，您可以根据代表应用程序无法识别的设备的节点将新设备添加到设备表中。

要将无法识别的设备节点添加到设备表中：

1. 在应用程序 Web 界面窗口中选择"**网络地图**"部分。

2. 在"**网络交互图**"选项卡上，选择代表应用程序无法识别的设备的节点。

   详细信息区域显示在 Web 界面窗口的右侧。

3. 点击"**添加到设备表**"。

4. 在**"设置"**选项卡的详细信息区域中，在设备信息字段中指定值。

5. 在"**地址信息**"选项卡的详细信息区域中：

   a. 在"**DHCP 服务器**"下拉列表中，如果设备是 DHCP 服务器，请选择**"是"**。

   b. 在"**DHCP 中继**"下拉列表中，如果设备是 DHCP 中继，请选择**"是"**。

   在学习模式下，对于作为 DHCP 服务器和 DHCP 中继的设备，这些属性是自动分配的。您可以禁用属性的自动更新（请参阅这些说明的第 6 步）。

   在监控模式下，只有具有"**高级安全官**"角色的用户可以编辑属性。

   c. 在"**地址空间**"下拉列表中，选择您希望设备所属的地址空间。

   d. "**IP 地址**"和"**MAC 地址**"字段会自动填写；我们不建议更改这些设置。

   您可以为设备的同一个网络接口指定多个 IP 地址。要创建 IP 地址列表，请执行以下操作之一：

   - 如果要添加 IP 地址，请单击"**添加 IP 地址**"。
   - 如果要删除 IP 地址，请点击 IP 地址字段右侧的 图标。

如果设备有多个网络接口，请创建网络接口列表：

- 如果要添加网络接口，请点击最后一个网络接口设置下方的“**添加接口**”。
- 如果要删除网络接口，请点击网络接口名称右侧的 × 图标（如果设备有两个或更多网络接口）。
- 如果要为网络接口输入不同的名称，请点击当前名称右侧的 图标，然后在显示的字段中输入新名称。

6. 在**“设置”**和**“地址信息”**选项卡的详细信息区域中，启用或禁用对设备信息某些元素的自动修改。为此，请点击 或者 图标。

   如果禁用设备 IP 地址的自动更新，则 IP 地址类型（静态或动态）和地址空间信息的自动更新也会被禁用。

7. 在“**自定义字段**”选项卡的详细信息区域中，创建自定义字段列表。

8. 单击“**保存**”。

   如果设备设置不包含所有必需的信息或某些指定的设置无效，则此按钮不可用。需要正确值的设置的选项卡标有 . 图标。

设备表中将出现一个“*已授权*”状态的新设备。网络交互图上以前代表应用程序无法识别的设备的节点，现在代表应用程序已知的设备。

根据拓扑图上非管理交换机添加设备

在管理拓扑图时，您可以根据代表非管理型交换机的节点将新设备添加到设备表中。

要将非管理型交换机节点添加到设备表：

1. 在应用程序 Web 界面窗口中选择“**网络地图**”部分。
2. 在“**网络交互图**”选项卡上，选择代表不受管理的交换机的节点。

   详细信息区域显示在 Web 界面窗口的右侧。

3. 点击“**添加到设备表**”。
4. 在**“设置”**选项卡的详细信息区域中，在设备信息字段中指定值。
5. 在“**地址信息**”选项卡的详细信息区域中：

   a. 在“**DHCP 服务器**”下拉列表中，如果设备是 DHCP 服务器，请选择**“是”**。

   b. 在“**DHCP 中继**”下拉列表中，如果设备是 DHCP 中继，请选择**“是”**。

   在学习模式下，对于作为 DHCP 服务器和 DHCP 中继的设备，这些属性是自动分配的。您可以禁用属性的自动更新（请参阅这些说明的第 6 步）。

   在监控模式下，只有具有“**高级安全官**”角色的用户可以编辑属性。

   c. 在“**地址空间**”下拉列表中，选择您希望设备所属的地址空间。

   d. 在“**MAC 地址**”字段中，输入设备的 MAC 地址。

e. 在“**IP 地址**”下拉列表中选择 IP 地址分配类型（静态或动态），并输入设备的 IP 地址。

您可以为设备的同一个网络接口指定多个 IP 地址。要创建 IP 地址列表，请执行以下操作之一：

- 如果要添加 IP 地址，请单击“**添加 IP 地址**”。
- 如果要删除 IP 地址，请点击 IP 地址字段右侧的 图标。

如果设备有多个网络接口，请创建网络接口列表：

- 如果要添加网络接口，请点击最后一个网络接口设置下方的“**添加接口**”。
- 如果要删除网络接口，请点击网络接口名称右侧的 图标（如果设备有两个或更多网络接口）。
- 如果要为网络接口输入不同的名称，请点击当前名称右侧的 图标，然后在显示的字段中输入新名称。

6. 在**“设置”**和**“地址信息”**选项卡的详细信息区域中，启用或禁用对设备信息某些元素的自动修改。为此，请点击 或者 图标。

> 如果禁用设备 IP 地址的自动更新，则 IP 地址类型（静态或动态）和地址空间信息的自动更新也会被禁用。

7. 在“**自定义字段**”选项卡的详细信息区域中，创建自定义字段列表。

8. 单击“**保存**”。

如果设备设置不包含所有必需的信息或某些指定的设置无效，则此按钮不可用。需要正确值的设置的选项卡标有 图标。

设备表中将出现一个新设备，带有“*已授权*”**状态。**拓扑图上先前代表非管理型交换机的节点现在代表应用程序已知的设备。

自动分配设备状态

在监控设备活动时，应用程序可以根据获取的设备的 MAC 和/或 IP 地址自动为发现的设备分配状态。根据当前资产管理模式指定状态。

在学习模式下，应用程序将“*已授权*”状态分配给所有设备（新设备以及之前添加到表中的设备），之前已分配“*未授权*”状态的设备除外。

在监控模式下，分配的状态取决于表现出活动的设备是否是应用程序已知或不识别的设备。在此模式下，状态根据以下规则分配：

- 如果设备是新的（在发现时它在设备表中不存在），则该设备被分配“*未授权*”状态。
- 如果设备存在于“*已授权*”或“*未授权*”状态的设备表中，则其状态不会改变。
- 如果设备存在于“*已存档*”状态的设备表中，则该设备被分配“*未授权*”状态。

默认情况下，如果处于“*已授权*”状态的设备已处于不活动状态超过 30 天，并且在此期间设备信息没有发生变化，则该设备将自动分配为“*已存档*”状态。您可以禁用在手动更改设备状态时自动分配“*已存档*”状态的功能（例如，为了防止很少连接到网络的设备从“*已授权*”状态更改为“*未授权*”）。

当使用“**Cisco 交换机**”类型的连接器时，设备的网络访问可能会在这些设备变为“*未授权*”状态后被自动限制。您需要考虑此类连接器的指定设置，以防止因状态改变而阻止必要的设备。

根据条件自动对设备进行分组

本节包含有关如何根据条件自动分组设备的说明。您可以根据以下条件之一自动对设备组树中的设备进行分组：

- 属于应用程序已知子网的 IP 地址
- 设备类别
- 设备供应商

只有具有“**高级安全官**”角色的用户才能自动分组设备。

根据条件自动对设备进行分组，从组树的根开始

要根据条件自动对设备进行分组，从组树的根开始：

1. 使用 Web 界面以高级安全官角色连接到 Central Node。
2. 在“**网络地图**”区域，“**网络交互图**”选项卡上，点击网络交互图显示区域左侧工具栏中的以下按钮之一，选择分组条件：
   - 按子网对设备进行分组。
   - 按类别对设备进行分组。
   - 按供应商对设备进行分组。

   这将打开一个提示窗口，您可以在其中选择一个分组选项。
3. 要基于地址空间按类别和供应商对设备进行分组，请在提示窗口中选择“**考虑地址空间**”复选框。
4. 根据您要执行的操作，单击下列按钮之一：
   - 要按子网对设备进行分组，请单击**“分组”**。
   - 要根据设备组树中所有组中的地址空间按类别和供应商对设备进行分组，请单击**“带子组”**。
   - 要仅根据设备组树层次结构顶层的地址空间按类别和供应商对设备进行分组，请单击“**仅限选定**”。

该应用程序识别符合所选分组条件的设备，为这些设备创建组，并将设备排列到这些组中。

自动将设备分组到选定的设备组中

要自动将设备分组到选定的设备组中：

1. 使用 Web 界面以高级安全官角色连接到 Central Node。
2. 在“**网络地图**”部分，“**网络交互图**”选项卡上，选择您想要自动分组设备的组。
3. 右键单击以打开上下文菜单。
4. 在上下文菜单中，选择以下命令之一：
   - **按子网分组**。
   - **按类别分组**。
   - **按供应商分组**。

   这将打开一个提示窗口，您可以在其中选择一个分组选项。
5. 要基于地址空间按类别和供应商对设备进行分组，请在提示窗口中选择“**考虑地址空间**”复选框。
6. 在提示窗口中，根据您要执行的操作，单击以下按钮之一：
   - 要按子网对设备进行分组，请单击“**分组**”。
   - 如果要按类别或供应商对选定组的所有子组中的设备进行分组，请单击“**带子组**”。
   - 如果您想按类别或供应商仅对选定组中的设备进行分组，请单击“**仅选定**”。

   该应用程序识别符合所选分组条件的设备，为这些设备创建组并将设备排列到这些组中（其他组中的设备不受影响）。

手动将设备分组

本节包含有关如何在组树中手动排列设备的说明。只有具有高级安全官角色的用户才能在组树中排列设备。

将设备添加到组

要在管理表时将单个设备添加到组：

1. 使用 Web 界面以高级安全官角色连接到 Central Node。
2. 在“**资产**”部分，“**设备**”选项卡上，或者“**网络地图**”部分选择设备。
   在“**网络地图**”部分，您可以选择要添加到网络交互图以及拓扑图上的组中的设备。
   详细信息区域显示在 Web 界面窗口的右侧。

3. 单击**"编辑"**。

4. 在详细信息区域中，转到"**设置**"选项卡。

5. 点击"**组**"字段右侧的 图标。
   出现**"在树中选择组"**窗口。

6. 在设备组树中，选择相关组。
   如果相关的组不在树中，您可以在当前显示的"**在树中选择组**"窗口中将其添加。

7. 单击**"选择"**。
   所选组的路径显示在"**组**"字段。

8. 点击详细信息区域中的"**保存**"。
   如果设备设置不包含所有必需的信息或某些指定的设置无效，则此按钮不可用。需要正确值的设置的选项卡标有 图标。

将多个设备添加到一个组

您可以在管理设备表的同时将多个设备添加到一个组中。

另外，在管理网络交互图时，您可以将网络交互图上的多个已知设备添加到一个组中。您可以单独选择组件服务器，也可以选择包含所需设备的折叠组的一部分。当您选择一个折叠的组时，所有嵌套级别的子组中的所有设备也都会被选择。

要在管理表时将多个设备添加到一个组：

1. 使用 Web 界面以高级安全官角色连接到 Central Node。

2. 选择"**资产**"部分。

3. 在"**设备**"选项卡上，选择要添加到组的设备。

4. 右键单击以打开上下文菜单。

5. 在上下文菜单中，选择"**组管理 → 移至组**"。
   出现**"在树中选择组"**窗口。

6. 在设备组树中，选择相关组。
   如果相关的组不在树中，您可以在当前显示的"**在树中选择组**"窗口中将其添加。

7. 单击**"选择"**。
   所选组的路径显示在"**组**"列。

要在管理网络交互图时将多个设备添加到一个组：

1. 使用 Web 界面以安全官或高级安全官角色连接到 Central Node。

2. 在"**网络图**"部分的"**网络交互图**"选项卡上，选择相关的组件服务器和/或折叠组。

要选择多个组件服务器和/或组，请执行以下操作之一：

- 按住 **SHIFT** 键，然后使用鼠标选择一个包含要选择的对象的矩形区域。
- 按住 **CTRL** 键并单击要选择的每个对象。

3. 右键单击以打开上下文菜单。
4. 在上下文菜单中，选择“**移至组**”。
   出现**“在树中选择组”**窗口。
5. 在设备组树中，选择相关组。
   如果相关的组不在树中，您可以在当前显示的“**在树中选择组**”窗口中将其添加。
6. 单击**“选择”**。
   选定的组件服务器显示在选定的组内。

从组中删除设备

要在管理表时从组中删除单个设备：

1. 使用 Web 界面以高级安全官角色连接到 Central Node。
2. 在“**资产**”部分，“**设备**”选项卡上，或者“**网络地图**”部分选择设备。
   在“**网络地图**”部分，您可以在网络交互图以及拓扑图上选择要从组中删除的设备。
   详细信息区域显示在 Web 界面窗口的右侧。
3. 单击**“编辑”**。
4. 在详细信息区域中，转到“**设置**”选项卡。
5. 在“**组**”字段，通过单击字段内的 × 图标删除组路径（如果定义了组，则显示图标）。
6. 单击“**保存**”。
   如果设备设置不包含所有必需的信息或某些指定的设置无效，则此按钮不可用。需要正确值的设置的选项卡标有 . 图标。

保存设备更改后，其“**组**”值将被清除，并且设备将被分配到组树的根级别。

从组中删除多个设备

使用设备表时，您可以从组中删除多个设备。选择从组中删除的设备可以属于同一组或不同的组。

此外，在管理网络交互图时，您可以从网络交互图上的组中排除多个已知设备。您可以单独选择组件服务器，也可以选择包含所需设备的折叠组的一部分。当您选择一个折叠的组时，所有嵌套级别的子组中的所有设备也都会被选择。

要在管理表时从组中删除多个设备：

1. 使用 Web 界面以高级安全官角色连接到 Central Node。
2. 选择“**资产**”部分。
3. 在“**设备**”选项卡上，选择要从组中删除的设备。
4. 右键单击以打开上下文菜单。
5. 在上下文菜单中，选择“**组管理 → 从组中删除**”。
   这将打开一个确认提示窗口。
6. 在提示窗口中确认从组中删除设备。

对于所有选定的设备，“**组**”值被清除，并且这些设备被分配到组树的根级别。

要在管理网络交互图时从组中删除多个设备：

1. 使用 Web 界面以安全官或高级安全官角色连接到 Central Node。
2. 在“**网络地图**”部分，在“**网络交互图**”选项卡上，选择展开组和/或折叠组中的组件服务器。
   要选择多个组件服务器和/或组，请执行以下操作之一：
   - 按住 **SHIFT** 键，然后使用鼠标选择一个包含要选择的对象的矩形区域。
   - 按住 **CTRL** 键并单击要选择的每个对象。
3. 右键单击以打开上下文菜单。
4. 在上下文菜单中，选择“**从组中删除**”。
   这将打开一个确认提示窗口。
5. 在提示窗口中确认从组中删除设备。

对于所有选定的设备，“**组**”值被清除并且这些设备显示在组之外。

将带有组件和组的服务器移动到网络交互图上的其他组

您可以通过拖放网络交互图上的对象来重新排列设备组树中的组件服务器和组。设备组树中移动的组件服务器和组的位置的变化方式与向组中添加设备或从组中删除设备时的变化方式相同。

只有具有高级安全官角色的用户才能将组件服务器和组移动到其他组。

要将组件服务器和/或组移动到其他组：

1. 使用 Web 界面以高级安全官角色连接到 Central Node。
2. 在“**网络图**”部分的“**网络交互图**”选项卡上，选择相关的组件服务器和/或折叠组。

要选择多个组件服务器和/或组，请执行以下操作之一：

- 按住 **SHIFT** 键，然后使用鼠标选择一个包含要选择的对象的矩形区域。
- 按住 **CTRL** 键并单击要选择的每个对象。

3. 指向选定的对象之一（一个组或一个组件服务器）。
4. 按住 **CTRL** 键并将选定的对象拖到所需的组中（如果要将选定的对象移动到组树的顶层层次结构，则拖到组外的任意空间）。

   这将打开一个确认提示窗口。
5. 在提示窗口中确认所选对象的移动。

设备组树

设备组树的目的是根据设备的功能、位置或任何其他任意属性来排列设备。可以手动或自动将设备分组（根据其所属子网的 IP 地址、类别或供应商）。

如果某个设备不包含在任何组中，则该设备属于组树的顶层。自动添加到表中的设备默认不包含在任何组中。

查看设备表时，您可以看到设备属于哪些组。组的路径在**"组"**列中指明。设备组也显示在网络交互图上。但是，如果这些组中的设备不满足在网络交互图上过滤对象的设置，则可能不会显示。

手动编辑设备组树

您可以在使用设备表、网络交互图和拓扑图时创建设备组树。树创建功能位于"**创建组树**"或"**在树中选择组**"窗口。

只有具有高级安全官角色的用户才能创建设备组树。

要使用设备树组编辑功能：

1. 使用 Web 界面以高级安全官角色连接到 Central Node。
2. 在"**资产**"部分，"**设备**"选项卡上，或"**网络地图**"部分中，执行以下操作之一：

   - 通过单击"**配置组**"打开"**创建组树**"窗口。

     "**资产**"部分中的"**配置组**"按钮可在工具栏中的"**组管理**"下拉列表中找到。

     "**网络地图**"部分中的"**配置组**"按钮仅在"**网络交互图**"选项卡上可用。
   - 在将设备添加到组中时，打开"**在树中选择组**"窗口。您还可以在按以下列过滤设备表时打开此窗口："**组**"列。

在"**创建组树**"或"**在树中选择组**"窗口中的设备组树中所做的更改将立即应用。

本节包含有关如何编辑设备组树的说明。

添加组

要将组添加到设备组树：

1. 在“**创建组树**”或“**在树中选择组**”窗口中，通过以下方式之一添加新组：
   - 如果树为空，而您想要添加第一个组，请单击“**添加**”或按 **INSERT** 或 **ENTER**。
   - 如果要添加与现有组处于同一层次结构的组，请选择该组并按 **ENTER**。
   - 如果要将子组添加到现有组，请选择该组并单击“**添加**”或按 **INSERT**。
2. 在文本框中输入组的名称。
   您可以使用字母、数字、空格字符和以下特殊字符：`! @ # № $ % ^ & ( ) [ ] { } ' , . - _ /`。
   组名称必须满足以下要求：
   - 以空格以外的任意字符开始和结束。
   - 最多包含 255 个字符。
   - 与同一父组下的另一个组名名称不同（不区分大小写）。
3. 单击文本框右侧的 ✓ 图标。

重命名组

要将组重命名为设备组树：

1. 在“**创建组树**”或“**在树中选择组**”窗口，选择要重命名的组。
2. 单击“**重命名**”或按 **F2**。
3. 在文本框中输入组的新名称。
   您可以使用字母、数字、空格字符和以下特殊字符：`! @ # № $ % ^ & ( ) [ ] { } ' , . - _ /`。
   组名称必须满足以下要求：
   - 以空格以外的任意字符开始和结束。
   - 最多包含 255 个字符。
   - 与同一父组下的另一个组名名称不同（不区分大小写）。
4. 单击文本框右侧的 ✓ 图标。

新的组名将显示在添加到此组或其子组的设备的设备信息中。

删除组

删除组不会删除添加到该组的设备。已删除组中的设备将移动到设备树中与已删除组相同的层级。

要从设备组树中删除组：

1. 在“**创建组树**”或“**在树中选择组**”窗口，选择要删除的组。
2. 点击 图标。
   这将打开一个提示窗口，您可以在其中选择删除选项。
3. 在提示窗口中，根据您要执行的操作，单击以下按钮之一：
   - 如果只想删除选定组并保留其子组，请单击“**仅选定**”。
   - 如果要删除选定组及其所有子组，请单击“**带有子组**”。

   这将打开一个确认提示窗口。
4. 在提示窗口中，单击“**确定**”。

移动组

要在设备组树中移动设备：

1. 在“**创建组树**”或“**在树中选择组**”窗口，选择要移动的组。
2. 使用箭头图标或相应的快捷键（**ALT+↓**、**ALT+↑**、**ALT+←**、**ALT+→**）将组相对于树的其他元素进行移动。如果无法执行操作，则该操作的图标不可用。

搜索组

您可以使用“**创建组树**”或“**在树中选择组**”窗口中的“**搜索组**”字段在设备组树中找到相关组。设备组树显示符合搜索条件的组。对于子组，还会显示其父组。

更新树

当您管理树时，可以在 Central Node 上修改设备组树的组成（例如，由连接到 Central Node 的另一个用户）。

您可以通过单击在“**创建组树**”或“**在树中选择组**”窗口中的 图标手动更新树。

添加和删除设备标签

本节提供有关如何添加或删除设备标签的说明。您添加到设备的标签可以是任意的。

*设备标签*包含文本描述，可让您快速查找或筛选表中的设备。您可以将任何您认为方便的文本描述保存为标签。一个设备最多可以有 16 个标签。每个设备可以有自己的一组标签。

设备标签列表显示在设备表的“**标签**”列中。单元格中的标签按字母顺序排序。

只有具有高级安全官角色的用户才能添加或删除设备标签。

为单个设备添加标签

要向一个设备添加标签：

1. 使用 Web 界面以高级安全官角色连接到 Central Node。
2. 在“**资产**”部分，“**设备**”选项卡上，或者“**网络地图**”部分选择设备。
   在“**网络地图**”部分，您可以选择设备以在网络交互图和拓扑图上添加标签。
   详细信息区域显示在 Web 界面窗口的右侧。
3. 单击**“编辑”**。
   在详细信息区域中，转到“**设置**”选项卡。
4. 在“**标签**”字段中，输入您想要用作标签的文本描述。要分隔标签，可以按 **ENTER** 使用换行符或使用分号字符 (`;`)。
   您可以使用大写和小写字母、数字、空格字符和以下特殊字符：`! @ # № $ % ^ & ( ) [ ] { } ' , . - _`。
   标签名称必须满足以下要求：
   - 以空格以外的任意字符开始和结束。
   - 在该设备标签列表中是唯一的（不区分大小写）。
   - 包含 1 至 255 个字符。
5. 如有必要，单击“**复制标签**”以复制标签列表。如果标签列表不为空，则会显示链接。
6. 单击“**保存**”。
   如果设备设置不包含所有必需的信息或某些指定的设置无效，则此按钮不可用。需要正确值的设置的选项卡标有 . 图标。

为多个设备添加标签

您可以在管理设备表时为多个设备添加标签。

另外，在管理网络交互图和拓扑图时，您可以为应用程序已知的设备（以图上的节点表示）添加标签。您可以单独选择节点，也可以选择包含所需设备的折叠组的一部分。当您选择一个折叠的组时，所有嵌套级别的子组中的所有设备也都会被选择。

要在管理表格时向多个设备添加标签：

1. 使用 Web 界面以高级安全官角色连接到 Central Node。
2. 选择“**资产**”部分。
3. 在“**设备**”选项卡上，选择要添加标签的设备。
4. 右键单击其中一个选定的设备以打开上下文菜单。
5. 在上下文菜单中，选择“**添加标签**”。
   这将打开“**添加标签**”窗口。
6. 在“**标签**”字段中，输入您想要用作标签的文本描述。要分隔标签，可以按 **ENTER** 使用换行符或使用分号字符 (**;**)。
   您可以使用大写和小写字母、数字、空格字符和以下特殊字符：**! @ # № $ % ^ & ( ) [ ] { } ' , . - _**。
   标签名称必须满足以下要求：
   - 以空格以外的任意字符开始和结束。
   - 在该设备标签列表中是唯一的（不区分大小写）。
   - 包含 1 至 255 个字符。
7. 如有必要，单击“**复制标签**”以复制标签列表。如果标签列表不为空，则会显示链接。
8. 如果要清除选定设备的当前标签列表并仅为这些设备提供新标签，请选中“**删除现有**”复选框。

   > 如果清除“**删除现有**”复选框，则当前标签列表将保留在每台设备上。新标签将附加到所有选定设备的标签列表中。对于某些选定的设备，这可能会导致标签总数超出限制（每个设备最多 16 个标签）。应用程序在添加新标签之前会检查限制。

9. 单击“**确定**”。
   如果输入的标签名称不符合要求，或者标签列表为空且未选中“**删除现有**”复选框，则该按钮不可用。

要在管理地图时为多个设备添加标签：

1. 使用 Web 界面以高级安全官角色连接到 Central Node。
2. 选择“**网络地图**”部分。
3. 在“**网络交互图**”或“**拓扑图**”选项卡上，选择已知设备和/或折叠组的相关节点。
   要选择多个节点和/或组，请执行以下操作之一：
   - 按住 **SHIFT** 键，然后使用鼠标选择一个包含要选择的对象的矩形区域。
   - 按住 **CTRL** 键并单击要选择的每个对象。
4. 右键单击其中一个选定的对象以打开上下文菜单。

5. 在上下文菜单中，选择“**添加标签**”。
   这将打开“**添加标签**”窗口。

6. 在“**标签**”字段中，输入您想要用作标签的文本描述。要分隔标签，可以按 **ENTER** 使用换行符或使用分号字符 (;)。
   您可以使用大写和小写字母、数字、空格字符和以下特殊字符：`! @ # № $ % ^ & ( ) [ ] { } ' , . - _`。
   标签名称必须满足以下要求：

   - 以空格以外的任意字符开始和结束。
   - 在该设备标签列表中是唯一的（不区分大小写）。
   - 包含 1 至 255 个字符。

7. 如有必要，单击“**复制标签**”以复制标签列表。如果标签列表不为空，则会显示链接。

8. 如果要清除选定设备的当前标签列表并仅为这些设备提供新标签，请选中“**删除现有**”复选框。

   > 如果清除“**删除现有**”复选框，则当前标签列表将保留在每台设备上。新标签将附加到所有选定设备的标签列表中。对于某些选定的设备，这可能会导致标签总数超出限制（每个设备最多 16 个标签）。应用程序在添加新标签之前会检查限制。

9. 单击“**确定**”。
   如果输入的标签名称不符合要求，或者标签列表为空且未选中“**删除现有**”复选框，则该按钮不可用。

从单个设备上删除标签

要从一个设备中删除标签：

1. 使用 Web 界面以高级安全官角色连接到 Central Node。

2. 在“**资产**”部分，“**设备**”选项卡上，或者“**网络地图**”部分选择设备。
   在“**网络地图**”部分，您可以选择设备以在网络交互图和拓扑图上删除标签。
   详细信息区域显示在 Web 界面窗口的右侧。

3. 单击**“编辑”**。
   在详细信息区域中，转到“**设置**”选项卡。

4. 在“**标签**”字段中，删除不再需要的标签：

   - 如果要删除单个标签，请点击标签名称旁边的 × 图标。
   - 如果要删除所有标签，请使用“**标签**”字段右侧的 × 图标。

5. 单击“**保存**”。
   如果设备设置不包含所有必需的信息或某些指定的设置无效，则此按钮不可用。需要正确值的设置的选项卡标有 . 图标。

清除多个设备的标签列表

您可以在管理设备表时清除多个设备的标签列表。

另外，在管理网络交互图和拓扑图时，您可以清除应用程序已知的设备（由图上的节点表示）的标签列表。您可以单独选择节点，也可以选择包含所需设备的折叠组的一部分。当您选择一个折叠的组时，所有嵌套级别的子组中的所有设备也都会被选择。

要在管理表格时清除多个设备的标签列表：

1. 使用 Web 界面以高级安全官角色连接到 Central Node。
2. 选择“**资产**”部分。
3. 在“**设备**”选项卡上，选择您想要清除标签列表的设备。
4. 右键单击其中一个选定的设备以打开上下文菜单。
5. 在上下文菜单中，选择“**添加标签**”。
   这将打开“**添加标签**”窗口。
6. 选中“**删除现有**”复选框。
7. 单击“**确定**”。

要在管理地图时清除多个设备的标签列表：

1. 使用 Web 界面以高级安全官角色连接到 Central Node。
2. 选择“**网络地图**”部分。
3. 在“**网络交互图**”或“**拓扑图**”选项卡上，选择已知设备和/或折叠组的相关节点。
   要选择多个节点和/或组，请执行以下操作之一：
   - 按住 **SHIFT** 键，然后使用鼠标选择一个包含要选择的对象的矩形区域。
   - 按住 **CTRL** 键并单击要选择的每个对象。
4. 右键单击其中一个选定的对象以打开上下文菜单。
5. 在上下文菜单中，选择“**添加标签**”。
   这将打开“**添加标签**”窗口。
6. 选中“**删除现有**”复选框。
7. 单击“**确定**”。

响应

如果使用 KEDR 功能单元，可以通过创建任务将威胁响应操作应用于设备。下表列出了应用程序中可用的响应操作以及创建任务所需的设置。

要创建应用响应操作的任务：

1. 在应用程序 Web 界面窗口中选择“**资产**”部分。
2. 转到“**设备**”选项卡。
3. 选中您要分配该任务的设备的名称左侧的复选框。

   如果列出的设备太多，您可以应用过滤器来显示您需要的设备。例如，您可以找到具有特定标签的设备或属于特定组的设备。
4. 在“**响应**”菜单中，选择任务类型。

   这将打开任务创建窗口。
5. 根据任务类型指定任务设置。

   下表列出了各项设置。
6. 单击“**保存**”。

任务已创建。任务创建后自动运行。

响应操作说明及创建任务的设置

响应操作	任务设置
终止进程 终止可能威胁设备或企业局域网安全的进程。	• 文件路径是您要终止的进程的可执行文件的路径，或者您要删除的文件的路径，具体取决于任务类型。 您还可以指定此文件的备用数据流的路径。在这种情况下，根据任务类型，将终止指定数据流的进程或删除相关文件。此文件的其他数据流将保持不变。 • **MD5/SHA256**是要终止的进程的可执行文件或要删除的文件的 MD5 或 SHA256 哈希值。该字段是可选的。 • **描述** – 任务描述。该字段是可选的。

响应操作	任务设置
删除文件 删除指定设备上的文件。 此操作无法撤销。	
获取文件 将设备中的文件复制到 Kaspersky Anti Targeted Attack Platform 的存储中，并能够将文件下载到本地计算机。 该任务只能分配给一台设备。	• 文件路径是您想接收的文件的路径。 如果请求的文件已链接到其他 NTFS 数据流，则运行该任务将生成请求的文件链接到的 NTFS 数据流的所有文件。 您还可以指定此文件的备用数据流的路径。在这种情况下，您仅接收指定流的文件。 • MD5/SHA256是要接收的文件的 MD5 或 SHA256 哈希。该字段是可选的。 • **发送以进行扫描**使用 Kaspersky Anti Targeted Attack Platform 扫描文件。 • **描述**是任务描述。该字段是可选的。
获取取证 从 Kaspersky Anti Targeted Attack Platform 的存储中获取指定设备的文件、进程或自动运行点的列表，并能够将这些数据下载到本地计算机。	• **信息类型**是所收集数据的类型。有以下类型可用： • **进程列表**获取任务执行时主机上运行的进程列表。 • **自动运行点列表**获取自动运行点列表。 自动运行点列表包括有关添加到启动文件夹或在注册表的 Run 键中注册的应用程序的信息，以及在带有 Endpoint Agent 组件的主机启动时以及用户登录指定主机上的操作系统时自动运行的应用程序的信息。 **支持的自动运行点列表** Kaspersky Endpoint Agent 支持收集以下自动运行点的数据： • Logon。 • Run。 • Explorer。 • Shell。 • Office。 • Internet Explorer®。 • Tasks。 • Services。 • Drivers。 • Telephony。 • Cryptography。 • Debuggers。 • COM。 • Session Manager。 • Network。 • LSA。 • Applications。 • Codecs。 • Shellex。 • WMI。 • Unspecified。

响应操作	任务设置
	Kaspersky Endpoint Security 支持收集上述自动运行点以及以下内容： • BootLog • Browsers • DriverLog • EfiLoader • GroupPolicy • 登录 • OsLoader • OsUpdate • Printer • Process • Scheduler • **文件列表**获取任务执行时存储在所选文件夹或所有主机文件夹中的文件列表。 • 如果您选择**文件列表**，则以下几种数据源类型可用： • **所有本地磁盘**包含在任务执行时存储在本地磁盘上所有文件夹中的文件。 • **目录**包括存储在指定文件夹及其子文件夹中的文件。 • 如果您选择**目录**，则以下设置可用： • **启动目录**是文件搜索的起始文件夹路径。 您可以使用系统或用户环境变量。 使用用户定义的环境变量时，文件列表包含有关设置了指定环境变量的所有用户的文件夹中的文件的信息。如果用户定义的环境变量覆盖系统环境变量，则文件列表将根据系统环境变量的值包含有关文件夹中文件的信息。 • **掩码**是要包含在文件列表中的文件的掩码。 • **备用数据流**启用在文件列表中记录有关备用数据流的信息。 如果请求的文件已链接到其他 NTFS 数据流，则运行该任务将生成请求的文件链接到的 NTFS 数据流的所有文件。 • **最大嵌套级别**是应用程序在其中搜索文件的文件夹的最大嵌套级别。 • **排除项**是要禁止在其中搜索文件信息的文件夹的路径。 • **描述**是任务描述。该字段是可选的。
获取注册表键 获取 Kaspersky Anti Targeted Attack Platform 存储中指定的注册表键及其值的列表，并可将数据下载到本地计算机。	• **注册表键** — 您想要获取的注册表项。 您可以采用以下格式之一输入注册表项： • 相对于根密钥。 例如，\REGISTRY\MACHINE\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator。 • 相对于根密钥的全名。 例如，HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator。 • 相对于用缩写代替根密钥的全名。 例如，HKLM\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator。 如果要从 HKEY_CURRENT_USER 获取数据，您必须指定 HKEY_USERS 和用户的 SID：HKEY_USERS\<SID of the user>。 • **描述**是任务描述。该字段是可选的。

响应操作	任务设置
开始 YARA 扫描 使用 YARA 规则扫描进程、自动运行点和文件。	• **选择规则**是规则的名称。您可以输入规则名称或规则名称中的字符序列，然后在列表中选择规则。 您可以添加多个规则。 • **扫描**是扫描范围。以下扫描范围可用： • **内存**扫描在执行任务时正在运行的进程。 应用程序不会扫描低优先级的进程。 • **自动运行点**扫描从**进行取证**任务获取的自动运行点。 要扫描自动运行点，您必须指定之前为其运行过**进行取证**的设备。 • **指定目录**扫描在任务执行时位于指定文件夹及其所有嵌套文件夹中的文件。 • **所有本地磁盘**扫描在任务执行时存储在本地磁盘上所有文件夹中的文件。 扫描所有本地磁盘可能会导致主机负载过高。 • 如果您选择**内存**，则以下设置可用： • **进程**列出了要扫描的进程的短名称或文件掩码。 应用程序扫描主机上运行的所有具有相同名称的进程。 如果**进程**字段留空，应用程序将扫描任务执行时正在运行的所有进程，除了 PID 小于 10 的进程和**排除项**字段中所列的进程。 • **排除项**列出了要从扫描中排除的进程的完整名称或文件掩码。 如果主机上正在运行多个具有相同名称的进程，应用程序将从扫描中排除所有此类进程。 • 如果您选择**自动运行点**，则以下设置可用： • **快速**扫描所有自动运行点，但 COM 对象除外。 • **全盘**扫描所有自动运行点及其关联文件。 如果您使用 Kaspersky Endpoint Security for Windows 作为 Endpoint Agent 组件，则无论选择的设置如何，都会执行完整扫描。 • 如果您选择**指定目录**，则以下设置可用： • **指定目录**是以 C:\<目录名称>* 格式指定的目录路径。 • **排除项**是以 C:\<目录名称>* 格式指定的目录路径。 • **最大扫描持续时间**是最大扫描持续时间。 当该时间过去后，即使未应用某些规则来扫描主机，扫描也会停止。任务报告包含扫描停止时的最新结果。 • **描述**是任务描述。该字段是可选的。
管理服务 启动、停止、暂停、删除、恢复指定设备上的服务，或更改服务的启动类型。	• **服务名称**是服务的名称。 • **MD5/SHA256**是服务的 MD5 或 SHA256 哈希值。该字段是可选的。 如果您输入从 DLL 加载的服务的哈希值，Kaspersky Anti Targeted Attack Platform 会同时将指定的哈希值与服务 DLL 的哈希值和 svchost 进程的哈希值进行比较。 • **操作**是您要对服务执行的操作。 支持以下服务操作： • **开始**。 • **停止**。 • **暂停**。

响应操作	任务设置
	• **恢复**。 • **删除**。 • **修改启动类型**。 当您删除某个服务时，该服务启动的进程将继续运行，直到系统重新启动或该进程终止。 • 如果您选择"**修改启动类型**"，您需要在"**启动类型**"字段中选择服务的启动类型。 • **描述**是任务描述。该字段是可选的。
隔离文件 隔离受感染或疑似受感染的文件。 如有必要，您可以从隔离区恢复文件。	• **文件路径** — 您想删除的文件的路径。 • **MD5/SHA256** — 要删除的文件的 MD5 或 SHA256 哈希。该字段是可选的。 • **描述** — 任务描述。该字段是可选的。
启动应用程序 运行应用程序或命令。 如有必要，您可以终止已启动的进程。有关终止进程任务的更多详细信息，请参见上表。	• 在**文件路径**和**工作目录**字段中，通过以下方式之一输入值： • 在**文件路径**字段中，输入可执行文件的完整路径（例如，`C:\Windows\System32\ipconfig.exe`）。留下**工作目录**字段为空。 创建任务时，应用程序不会检查指定的可执行文件路径是否有效。 • 在**文件路径**字段中，输入可执行文件的名称和扩展名（例如 `ipconfig.exe`）。在**工作目录**字段中，输入工作目录（例如 `C:\Windows\System32\`）。 • **参数**是运行文件或任务的其他选项（例如，`/all` 参数）。 • **描述**是任务描述。该字段是可选的。
创建预防规则 防止文件和进程在指定的设备上启动。 如有必要，您可以删除、启用或禁用创建的防护规则。	• **状态** — 防护规则的状态。 • **MD5/SHA256** — 要阻止启动的文件或数据流的 MD5 或 SHA256 哈希。 • **名称** — 防护规则的名称。 • **通知用户阻止文件执行**向应用该防护规则的计算机用户显示有关该防护规则已激活的通知。

监控设备上的用户

Kaspersky Anti Targeted Attack Platform 可以监控应用程序已知的设备上的用户账户。在监控用户时，应用程序会自动获取有关在设备操作系统中注册的用户账户的信息。根据这些信息，应用程序生成用户表。

当获取有关用户账户的信息时，应用程序会使用此信息监控设备上的所有用户账户，但某些本地系统用户除外，这些用户只有操作系统服务可以使用。例如，应用程序不监控 Windows 设备上的 LocalSystem 和 NetworkService 账户。

要使用用户监控功能，必须启用资产管理方法来检测设备活动和设备信息。必须在所有具有从其接收信息的应用程序组件的服务器上启用这些方法。

用户监控基于从以下类型的来源收到的信息：

1. **遥测 (Endpoint Agent)**

   当Endpoint Agent 组件与 NDR 功能集成时，将收到有关设备及其在这些设备上运行的进程的信息。

2. **外部源**

   信息接收自使用 Kaspersky Anti Targeted Attack Platform API NDR 并向 Kaspersky Anti Targeted Attack Platform 发送有关用户的信息的系统。

来源按来自这些来源的信息的优先级从高到低的顺序列出。应用程序根据收到的信息的优先级来处理有关用户的信息。来自较高优先级来源的用户信息可能会覆盖来自其他来源的信息。如果关于此类用户的信息是从"**外部来源**"获得的，但是从这些来源收到的新信息中缺少用户，则应用程序还会自动从表中删除用户。

您可以在**"资产"**部分的**"用户"**选项卡上查看有关用户的信息。

查看用户表时，您可以配置、过滤、搜索和排序用户，以及导航到相关项目。所有用户表最多可包含 200000 个用户。

应用程序在表格中以及选定用户的详细信息区域中显示有关设备用户的以下信息：

- **用户 ID** 是 Kaspersky Anti Targeted Attack Platform 中分配的用户 ID。
- **用户名**是不含设备域名或主机名的用户账户名称。
- **全名**是包含设备域名或主机名的用户账户名称。
- **组**列出了用户所属的用户组的名称。
- **设备**是设备的名称和地址。
- **来源**是有关用户的信息来源。
- **SID** 是用户的安全 ID。
- **账户状态**是与收到的启用或禁用账户的值对应的状态。
- **锁定**是与收到的账户阻止设置的值对应的状态。
- **下次登录时更改密码**是一个反映用户是否必须在下次登录时更改密码的属性。
- **阻止用户更改密码**是反映是否禁止用户更改用户自己的密码的属性。
- **密码有效期**是与收到的启用或禁用用户密码有效期限制的设置的值对应的状态。
- **收到的数据**是上次收到有关用户账户的信息的日期和时间。
- **描述**是为用户账户指定的描述。

在监控用户时，应用程序使用**资产管理**技术注册事件。事件注册的系统事件类型代码为 4000005600。当设备上自动添加、修改或删除用户账户时，会记录事件。

您可以编辑事件类型的可用设置。

监控设备上的文件执行情况

Kaspersky Anti Targeted Attack Platform 可以监控应用程序已知的设备上的文件执行情况。根据从 EPP 应用程序收到的信息来监控文件执行情况。根据这些信息，应用程序生成一个可执行文件表。

要从 EPP 应用程序自动获取有关文件执行的信息，必须满足以下条件：

- 必须在设备上安装 Endpoint Agent。
- 必须启用资产管理方法来检测设备活动和设备信息。

对于可执行文件表，项目数量和存储期限有以下限制：

- 可执行文件的总数不得超过 100000 个。
  如果达到可执行文件的最大数量，应用程序会自动删除 10% 的最旧条目。
- 在再次收到有关可执行文件执行的信息之前，可执行文件的最长存储期限为 90 天。
  如果在最大存储期限到期之前没有收到有关文件执行的新信息，应用程序将自动删除该文件的条目。

如果有必要，具有管理员角色的用户可以手动删除可执行文件。

要查看可执行文件表：

1. 在应用程序 Web 界面窗口中选择“**资产**”部分。
2. 转到“**可执行文件**”选项卡。

   可执行文件表将显示。

查看可执行文件表时，您可以配置、过滤、搜索和排序文件，以及导航到相关项目。

该表显示以下信息：

- **文件 ID** 是 Kaspersky Anti Targeted Attack Platform 中分配的文件 ID。
- **设备**是设备的名称和地址。
- **名称**是应用程序的名称和版本，或者文件名。
- **接收日期**是上次接收有关文件信息的日期和时间。
- **产品**是保存在设备操作系统中的软件产品的名称。
- **产品版本**是设备操作系统中保存的软件产品的版本。
- **供应商**是应用程序供应商的名称。
- **路径** 是文件的完整路径。
- **文件大小**是文件占用的磁盘空间量。

- **MD5 哈希**是使用 MD5 哈希算法计算的文件校验和。
- **SHA256 哈希**是使用 SHA256 哈希算法计算的文件校验和。
- **签名**是验证文件数字签名的结果：**有效**（如果数字签名验证成功）或**无效**（例如，如果证书已过期）。
- **创建日期**是文件创建的日期和时间。
- **更改日期**是文件最后修改的日期和时间。
- **来源**是文件信息的来源。
- **属性**是文件属性的列表。
- **描述**是针对文件设置的描述。

主动设备轮询作业

使用主动轮询作业，您可以直接从设备本身接收有关设备及其配置的准确完整信息，从而对受监控的设备进行安全审计。使用连接器实现主动轮询。要主动轮询设备，您需要向应用程序添加一个或多个**主动轮询**连接器。

连接器提供不同的主动轮询方法。*主动轮询方法*规定了协议以及这些协议的命令和功能。内置**主动轮询**连接器类型包含一组方法，这些方法支持通过应用层协议和常规协议进行主动轮询。Kaspersky Anti Targeted Attack Platform 支持以下设备主动轮询方法：

- 通过 ARP 轮询（仅适用于内核版本 4.3 或更高版本的计算机）
- 通过 SMB 轮询
- 通过 SNMP 轮询
- 通过 SSH 轮询
- 通过 WinRM HTTP 轮询
- 通过 WinRM HTTPS 轮询
- 通过 WMI 轮询

这些方法可以让您获取不同的设备信息集。您可以选择配置主动轮询时所需的信息和要使用的方法。

一些方法使用 Secret 来连接设备。设备连接是使用添加到应用程序的 Secret 的凭证建立的。

使用适当的方法，应用程序可以根据主动轮询结果自动更新以下设备信息：

- 代表应用程序中的设备的名称
- 代表网络上的设备的名称（网络名称）
- 设备硬件供应商的名称
- 设备型号

- 设备硬件的版本号
- 设备软件供应商的名称
- 设备软件名称
- 设备软件的版本号
- 设备的网络接口的地址信息
- 设备上安装的操作系统的名称（仅适用于运行 Windows 和 Linux 操作系统的设备）

有关应用程序支持的主动轮询设备的操作系统列表，请参阅附录。

当添加设备或编辑设备信息时，应用程序不会更新使用“**自动更新**”拨动按钮禁用自动更新功能的数据。该应用程序还评估接收到的设备信息的准确性，并且在某些情况下可能不更新先前接收到的信息。

一些主动轮询方法支持检测风险和利用获取的设备信息修改拓扑图。

您可以手动运行安全审计作业，也可以将计划配置为自动运行每个作业。只有具有高级安全官角色的用户才能运行主动轮询作业。

使用主动轮询功能时，必须牢记以下特殊注意事项和限制：

- 添加授权许可密钥后，该功能可用。
- 用于主动轮询设备的连接器的应用程序模块需要通过网络访问设备，以便向设备发送请求并接收数据。如果应用程序模块在安装了应用程序组件的主机上运行，为了确保对设备的网络访问，此计算机必须具有与要轮询的设备的网络连接的网络接口。如果监控点的网络接口接收镜像的公司 LAN 流量（例如，来自网络交换机的 SPAN 端口），则这些网络接口不能用于此目的。
- 如果主动轮询设备误解了活动轮询的命令，则可能出现意外问题。这些问题可能是由设备的错误配置或高度专业化配置引起的。此外，网络配置中隐藏的错误也可能引发问题，而这些错误在设备正常通信时不会显现出来。因此，主动轮询设备可能会带来以下潜在后果的风险：
  - 设备关闭
  - 设备连接中断
  - 设备完全或部分故障
  - 运行速度比正常情况下慢
  - 网络和部件的其他潜在故障

添加主动轮询作业

对于应用程序已知的设备，您可以添加活动轮询作业。

只有具有高级安全官角色的用户才能添加主动轮询作业。添加授权许可密钥后，才可以添加主动轮询作业。

使用向导配置主动轮询作业。该向导可让您逐步配置作业。完成配置后，您可以等待扫描按计划开始或手动启动作业。

添加活动轮询作业时，您可以通过以下方式调用配置向导：

- 添加具有空白设置的作业。为此：

  1. 选择“**资产**”部分。
  2. 在“**主动轮询**”选项卡上，单击“**添加作业**”。

  配置向导的设置没有默认值。

- 为所选设备添加作业。为此：

  1. 选择“**资产**”部分。
  2. 在“**设备**”选项卡上，选择要为其添加主动轮询作业的设备。您可以选择不超过 100 台设备。
  3. 在设备表上方的工具栏中，打开“**创建作业**”下拉列表，然后选择“**主动轮询**”。

  默认情况下，在配置向导的设置中会创建由选定的设备组成的设备列表。

要在配置向导窗口中配置作业：

1. 阅读警告窗口中的主动轮询注意事项，并确认您接受使用主动轮询模块所带来的风险。
2. 在向导的“**选择设备**”部分，创建要执行主动轮询的设备列表。最多可选择 100 台设备。

   您可以使用“**添加到作业**”和“**从作业中删除**”按钮创建设备列表。要添加设备，应用程序会打开一个带有设备分类表的窗口。您可以对表格进行过滤和排序，以显示所需的设备。
3. 在向导的“**选择参数**”部分，选中要使用主动轮询更新的特定设备信息的复选框。您还可以启用风险检测（“**风险**”复选框）和发现设备的拓扑设置（“**拓扑设置**”复选框）。
4. 在向导的“**选择方法**”部分，执行以下操作：

   a. 选择一个主动轮询模块。

   b. 选中要用于获取设备信息、风险检测和/或读取拓扑设置的特定方法的复选框。

   可以使用的方法按提供主动轮询设备功能的连接器分组。该列表仅包含支持获取所选信息的方法。如果连接器不能用于所选设备的主动轮询，则不会显示此连接器的可用方法（例如，如果连接器被禁用，或者如果为连接器选择了不包含所选设备地址的地址空间）。

   c. 根据需要配置每个连接器的方法。例如，对于“**通过 SSH 进行轮询**”，指定端口和凭证 Secret。

   如果尚未将具有所需凭据的 Secret 添加到应用程序中，您可以在不关闭配置向导窗口的情况下在浏览器中打开新选项卡，连接到服务器并添加 Secret，然后使用配置向导窗口中的按钮刷新 Secret 列表。

   我们不建议使用相同的 Secret 对网络上的设备执行主动轮询，因为这会对信息安全级别产生负面影响。

   需要配置设置的方法以红色突出显示。要更新设置，请单击所需方法右侧的 按钮。

5. 在向导的“**作业配置**”部分，配置其余作业设置：

   a. 输入作业的名称和说明。

   您可以使用字母、数字、空格和以下特殊字符：`! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . - _`。作业名称必须以空格以外的任何有效字符开始和结束。

   作业名称不得超过 256 个字符作业描述不得超过 4096 个字符

   b. 要根据计划运行作业，请启用“**根据计划运行作业**”选项并配置计划设置：

   - 在“**频率**”下拉列表中，选择运行作业的频率：**每小时**、**每天**、**每周**或**每月**。
   - 根据所选选项，指定设置值以定义精确的作业启动时间。

   > 应用程序根据计划运行作业，前提是此作业的上一次运行已完成。如果在启动计划作业时，其上次启动的状态为“*正在运行*”，则应用程序将跳过计划作业的运行。

6. 单击“**创建作业**”或“**创建和运行**”关闭向导。

指定的设置显示在作业详细信息中。

编辑主动轮询作业

只有具有高级安全官角色的用户才能编辑主动轮询作业。

要编辑主动轮询作业：

1. 选择“**资产**”部分。
2. 在“**主动轮询**”选项卡上，选择要更改其设置的作业。
3. 单击**“编辑”**。

   配置向导启动。所选作业的设置在配置向导的设置中指定为默认值。

4. 在向导的“**作业配置**”部分，配置其余作业设置：

   a. 输入作业的名称和说明。

   您可以使用字母、数字、空格和以下特殊字符：`! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . - _`。作业名称必须以空格以外的任何有效字符开始和结束。

   作业名称不得超过 256 个字符作业描述不得超过 4096 个字符

   b. 要根据计划运行作业，请启用“**根据计划运行作业**”选项并配置计划设置：

   - 在“**频率**”下拉列表中，选择运行作业的频率：**每小时**、**每天**、**每周**或**每月**。
   - 根据所选选项，指定设置值以定义精确的作业启动时间。

应用程序根据计划运行作业，前提是此作业的上一次运行已完成。如果在启动计划作业时，其上次启动的状态为“*正在运行*”，则应用程序将跳过计划作业的运行。

5. 单击“**编辑作业**”关闭向导。

指定的设置显示在作业详细信息中。

查看主动轮询作业表

主动轮询作业表显示在“**资产**”部分的“**主动轮询**”选项卡上。

作业设置显示在表格以下列中：

- **作业 ID**。
  Kaspersky Anti Targeted Attack Platform 中分配的作业 ID。
- **名称**。
  代表应用程序中的作业的名称。
- **描述**。
  作业描述
- **创建日期**。
  将作业添加到应用程序的日期和时间。
- **更改时间**。
  应用程序中最后修改的日期和时间。
- **所选设备**。
  为作业选择的设备数量。
- **计划**。
  有关应用程序运行作业所用的计划的信息。
- **上次运行状态**。
  作业上次运行时所有设备扫描的结果状态。
- **上次运行**。
  作业上次运行的日期和时间。
- **下次运行**。
  作业下次计划运行的日期和时间。

查看主动轮询作业表时，您可以使用配置、过滤、搜索和排序功能。

启动和停止主动轮询作业

您可以手动启动和停止主动轮询作业。当您启动或停止作业时，应用程序将启动或停止为此作业选择的设备上的所有扫描。

您可以根据上次作业运行的状态停止或启动该作业。例如，如果作业上次运行的状态为"*正在运行*"，则无法启动该作业。

只有具有高级安全官角色的用户才能手动启动和停止主动轮询作业。

要启动主动轮询作业：

1. 使用 Web 界面以高级安全官角色连接到 Central Node。
2. 选择"**资产**"部分。
3. 在"**主动轮询**"选项卡上，选择要启动的作业。
   详细信息区域显示在 Web 界面窗口的右侧。
4. 单击"**启动**"。如果无法启动作业，则该按钮将被禁用。
   Kaspersky Anti Targeted Attack Platform 启动作业。您可以在作业详细信息的**"运行"**选项卡上查看有关正在进行的设备扫描的信息。

要停止主动轮询作业：

1. 使用 Web 界面以高级安全官角色连接到 Central Node。
2. 选择"**资产**"部分。
3. 在"**主动轮询**"选项卡上，选择要停止的作业。
   详细信息区域显示在 Web 界面窗口的右侧。
4. 单击"**停止**"。如果作业无法停止，则该按钮将被禁用。

查看有关主动轮询作业运行的一般信息

您可以在作业表中查看有关主动轮询作业运行的一般信息。该表显示有关最近运行的信息，但不包括有关设备扫描的信息。要查看所有作业运行的常规信息，包括设备扫描的信息，请选择作业，然后在详细信息区域打开**"运行"**选项卡。

有关主动轮询作业运行的一般信息包括以下内容：

- 作业或设备扫描的状态。
  可以有以下状态：
  - **挂起** – 尚未发送启动扫描的命令。
  - **进行中** – 作业正在启动，或者扫描正在进行中。
  - **正在取消** – 正在停止作业或扫描的启动。

- **已取消** – 已停止作业或扫描的启动。
- **已完成** – 扫描已成功完成，或者作业运行中的所有扫描都已成功完成。
- **错误** – 扫描过程中发生错误，或者作业运行中的所有扫描中都发生错误。
- **部分成功** – 作业已完成，但部分成功：某些扫描的状态为“**已完成**”，而某些扫描的状态为“**已取消**”或“**错误**”。

- 启动日期和时间。
- 结束日期和时间。
- 运行时间

查看有关主动轮询作业执行的报告

查看主动轮询作业运行的详细信息时，您可以查看包含设备扫描结果的报告。应用程序将为用以下状态完成的作业生成报告：**已完成**、**部分成功**、**已取消**和**错误**。

报告中显示以下详细信息：

- 被扫描的设备的名称。
- 设备设置更新状态。
- 按更新状态分组的设备设置列表。
- 按执行状态分组的方法列表。如果在使用某种方法时发生错误，应用程序将显示其原因。

要查看有关主动轮询作业执行的报告：

1. 使用 Web 界面以高级安全官角色连接到 Central Node。
2. 选择“**资产**”部分。
3. 在“**主动轮询**”选项卡上，选择要查看运行报告的作业。
   详细信息区域显示在 Web 界面窗口的右侧。
4. 在详细信息区域中，转到“**运行**”选项卡并选择所需的作业运行。
   详细信息区域显示在 Web 界面窗口的右侧。详细信息区域显示有关所选作业运行的详细信息。

删除主动轮询作业

您可以删除主动轮询作业。但是，您不能删除上次运行状态为“**正在运行**”或“**挂起**”的作业。

只有具有高级安全官角色的用户才能删除主动轮询作业。

要删除主动轮询作业：

1. 使用 Web 界面以高级安全官角色连接到 Central Node。
2. 选择“**资产**”部分。
3. 在“**主动轮询**”选项卡上，选择要删除的作业。
4. 单击“**删除**”。

   这将打开一个确认提示窗口。
5. 在提示窗口中，确认删除作业。

   您只能删除上次运行状态不是“**正在运行**”或“**挂起**”的作业。如果所选作业中存在状态为“**正在运行**”或“**挂起**”的作业，则会显示相应的消息。要删除此类作业，您必须首先停止这些作业。

配置地址空间

Kaspersky Anti Targeted Attack Platform 监控设备及其交互，同时考虑地址空间（以下也称为“AS”）。*地址空间*用于根据某些属性（例如，根据设备所属的网络段）将设备地址分类为集合。

为了描述地址空间，应用程序使用规则和子网列表。

*地址空间规则*是一组确定某个地址是否属于该地址空间的参数。要与地址空间关联， MAC 或 IP 地址必须至少匹配一条地址空间规则。如果一个地址与多个规则匹配，应用程序将选择其规则以最不通用的方式定义关联条件的地址空间（例如，如果规则中明确指定了该地址）。

*地址空间子网*用于检查应用程序发现的 IP 地址。根据发现的 IP 地址所属的子网类型，应用程序可能会执行不同的资产监控操作和交互控制操作。

您可以在“**地址空间**”选项卡的“**资产**”部分配置地址空间。每个地址空间由一个包含有关该地址空间的信息的部分表示。该部分由标题和包含规则和子网表格的子部分组成。查看有关地址空间的信息时，您可以展开和折叠部分。

“**默认**”地址空间

默认情况下，应用程序配置了一个地址空间，即**默认**地址空间。此地址空间包含一条将所有 MAC 和 IP 地址与此地址空间关联起来的规则。默认情况下，“**默认**”地址空间的子网列表包含企业网络中最常用的一组标准子网。

您不能编辑“**默认**”地址空间的规则或将其他规则添加到此地址空间。但是，具有高级安全官员角色的用户可以编辑此地址空间中的子网列表，以配置一组子网，其中考虑到公司网络中设备 IP 寻址的设置方式。如果 Kaspersky Anti Targeted Attack Platform 接收来自 EPP 应用程序的数据，应用程序可以使用这些数据自动将子网添加到子网列表中。

附加地址空间

如有必要，除“**默认**”地址空间外，您还可以在应用程序中配置多个地址空间。您可以为添加的地址空间创建任意规则和子网集。符合所添加地址空间条件的地址将与这些地址空间相关联。其余地址仍然与“**默认**”地址空间相关联。

您可能需要添加地址空间，例如，如果您在不同的网段中使用具有相同地址的设备。在这种情况下，在添加和配置地址空间后，应用程序可以通过应用程序添加到地址的附加属性（即地址空间名称）来消除地址信息的歧义。

有关地址空间使用示例，请参阅附录。

地址和地址空间的关系

当使用多个地址空间时，应用程序会将地址空间名称属性添加到应用程序对象中指定的所有地址：设备、风险、规则、事件和其他对象。如果删除所有非默认地址空间，则不再显示地址的地址空间名称属性（地址空间属性仅为事件中的地址和某些与设备相关的风险保留）。

地址空间名称属性表示地址和地址空间之间的关系。与地址空间的关系使得地址依赖于这些地址空间。

地址和地址空间之间的关系导致删除地址空间时需要特别考虑以下事项：应用程序会自动删除与所删除地址空间关联的所有地址。此类地址将从除事件之外的所有应用程序对象中删除。当从对象中删除地址时，应用程序会检查该对象中是否还剩余其他地址，如果没有其他地址，应用程序还会删除该对象本身（例如，设备）。

关于地址空间规则

地址空间的规则显示在地址空间描述内的“**规则**”块中。有关规则的信息显示在地址空间的标题栏和规则表中。

地址空间规则设置显示在表格以下列中：

- **来源**。
  地址信息的数据源类型和选定的数据源列表。可能的数据源类型如下：
  - **监控点** – 为规则选择的监控点。
  - **集成服务器** – 为规则选择的集成服务器（从所选集成服务器接收到的地址信息数据将满足地址空间规则）。
  - **主动轮询模块** – 为规则选择的主动轮询模块连接器（从所选择的主动轮询模块接收到的地址信息数据将满足地址空间规则）。

  将要用作源的对象添加到应用程序后，必须在地址空间规则中指定数据源。例如，在添加“**主动轮询**”类型的连接器后，必须指定**主动轮询模块**数据源的连接器。
- **OSI 模型层**

为地址空间规则选定的 OSI（开放系统互连）网络协议栈层。您可以为 OSI 模型以下层的地址配置规则：

- **数据链路 (L2)** – MAC 地址。
- **网络 (L3)** – IP 地址。
- **数据链路和网络（L2 和 L3）** – MAC 地址和 IP 地址。

- **VLAN ID**。
  符合 IEEE 802.1q 标准的 VLAN 技术所使用的 VLAN ID。当用于地址空间规则时，**VLAN ID** 可以采用以下值：
  - **任何** – VLAN 技术用于设备之间的网络交互，可以使用任何 VLAN ID。
  - **不允许** – VLAN 技术不用于设备之间的网络交互。
  - **任何或不使用** – VLAN 技术要么不用于设备之间的网络交互，要么与任何 VLAN ID 一起使用。
  - **带有 VLAN ID 列表的固定值** – VLAN 技术用于设备之间的网络交互，地址空间只能包含具有列出的 VLAN ID 之一的地址信息。
- **IP 地址**
  包含在地址空间中的 IP 地址。您可以单独指定地址，将其指定为范围或 CIDR 子网地址。

查看规则表时，您可以使用配置功能（通过单击 图标）和搜索功能。

关于地址空间子网

地址空间的子网显示在地址空间描述内的“**子网**”块中。

该应用程序将发现的 IP 地址与地址空间子网列表进行匹配，并且根据 IP 地址是否属于某些类型的子网，可以执行以下操作：

- 将具有其发现的 IP 地址的设备添加到设备表中并监控该设备的活动。
- 在网络交互图和拓扑图上显示具有其检测到的 IP 地址的设备作为其对应的节点类型（已知设备、未知设备或 WAN 节点）。
- 在网络交互图上显示连接，其中交互方之一是具有发现的 IP 地址的设备。
- 根据配置的规则（交互控制规则、入侵检测规则和关联规则）扫描设备与发现的 IP 地址的交互。
- 忽略具有发现的 IP 地址的设备的活动。

地址空间规则的子网设置显示在表格的以下列中：

- **子网**。
  无类域间路由 (CIDR) 格式的子网地址：<子网的基地址>/<掩码中的位数>。子网地址显示为表示子网嵌套层次结构的树。
- **类型**。

规定其用途的子网类型。有以下类型可用：

- **私有，IT** – 用于作为信息技术 (IT) 资源的设备（例如文件服务器）的子网。
- **私有，DMZ** – 位于非军事区 (DMZ) 网络段内的设备的子网，例如处理来自外部网络的请求的服务器。
- **公共** – 被视为其他类型子网中设备的外部（全局）网络的子网。该子网的 IP 地址由网络交互图上的 WAN 节点表示。
- **链路-本地** – 局域网（未路由）一段内网络交互的子网。

- **范围**

  子网中包含的 IP 地址范围。

- **自动添加子网**

  指示是否启用或禁用根据从 EPP 应用程序收到的信息自动添加嵌套子网。如果启用此模式，应用程序将根据从 EPP 应用程序收到的信息添加嵌套子网。

查看子网表时，您可以使用配置功能（通过单击 图标）以及过滤、搜索和排序功能。

添加地址空间

如果您需要根据某些标准（例如，基于属于网络段的设备）将设备地址分类为集合，则可以将地址空间添加到应用程序中。

应用程序中的最大地址空间数为 100。

只有具有高级安全官角色的用户才能添加地址空间。

要添加地址空间：

1. 使用 Web 界面以高级安全官角色连接到 Central Node。
2. 选择“**资产**”部分。
3. 在“**地址空间**”选项卡上，单击“**添加地址空间**”打开详细信息区域。
4. 输入地址空间的名称。

   您可以使用字母、数字、空格字符和以下特殊字符：`! @ # № $ % ^ & ( ) [ ] { } ' , . - _`。

   地址空间名称必须满足以下要求：

   - 以空格以外的任意字符开始和结束。
   - 最多包含 255 个字符。
   - 不要重复使用另一个地址空间的名称（不区分大小写）。

   > 我们建议使用长度为 6-8 个字符或更短的地址空间。如果名称包含较多字符，某些数据表（例如设备表）的单元格中可能无法完整显示地址信息。

5. 如有必要，请输入地址空间的文本描述。

6. 配置第一个地址空间规则的设置。

7. 如有必要，请单击“**添加规则**”添加并配置附加地址空间规则。

   地址空间中的规则总数不能超过 10 条。

8. 单击“**保存**”按钮。

   如果未指定所有必需的设置，或者某些设置无效，则此按钮不可用。

“**地址空间**”选项卡的下部将显示一个单独的块，其中包含有关添加的地址空间的信息。

为资产管理创建子网列表

本节包含有关可用于生成资产管理子网列表的功能的信息。

对于地址空间，您可以创建子网列表，其中考虑到设备寻址在公司网络中的工作方式。本节提供有关使用功能生成子网列表的说明。

如果 Kaspersky Anti Targeted Attack Platform 接收来自 EPP 应用程序的数据，应用程序可以使用这些数据自动将子网添加到相应地址空间中。如果发现的子网嵌套在启用了自动子网添加模式的子网内，应用程序会自动添加这些子网。

只有具有高级安全官角色的用户才能管理子网列表。

添加子网

要添加子网：

1. 使用 Web 界面以高级安全官角色连接到 Central Node。

2. 选择“**资产**”部分。

3. 在“**地址空间**”选项卡上，展开包含有关要添加子网的地址空间的信息的块。

4. 在“**子网**”块的标题中，点击 + 图标。

   详细信息区域显示在 Web 界面窗口的右侧。

5. 在“**子网**”字段中，以 CIDR 格式输入子网地址：<子网的基地址>/<掩码中的位数>。

6. 在“**类型**”下拉列表中，根据子网的用途选择子网的类型。

7. 启用或禁用“**自动添加子网**”切换开关，以根据从EPP 应用程序收到的数据启用或禁用自动添加嵌套子网。

   如果启用此模式，应用程序将根据从 EPP 应用程序收到的信息在此子网下添加嵌套子网。对于这些嵌套子网，默认类型是为当前子网选择的类型。

8. 单击“**保存**”按钮。

子网将添加到树的相应级别的子网列表中。

编辑子网设置

要编辑子网设置：

1. 使用 Web 界面以高级安全官角色连接到 Central Node。
2. 选择“**资产**”部分。
3. 在“**地址空间**”选项卡上，展开包含有关要编辑子网设置的地址空间的信息的块。
4. 展开“子**网**”块并选择相关子网。
   详细信息区域显示在 Web 界面窗口的右侧。
5. 单击**“编辑”**。
6. 根据您的需要，执行以下操作：
   - 在“**子网**”字段中，以 CIDR 格式输入子网地址：<子网的基地址>/<掩码中的位数>。
     根子网的地址无法编辑。
   - 在“**类型**”下拉列表中，根据子网的用途选择子网的类型。

     更改子网类型时，请记住新的子网类型可能会影响应用程序使用子网中的 IP 地址执行的操作。例如，如果您选择“**公共**”类型，网络交互图将不再显示从该子网分配 IP 地址的设备的链接。
   - 启用或禁用“**自动添加子网**”切换开关，以根据从EPP 应用程序收到的数据启用或禁用自动添加嵌套子网。
     如果启用此模式，应用程序将根据从 EPP 应用程序收到的信息在此子网下添加嵌套子网。对于这些嵌套子网，默认类型是为当前子网选择的类型。
7. 单击“**保存**”按钮。

如果更改了“**子网**”值，则子网的树形层次结构级别也可能会更改。

删除子网

在地址空间的子网列表中，您可以删除树中除根子网（子网 0.0.0.0/0）之外的任何子网。

若要删除子网：

1. 使用 Web 界面以高级安全官角色连接到 Central Node。
2. 选择“**资产**”部分。
3. 在“**地址空间**”选项卡上，展开包含要从中删除子网的地址空间信息的块。
4. 展开“**子网**”块并选择要删除的子网。
   详细信息区域显示在 Web 界面窗口的右侧。

5. 单击“**删除**”。

   这将打开一个确认提示窗口。

6. 在提示窗口中，确认删除子网。

已删除的子网将从子网列表中移除。如果删除的子网包含嵌套子网，这些子网将保留在列表中（但是，这些子网在层次树中的级别会发生变化）。

查看所选子网中具有 IP 地址的设备的信息

您可以查看具有地址空间中选定子网的 IP 地址的设备的信息。有关设备的信息显示在设备表中。设备表会根据子网地址自动应用过滤器。

要查看设备表中有关设备的信息：

1. 选择“**资产**”部分。
2. 在“**地址空间**”选项卡上，展开带有包含相关子网的地址空间的信息的块。
3. 展开“**子网**”块并选择您想要查看设备信息的子网。

   详细信息区域显示在 Web 界面窗口的右侧。

4. 单击“**显示设备**”。

这将打开“**资产**”部分中的“**设备**”选项卡。设备表是通过设备地址信息中的 IP 地址进行过滤的。

更改地址空间

对于添加的地址空间，您可以编辑其名称、文字描述以及规则设置。但是，您无法为**默认**地址空间编辑任何这些内容。

您还可以为任何地址空间创建子网列表（包括“**默认**”地址空间的子网列表）。

管理地址空间的规则设置时，必须考虑此地址空间与应用程序对象（包括设备、风险、规则、事件和其他对象）中指定的地址之间的关系。如果编辑地址空间的规则设置切断了该地址空间与地址的关系，应用程序会自动删除这些地址。如果这些对象没有任何其他地址，这可能会导致对象本身（例如，设备）被删除。

只有具有高级安全官员角色的用户才能编辑地址空间的名称、文本描述和规则设置。

要编辑地址空间的名称、文本描述或规则设置：

1. 使用 Web 界面以高级安全官角色连接到 Central Node。
2. 选择“**资产**”部分。
3. 在“**地址空间**”选项卡上，单击包含相关地址空间信息的块中的 图标。

   详细信息区域显示在 Web 界面窗口的右侧。

4. 根据您的需要，执行以下操作：

   - 输入地址空间的名称。
     您可以使用字母、数字、空格字符和以下特殊字符：`! @ # № $ % ^ & ( ) [ ] { } ' , . - _`。
     地址空间名称必须满足以下要求：

     - 以空格以外的任意字符开始和结束。
     - 最多包含 255 个字符。
     - 不要重复使用另一个地址空间的名称（不区分大小写）。

     > 我们建议使用长度为 6-8 个字符或更短的地址空间。如果名称包含较多字符，某些数据表（例如设备表）的单元格中可能无法完整显示地址信息。

   - 输入地址空间的描述。
   - 管理地址空间规则的设置。
   - 如有必要，请单击“**添加规则**”添加和配置其他地址空间规则，或使用 × 图标删除任何不必要的规则。
     地址空间中的规则总数不能超过 10 条。

5. 单击“**保存**”按钮。
   如果未指定所有必需的设置，或者某些设置无效，则此按钮不可用。

6. 在提示窗口中，确认地址空间设置的更改。

删除地址空间

您可以删除已添加的地址空间。无法删除“**默认**”地址空间。

删除地址空间时，必须考虑此地址空间与应用程序对象（包括设备、风险、规则、事件和其他对象）中指定的地址之间的关系。如果删除某个地址空间会切断该地址空间与地址的关系，则应用程序会自动删除这些地址。如果这些对象没有任何其他地址，这可能会导致对象本身（例如，设备）被删除。

只有具有高级安全官角色的用户才能删除地址空间。

要删除地址空间：

1. 使用 Web 界面以高级安全官角色连接到 Central Node。
2. 选择“**资产**”部分。
3. 在“**地址空间**”选项卡上，单击包含要删除的地址空间信息的块中的 🗑 图标。
   这将打开一个确认提示窗口。
4. 在提示窗口中，确认删除地址空间。

使用网络交互图

网络交互图是设备之间发现的交互的直观显示。您可以使用网络交互图来查看有关各个时间段的设备交互的信息。

要查看网络交互图：

1. 在应用程序 Web 界面窗口中选择“**网络地图**”部分。
2. 转到“**网络交互图**”选项卡。

显示网络交互图。

以下对象可以显示：

- 节点。这些对象代表网络数据包的发送者和接收者。
- 设备组。这些对象与设备组树中的组相对应。组包含代表这些组及其子组中设备的节点。
- 链接。这些对象代表节点之间的交互。

节点和链接根据一定时期内从流量或 Endpoint Agent 获取的数据出现在网络交互图上。设备组连续显示。

您可以过滤节点和链接。默认情况下，网络交互图以一小时的定义过滤期实时显示对象。

网络交互图可显示最多 1000 个连接。

在网络交互图上，可以突出显示存在问题的对象。应用程序认为以下对象存在问题：

- 节点，如果其具有未处理的事件，并且分数为 4.0 或更高，或者它代表具有*未授权*状态的设备。
- 链接，如果其与分数为 4.0 或更高的事件有关。仅考虑在给定的对象过滤期间注册的事件。事件的当前状态未被考虑在内。
- 一个组，如果它包含存在问题的设备，或者这个组中的节点具有存在问题的链接。考虑的对象可以属于组本身，也可以属于任何嵌套级别的子组。

网络交互图上的节点

网络交互图上的节点可以具有以下类型：

- 应用程序已知的设备。此类型的节点代表设备表中列出的设备。
- 应用程序未知的设备。此类型的节点代表具有唯一 IP 或 MAC 地址且未在设备表中列出的设备。这样的节点可能出现在网络交互图上，例如，如果您使用 `ping` 命令向不存在的设备发送网络数据包。如果应用程序无法识别的设备节点总数（根据网络交互图上的当前过滤设置）不超过 100，则会单独显示这些节点。如果存在更多这样的设备，则未知设备由单个节点联合表示。

显示在代表应用程序已知的设备的节点上的信息

对于代表应用程序已知的设备的节点，在最大缩放比例下，网络交互图上会显示以下信息：

- 指定的设备名称。
- 设备类别的图标。
- 设备的 IP 地址（如果没有 IP 地址，则显示 MAC 地址）。
- 根据以下条件的各种图标：
  - 设备是否设置“路由器”属性
  - 设备上是否安装了 Endpoint Agent（图标的颜色取决于其连接状态）
  - 设备是否具有“*已存档*”状态
- 节点左边框上的粗线采用下列颜色之一，具体取决于设备的安全状态：
  - 绿色表示“*正常*”安全状态
  - 黄色表示“*警告*”安全状态
  - 红色表示“*严重*”安全状态

如果设备具有“*未授权*”状态或者设备的安全状态不是“*正常*”，则节点的背景为红色。

显示在代表应用程序未知的设备的节点上的信息

对于代表应用程序未知的设备的节点，在最大缩放比例下，网络交互图上会显示以下信息：

- 如果节点代表单个未知设备，则显示该设备的 IP 或 MAC 地址。如果节点代表多个未知设备（一个节点包含超过 100 个应用程序未知的设备），则会显示“**未知设备**”。
- 未知设备及其状态的图标。

代表应用程序未知的设备的节点具有灰色背景。

网络交互图上的设备组

属于设备组树的组可以在网络交互图上折叠或展开。折叠的组显示为类似于节点的图标。扩展的组显示为包含节点和其他组的框。

折叠组中显示的信息

如果某个组被折叠，则当网络交互图最大化时会显示以下信息：

- 组的名称。
- 网络交互图上满足当前过滤设置的设备数量。此组及其所有子组中所有嵌套级别的设备均被考虑在内。
- 所有嵌套级别的子组的数量。

如果某个组包含存在问题的设备或链接（包括任何嵌套级别的子组），则该组的边框将显示为红色。展开的组上显示的信息

扩展组的框包含一个带有组名称的标题栏和一个用于显示对象的区域。组框显示此组中包含的设备，以及其下嵌套级别的子组。在组中包含的设备中，只有符合当前过滤设置的设备才会显示在网络交互图上。

如果某个组包含存在问题的设备或链接（包括任何嵌套级别的子组），则该框具有红色背景。

折叠和展开组

您可以通过双击组图标来展开折叠的组。您可以通过双击该组框的标题栏或单击标题栏中的 来折叠展开的组。

要同时展开多个折叠的组：

1. 在网络交互图上，通过执行以下操作之一选择多个折叠组：
   - 按住 **SHIFT** 键，然后使用鼠标选择一个包含要选择的组的矩形区域。
   - 按住 **CTRL** 键并单击要选择的每个折叠组。
2. 点击位于网络交互图显示区域左侧的工具栏中的 （如果选择了至少一个折叠组，则该按钮可用）。

要同时折叠所有展开的组：

点击位于网络交互图显示区域左侧的工具栏中的 （如果至少展开了一个组，则该按钮可用）。

网络交互图上的链接

根据检测到的网络数据包来识别网络交互图上的链接，可以将该网络数据包的源地址和目标地址映射到节点的地址。

每个链接代表交互的双方。链接中的通信方可能是网络交互图上的下列对象之一：

- 下列类型之一的节点：
  - 应用程序已知的设备。
  - 应用程序未知的设备。
  - 未知设备的公共节点（如果链接显示与此节点内的一个或多个未知设备的交互）。
- 如果链接显示与该组中一个或多个设备的交互，则为折叠的组。

根据检测交互时注册的事件的分数，链接可以显示为彩色线：

- 灰色表示交互未导致记录任何事件或仅导致记录分数为 0.0–3.9 的事件。
- 红色表示交互已导致分数为 4.0 至 10.0 的事件被记录。

对于链接，仅考虑在给定的对象过滤期间内注册的事件。事件的当前状态未被考虑在内。

应用程序将链接信息存储在数据库中。存储记录的总量不能超出配置的限制。如果数量超出限制，应用程序会自动删除 10% 的最旧记录。您可以在配置存储设置时设置最大网络交互图大小。

查看对象详细信息

有关网络交互图上显示的对象的详细信息显示在详细信息区域中。要显示详细信息，您可以用鼠标选择一个对象（如果要查看某个组的详细信息，必须先折叠该组）。

对于节点，将显示以下信息：

- 如果该节点代表应用程序已知的设备，则详细信息区域将显示与设备表中相同的信息。
- 如果节点代表应用程序未知的单个设备，则详细信息区域将显示设备的 MAC 和/或 IP 地址（如果已向应用程序添加额外的地址空间，则显示地址空间的名称）。
- 若选择未知设备的公共节点，则显示以下信息：
  - 考虑到当前的过滤设置，此节点包含的节点数。
  - **IP 地址**显示未知设备的 IP 地址数量和前 100 个 IP 地址（如果应用程序中添加了额外的地址空间，则显示地址空间名称）。如果某些未知的设备节点具有 IP 地址，则会显示此部分。
  - **MAC 地址**显示未知设备的 MAC 地址数量和前 100 个 MAC 地址（如果应用程序中添加了额外的地址空间，则显示地址空间名称）。如果某些未知的设备节点具有 MAC 地址，则会显示此部分。

对于组，将显示以下信息：

- **父组**显示设备组树中组的路径。如果该组位于层次结构的顶层，则显示**N/A（这是一个顶层组）**。
- 此组及其所有嵌套级别的子组中的设备数量。
- 有关所选组及其所有嵌套级别的子组中存在问题的对象的数量的信息。如果不存在这样的对象，则安全状态显示为“*正常*”。

对于链接，将显示以下信息：

- **严重级别**是与链接相关的事件的最高严重级别对应的图标。如果没有与链接关联的事件，则显示“**无事件**”。仅考虑在给定的对象过滤期间注册的事件。事件的当前状态未被考虑在内。
- 包含交互的第一方和第二方基本信息的部分：
  - 如果未知设备节点是交互的一方，则此部分显示设备的名称或地址、类别和地址信息（而对于应用程序已知的设备，仅显示参与交互的网络接口的地址信息）。对于已知设备，还会显示设备状态。
  - 如果折叠组是交互的一方，则此部分将显示该组的名称以及它包含的设备和子组的数量。
  - 若未知设备的公共节点是交互的一方，则此部分显示节点的名称、**未知设备**、以及此节点代表的节点数。
- **协议**是一个包含参与交互的协议列表的部分。对于每种协议，都会指示传输的数据量，该量是根据检测到的网络数据包计算得出的。如果交互的一方是未知设备的公共节点，则不显示该部分。

缩放网络交互图

网络交互图可以按 1–100% 的比例显示。当前比例值显示在位于网络交互图显示区域左侧的工具栏中。

要更改网络交互图的比例，请执行以下操作：

使用鼠标滚轮或位于当前比例值旁边工具栏中的 **+** 和 **–** 按钮。

减小网络交互图的比例会减少显示节点和折叠组的信息量。

当缩放级别低于 25% 时，图标和文本信息会隐藏在节点和折叠组中。节点和折叠组的显示变化如下：

- 在代表应用程序已知的设备的节点上，设备状态在右上角显示为彩色三角形：
  - 绿色表示设备具有“*已授权*”状态。
  - 红色表示设备具有“*未授权*”状态。
  - 灰色表示设备具有“*已存档*”状态。
- 在折叠的组上，右上角的三角形表示存在带有问题的对象。该三角形填充有下列颜色之一：
  - 如果该组不包含需要注意的对象，则显示为绿色。
  - 如果该组包含存在问题的对象，则显示红色。

定位网络地图

如有必要，您可以手动或自动更改网络交互图的位置。自动定位使您能够移动网络交互图并更改其比例以显示满足定义的过滤器设置的所有节点以及所有扩展组。

要手动定位网络交互图：

1. 将鼠标光标放置在网络交互图上未被对象占据的任何部分上。
2. 单击并按住鼠标左键拖动网络交互图。

要自动定位网络交互图：

点击网络交互图显示区域左侧工具栏中的 按钮。

网络交互图的定位和比例将发生变化，以显示所有节点和扩展组。

固定和取消固定节点和组

默认情况下，节点和折叠组未固定在网络交互图上。取消固定的节点和折叠的组可以自动移动，以优化其他对象的显示。

当节点和组的位置被手动改变或者在自动分配过程中发生变化时，它们将被固定。您还可以固定显示的对象而不移动它们。

要固定或取消固定对象而不移动它们，您可以使用以下控件：

- 网络交互图显示区域左侧工具栏中的按钮。您可以使用 和 按钮固定和取消固定网络交互图上显示的所有节点和组（包括扩展组中的节点）。
- 扩展组框的标题栏中的按钮。您可以点击 或者 仅固定或取消固定扩展组框中（但不是在嵌套组框中）的节点和组。

如果网络交互图包含可以应用相应操作的对象，则这些按钮可用。

固定节点或折叠组的位置后， 图标出现在该元素的右上角（如果网络交互图的比例不小于 25%）。您还可以使用此图标取消固定对象。

固定的节点或组留在原处。如果固定节点从网络交互图中消失（例如，由于过滤），则该节点下次出现时将显示在同一位置。

手动重新排列节点和组

您可以以最方便的方式排列网络交互图上的节点和组，手动更改它们的位置。

已移动的节点和组将被固定到新的位置。如有必要，您可以取消固定它们。

组中包含的对象只能在该组的框范围内移动。

要重新排列节点和/或折叠组：

1. 在网络交互图上，选择一个或多个与节点和/或折叠组相对应的对象。

要选择多个节点和/或折叠组，请执行以下操作之一：

- 按住 **SHIFT** 键，然后使用鼠标选择一个包含要选择的对象的矩形区域。
- 按住 **CTRL** 键并单击要选择的每个对象。

2. 将选定的对象拖动到您想要放置它们的位置。

节点和折叠组在移动后仍保持固定状态。 图标被添加到这些对象中。

要重新定位展开的组：

单击展开的组框的标题栏并将其拖动到新位置。

自动排列节点和组

为了在网络交互图上实现对象的最佳排列，您可以使用算法自动更改节点和组的位置（排列）。提供以下算法：

- 径向排列
- 与网格对齐

您可以将自动排列算法应用于以下对象：

- 组树中层次结构顶层的所有显示的节点和组。使用位于网络交互图显示区域左侧的工具栏中的 （径向排列）按钮和 （网格对齐排列）按钮进行自动排列。
- 扩展组内显示的所有节点和组。要执行自动排列，您可以点击扩展组框的标题栏中的（径向排列）和 （与网格对齐）按钮。
- 仅选定的节点和折叠的组。自动排列之前，您必须选择展开组内或层次结构顶层的至少三个节点和/或折叠组。要选择多个对象，您可以按住 **SHIFT** 键并在必要的对象周围绘制一个选择框，或者您可以通过按住 **CTRL** 键并单击来选择多个对象。使用位于网络交互图显示区域左侧的工具栏中的 （径向排列）按钮和 （网格对齐排列）按钮进行自动排列。

已自动排列的节点和组将固定到新的位置。 图标被添加到这些对象中。如有必要，您可以取消固定它们。

在网络交互图上搜索节点

您可以根据有关节点的信息在网络交互图上搜索这些节点。所有满足当前过滤条件的节点，包括折叠组内的节点和网络交互图显示地区之外的节点。

对于表示应用程序已知的设备的节点，将通过设备表的所有列（**状态**、**安全状态**、**上次查看**、**上次修改**和**创建时间**除外）执行搜索。搜索也是通过设备自定义字段的值来执行的。

如果找到与搜索查询匹配的节点，则这些节点的轮廓将以黄色突出显示。包含找到的节点的折叠组的轮廓以相同的方式突出显示。同时，“**搜索节点**”字段右侧出现以下元素：

- 搜索结果中当前选定的对象（找到的节点或包含找到的节点的折叠组）的序数。
- 找到的对象（节点和/或包含找到的节点的折叠组）的总数。

  找到的对象总数不考虑折叠组中的节点数。如果您希望组中的节点计入搜索结果总数，请展开折叠的组。

- 在找到的对象之间移动的箭头。您可以按照名称的字母顺序在找到的对象之间移动。当移动到下一个对象时，网络交互图会自动定位以显示该对象。

要在网络交互图上查找节点：

过滤网络交互图上的对象

本节提供有关过滤网络交互图上的对象以限制显示的节点和链接数量的说明。

节点和链接的全面过滤

本节包含有关节点和链接全面过滤的说明。

使用时间线上的期间进行过滤

要过滤节点和链接，您可以在时间线上选择一个时间段。时间线显示在网络交互图窗口的下部。

时间线包含以下元素：

- 时间线的开始日期和时间。
- 记录分数为 4.0 及以上的事件的时间段。这些时间段在刻度尺的下部显示为红色条。如果配置的时间线长度超过七天，则不会显示时间段。
- 过滤时间段。此时间段显示为一条黄色条，两端带有拖动手柄。
- 应用程序处理的流量图。如果配置的时间线长度超过七天，则不会显示图表。
- 时间线的结束。根据过滤时间段，时间线的结束显示为日期和时间（如果指定了日期和时间）或“**现在**”链接。

以下类型的过滤时间段是可能的：

- 以当前时刻为参考的时间段。这样一个时间段的右端与当前时刻对应的时间线的右端重合。
- 不参考当前时刻的时间段。此类时间段可放置在时间线的任何位置。

要配置参考当前时刻按时间段过滤对象：

1. 单击时间线右侧的“**现在**”按钮。如果已经参考当前时刻定义了时间段，则不会显示此按钮。

2. 如果要指定不同的时间段长度，请执行以下操作之一：

   - 将黄色时间段条的左端拖动到所需位置（时间段最大长度为 7 天）。

   - 单击黄色时间段条上方的按钮打开设置窗口，选中**“锚定到边界”**复选框，然后选择持续时间（**小时**、**天**、 **7 天**），然后单击**“确定”**。

网络交互图仅显示自指定时间段开始到当前时刻检测到通信的节点和链接。

要配置按时间段进行过滤而不参考当前时刻：

1. 如果您要设置的时间段超出了时间线的范围，请更改时间线的开始和/或结束日期和时间：

   a. 要更改时间线的开始日期和时间，请单击时间线左侧的链接打开一个窗口，然后在该窗口中选择以下选项之一：

      - **天**。

      - **7 天**。

      - **30 天**。

      - **设置日期**。对于此选项，请在打开的字段中指定日期和时间。

   b. 要更改时间线的结束日期和时间，请单击时间线右侧的链接以打开一个窗口，然后在该窗口中选择以下选项之一：

      - **现在**。

      - **指定日期**。对于此选项，请在打开的字段中指定日期和时间。

2. 设定您想要的时间段。为此，请执行以下操作之一：

   - 将时间线上的时间段拖到您想要的位置。

   - 将时间线上黄色时间段条的一端或两端移动到您想要的时间段位置（时间段的最大长度为 7 天）。

   - 单击黄色时间段条上方的按钮打开设置窗口，然后选择持续时间（**小时**、**天**、 **7 天**）并单击“**确定**”。

3. 如果时间段自动锚定到当前时刻（当您将时间段移动到最右边的位置时，时间线右侧的**“现在”**按钮不再显示）但您不想要这样，请禁用自动锚定。为此，请单击黄色时间段条上方的按钮打开设置窗口，清除**“锚定到边界”**复选框，然后单击**“确定”**。

按已注册事件进行过滤

您可以配置网络交互图以显示与所选节点相关的事件中保存其信息的节点和链接。

如果在网络交互图上选择的节点不超过 200 个，则可以按事件进行过滤。您可以单独选择节点，也可以选择包含所需设备的折叠组的一部分。当您选择一个折叠的组时，所有嵌套级别的子组中的所有设备也都会被选择。

您可以使用以下方式按事件进行过滤：

- 按事件进行初步过滤。使用此方法可以按仅与选定节点相关的事件过滤对象。
- 按事件进行附加过滤。如果已经执行了按事件进行的初步过滤（例如，从事件表切换到网络交互图时），并且您还需要从网络交互图上显示的节点列表中过滤与另外选择的节点相关的事件，则应用此方法。

要根据初始事件过滤显示节点和链接：

1. 在网络交互图上，选择一个或多个节点和/或折叠组。

   要选择多个节点和/或组，请执行以下操作之一：

   - 按住 **SHIFT** 键，然后使用鼠标选择一个包含要选择的对象的矩形区域。
   - 按住 **CTRL** 键并单击要选择的每个对象。

2. 在网络交互图上方的工具栏中，打开“**事件过滤器**”下拉列表。
3. 在下拉列表中，选择“**过滤器**”。

   网络交互图仅显示其信息包含在与所选节点相关的事件中的节点和链接。在网络交互图上方的工具栏中，显示了一个带有事件 ID 的列表（ID 按相关事件的检测时间顺序列出）。

要使用按事件进行的附加过滤将节点和链接添加到显示的对象：

1. 确保已按事件执行了初始过滤。为此，请检查网络交互图上方的工具栏中是否有包含事件 ID 的列表。
2. 在网络交互图上显示的节点中，选择您想要向过滤器添加关联事件的节点。

   详细信息区域显示在 Web 界面窗口的右侧。

3. 在网络交互图上方的工具栏中，打开“**事件过滤器**”下拉列表。
4. 在下拉列表中，选择“**添加到过滤器**”。

   网络交互图还显示与所选节点相关的事件中包含其信息的节点和链接。检测到的事件的 ID 被添加到工具栏中的 ID 列表中。

节点过滤

本节提供有关过滤节点的说明。

按设备状态过滤节点

要按设备状态过滤节点：

1. 在网络交互图上方的工具栏中，打开“**设备状态**”下拉列表。

   将显示一个列表，其中包含应用程序已知的设备的状态名称（*未授权*、*已授权*、*已存档*），以及应用程序无法识别的设备的“*未知设备*”状态。

2. 在下拉列表中，选择要用作网络交互图上显示的节点的过滤条件的状态复选框。

3. 单击“**确定**”。

网络交互图仅显示与所选状态的设备相对应的节点。

按设备安全状态过滤节点

要按设备安全状态过滤节点：

1. 在网络交互图上方的工具栏中，打开“**设备状态**”下拉列表。
   将显示一个列表，其中包含设备的安全状态名称（*正常*、*警告*、*严重*）。

2. 在下拉列表中，选中需要在网络交互图上显示的节点的安全状态的复选框。

3. 单击“**确定**”。

网络交互图仅显示与所选安全状态的设备相对应的节点。

按设备类别过滤节点

要按设备类别过滤节点：

1. 在网络交互图上方的工具栏中，打开“**设备类别**”下拉列表。
   将显示的列表包含应用程序已知的设备类别的名称以及未知设备的特殊类别。

2. 在下拉列表中，选择要用作网络交互图上显示的节点的过滤条件的类别的复选框。

3. 单击“**确定**”。

网络交互图仅显示与所选类别的设备相对应的节点。

显示和隐藏链接到已过滤节点的节点

过滤节点后，网络交互图仅显示满足定义的过滤设置的节点。此外，要使节点显示在网络交互图上，它必须与另一个显示的节点有连接（链接）。如果根据指定的过滤参数，网络交互图未显示与某个节点交互的任何节点，则该节点也不会显示在网络交互图上。过滤以相同的方式应用于未知设备的公共节点：如果不是所有与未知设备节点有交互的节点，该节点被排除在未知设备的公共节点的节点列表之外。

如有必要，您可以启用网络交互图来显示与过滤节点相关的所有节点。所有曾经交互过的节点都会和过滤后的节点一起显示（无论当前的过滤条件如何）。

要显示或隐藏与已过滤节点关联的节点：

使用网络交互图上方工具栏中的**“链接设备”**切换开关。

过滤链接

本节提供有关过滤链接的说明。

按严重性分数过滤链接

要按关键性分数过滤网络交互图上的链接：

1. 在网络交互图上方的工具栏中，打开“**链接分数**”下拉列表。

   将显示事件严重性级别和范围的列表：低（0.0-3.9）、中（4.0-7.9）、高（8.0-10.0）；以及**无事件**项，其可让您过滤没有注册事件的链接。

2. 在下拉列表中，选中要按其进行过滤的严重性级别的复选框。

3. 单击“**确定**”。

网络交互图仅显示与具有所选严重性级别的事件相关的链接。

按通信协议过滤链接

要按通信协议过滤网络交互图上的链接：

1. 在网络交互图上方的工具栏中，打开“**协议**”下拉列表。

   这将打开一个窗口，其中显示以协议堆栈树形式显示的协议表。您可以使用包含下一层协议的协议名称旁边的 **+** 和 **-** 按钮来控制树节点的显示。

   表列包含以下信息：

   - **协议**是协议栈树中协议的名称。
   - **EtherType** 是以太网协议封装的下一层协议的编号（如果该协议有指定的编号）。以十进制格式显示。
   - **IP 编号**是 IP 协议封装的下一层协议的编号（如果该协议有指定的编号）。仅为属于 IP 协议结构的协议指定。以十进制格式显示。

2. 如有必要，请使用表格上方的搜索栏查找所需的协议。

3. 在协议列表中，选中要在搜索条件中使用的协议的复选框。

   如果选中或清除包含嵌套协议的协议的复选框，则也会自动选中或清除所有嵌套协议的复选框。

4. 单击“**确定**”。

网络交互图仅显示使用所选协议的链接。

按 OSI 模型层过滤链接

您可以按照与 Open Systems Interconnection (OSI) 网络协议栈的层相对应的交互层来过滤链接。

要根据 OSI 网络模型的层次过滤网络交互图上的链接，请执行以下操作：

1. 在网络交互图上方的工具栏中，打开“**OSI 模型层**”下拉列表。

将显示 OSI 模型层名称列表：

- **数据链接**。该层包括使用 MAC 地址与设备通信的连接。
- **网络**。该层包括使用 IP 地址与设备通信的连接。

2. 在下拉列表中，选中其链接需要在网络交互图上显示的 OSI 模型层的复选框。
3. 单击“**确定**”。

只有属于所选 OSI 模型层的链接才会显示在网络交互图上。

重置过滤条件

您可以将指定的节点和链接过滤条件重置为其默认条件。

要重置网络交互图上定义的过滤器设置，请执行以下操作：

在网络交互图上方的工具栏中，单击“**默认过滤器**”（如果指定了非默认过滤条件，则显示该按钮）。

网络交互图将显示在指定时间段内检测到通信的所有节点和链接。

保存和加载网络交互图的显示设置

本节包含有关管理网络交互图的显示设置的信息。

应用程序允许您保存网络交互图的当前显示设置。一组可保存的显示设置称为*视图*。您可以使用视图应用保存的网络交互图的显示设置（例如，在进行某些更改后快速恢复显示设置，或在不同计算机上使用网络交互图）。

当保存了网络交互图视图时，会保存以下显示设置：

- 缩放级别
- 网络交互图定位
- 固定节点和组的位置
- 节点和链接的过滤

您最多可以保存并使用 10 个视图。

只有具有“管理员”角色的用户可以管理视图列表（包括将当前显示设置保存为视图）。然而，所有具有“管理员”、“安全审计员”、“高级安全官”和“安全官”角色的用户都可以查看视图列表并将视图应用到网络交互图。

添加新视图并保存网络交互图的当前显示设置

要i添加新视图并保存网络交互图的当前显示设置

1. 使用“**管理员**”凭据登录 Kaspersky Anti Targeted Attack Platform Web 界面。
2. 在应用程序 Web 界面窗口中选择“**网络地图**”部分。
3. 转到“**网络交互图**”选项卡。
4. 单击“**管理视图**”按钮打开“**配置网络地图视图**”窗口。
5. 单击**“添加”**。
6. 在文本框中输入视图的名称。
   您可以使用字母、数字、空格字符和以下特殊字符：`! @ # № $ % ^ & ( ) [ ] { } ' , . - _`。
   视图名称必须满足以下要求：
   - 以空格以外的任意字符开始和结束。
   - 最多包含 100 个字符。
   - 不重复使用另一个视图的名称（不区分大小写）。
7. 单击文本框右侧的 ✓ 图标。

刷新视图并保存网络交互图的当前显示设置

要更新视图并保存网络交互图的当前显示设置

1. 使用“**管理员**”凭据登录 Kaspersky Anti Targeted Attack Platform Web 界面。
2. 在应用程序 Web 界面窗口中选择“**网络地图**”部分。
   转到“**网络交互图**”选项卡。
3. 单击“**管理视图**”按钮打开“**配置网络地图视图**”窗口。
4. 选择要保存当前网络交互图显示设置的视图。
5. 单击**“覆盖”**。
   这将打开一个确认提示窗口。
6. 在提示窗口中确认保存所选视图中的当前设置。

重命名网络交互图视图

要重命名视图：

1. 使用“**管理员**”凭据登录 Kaspersky Anti Targeted Attack Platform Web 界面。
2. 在应用程序 Web 界面窗口中选择“**网络地图**”部分。
3. 转到“**网络交互图**”选项卡。
4. 单击“**管理视图**”按钮打开“**配置网络地图视图**”窗口。
5. 选择要重命名的视图。
6. 单击当前视图名称右侧的 图标。
7. 在文本框中输入视图的新名称。
   您可以使用字母、数字、空格字符和以下特殊字符：`! @ # № $ % ^ & ( ) [ ] { } ' , . - _`。
   视图名称必须满足以下要求：
   - 以空格以外的任意字符开始和结束。
   - 最多包含 100 个字符。
   - 不重复使用另一个视图的名称（不区分大小写）。
8. 单击文本框右侧的 图标。

删除网络交互图视图

要删除视图：

1. 使用“**管理员**”凭据登录 Kaspersky Anti Targeted Attack Platform Web 界面。
2. 在应用程序 Web 界面窗口中选择“**网络地图**”部分。
3. 转到“**网络交互图**”选项卡。
4. 单击“**管理视图**”按钮打开“**配置网络地图视图**”窗口。
5. 选择您想删除的视图。
6. 单击“**删除**”。
   这将打开一个确认提示窗口。
7. 在提示窗口中确认删除所选视图。

将视图中保存的设置应用于网络交互图

要将视图中保存的设置应用到网络交互图：

1. 使用“**管理员**”凭据登录 Kaspersky Anti Targeted Attack Platform Web 界面。
2. 在应用程序 Web 界面窗口中选择“**网络地图**”部分。
3. 转到“**网络交互图**”选项卡。
4. 单击“**管理视图**”按钮打开“**配置网络地图视图**”窗口。
5. 在列表中，选择您要应用的视图。
6. 单击“**应用**”。
   这将打开一个确认提示窗口。
7. 在提示窗口中，确认应用所选的视图。

监控网络会话

Kaspersky Anti Targeted Attack Platform 可以扫描流量以检测设备创建的用于连接其他设备的网络会话。应用程序注册检测到的网络会话并保存信息，可帮助您分析设备的网络活动并从流量转储文件下载有关传输的网络数据包的数据。与网络交互图上的链接不同，注册的网络会话允许您获得有关设备交互的更细粒度的信息，部分原因是对用于交互的不同端口和协议的会话进行了独立注册。

如果对资产管理技术启用了网络会话检测方法，则应用程序会检测网络会话。在分析到达监控点的流量时以及接收来自 Endpoint Agent 组件的信息时可以执行网络会话检测。

每个注册的网络会话都包含有关参与交互的两个设备之间的连接的信息。网络会话的特征在于交互方的地址信息（MAC 和/或 IP 地址）、端口号以及用于连接的应用程序协议。网络会话中的第一个设备通常是发起向其他设备发送网络数据包的设备。

您可以在“*Kaspersky Anti Targeted Attack Platform 检测到的协议*”部分查看 Kaspersky Anti Targeted Attack Platform 检测到的完整协议列表。

如果一分钟内没有发送任何网络数据包，或者相关节点或监控点上的网络会话检测技术被禁用，则认为网络会话已关闭。

当检测到过多的网络会话时，应用程序将应用以下会话注册限制：

- 使用同一应用程序协议的两方交互方之间注册的会话数每分钟不得超过1000个。
- 双方注册的会话总数每分钟不得超过5000次。

该应用程序将有关网络会话的信息存储在 Central Node 服务器上的数据库中。存储记录的总量不能超出配置的限制。如果数量超出限制，应用程序会自动删除 10% 的最旧记录。

在分布式解决方案和多租户模式下，SCN 服务器的网络会话信息不会显示在 PCN 上。

网络会话表

要查看网络会话列表：

1. 在应用程序 Web 界面窗口中选择“**网络地图**”部分。
2. 转到“**网络会话**”选项卡。

显示网络会话表。

表包含以下信息：

- “**状态**”是网络会话的状态。注册的网络会话可以具有以下状态之一：
  - **活动**。在注册网络会话时会分配此状态，并且只要设备在此会话内持续发送网络数据包，此状态就会保留。
  - **已关闭**。如果一分钟内没有发送任何网络数据包，或者相关节点或监控点上的网络会话检测技术被禁用，则将此状态分配给网络会话。
- **面 1** 是网络交互一端的 MAC 和/或 IP 地址。可以打开或关闭 MAC 和 IP 地址的显示。
- **面 1 端口**是交互第一端的端口号。
- **面 2** 是网络交互的另一端的 MAC 和/或 IP 地址。可以打开或关闭 MAC 和 IP 地址的显示。
- **面 2 端口**是交互的第二端的端口号。
- **设备 1** 是应用程序已知的设备名称，对应的是交互第一方的地址信息。
- **设备 2** 是应用程序已知的设备名称，对应的是交互的第二方的地址信息。
- **传输协议**是网络会话中使用的传输协议的名称。
- **应用协议**是网络会话中使用的应用层协议的名称。
- **当前速度**是网络会话的当前数据传输速率。
- **平均速度**是网络会话的平均数据传输速率。
- **总传输量**是网络会话期间传输的字节数。
- **监控点**列出了已接收网络会话流量的监控点的名称。
- **开始**是网络会话中第一个网络包的日期和时间，或者是由 EPP 应用程序的数据定义的时间段的开始日期和时间。
- **最后一次交互**是网络会话中最后一个网络包的日期和时间，或者是由 EPP 应用程序的数据定义的时间段的结束日期和时间（如果在网络会话中仅收到一个数据包，则该值与**开始**相同）。
- **数据包数**是网络会话期间传输的网络数据包的数量。

查看网络会话表时，您可以配置、过滤和排序网络会话，以及导航到相关项目和导出数据。

查看网络会话详细信息

有关网络会话的详细信息包括来自网络会话表的信息，以及启动网络会话时处于活动状态的应用程序的名称（如果 Kaspersky Anti Targeted Attack Platform 能够确定应用程序的名称）。

要查看网络会话的详细信息：

1. 在应用程序 Web 界面窗口中选择“**网络地图**”部分。
2. 转到“**网络会话**”选项卡。
3. 单击与相关会话相关的行。

这将打开一个窗口，其中包含有关网络会话的信息。

下载网络会话流量

查看网络会话表时，您可以下载与所选网络会话相关的流量。流量以 PCAP 文件形式下载。为了仅下载您需要的数据，您可以配置网络包过滤。

应用程序从流量转储文件存储中下载网络会话的流量。可以从 Sensor 安装过程中自动创建的内部存储以及已连接的外部存储下载流量。

下载网络会话流量时，请考虑以下事项：

- 仅可下载在分析到达监控点的流量时注册的网络会话的流量。如果网络会话是根据从 Endpoint Agent 组件收到的信息注册的，则您无法下载此类会话的流量。
- 流量转储文件临时存储在存储中，并随着新流量的到来自动删除（轮换周期取决于流量量和应用程序存储配置）。如果相应的流量转储文件已从存储中删除，则您无法下载网络会话的流量。

要下载网络会话流量：

1. 在应用程序 Web 界面窗口中选择“**网络地图**”部分。
2. 转到“**网络会话**”选项卡。
3. 选中您想要下载其流量的网络会话旁边的复选框。

   您最多可以选择 100 个网络会话。
4. 单击“**下载流量**”。

   详细信息区域显示在 Web 界面窗口的右侧。
5. 执行以下操作：

   - 如果您想要下载特定时间段内的流量，请使用“**流量下载期限**”设置来设置界限。

     默认情况下，选择最长可能的期限，从建立最早网络会话的日期和时间开始，到选择的最新会话结束的日期和时间结束。如有必要，您可以在此期限内移动边界，或者为其中一个边界设置一个空值（例如，为右边界设置空值以下载尚未结束的会话的新流量）。

- 在“**下载量限制**”下，设置最大下载流量。

  如果下载的流量超过指定的限制，则会丢弃最新的流量。

- 如有必要，请在**“按监控点过滤”**下启用过滤，并指定获得所需流量的监控点。

  默认情况下，指定获取选定网络会话的流量的监控点。

- 如有必要，请在“**按地址空间过滤”**部分中启用过滤，并指定所选网络会话的网络数据包中的地址所属的地址空间（如果向应用程序添加其他地址空间，则会显示此部分）。

  默认情况下，指定应用程序中创建的所有地址空间。

- 如有必要，请在**“使用 BPF 过滤”**下启用过滤，并输入使用 BPF (Berkley Packet Filter) 技术通过所选网络会话的网络数据包中的地址参数进行过滤的表达式。

  过滤表达式的示例：

  ```
  tcp port 102 or tcp port 502
  ```

- 如有必要，请在“**使用正则表达式过滤**”下启用过滤，并输入正则表达式，以便根据所选网络会话的网络数据包的有效负载数据进行过滤。

  过滤表达式示例：

  ```
  ^test.+xABxCD
  ```

6. 单击**下载**。

7. 如果文件生成需要很长时间（超过 15 秒），则文件生成操作将成为后台操作。在这种情况下，请按照以下步骤下载文件：

   a. 点击应用程序 Web 界面菜单中的 按钮。

   这将打开后台操作列表。

   b. 等待文件生成操作完成。

   c. 单击“**下载文件**”按钮。

您的浏览器保存了下载的文件。根据您的浏览器的设置，屏幕上可能会显示一个窗口，您可以在其中指定下载文件的路径和名称。

搜索网络数据包

您可以查找并查看与所选网络数据包相关的流量。如果有必要，您可以下载发现的流量的转储。

要查找与选定的网络数据包相关的流量：

1. 在应用程序 Web 界面窗口中选择“**网络地图**”部分。

2. 转到“**网络会话**”选项卡。

3. 单击“**在数据包中搜索**”。

   这将打开带有网络数据包搜索设置的窗口。

4. 执行以下操作：

   - 在“**要下载的流量期限**”字段中，设置您想要搜索网络数据包的范围。
   - 如有必要，请在**“使用 BPF 过滤”**下启用过滤，并输入使用 BPF (Berkley Packet Filter) 技术通过所选网络会话的网络数据包中的地址参数进行过滤的表达式。BPF 过滤表达式的写入格式为 libpcap。有关语法的更多详细信息，请参阅 pcap-filter 手册页。

     过滤表达式的示例：
     ```
     tcp port 102 or tcp port 502
     ```
   - 如有必要，请在“**使用正则表达式过滤**”部分启用过滤，并输入基于网络数据包中的有效负载数据进行过滤的表达式。

     过滤表达式示例：
     ```
     ^test.+xABxCD
     ```
   - 如果需要，请在**“按监控点过滤”**下启用过滤，并指定要从中获取流量的监控点。
   - 如有必要，请在**“按地址空间过滤”**下启用过滤，并指定网络数据包中的地址所属的地址空间。

5. 单击“**搜索**”。

   表格显示符合过滤条件的数据。

6. 如果您想要下载找到的网络数据包的转储，请单击“**下载**”。

   原始网络流量转储以 PCAP 格式下载。

预配置网络包搜索规则

您可以使用使用 BPF 和正则表达式的预配置规则在流量中进行搜索。

要使用预配置规则搜索网络数据包：

1. 在应用程序 Web 界面窗口中选择“**网络地图**”部分。
2. 转到“**网络会话**”选项卡。
3. 单击“**在数据包中搜索**”。

   这将打开带有网络数据包搜索设置的窗口。
4. 在“**要下载的流量期限**”字段中，设置您想要搜索网络数据包的范围。
5. 在下表中，从“**使用 BPF 过滤**”或“**使用正则表达式过滤**”列中复制一个过滤表达式，并将其粘贴到 Web 界面的相应部分，以便在网络数据包中进行搜索。
6. 单击“**搜索**”。

   表格显示符合过滤条件的数据。

预配置的规则如下表所列。

规则目的	使用 BPF 进行过滤	使用正则表达式进行过滤
按 IP 地址搜索流量	host <地址>	
搜索两台主机之间的流量	host <地址 1> and host <地址 2>	
搜索单个 TCP 会话的流量	tcp <端口 1> and host <地址 1> and tcp <端口 2> and host <地址 2>	
按多个 IP 地址搜索流量	host <地址 1> or host <地址 2> or ... host <地址 N>	
查找来自一组主机的所有 DNS 查询	udp and dst port 53 and (src host <地址 1> or src host <地址 2> or ... src host <地址 N>)	
搜索 HTTP 流量		" HTTP/"
搜索 DNS 流量	udp dst port 53 or tcp dst port 53	
使用针对特定域的 GET 请求搜索 HTTP 流量	tcp port 80 or tcp port 8000 or tcp port 8080 or tcp port 8888	GET.{1,1000}<域>
搜索特定主机的 ICMP 流量	icmp and host <地址>	
搜索以纯文本传输的身份验证数据	tcp port 80 or tcp port 8000 or tcp port 8080 or tcp port 8888 or port ftp or port smtp or port imap or port pop3 or port telnet	"pass=|pwd=|log=|login=|user=|username=|pw=|passw=|passwd=|password=|pass:|user:|username |user|VXNlcm5hbWU6|UGFzc3dvcmQ6|LOGIN |USER|PASS "
搜索主机作为客户端的 TCP 会话	tcp[tcpflags] = tcp-syn and host <address>	
在给定子网中搜索 HTTP 流量	net xx.xx.xx.xx/yy and (port 8080 or port 80)	

规则目的	使用 BPF 进行过滤	使用正则表达式进行过滤
搜索本地交互流量	`ip and src net (10 or 172.16/12 or 192.168/16) and dst net (10 or 172.16/12 or 192.168/16)`	
搜索与互联网上对象交互的流量	`ip and not (src net (10 or 172.16/12 or 192.168/16) and dst net (10 or 172.16/12 or 192.168/16)) and not multicast and not broadcast and not net 169.254/16`	
根据 HTTP 流量中的 UserAgent 字段搜索流量	用户代理：	

Kaspersky Anti Targeted Attack Platform 检测到的协议

Kaspersky Anti Targeted Attack Platform 检测到的协议如下表所示。

Kaspersky Anti Targeted Attack Platform 检测到的协议

类别	协议
链路层协议	ARP
	RARP
	Ethernet I
	Ethernet II
	MPLS
	MPLS multi
	STP
	LLDP

类别	协议
网络层协议	IPv4
	IPv6
	IPv6 encapsulated
	IPX
	IS-IS 通过 IP
	IS-IS 通过 Ethernet I
	IS-IS 通过 Ethernet II
	Loopback
	DHCP
	VRRP
传输层协议	TCP
	UDP
	SCTP
	GRE
	ICMP
	IGMP
	PIM
	PRP
	QTP 通过 UDP
远程访问和管理	RDP
	SSH
	Telnet
	RLOGIN 通过 TCP
	RSH 通过 TCP
	VNC
	AeroAdmin
	AmmyyAdmin
	AnyDesk
	TeamViewer 通过 TCP
	TeamViewer 通过 UDP
	远程实用程序
	Srv Tcp DameWare Mini Remote Control
	Radmin 通过 TCP

类别	协议
数据传输	AFP 通过 TCP
	FTP 通过 TCP
	Tftp 通过 TCP
	Tftp 通过 UDP
	SFTP 通过 TCP
	SMB 通过 UDP
	Smb2 通过 TCP
	Smb2 通过 UDP
	Smb3 通过 TCP
	Smb3 通过 UDP
	BitTorrent
	NFS
名称和网络服务解析	DNS
	DNS LLMNR 通过 TCP
	DNS LLMNR 通过 UDP
	mDNS 通过 UDP
邮件协议	IMAP
	POP3
	SMTP
时间同步	NTP
	PTP
身份验证和目录	Kerberos
	LDAP
	LDP 通过 UDP
	RADIUS
Web 协议和安全	HTTP 通过 TCP
	HTTPS
	WebSocket
	安全套接字层
通信协议	VoIP: SIP
	IRC
	MSNP 通过 TCP
	MSNP 通过 UDP
多媒体和流媒体	Flash Media Server 通过 TCP
	Voice IP: SIP
	MQTT
云和文件共享服务	DropBox sync 通过 UDP
	Napster 通过 TCP

类别	协议
服务和诊断协议	ICMP
	Syslog
	Ident 通过 TCP
	SNMP
路由和高可用性	HSRP 通过 UDP
	GLBP 通过 UDP
	RIP
	EIGRP
隧道和 VPN	L2TP
	PPTP 通过 TCP
	Tor 通过 TCP
	Tor 通过 UDP
应用程序和数据库	Microsoft SQL
	MySQL
	Oracle
	DB2
	Tns 通过 TCP
	Tns 通过 UDP
检测	SSDP 通过 UDP
会话层协议	NetBIOS 通过 TCP
	NetBIOS 通过 UDP
辅助协议	Finger 通过 TCP
专门的协议	Bitcoin 通过 TCP

监控风险

Kaspersky Anti Targeted Attack Platform 可以检测信息系统资源所面临的风险。应用程序根据流量分析结果和接收到的设备信息识别风险。

检测到的风险可属于以下类别：

- 漏洞。检测到的设备漏洞属于此类别。
- 配置问题。此类别包括因配置不正确而导致的安全风险，以及在写入和读取设备配置时泄漏数据的风险。
- 不安全的网络架构。此类别包括与检测到的不安全的网络交互、设备、协议和软件相关的风险；由于授权设备处于非活动状态而导致的风险；以及由于 EPP 应用程序在设备上不存在或未完全发挥作用而导致的风险。

每个风险的评分从 0.0 到 10.0。在计算风险评分时，应用程序会考虑与检测到的风险相关的设备的可用信息。在计算分数时，应用程序会考虑设备的重要级别以及与该设备相关的其他风险。*基准分数*被用作计算的初始值。漏洞类别中风险的基本评分遵循通用漏洞评分系统 (CVSS)。对于其余风险类别，基本分数取自风险类型表。

风险信息被上传到 Central Node 上的检测到的风险数据库。数据库中存储的记录总数不能超过指定的限制。如果数量超出限制，应用程序会自动删除 10% 的最旧记录。您可以在配置存储设置时设置检测到的风险信息的最大大小。

检测到的风险数据库的内容显示在应用程序 Web 界面的“**风险**”部分。您还可以在“**资产**”部分的“**设备**”选项卡上查看设备风险概述。

关于漏洞类别中的风险

当应用程序检测到企业 LAN 上受监控设备中的漏洞时，就会记录漏洞风险。*漏洞*是设备软件或硬件中的缺陷，攻击者可以利用该缺陷破坏信息系统或获取未经授权的信息访问。

应用程序通过分析可用的设备信息来检测漏洞。可以帮助识别设备已知漏洞的信息将被与*已知漏洞数据库*中的某些字段进行比较。已知漏洞的数据库已内置于应用程序中。该数据库由卡巴斯基专家维护，包含有关最相关或最常见的设备漏洞的信息。

已知漏洞数据库包含漏洞的描述以及受这些漏洞影响的设备的描述。此外，该数据库还以文本或公共资源链接的形式包含保护系统的建议。已知漏洞数据库包含来自各种来源（可能包括设备和软件供应商以及各种安全组织）的描述和建议。数据库中的描述和建议都是英文的。

应用程序安装后，使用原有的已知漏洞数据库。您可以通过安装更新来使数据库保持最新。

Kaspersky Anti Targeted Attack Platform 将有关设备的可用信息与已知漏洞数据库中描述受漏洞影响的设备的字段进行比较。应用程序使用以下设备信息来检测漏洞：

- **硬件供应商**。
- **硬件型号**。
- **硬件版本**。
- **软件供应商**。如果在设备信息中找不到软件供应商信息， Kaspersky Anti Targeted Attack Platform 将重新使用**硬件供应商**值。
- **软件名称**。如果在设备信息中找不到软件名称， Kaspersky Anti Targeted Attack Platform 将重新使用**硬件型号**值。
- **软件版本**。

在已知漏洞数据库中，设备描述以 CPE (Common Platform Enumeration) 格式存储。应用程序将可用的设备信息与这些描述进行比较，自动将信息转换为 CPE 格式。对于每个漏洞，匹配描述的内容会列在“**匹配的 CPE**”部分的风险详细信息区域中。

识别漏洞的主要参数是其在 Common Vulnerabilities and Exposures (CVE) 列表中的 ID。此识别号称为“*CVE ID*”。如果漏洞尚未有 CVE ID，则指定从其他公共资源获取的带有漏洞描述的 ID。

Kaspersky Anti Targeted Attack Platform 支持获取俄罗斯联邦技术和出口管制局（FSTEC）在信息安全威胁数据库（以下也称为“BDU”）中提供的漏洞 ID 和描述链接。如果下载的漏洞信息包含来自 FSTEC's BDU 的此类信息，则应用程序会以“BDU:<year>-<number>”格式的相应 ID 的形式显示此信息。

持续风险管理流程的实施方案

风险检测功能允许在您的信息系统中实施持续（周期性）风险管理。为了帮助您管理风险，Kaspersky Anti Targeted Attack Platform 提供了有关检测到的风险的信息，您可以使用这些信息采取必要的补救或缓解措施。

持续风险管理流程的实施方案涉及以下步骤：

1. **清点设备清单**

   此步骤使用设备活动检测和设备信息检测方法执行（必须启用这些方法）。此步骤，应用程序会自动检测新设备并更新设备信息。如果未自动检测到网络上的某些设备，则需要手动添加它们或从外部项目导入它们。

   您必须在设备设置中启用自动更新，以获取确定设备分类和操作特性的所有信息（例如，型号和软件版本）。如果由于某种原因无法自动更新此类信息，则必须手动保持此信息的最新状态。

2. **被动或主动扫描时的风险检测**

   应用程序使用有关设备的可用信息被动扫描设备是否存在风险。应用程序还分析公司 LAN 流量中的网络交互以检测风险。风险检测通过风险检测方法实现（必须启用该方法）。

   您还可以主动轮询设备以快速获取其信息。在对设备进行主动轮询时，如果选择了相应的风险分析方法，您还可以检测特定类型的风险。要主动轮询设备，您需要向应用程序添加一个或多个**主动轮询**连接器。

   在更新应用程序已知漏洞数据库后，或者添加或更新用于匹配的设备信息后（例如，保存软件型号和版本信息后），会自动检测漏洞类别的风险。

3. **对检测到的风险进行评分和分类**

   对于检测到的每一个风险，应用程序都会计算一个分数。分数反映风险的严重程度。根据分数，风险的严重程度可以是*低*（分数 0.0–3.9）、*中*（分数 4.0–7.9）或*高*（分数 8.0–10.0）。

   根据严重性级别和分数，并考虑到信息系统中设备的特殊使用方式，您可以根据重要性对检测到的风险进行分类。如果您评估风险不大，则可以手动将其状态从*"活动"*状态（检测后默认分配）更改为*"已接受"*状态，例如，如果无法重现利用漏洞的先决条件。当改变风险状态时，我们建议添加或编辑评论。

   所有需要采取措施的风险都应保持*"活动"*状态。

4. **补救措施**

   在此步骤中，您必须对检测到的风险采取补救或缓解措施。为此，请检查所有检测到的"*活动*"风险，从得分最高的风险开始。在您的信息系统中采取必要的措施（例如，修补设备的漏洞，安装修复该漏洞的软件更新，如果不可能，则将该设备与外部网络隔离）。对于某些风险（例如，漏洞），提供了推荐操作的信息。

   > Kaspersky Anti Targeted Attack Platform 不参与修复检测到的风险。

5. **验证补救措施**

   此步骤与扫描时的风险检测类似。完成此步骤后，风险表中将不再有任何"*活动*"风险。

   对于应用程序在被动扫描期间检测到的大多数风险（例如，漏洞），如果检测这些风险的条件不再满足，应用程序将自动分配*"已修复"*状态。例如，在设备的软件版本发生更改后，应用程序会将因之前指定的漏洞软件版本而注册的漏洞风险分配为*"已修复"*状态。"*已修复*"状态也被分配给已知漏洞数据库中不再具有描述的风险（如果下载更新后从数据库中删除了描述）。

   当设备被移除时，应用程序也会删除与这些设备相关的风险。

   如果修复后，检测风险的条件没有改变（例如，存在漏洞的设备与外部网络隔离，但是该设备的信息没有改变），则可以手动将*"已接受"*状态分配给此风险。当改变风险状态时，我们建议添加或编辑评论。

   某些风险无法自动分配"*已修复*"状态（例如，无法将"*已修复*"自动分配给在设备主动轮询期间检测到的风险）。对于此类风险，您还必须在风险补救完成后手动分配*"已接受"*状态。

   如果某个风险与某个事件相关联，您可以在*将事件状态更改为*"已解决"的同时为该风险分配"*已接受*"状态。

查看风险表

风险表显示在应用程序 Web 界面窗口的"**风险和异常**"部分。

风险设置显示在表格以下列中：

- **类别**。

  风险类别的名称。

- **名称**。

  风险名称。对于漏洞类别的风险，使用检测到的漏洞的 CVE ID（如果没有 CVE ID，则显示从其他带有漏洞描述的公共资源中获取的 ID）。

- **CVE**。

  对于漏洞类别的风险：检测到的漏洞的 CVE ID。

- **BDU**。

  对于漏洞类别的风险：BDU 数据库中漏洞的 ID。如果具有不同 BDU ID 的多个漏洞与具有 CVE ID 的一个漏洞相对应，则该列会列出所有此类 ID。

- **风险 ID**。

  风险的唯一 ID。

- **分数**。

  计算出的风险评分。该数值决定了风险的严重级别。根据严重级别，分数可以用以下颜色之一显示：

  - 红色表示*高*严重级别风险。
  - 黄色表示*中等*严重级别风险。
  - 蓝色表示*低*严重级别风险。

  对于“*活动*”风险，分数的颜色很鲜艳。对于“*已修复*”或“*已接受*”风险，分数颜色较淡。

  在详细信息区域中，此设置称为**“基本分数”**。

- **面 1**。

  网络交互一方的地址信息（针对某些风险类型有提示）。可以分别打开或关闭 MAC 地址和 IP 地址的显示。如果在应用程序中添加了额外的地址空间，则在配置风险表时，可以使用“**显示地址空间**”设置启用或禁用地址空间名称的显示。

- **面 2**。

  网络交互另一方的地址信息（针对某些风险类型有提示）。地址信息的显示可以按照与**面 1** 列相同的方式配置。

- **设备组**。

  检测到风险的设备所在组的名称（包含组本身的名称及其所有父组的名称）。

- **设备**。

  设备的名称和地址。

- **来源**。

  对于漏洞类别的风险：将其信息上传到已知漏洞数据库的来源的名称。在详细信息区域中，此设置称为**“漏洞来源”**。

- **状态**。

当前风险状态。可以有以下状态：

- 首次检测到风险时，默认分配“*活动*”状态（如果风险已被分配“*已修复*”状态，则在重复检测时也会分配）。如果风险当前状态为“*已接受*”，您还可以手动为风险分配“*活动*”状态。
- 如果检测风险的条件不再满足，则会自动分配“*已修复*”状态。
- 如果风险评估为无关紧要，或所采取的补救措施没有导致自动分配“*已修复*”状态，则可以手动将“*已接受*”状态分配给风险。

- **检测于**。
  检测到风险的日期和时间。
- **最后状态更改**。
  上次风险状态发生变化的日期和时间。
- **匹配的 CPE**。
  对于漏洞类别的风险：存储在已知漏洞数据库中的设备描述。这些是与设备表中的设备信息匹配的描述。

查看风险表时，您可以配置、过滤、搜索和排序文件，以及导航到相关项目。

查看风险信息

风险详情包括风险表中的信息以及以下字段：

- **风险类型**是风险类型的代码。
- **描述**是针对风险类型或漏洞指定的描述。
- **基础分数**是计算风险分数的初始值。

对于漏洞类别的风险，以下字段和字段组中会显示附加信息：

- **CVSS 向量**是用于计算 CVSS 漏洞分数的指标记录。
- **攻击条件**是对漏洞被利用所必须满足的条件的描述。
- **影响**是对利用漏洞可能造成的后果的描述。
- **缓解**列出了修复漏洞的建议（例如，有关推荐在设备上安装某个软件版本的信息）。
- **链接**列出了可以提供有关该漏洞的更多信息的公共资源的链接。
- **CVE 历史**列出了漏洞被识别、确认和在公共来源中发布的日期。

要查看风险信息：

1. 在应用程序 Web 界面窗口中选择“**资产**”部分。
2. 转到“**设备**”选项卡。
3. 单击“**风险**”列中的漏洞名称（CVE ID 或其他漏洞 ID）。

   这将打开一个窗口，其中包含有关漏洞的信息。

手动更改风险状态

在管理“**风险和异常**”部分时，您可以手动将任何风险的状态从“*活动*”更改为“*已接受*”，反之亦然。在管理“**资产**”部分时，您只能更改漏洞类别风险的状态，并且只能从“*活动*”更改为“*已接受*”。

在将“*已解决*”状态分配给与该风险关联的事件时，您还可以将“*已接受*”状态分配给风险。

要手动更改风险状态：

1. 打开风险详情区域或风险详情窗口。
2. 打开“**更改状态**”下拉列表。
3. 根据您想要分配给风险的状态，从下拉列表中选择以下选项之一：
   - 如果您想将风险状态从“**活动**”更改为“*已接受*”，请选择“*已接受*”。
   - 如果您想将风险重新分配为**“活动”**状态，则选择“*活动*”。

   这将打开一个确认提示窗口。
4. 如果选定的风险具有相关事件，并且您想要同时将“*已解决*”状态分配给所有这些事件，请选中**“将“已解决”状态分配给所有相关事件”**复选框。

   当使用资产管理技术注册某些类型的事件时，风险可能会与事件相关。
5. 在提示窗口中，单击“**确定**”。

使用设备表时查看风险详细信息

使用设备表时，您可以查看有关在设备上检测到的风险的信息。对于每个具有漏洞类别风险的设备，都会显示检测到的漏洞的名称（作为 CVE ID 或其他漏洞 ID）。如果在设备上检测到其他类别的风险，则会显示该设备的这些风险类别名称。当选择设备时，漏洞名称和风险类别将显示在**“风险”**列和详细信息区域中。

默认情况下，设备表仅显示有关“*活动*”风险的信息。如有必要，您可以在配置设备表时选中“**显示已修复和已接受的风险**”复选框来显示所有风险的信息。

为了表明风险的严重级别，漏洞和类别的名称采用以下颜色：

- 红色表示*高*严重级别风险。
- 黄色表示*中等*严重级别风险。
- 蓝色表示*低*严重级别风险。

对于"*活动*"风险，名称的颜色很鲜艳。对于"*已修复*"或"*已接受*"的风险，名称的颜色较暗。

如果设备存在同一类别的风险，则该类别的名称将以所有风险中严重级别最高的颜色显示。

如果您想查看风险详情，可以点击漏洞名称和类别名称。单击漏洞名称（作为 CVE ID 或其他漏洞 ID）将打开漏洞详细信息窗口。单击风险类别名称将转到经过过滤的风险表，显示该设备所选类别的风险。

查看设备表时，您可以根据风险过滤设备。您还可以通过漏洞名称（作为 CVE ID 或其他漏洞 ID）搜索设备。

配置 NDR 事件类型

*事件类型*决定注册事件时使用的参数：标题、描述、基本分数和注册设置。在 Kaspersky Anti Targeted Attack Platform 中，您可以查看事件类型的设置、编辑某些事件类型的设置以及配置自动保存流量和通过连接器传输已注册事件。

查看事件类型表

应用程序中提供的事件类型显示在应用程序 Web 界面的"**设置**"部分，"**事件类型**"子部分。

事件类型表包含*系统事件类型*。这些事件类型是由应用程序在安装过程中创建的，不能从列表中删除。应用程序中实现的事件注册技术使用不同的系统事件类型集。

在某些系统事件类型的基础上，您可以配置*用户定义的事件设置*，以便在特定情况下注册事件时使用。可以为外部系统技术的事件类型（代码 4000005400）定义用户定义设置，以用于使用 Kaspersky Anti Targeted Attack Platform API NDR 注册事件。

注册事件时，用户定义的设置优先。如果没有用户定义的设置，则使用系统事件类型中定义的设置。

以下设置可用于事件类型：

- **代码** – 事件类型的唯一编号（标识符）。在事件类型表中，编号与事件标题一起显示在"**代码和标题**"列中。在已注册事件表中，事件类型 ID 显示在"**事件类型**"列中。
- **标题** – 以文本和/或变量形式呈现的事件标题的内容。系统事件类型可以使用仅特定于这些类型事件的变量，或者一般变量，这些也可以在用户自定义设置中使用。在事件类型表中，标题的内容与事件类型编号一起显示在"**代码和标题**"列中。在已注册事件表中，标题文本和/或接收到的变量值显示在"**标题**"列中。
- **基本分数** – 用于计算注册事件的分数的初始值。如果一个事件类型可以有不同的基本分数，则会显示最大值。此设置显示在事件类型表中。
- **技术** – 用于事件注册的技术。此设置显示在事件类型表中。

- **描述** – 描述事件类型的附加文本。与标题类似，可以包含变量。此设置不会显示在事件类型表中。您可以在所选事件类型的详细信息区域中查看描述。在已注册事件表中，描述文本和/或变量结果值显示在“**描述**”列中。

- **<收件人连接器名称>** – 应用程序用于将事件转发到第三方系统的连接器的名称。该应用程序仅向第三方系统发送配置为通过连接器发送的类型的事件。每个连接器（通过该连接器配置将事件转发到第三方系统）都显示在风险类型表的单独列中。此设置不会显示在所选事件类型的详细信息区域中。

- **事件再生期** – 事件可再次注册的最长时间。如果在指定的时间段过去之前重复事件注册的条件，则不注册新的事件，但是会增加先前注册的事件的重复次数的计数器，并且会更新事件最后发生的日期和时间。在此期限结束后，当注册事件的条件再次出现时，应用程序将注册该类型的新事件。再生期从最后一次注册此类事件的时刻开始计算。例如，如果再生周期设置为 8 小时，并且注册此事件的条件在前一个事件发生两小时后再次出现，则不会注册新事件。如果在 8 小时或更晚之后检测到该情况，则会记录新事件。此设置不会显示在事件类型表中。您可以在所选事件类型的详细信息区域中查看和配置此设置。

  对于已注册的事件，再生期可能比配置的早到期。如果事件被分配了 *“已解决”*状态，或者 Central Node 计算机重新启动，则允许在配置的时间之前重复注册事件。

- **保存流量** – 此设置启用或禁用在注册事件时自动保存流量。此设置不会显示在事件类型表中。您可以在所选事件类型的详细信息区域中查看和配置此设置。

  如果禁用了流量的自动保存，则可以在注册此类事件后一段时间手动下载流量。当应用程序收到下载流量的请求时，它会在其临时生成的流量转储文件中搜索网络数据包。如果在流量转储文件中找到必要的网络数据包，则下载这些数据包（首先保存在数据库中）。

查看事件类型表时，您可以使用配置、过滤、搜索和排序功能。

编辑系统事件类型的设置

要编辑系统事件类型的设置：

1. 在应用程序 Web 界面窗口中，选择“**设置**”部分，“**事件类型**”子部分。
2. 在事件类型表中，选择您要编辑的事件类型。

   详细信息区域显示在 Web 界面窗口的右侧。
3. 单击**“编辑”**。
4. 编辑可编辑设置：再生周期和流量节省设置。
5. 单击“**保存**”。

配置自动保存系统事件类型的流量

当编辑事件类型时，您可以启用或禁用注册事件时自动保存流量的功能。如果启用了流量节省，数据库将存储导致事件注册的网络包，以及在注册事件的网络会话中检测到的事件注册之前和之后的数据包。流量节省设置决定节省多少网络数据包以及时间限制。

如果某个事件类型的自动流量节省功能被禁用，并且该事件类型配置了启用流量节省的用户自定义设置，则您只能在注册该类型的事件后的特定时间范围内下载流量。在这种情况下，应用程序使用流量转储文件来下载流量。这些文件会被临时存储，并会在新流量到达时自动删除。从这些文件下载流量时，当您为事件类型启用流量保存时，数据库中将保存与默认配置相同的网络数据包。

仅当注册事件时，应用程序才会在数据库中保存流量。如果在再生期间再次出现注册此事件的条件，则该时刻的流量不会保存在数据库中。

您可以为任何事件类型启用和配置流量节省。

如果为聚合事件（即系统事件类型 8000000001）启用了流量节省，则应用程序在注册聚合事件时会保存所有嵌套事件的流量。保存嵌套事件的流量时，将应用为聚合事件指定的设置。但是，直接为聚合事件中嵌套的事件类型指定的流量节省设置将覆盖为聚合事件指定的设置。也就是说，嵌套事件的流量按照针对这些事件类型指定的设置进行保存，如果没有指定此类设置，则使用聚合事件的设置。

要为事件类型启用和配置流量节省：

1. 在应用程序 Web 界面窗口中，选择“**设置**”部分，“**事件类型**”子部分。
2. 在事件类型表中，选择您要编辑的事件类型。

   详细信息区域显示在 Web 界面窗口的右侧。
3. 单击**“编辑”**。
4. 将“**保存流量**”切换开关设置为“*已启用*”。
5. 配置事件注册之前的流量保存。为此，请在“**事件前的数据包总数**”和/或“**到事件发生的时间（毫秒）**”中指定相关值。零表示未应用该设置。如果在这两个字段中都指定了值，则应用程序将保存与指定值之一匹配的最小数量的数据包。
6. 配置事件注册后的流量保存。为此，请在“**事件后的数据包总数**”和/或“**事件后的时间（毫秒）**”中指定相关值。零表示未应用该设置。如果在这两个字段中都指定了值，则应用程序将保存与指定值之一匹配的最小数量的数据包。

   对于某些技术（特别是是深度包检测），注册后在事件中保存的数据包可能比流量节省设置中配置的要少。这是由于流量监控技术的特殊性造成的。
7. 单击**“保存”**。

配置通过连接器转发事件

配置系统事件类型时，您可以指定希望 Kaspersky Anti Targeted Attack Platform 将已注册事件转发到第三方系统的连接器。Kaspersky Anti Targeted Attack Platform 可以同时通过多个连接器发送事件信息。

要配置通过连接器将事件转发到第三方系统：

1. 在应用程序 Web 界面窗口中，选择“**设置**”部分，“**事件类型**”子部分。
2. 确保事件类型表显示带有您需要的连接器的列。

   如果缺少相关连接器的列，请检查列显示设置。如果连接器尚未被添加到连接器列表中，请添加它。

3. 在事件类型表中，选择要启用或禁用通过连接器转发的事件类型。
   如果您选择单个事件类型，详细信息区域将显示在 Web 界面窗口的右侧。
4. 执行以下操作之一：
   - 如果您选择一种事件类型，请单击详细信息区域中的“**选择连接器**”。
   - 如果选择多种事件类型，请单击窗口上部的“**选择连接器**”。

   这将打开“**事件收件人连接器**”窗口。
5. 选中要将事件转发到第三方系统的连接器旁边的复选框。
6. 单击“**确定**”。

Kaspersky Anti Targeted Attack Platform 中的常见替换变量

您可以使用通用变量来替代 Kaspersky Anti Targeted Attack Platform 中的当前值。您可以在以下设置中使用常用变量：

- 事件注册的用户自定义设置中的事件标题和描述
- 使用电子邮件连接器的事件转发、应用程序消息或审计记录的设置

要将通用变量插入到输入字段中：

开始以 $ 字符开头输入变量的名称，然后从显示的列表中选择通用变量。

通用变量可用于不同设置中的插值，具体取决于变量的用途（见下表）。

用于替换值的常用变量

变量	描述	用法
`$communications`	网络交互描述字符串（每个网络交互一个字符串），指定网络包的协议以及发送者和接收者的地址	• 用于注册事件的用户定义的设置。 • 通过连接器转发事件的设置。
`$dst_address`	网络数据包接收者地址（根据协议提供的信息，可以是 IP 地址、端口号、 MAC 地址和/或其他地址信息）	• 用于注册事件的用户定义的设置。
`$extra.<paramName>`	使用 `AddEventParam` 函数为外部系统或 Lua 脚本添加的附加变量	• 用于注册事件的用户定义的设置。
`$monitoring_point`	其流量导致事件被注册的监控点的名称	• 用于注册事件的用户定义的设置。 • 通过连接器转发事件的设置。
`$occurred`	注册的日期和时间	• 用于注册事件的用户定义的设置。 • 通过连接器转发事件的设置。 • 通过连接器转发应用程序消息的设置。 • 通过连接器转发审计条目的设置。
`$protocol`	记录事件的应用程序层协议的名称	• 用于注册事件的用户定义的设置。
`$src_address`	网络数据包发送方地址（根据协议提供的信息，可以是 IP 地址、端口号、 MAC 地址和/或其他地址信息）	• 用于注册事件的用户定义的设置。
`$technology_rule`	事件中规则的名称。	• 用于注册事件的用户定义的设置。 • 通过连接器转发事件的设置。
`$top_level_protocol`	顶级协议的名称。	• 用于注册事件的用户定义的设置。
`$type_id`	事件类型、应用程序消息或审计条目的代码。	• 用于注册事件的用户定义设置（也可以使用 `$event_type_id` 变量）。 • 通过连接器转发事件的设置。 • 通过连接器转发应用程序消息的设置。 • 通过连接器转发审计条目的设置。
`$closed`	分配“*已解决*”状态时的日期和时间或事件重新生成期间的日期和时间（对于非聚合事件的事件），或事故中包含的最后一个事件的注册日期和时间（对于聚合事件）。	• 通过连接器转发事件的设置。
`$count`	嵌套事件或聚合事件被触发的次数	• 通过连接器转发事件的设置。
`$description`	描述	• 通过连接器转发事件的设置。 • 通过连接器转发应用程序消息的设置。 • 通过连接器转发审计条目的设置。
`$id`	已注册事件、应用程序消息或审计条目的唯一 ID。	• 通过连接器转发事件的设置。 • 通过连接器转发应用程序消息的设置。 • 通过连接器转发审计条目的设置。
`$message_category`	已传输数据的类别（事件、应用程序消息或审计记录）。	• 通过连接器转发事件的设置。 • 通过连接器转发应用程序消息的设置。 • 通过连接器转发审计条目的设置。
`$message_count`	传输的事件、应用程序消息或审计记录的数量。	• 通过连接器转发事件的设置。 • 通过连接器转发应用程序消息的设置。 • 通过连接器转发审计条目的设置。
`$messages`	由包含数据列表的块组成的模板。	• 通过连接器转发事件的设置。 • 通过连接器转发应用程序消息的设置。 • 通过连接器转发审计条目的设置。
`$msg_line_templ`	电子邮件通知字符串模板	• 通过连接器转发事件的设置。 • 通过连接器转发应用程序消息的设置。 • 通过连接器转发审计条目的设置。
`$node`	包含发送数据的已安装应用程序组件的节点。	• 通过连接器转发应用程序消息的设置。 • 通过连接器转发审计条目的设置。
`$result`	审计条目中的操作结果。	• 通过连接器转发审计条目的设置。

$score	事件分数值。	• 通过连接器转发事件的设置。
$severity	事件严重性级别。	• 通过连接器转发事件的设置。
$status	应用程序消息状态	• 通过连接器转发应用程序消息的设置。
$system_process	导致消息被注册的应用程序进程	• 通过连接器转发应用程序消息的设置。
$technology	与事件相关的技术。	• 通过连接器转发事件的设置。
$title	事件标题、消息文本或已注册的操作。	• 通过连接器转发事件的设置。 • 通过连接器转发应用程序消息的设置。 • 通过连接器转发审计条目的设置。
$user	执行注册的操作的用户的名称。	• 通过连接器转发审计条目的设置。

NDR 事件注册技术

Kaspersky Anti Targeted Attack Platform 使用以下技术之一来记录 NDR 事件：

- *入侵检测* (IDS)

  该技术会记录与检测流量异常相关的 NDR 事件，这些异常是攻击的指标（例如，NDR 事件可以记录检测到 ARP 欺骗的指标）。

- *外部* (EXT)

  该技术注册 Kaspersky Anti Targeted Attack Platform 使用 Kaspersky Anti Targeted Attack Platform API 的方法从第三方系统接收的聚合和嵌套 NDR 事件。

- *资产管理* (AM)

  该技术会注册涉及检测流量中或从 EPP 应用程序接收的数据中的设备信息的 NDR 事件（例如，当发现设备具有新的 IP 地址时，可以注册 NDR 事件）。

- *端点保护平台* (EPP)

  该技术会为保护工作站和服务器的卡巴斯基应用程序检测到的威胁注册 NDR 事件（例如，恶意软件检测事件）。

Kaspersky Anti Targeted Attack Platform 中的系统事件类型

为了注册事件，Kaspersky Anti Targeted Attack Platform 使用在应用程序安装期间自动创建的系统事件类型。

每种事件类型都属于一种特定的事件注册技术。

入侵检测技术的系统事件类型

本文介绍了入侵检测技术的系统事件类型（见下表）。

入侵检测 (IDS) 系统事件类型

代码	事件类型标题	注册条件
4000003000	来自 $fileName 集（系统规则集）的规则被触发	来自系统规则集的入侵检测规则被触发。 事件类型的标题和描述中使用了以下变量： • $fileName：规则集的名称 • $category：规则的类别 • $ruleName：规则的名称 • $signature_id：规则的 ID（sid）
4000003001	来自 $fileName 集（用户自定义规则集）的规则被触发	来自用户自定义规则集中的入侵检测规则被触发。 事件类型的标题和描述中使用了以下变量： • $fileName：规则集的名称 • $category：规则的类别 • $ruleName：规则的名称 • $signature_id：规则的 ID（sid） • $action：规则中定义的网络数据包操作类型（Kaspersky Anti Targeted Attack Platform 中不执行 丢弃 或 拒绝 操作）
4000003002	检测到暴力攻击或扫描的迹象	检测暴力破解或扫描攻击的规则被触发。 在事件类型描述中，$ruleName 变量用于规则名称。
4000004001	在 ARP 回复中检测到 ARP 欺骗的症状	检测到 ARP 数据包中存在地址欺骗的迹象：多个与 ARP 请求无关的 ARP 相应。 事件类型的描述中使用了以下变量： • $senderIp: 被欺骗的 IP 地址 • $targetIp：目标主机的 IP 地址 • $attackStartTimestamp：检测到第一个 ARP 相应的时间
4000004002	在 ARP 请求中检测到 ARP 欺骗的症状	检测到 ARP 数据包中存在地址欺骗的迹象：从同一 MAC 地址向不同目的地发出的多个 ARP 请求。 事件类型的描述中使用了以下变量： • $senderIp: 被欺骗的 IP 地址 • $targetIp：目标主机的 IP 地址 • $attackStartTimestamp：检测到第一个 ARP 相应的时间
4000005100	检测到 IP 协议异常: 组装 IP 数据包时发生数据冲突	检测到 IP 协议异常：重叠 IP 数据包片段中的数据不匹配。
4000005101	检测到 IP 协议异常: 超过碎片 IP 数据包大小	检测到 IP 协议异常：重新组装后碎片 IP 数据包的实际总大小超出允许的限制。
4000005102	检测到 IP 协议异常: IP 数据包的初始片段的大小小于预期	检测到 IP 协议异常：IP 数据包的初始片段的大小小于允许的最小值。
4000005103	检测到 IP 协议异常: 误相关片段	检测到 IP 协议异常：正在组装的 IP 数据包的片段包含有关碎片数据包长度的不同信息。
4000002701	检测到 TCP 协议异常: 重叠 TCP 段中的内容替换	检测到 TCP 协议异常：数据包包含不同内容的重叠 TCP 段。
4000000003	测试事件 (IDS)	检测到测试网络数据包（启用了基于规则的入侵检测）。

资产管理技术的系统事件类型

本文介绍了资产管理技术的系统事件类型（见下表）。

资产管理 (AM) 技术的系统事件类型

代码	事件类型标题	注册条件
4000005003	检测到地址为 ' + $owner_ip_or_mac + ' 的新设备'	在资产监控处于监控模式时，会通过检测到的 IP 或 MAC 地址自动添加新设备，而表中的其他设备则未指定该地址。 应用程序在注册该事件的时候，可能会同时为该设备注册"**未经授权的设备**"风险。在这种情况下，风险和事件之间建立了关系。 事件类型的标题和描述中使用了以下变量： • $owner_ip_or_mac – 设备的 IP 或 MAC 地址 • $asset_name – 设备的指定名称 • $assigned_mac – 分配的 MAC 地址（如果已定义） • $owner_ip – 分配的 IP 地址（如果已定义） • $asset_id – 设备的 ID

代码	事件类型标题	注册条件
4000005004	收到关于地址为 ' + $owner_ip_or_mac + ' 的设备的新信息	在资产监控处于监控模式时，设备信息会根据从流量收到的信息自动更新。 事件类型的标题和描述中使用了以下变量： • $owner_ip_or_mac – 设备的 IP 或 MAC 地址 • $asset_name – 设备名称 • $updated_params – 更新信息列表 • $asset_id – 设备的 ID
4000005005	检测到 IP 地址冲突 $owner_ip	在资产监控处于监控模式时，检测到指定 IP 地址的设备未使用该 IP 地址。 事件类型的标题和描述中使用了以下变量： • $owner_ip – IP 地址 • $challenger_asset_name – 使用该 IP 地址的设备名称 • $challenger_mac – 使用该 IP 地址的设备的 MAC 地址 • $asset_name – 在其设置中指定了该 IP 地址的设备的名称 • $owner_mac – 在其设置中指定了该 IP 地址的设备的 MAC 地址 • $challenger_ips_list：使用该 IP 地址的设备的其他 IP 地址列表 • $asset_id – 在其设置中指定了该 IP 地址的设备的 ID • $challenger_id – 使用该 IP 地址的设备的 ID
4000005006	检测到来自地址 $owner_ip_or_mac 的流量，该地址被分配给具有“已存档”状态的设备	在资产监控处于监控模式时，或根据从 EPP 应用程序收到的数据，检测到具有“*已存档*”状态的设备的活动。 应用程序在注册该事件的时候，可能会同时为该设备注册“**未经授权的设备**”风险。在这种情况下，风险和事件之间建立了关系。 事件类型的标题和描述中使用了以下变量： • $owner_ip_or_mac – 设备的 IP 或 MAC 地址 • $asset_name – 设备名称 • $last_seen_timestamp – 设备最后一次出现在网络中的日期和时间 • $asset_id – 设备的 ID
4000005007	检测到具有 MAC 地址 $owner_mac 的设备的新 IP 地址 $new_ip_addr	在资产监控处于监控模式时，检测到设备使用的新 IP 地址。 事件类型的标题和描述中使用了以下变量： • $new_ip_addr – 检测到的 IP 地址 • $owner_mac – 设备的 MAC 地址 • $asset_name – 设备名称 • $owner_ips_list – 设备的其他 IP 地址列表 • $asset_id – 设备的 ID
4000005008	新的 MAC 地址（$owner_mac）被添加到 IP 地址为 $owner_ip 的设备	在资产管理监控模式下，对于仅指定了 IP 地址的网络接口（设备处于“*未授权*”或“*已存档*”状态），会自动添加 MAC 地址。 事件类型的标题和描述中使用了以下变量： • $owner_mac – 检测到的设备的 MAC 地址 • $owner_ip – 设备的 IP 地址 • $asset_name – 设备名称 • $asset_id – 设备的 ID
4000005009	新的 IP 地址 $owner_ip 被添加到 MAC 地址为 $owner_mac 的设备	在资产管理监控模式下，对于仅指定了 MAC 地址的网络接口（设备处于“*未授权*”或“*已存档*”状态），会自动添加 IP 地址。 事件类型的标题和描述中使用了以下变量： • $owner_ip – 检测到的设备的 IP 地址 • $owner_mac – 设备的 MAC 地址 • $asset_name – 设备名称 • $asset_id – 设备的 ID
4000005010	检测到 IP 地址为 $owner_ip 的设备的新 MAC 地址 $new_mac_addr	在资产监控处于监控模式时，检测到设备使用的新 MAC 地址（此设备已禁用地址信息的自动更新）。 事件类型的标题和描述中使用了以下变量： • $new_mac_addr – 检测到的 MAC 地址 • $owner_ip – 设备的 IP 地址 • $asset_name – 设备名称 • $asset_id – 设备的 ID
4000005011	在从 EPP 应用程序接收到的设备数据中检测到 MAC地址 $owner_mac 更改为 $challenger_mac	根据从 EPP 应用程序收到的信息，设备的 MAC 地址已更新。 事件类型的标题和描述中使用了以下变量： • $owner_mac – 设备的旧 MAC 地址 • $challenger_mac – 设备的新 MAC 地址 • $asset_name – 设备名称 • $asset_id – 设备的 ID

代码	事件类型标题	注册条件
4000005012	在从 EPP 应用程序接收的数据中发现设备 $asset_name 的新地址信息	在从 EPP 应用程序接收的数据中发现设备的新地址信息。如果设备地址信息的改变还未被应用程序处理，则会注册此类事件，如事件 4000005009 或 4000005010。 事件类型的标题和描述中使用了以下变量： • $asset_name – 设备名称 • $detected_epp_addresses – 地址信息 • $asset_id – 设备的 ID
4000005013	从 EPP 应用程序接收数据后，在设备地址 $conflicted_epp_assets 中检测到冲突	根据从 EPP 应用程序收到的信息，检测到 Kaspersky Anti Targeted Attack Platform 中多个设备的地址存在冲突。根据来自 EPP 应用程序的信息，这些地址属于同一设备。 事件类型的标题和描述中使用了以下变量： • $conflicted_epp_assets – 检测到具有冲突地址的设备 • $unaccepted_epp_addresses – 属于同一设备的地址
4000005014	从 EPP 应用程序数据添加了子网 $subnet_mask	从 EPP 应用程序获取信息后，新子网会自动添加到已知子网列表中。该子网被添加到一个地址空间，其中数据源可以是从 EPP 应用程序获取信息的集成服务器。如果存在多个这样的地址空间，则选择包含最合适子网的地址空间来自动添加新的嵌套子网。 事件类型的标题和描述中使用了以下变量： • $subnet_mask – 子网地址 • $subnet_type – 子网类型
4000005016	检测到 IP 地址为 $owner_ip 的未授权的 DHCP 服务器	地址为 $owner_ip_or_mac 的 $asset_name 设备（ID：$asset_id）被识别为未经授权的 DHCP 服务器。 事件类型的标题和描述中使用了以下变量： • $asset_id – 设备的 ID • $owner_ip_or_mac – 设备的 IP 或 MAC 地址
4000005017	检测到 IP 地址为 $owner_ip 的未授权的 DHCP 中继	地址为 $owner_ip_or_mac 的 $asset_name 设备（ID：$asset_id）被识别为未经授权的 DHCP 中继。 事件类型的标题和描述中使用了以下变量： • $asset_name – 设备名称 • $owner_ip_or_mac – 设备的 IP 或 MAC 地址
4000005600	检测到地址为 $owner_ip_or_mac 的设备上的用户列表发生变化	在设备上控制用户时检测到用户信息发生变化。 事件类型的标题和描述中使用了以下变量： • $owner_ip_or_mac – 设备的 IP 或 MAC 地址 • $asset_name – 设备名称 • $asset_id – 设备的 ID • $added_asset_users – 已添加的用户列表 • $modified_asset_users – 修改的用户列表 • $removed_asset_users – 已删除的用户列表
4000005601	在地址为 $owner_ip_or_mac 的设备上的应用程序列表中检测到更改	在监控设备上的应用程序和补丁时检测到有关设备上应用程序的信息被修改。 事件类型的标题和描述中使用了以下变量： • $owner_ip_or_mac – 设备的 IP 或 MAC 地址 • $asset_name – 设备名称 • $asset_id – 设备的 ID • $added_asset_apps – 已添加的应用程序列表 • $removed_asset_apps – 已删除的应用程序列表
4000005602	在地址为 $owner_ip_or_mac 的设备上检测到补丁列表中的更改	在监控设备上的应用程序和补丁时检测到设备补丁信息被修改。 事件类型的标题和描述中使用了以下变量： • $owner_ip_or_mac – 设备的 IP 或 MAC 地址 • $asset_name – 设备名称 • $asset_id – 设备的 ID • $added_asset_patches – 已添加补丁的列表 • $removed_asset_patches – 已删除补丁的列表
4000005603	在设备上的配置组件 $inventory_loc_key 中检测到更改	在监控设备配置时，根据设备扫描结果与以前的配置进行比较时检测到配置组件中的更改（对于在“**仅更新**”和/或“**存档版本**”配置处理模式下运行的作业）。 事件类型的标题和描述中使用了以下变量： • $inventory_loc_key – 配置组件的名称 • $device_config_inventory_changed_format – 在配置组件中检测到的更改
4000005604	与设备上的参考配置组件 $inventory_loc_key 相比检测到差异	监控设备配置时，根据设备扫描结果发现与参考配置组件相比存在差异（对于在“**与基准比较**”配置处理模式下运行的作业）。 事件类型的标题和描述中使用了以下变量： • $inventory_loc_key – 配置组件的名称 • $device_config_diverged_format – 与参考配置组件相比检测到差异

代码	事件类型标题	注册条件
4000005700	远程连接设备时检测到公钥不匹配	远程连接到设备时，检测到收到的设备公钥与应用程序中存储的值不匹配。设备扫描已取消。 事件类型的描述中使用了以下变量： • $asset_name – 设备名称 • $new_asset_sshpublickey – 收到的公钥 • $old_asset_sshpublickey – 存储的公钥
4000005701	设备主动轮询期间检测到公钥不匹配	在主动轮询设备时，检测到接收到的设备公钥与应用程序中存储的值不匹配。已取消该设备的主动轮询。 事件类型的描述中使用了以下变量： • $asset_name – 设备名称 • $new_asset_sshpublickey – 收到的公钥 • $old_asset_sshpublickey – 存储的公钥
4000000004	测试事件 (AM)	检测到测试网络数据包（启用了设备活动检测方法）。

外部系统技术的系统事件类型

本文介绍了外部系统技术的系统事件类型（见下表）。

外部系统 (EXT) 技术的系统事件类型

代码	事件类型标题	注册条件
8000000001	聚合事件	检测到满足关联规则条件的事件序列。 当注册聚合事件时，关联规则中的标题和描述将被用作事件的标题和描述。
4000005400	来自外部系统的事件	使用 Kaspersky Anti Targeted Attack Platform API NDR 从外部系统接收的事件。 当注册事件时，标题和描述由外部系统确定。

端点保护平台技术的系统事件类型

本文介绍了 Endpoint Protection Platform 的系统事件类型（见下表）。

使用 Endpoint Protection Platform (EPP) 技术的系统事件类型

代码	事件类型标题	注册条件
4000005500	特定于网络攻击的活动	集成服务器收到有关触发 EPP 应用程序的网络威胁防护组件的信息。 在事件类型的描述中，$epp_event_description 变量被用于来自 EPP 应用程序的信息。
4000005501	连接不受信任的外部设备	集成服务器收到有关触发 EPP 应用程序的设备控制组件的信息。 在事件类型的描述中，$epp_event_description 变量被用于来自 EPP 应用程序的信息。
4000005502	尝试运行未经授权或不受信任的应用程序	集成服务器收到有关触发 EPP 应用程序的设备控制组件的信息。 在事件类型的描述中，$epp_event_description 变量被用于来自 EPP 应用程序的信息。
4000005503	指定监控范围中被禁止的文件操作	集成服务器收到有关触发 EPP 应用程序的文件完整性监控组件的信息。 在事件类型的描述中，$epp_event_description 变量被用于来自 EPP 应用程序的信息。
4000005504	指定监控范围内的文件被修改	集成服务器收到有关触发 EPP 应用程序的基线文件完整性监控组件的信息。 在事件类型的描述中，$epp_event_description 变量被用于来自 EPP 应用程序的信息。
4000005505	网络连接不被防火墙规则允许	集成服务器收到有关触发 EPP 应用程序的防火墙管理组件的信息。 在事件类型的描述中，$epp_event_description 变量被用于来自 EPP 应用程序的信息。

代码	事件类型标题	注册条件
4000005506	指定监视范围内的系统注册表修改	集成服务器接收到有关触发 EPP 应用程序的注册表访问监视器组件的信息。 在事件类型的描述中，$epp_event_description 变量被用于来自 EPP 应用程序的信息。
4000005507	日志分析规则被触发	集成服务器收到有关触发 EPP 应用程序的日志审查组件的信息。 在事件类型的描述中，$epp_event_description 变量被用于来自 EPP 应用程序的信息。
4000005508	尝试利用受保护进程中的漏洞	集成服务器收到有关触发 EPP 应用程序的漏洞保护组件的信息。 在事件类型的描述中，$epp_event_description 变量被用于来自 EPP 应用程序的信息。
4000005509	尝试恶意加密网络文件资源	集成服务器收到了有关触发 EPP 应用程序的反加密勒索组件的信息。 在事件类型的描述中，$epp_event_description 变量被用于来自 EPP 应用程序的信息。
4000005510	尝试连接到 Wi-Fi 网络	集成服务器收到有关触发 EPP 应用程序的 Wi-Fi 控制组件的信息。 在事件类型的描述中，$epp_event_description 变量被用于来自 EPP 应用程序的信息。
4000005512	检测到受感染或可能受感染的对象	集成服务器收到有关触发 EPP 应用程序的实时文件保护组件的信息。 在事件类型的描述中，$epp_event_description 变量被用于来自 EPP 应用程序的信息。
4000005513	Sigma 规则 $sigmaAlertTitle 已触发	集成服务器收到有关触发 Endpoint Agent 组件 Sigma 规则的数据。 事件类型的标题和描述中使用了以下变量： • $sigmaAlertTitle – Sigma 规则名称 • $sigma_detection_type – 检测技术 • $sigma_object_type – 触发 Sigma 规则的对象类型 • $sigma_object_name – 触发 Sigma 规则的对象名称或第一个触发的 Sigma 规则的名称 • $sigma_status – 检测状态

配置风险类型

*风险类型*定义在 Kaspersky Anti Targeted Attack Platform 中注册风险时使用的设置：风险的名称、类别和基本分数。您可以查看风险类型的设置，并在必要时更改某些风险类型的基本分数。

安装后，应用程序使用原始风险类型列表。您可以通过安装更新来更新和添加支持的风险类型。

查看风险类型表

风险类型表显示在应用程序 Web 界面的“**设置**”区域，“**风险类型**”子区域下。

风险类型显示在表格以下列中：

- **代码**。

  风险类型的唯一编号。在已注册风险表中，风险类型的编号显示在所选风险的详细信息区域。

- **名称**。

  风险类型表中显示的风险类型名称。注册风险时，其名称可能与所用风险类型的名称不完全匹配。某些风险类型的名称可能被完全替换为已注册风险的其他名称。例如，具有此类名称的风险类型包括“**外部系统风险**”类型的风险。如果注册了此类风险，应用程序将保留风险信息源中指定的风险名称（例如，在使用 Kaspersky Anti Targeted Attack Platform API NDR 的外部系统中）。

- **类别**。

  风险类别的名称。

- **基本分数**

  用于计算注册风险得分的基线。在注册除外部系统风险外的所有风险时，将应用配置的基本分数。名为**"来自外部系统的风险"**的风险类型的基本分数为零。必须在使用 Kaspersky Anti Targeted Attack Platform API NDR 注册风险的外部系统中指定此类风险的基本分数。

查看风险类型表时，您可以使用配置、过滤、搜索和排序功能。

更改风险类型的基本分数

无法更改名为"**来自外部系统的风险**"的风险类型的基本分数。如果注册了此类风险，则该风险的基本分数必须由风险信息源提供（例如，使用 Kaspersky Anti Targeted Attack Platform API NDR 的外部系统）。

要更改风险类型的基本分数：

1. 在应用程序 Web 界面窗口中，选择"**设置**"部分，"**风险类型**"子部分。
2. 在风险类型表中，选择您想要更改基本分数的风险类型。

   详细信息区域显示在 Web 界面窗口的右侧。
3. 单击**"编辑"**。
4. 输入新的基本分数。
5. 单击**"保存"**。

管理存储风险的设置

您可以更改存储的风险的最大总大小限制。

要更改风险存储设置：

1. 使用应用程序管理员账户登录 Web 界面。
2. 选择"**Sensor 服务器**"部分。
3. 选择 Central Node 服务器的卡。

   详细信息区域显示在 Web 界面窗口的右侧。
4. 单击**"编辑"**。

   在详细信息区域，会显示选项卡，您可以在其中管理服务器的设置。
5. 在"**常规**"选项卡上，转到"**风险**"选项卡并使用"**最大容量**"设置来设置存储风险的大小限制。

   您可以选择大小限制的计量单位：**MB** 或 **GB**。

   编辑值时，还需要考虑到所有大小限制的总和不得超过节点指定的最大存储容量。

6. 如有必要，请使用“**存储时间（天）**”设置启用风险的最短存储时间，并指定最短天数。

7. 单击**“保存”**。

Kaspersky Anti Targeted Attack Platform 中的系统事件类型

为了注册事件，Kaspersky Anti Targeted Attack Platform 使用在应用程序安装期间自动创建的系统事件类型。

每种事件类型都属于一种特定的事件注册技术。

入侵检测技术的系统事件类型

本文介绍了入侵检测技术的系统事件类型（见下表）。

入侵检测 (IDS) 系统事件类型

代码	事件类型标题	注册条件
4000003000	来自 $fileName 集（系统规则集）的规则被触发	来自系统规则集的入侵检测规则被触发。 事件类型的标题和描述中使用了以下变量： • $fileName：规则集的名称 • $category：规则的类别 • $ruleName：规则的名称 • $signature_id：规则的 ID（sid）
4000003001	来自 $fileName 集（用户自定义规则集）的规则被触发	来自用户自定义规则集中的入侵检测规则被触发。 事件类型的标题和描述中使用了以下变量： • $fileName：规则集的名称 • $category：规则的类别 • $ruleName：规则的名称 • $signature_id：规则的 ID（sid） • $action：规则中定义的网络数据包操作类型（Kaspersky Anti Targeted Attack Platform 中不执行 丢弃 或 拒绝 操作）
4000003002	检测到暴力攻击或扫描的迹象	检测暴力破解或扫描攻击的规则被触发。 在事件类型描述中，$ruleName 变量用于规则名称。
4000004001	在 ARP 回复中检测到 ARP 欺骗的症状	检测到 ARP 数据包中存在地址欺骗的迹象：多个与 ARP 请求无关的 ARP 相应。 事件类型的描述中使用了以下变量： • $senderIp: 被欺骗的 IP 地址 • $targetIp：目标主机的 IP 地址 • $attackStartTimestamp：检测到第一个 ARP 相应的时间
4000004002	在 ARP 请求中检测到 ARP 欺骗的症状	检测到 ARP 数据包中存在地址欺骗的迹象：从同一 MAC 地址向不同目的地发出的多个 ARP 请求。 事件类型的描述中使用了以下变量： • $senderIp: 被欺骗的 IP 地址 • $targetIp：目标主机的 IP 地址 • $attackStartTimestamp：检测到第一个 ARP 相应的时间
4000005100	检测到 IP 协议异常: 组装 IP 数据包时发生数据冲突	检测到 IP 协议异常：重叠 IP 数据包片段中的数据不匹配。
4000005101	检测到 IP 协议异常: 超过碎片 IP 数据包大小	检测到 IP 协议异常：重新组装后碎片 IP 数据包的实际总大小超出允许的限制。
4000005102	检测到 IP 协议异常: IP 数据包的初始片段的大小小于预期	检测到 IP 协议异常：IP 数据包的初始片段的大小小于允许的最小值。

代码	事件类型标题	注册条件
4000005103	检测到 IP 协议异常: 误相关片段	检测到 IP 协议异常：正在组装的 IP 数据包的片段包含有关碎片数据包长度的不同信息。
4000002701	检测到 TCP 协议异常: 重叠 TCP 段中的内容替换	检测到 TCP 协议异常：数据包包含不同内容的重叠 TCP 段。
4000000003	测试事件 (IDS)	检测到测试网络数据包（启用了基于规则的入侵检测）。

资产管理技术的系统事件类型

本文介绍了资产管理技术的系统事件类型（见下表）。

资产管理 (AM) 技术的系统事件类型

代码	事件类型标题	注册条件
4000005003	检测到地址为 ' + $owner_ip_or_mac + ' 的新设备'	在资产监控处于监控模式时，会通过检测到的 IP 或 MAC 地址自动添加新设备，而表中的其他设备则未指定该地址。 应用程序在注册该事件的时候，可能会同时为该设备注册"**未经授权的设备**"风险。在这种情况下，风险和事件之间建立了关系。 事件类型的标题和描述中使用了以下变量： • $owner_ip_or_mac – 设备的 IP 或 MAC 地址 • $asset_name – 设备的指定名称 • $assigned_mac – 分配的 MAC 地址（如果已定义） • $owner_ip – 分配的 IP 地址（如果已定义） • $asset_id – 设备的 ID
4000005004	收到关于地址为 ' + $owner_ip_or_mac + ' 的设备的新信息	在资产监控处于监控模式时，设备信息会根据从流量收到的信息自动更新。 事件类型的标题和描述中使用了以下变量： • $owner_ip_or_mac – 设备的 IP 或 MAC 地址 • $asset_name – 设备名称 • $updated_params – 更新信息列表 • $asset_id – 设备的 ID
4000005005	检测到 IP 地址冲突 $owner_ip	在资产监控处于监控模式时，检测到指定 IP 地址的设备未使用该 IP 地址。 事件类型的标题和描述中使用了以下变量： • $owner_ip – IP 地址 • $challenger_asset_name – 使用该 IP 地址的设备名称 • $challenger_mac – 使用该 IP 地址的设备的 MAC 地址 • $asset_name – 在其设置中指定了该 IP 地址的设备的名称 • $owner_mac – 在其设置中指定了该 IP 地址的设备的 MAC 地址 • $challenger_ips_list：使用该 IP 地址的设备的其他 IP 地址列表 • $asset_id – 在其设置中指定了该 IP 地址的设备的 ID • $challenger_id – 使用该 IP 地址的设备的 ID
4000005006	检测到来自地址 $owner_ip_or_mac 的流量，该地址被分配给具有"已存档"状态的设备	在资产监控处于监控模式时，或根据从 EPP 应用程序收到的数据，检测到具有"*已存档*"状态的设备的活动。 应用程序在注册该事件的时候，可能会同时为该设备注册"**未经授权的设备**"风险。在这种情况下，风险和事件之间建立了关系。 事件类型的标题和描述中使用了以下变量： • $owner_ip_or_mac – 设备的 IP 或 MAC 地址 • $asset_name – 设备名称 • $last_seen_timestamp – 设备最后一次出现在网络中的日期和时间 • $asset_id – 设备的 ID
4000005007	检测到具有 MAC 地址 $owner_mac 的设备的新 IP 地址 $new_ip_addr	在资产监控处于监控模式时，检测到设备使用的新 IP 地址。 事件类型的标题和描述中使用了以下变量： • $new_ip_addr – 检测到的 IP 地址 • $owner_mac – 设备的 MAC 地址 • $asset_name – 设备名称 • $owner_ips_list – 设备的其他 IP 地址列表 • $asset_id – 设备的 ID

代码	事件类型标题	注册条件
4000005008	新的 MAC 地址（$owner_mac）被添加到 IP 地址为 $owner_ip 的设备	在资产管理监控模式下，对于仅指定了 IP 地址的网络接口（设备处于“*未授权*”或“*已存档*”状态），会自动添加 MAC 地址。 事件类型的标题和描述中使用了以下变量： • $owner_mac – 检测到的设备的 MAC 地址 • $owner_ip – 设备的 IP 地址 • $asset_name – 设备名称 • $asset_id – 设备的 ID
4000005009	新的 IP 地址 $owner_ip 被添加到 MAC 地址为 $owner_mac 的设备	在资产管理监控模式下，对于仅指定了 MAC 地址的网络接口（设备处于“*未授权*”或“*已存档*”状态），会自动添加 IP 地址。 事件类型的标题和描述中使用了以下变量： • $owner_ip – 检测到的设备的 IP 地址 • $owner_mac – 设备的 MAC 地址 • $asset_name – 设备名称 • $asset_id – 设备的 ID
4000005010	检测到 IP 地址为 $owner_ip 的设备的新 MAC 地址 $new_mac_addr	在资产监控处于监控模式时，检测到设备使用的新 MAC 地址（此设备已禁用地址信息的自动更新）。 事件类型的标题和描述中使用了以下变量： • $new_mac_addr – 检测到的 MAC 地址 • $owner_ip – 设备的 IP 地址 • $asset_name – 设备名称 • $asset_id – 设备的 ID
4000005011	在从 EPP 应用程序接收到的设备数据中检测到 MAC地址 $owner_mac 更改为 $challenger_mac	根据从 EPP 应用程序收到的信息，设备的 MAC 地址已更新。 事件类型的标题和描述中使用了以下变量： • $owner_mac – 设备的旧 MAC 地址 • $challenger_mac – 设备的新 MAC 地址 • $asset_name – 设备名称 • $asset_id – 设备的 ID
4000005012	在从 EPP 应用程序接收的数据中发现设备 $asset_name 的新地址信息	在从 EPP 应用程序接收的数据中发现设备的新地址信息。如果设备地址信息的改变还未被应用程序处理，则会注册此类事件，如事件 4000005009 或 4000005010。 事件类型的标题和描述中使用了以下变量： • $asset_name – 设备名称 • $detected_epp_addresses – 地址信息 • $asset_id – 设备的 ID
4000005013	从 EPP 应用程序接收数据后，在设备地址 $conflicted_epp_assets 中检测到冲突	根据从 EPP 应用程序收到的信息，检测到 Kaspersky Anti Targeted Attack Platform 中多个设备的地址存在冲突。根据来自 EPP 应用程序的信息，这些地址属于同一设备。 事件类型的标题和描述中使用了以下变量： • $conflicted_epp_assets – 检测到具有冲突地址的设备 • $unaccepted_epp_addresses – 属于同一设备的地址
4000005014	从 EPP 应用程序数据添加了子网 $subnet_mask	从 EPP 应用程序获取信息后，新子网会自动添加到已知子网列表中。该子网被添加到一个地址空间，其中数据源可以是从 EPP 应用程序获取信息的集成服务器。如果存在多个这样的地址空间，则选择包含最合适子网的地址空间来自动添加新的嵌套子网。 事件类型的标题和描述中使用了以下变量： • $subnet_mask – 子网地址 • $subnet_type – 子网类型
4000005016	检测到 IP 地址为 $owner_ip 的未授权的 DHCP 服务器	地址为 $owner_ip_or_mac 的 $asset_name 设备（ID：$asset_id）被识别为未经授权的 DHCP 服务器。 事件类型的标题和描述中使用了以下变量： • $asset_id – 设备的 ID • $owner_ip_or_mac – 设备的 IP 或 MAC 地址
4000005017	检测到 IP 地址为 $owner_ip 的未授权的 DHCP 中继	地址为 $owner_ip_or_mac 的 $asset_name 设备（ID：$asset_id）被识别为未经授权的 DHCP 中继。 事件类型的标题和描述中使用了以下变量： • $asset_name – 设备名称 • $owner_ip_or_mac – 设备的 IP 或 MAC 地址

代码	事件类型标题	注册条件
4000005600	检测到地址为 $owner_ip_or_mac 的设备上的用户列表发生变化	在设备上控制用户时检测到用户信息发生变化。 事件类型的标题和描述中使用了以下变量： • $owner_ip_or_mac – 设备的 IP 或 MAC 地址 • $asset_name – 设备名称 • $asset_id – 设备的 ID • $added_asset_users – 已添加的用户列表 • $modified_asset_users – 修改的用户列表 • $removed_asset_users – 已删除的用户列表
4000005601	在地址为 $owner_ip_or_mac 的设备上的应用程序列表中检测到更改	在监控设备上的应用程序和补丁时检测到有关设备上应用程序的信息被修改。 事件类型的标题和描述中使用了以下变量： • $owner_ip_or_mac – 设备的 IP 或 MAC 地址 • $asset_name – 设备名称 • $asset_id – 设备的 ID • $added_asset_apps – 已添加的应用程序列表 • $removed_asset_apps – 已删除的应用程序列表
4000005602	在地址为 $owner_ip_or_mac 的设备上检测到补丁列表中的更改	在监控设备上的应用程序和补丁时检测到设备补丁信息被修改。 事件类型的标题和描述中使用了以下变量： • $owner_ip_or_mac – 设备的 IP 或 MAC 地址 • $asset_name – 设备名称 • $asset_id – 设备的 ID • $added_asset_patches – 已添加补丁的列表 • $removed_asset_patches – 已删除补丁的列表
4000005603	在设备上的配置组件 $inventory_loc_key 中检测到更改	在监控设备配置时，根据设备扫描结果与以前的配置进行比较时检测到配置组件中的更改（对于在“**仅更新**”和/或“**存档版本**”配置处理模式下运行的作业）。 事件类型的标题和描述中使用了以下变量： • $inventory_loc_key – 配置组件的名称 • $device_config_inventory_changed_format – 在配置组件中检测到的更改
4000005604	与设备上的参考配置组件 $inventory_loc_key 相比检测到差异	监控设备配置时，根据设备扫描结果发现与参考配置组件相比存在差异（对于在“**与基准比较**”配置处理模式下运行的作业）。 事件类型的标题和描述中使用了以下变量： • $inventory_loc_key – 配置组件的名称 • $device_config_diverged_format – 与参考配置组件相比检测到差异
4000005700	远程连接设备时检测到公钥不匹配	远程连接到设备时，检测到收到的设备公钥与应用程序中存储的值不匹配。设备扫描已取消。 事件类型的描述中使用了以下变量： • $asset_name – 设备名称 • $new_asset_sshpublickey – 收到的公钥 • $old_asset_sshpublickey – 存储的公钥
4000005701	设备主动轮询期间检测到公钥不匹配	在主动轮询设备时，检测到接收到的设备公钥与应用程序中存储的值不匹配。已取消该设备的主动轮询。 事件类型的描述中使用了以下变量： • $asset_name – 设备名称 • $new_asset_sshpublickey – 收到的公钥 • $old_asset_sshpublickey – 存储的公钥
4000000004	测试事件 (AM)	检测到测试网络数据包（启用了设备活动检测方法）。

外部系统技术的系统事件类型

本文介绍了外部系统技术的系统事件类型（见下表）。

外部系统 (EXT) 技术的系统事件类型

代码	事件类型标题	注册条件
8000000001	聚合事件	检测到满足关联规则条件的事件序列。 当注册聚合事件时，关联规则中的标题和描述将被用作事件的标题和描述。
4000005400	来自外部系统的事件	使用 Kaspersky Anti Targeted Attack Platform API NDR 从外部系统接收的事件。 当注册事件时，标题和描述由外部系统确定。

端点保护平台技术的系统事件类型

本文介绍了 Endpoint Protection Platform 的系统事件类型（见下表）。

使用 Endpoint Protection Platform (EPP) 技术的系统事件类型

代码	事件类型标题	注册条件
4000005500	特定于网络攻击的活动	集成服务器收到有关触发 EPP 应用程序的网络威胁防护组件的信息。 在事件类型的描述中，$epp_event_description 变量被用于来自 EPP 应用程序的信息。
4000005501	连接不受信任的外部设备	集成服务器收到有关触发 EPP 应用程序的设备控制组件的信息。 在事件类型的描述中，$epp_event_description 变量被用于来自 EPP 应用程序的信息。
4000005502	尝试运行未经授权或不受信任的应用程序	集成服务器收到有关触发 EPP 应用程序的设备控制组件的信息。 在事件类型的描述中，$epp_event_description 变量被用于来自 EPP 应用程序的信息。
4000005503	指定监控范围中被禁止的文件操作	集成服务器收到有关触发 EPP 应用程序的文件完整性监控组件的信息。 在事件类型的描述中，$epp_event_description 变量被用于来自 EPP 应用程序的信息。
4000005504	指定监控范围内的文件被修改	集成服务器收到有关触发 EPP 应用程序的基线文件完整性监控组件的信息。 在事件类型的描述中，$epp_event_description 变量被用于来自 EPP 应用程序的信息。
4000005505	网络连接不被防火墙规则允许	集成服务器收到有关触发 EPP 应用程序的防火墙管理组件的信息。 在事件类型的描述中，$epp_event_description 变量被用于来自 EPP 应用程序的信息。
4000005506	指定监视范围内的系统注册表修改	集成服务器接收到有关触发 EPP 应用程序的注册表访问监视器组件的信息。 在事件类型的描述中，$epp_event_description 变量被用于来自 EPP 应用程序的信息。
4000005507	日志分析规则被触发	集成服务器收到有关触发 EPP 应用程序的日志审查组件的信息。 在事件类型的描述中，$epp_event_description 变量被用于来自 EPP 应用程序的信息。
4000005508	尝试利用受保护进程中的漏洞	集成服务器收到有关触发 EPP 应用程序的漏洞保护组件的信息。 在事件类型的描述中，$epp_event_description 变量被用于来自 EPP 应用程序的信息。
4000005509	尝试恶意加密网络文件资源	集成服务器收到了有关触发 EPP 应用程序的反加密勒索组件的信息。 在事件类型的描述中，$epp_event_description 变量被用于来自 EPP 应用程序的信息。
4000005510	尝试连接到 Wi-Fi 网络	集成服务器收到有关触发 EPP 应用程序的 Wi-Fi 控制组件的信息。 在事件类型的描述中，$epp_event_description 变量被用于来自 EPP 应用程序的信息。
4000005512	检测到受感染或可能受感染的对象	集成服务器收到有关触发 EPP 应用程序的实时文件保护组件的信息。 在事件类型的描述中，$epp_event_description 变量被用于来自 EPP 应用程序的信息。

代码	事件类型标题	注册条件
4000005513	Sigma 规则 $sigmaAlertTitle 已触发	集成服务器收到有关触发 Endpoint Agent 组件 Sigma 规则的数据。 事件类型的标题和描述中使用了以下变量： • $sigmaAlertTitle – Sigma 规则名称 • $sigma_detection_type – 检测技术 • $sigma_object_type – 触发 Sigma 规则的对象类型 • $sigma_object_name – 触发 Sigma 规则的对象名称或第一个触发的 Sigma 规则的名称 • $sigma_status – 检测状态

管理 Endpoint Agent 主机信息

用作Endpoint Agent 组件的应用程序安装在组织的 IT 基础架构中的各个计算机（以下也称为“主机”）上。应用程序持续监控在这些主机上运行的进程、活动的网络连接和正在被修改的文件。

具有**高级安全官**、**安全官**、**安全审计员**或者**管理员**角色的用户可以在**Endpoint Agent**选项卡上评估从具有 Endpoint Agent 组件的主机接收数据的频率，该选项卡位于用户可以访问其数据的租户的 Central Node 服务器的 Web 界面窗口中。如果您使用分布式解决方案和多租户模式，PCN 服务器的 Web 界面将为 PCN 以及所有连接的 SCN 显示具有 Endpoint Agent 组件的主机列表。

具有**管理员**角色的用户可以为他们有权访问数据的租户配置显示从具有 Endpoint Agent 的主机接收数据的频率。

如果检测到可疑的网络活动，具有**高级安全官**角色的用户可以为有权访问其数据的租户将任何带有 Kaspersky Endpoint Agent 的主机与网络隔离。在这种情况下，服务器与 Central Node 组件和具有 Endpoint Agent 组件的主机之间的连接不会中断。

为了在 Endpoint Agent 组件出现问题时提供支持，技术支持人员可能会要求您执行以下操作以进行调试（包括在技术支持模式下）：

- 激活扩展诊断信息的收集。
- 修改个体应用程序组件的设置。
- 修改用于存储和发送获取的诊断信息的设置。
- 配置要被拦截并保存到文件的网络流量。

技术支持人员会提供执行这些操作所需的所有信息（步骤顺序说明、要修改的设置、配置文件、脚本、附加的命令行功能、调试模块、特定用途的实用程序和其他资源等），并会告知您出于调试目的所获取的数据的范围。检索到的诊断信息保存在用户的计算机上。检索到的数据不会自动发送到卡巴斯基。

以上列出的操作只能在技术支持专家的指导和监督下进行。未按照本手册或技术支持专家的说明更改应用程序设置，将会导致操作系统变慢或崩溃，降低计算机安全，并可能会影响正在处理的数据的可用性和完整性。

查看具有 Endpoint Agent 组件的主机表

要查看具有 Endpoint Agent 组件的主机表：

1. 在应用程序 Web 界面窗口中选择“**资产**”部分。
2. 转到“**Endpoint Agent**”选项卡。

显示具有 Endpoint Agent 组件的主机表。

如果您使用分布式解决方案和多租户模式，则该表包含有关具有 Endpoint Agent 组件的主机的信息，主机已连接到 PCN 和所有 SCN 服务器。

该表可以显示以下数据：

- Endpoint Agent 组件的活动指示器和主机数量：
  - **严重不活动**是很久以前从其收到最新数据的主机数量。
  - **警告**是长久以前从其收到最新数据的主机数量。
  - **正常活动**是最近从其收到最新数据的主机数量。
- **主机** — 具有 Endpoint Agent 组件的主机的名称。
- **服务器**是具有 Endpoint Agent 组件的主机所连接的服务器的名称。
  如果您使用分布式解决方案和多租户模式，则此字段会显示。
- IP是安装 Endpoint Agent 组件的主机的 IP 地址。
- **操作系统**是安装在具有 Endpoint Agent 组件的主机上的操作系统的版本。
- **版本** — 安装的 Endpoint Agent 组件的版本。
- **活动** — Endpoint Agent 组件的活动指示器。
  - **正常活动**用于最近从其收到最新数据的主机。
  - **警告**用于长久以前从其收到最新数据的主机。
  - **严重不活动**用于很久很久以前从其收到最新数据的主机。
- **最后一次连接**用于 Endpoint Agent 组件上次连接到 Central Node 服务器时的日期和时间。

单击具有主机名的链接将打开一个列表，您可以从其中选择以下操作之一：

- **按照此值进行过滤**。
- **从过滤器中排除**。

- 运行以下任务：
  - **杀死进程**。
  - **删除文件**。
  - **使用唯一的 PID 杀死进程**。
  - **获取文件**。
  - **进行取证**。
  - **隔离文件**。
  - **运行应用程序**。
- **新的防止规则**。
- **从网络隔离**。
- **查找事件**。
- **查找警报**。
- **复制值到剪贴板**。

可用操作列表取决于 Endpoint Agent 组件的类型：适用于 Windows、Linux 或 Mac（有关详细信息，请参阅“*应用程序的操作原则*”部分）。

单击具有 IP 的链接将打开一个列表，您可以从其中选择以下操作之一：

- **按照此值进行过滤**。
- **从过滤器中排除**。
- **查找警报**。
- **复制值到剪贴板**。

如果您仅使用 KATA 功能（KATA 键），则在单击主机名链接后显示的列表中，您可以执行以下操作：

- **查找警报**（显示给具有“**高级安全官**”角色的用户）。
- **按照此值进行过滤**。
- **从过滤器中排除**。
- **复制值到剪贴板**。

单击表格中任何其他列中的链接将打开一个列表，您可以从其中选择以下操作之一：

- **按照此值进行过滤**。
- **从过滤器中排除**。
- **复制值到剪贴板**。

配置具有 Endpoint Agent 组件的主机表的显示

您可以显示或隐藏列并更改具有 Endpoint Agent 组件的主机表中的列顺序。

配置具有 Endpoint Agent 组件的主机表的显示：

1. 在应用程序 Web 界面窗口中选择“**资产**”部分。
2. 转到“**Endpoint Agent**”选项卡。
3. 在表格的标题部分，单击 。
4. 这将打开**定制表格**窗口。
5. 如果要在表中显示列，请选择要在表中显示的参数名称旁边的复选框。
   如果要隐藏表中的参数，请清除该复选框。

   > 必须选择至少一个复选框。

6. 如果要更改表格中列的顺序，请将鼠标光标移动到具有相关参数的行，单击 并将该行移动到新位置。
7. 如果要恢复默认表格显示设置，请单击**默认**。
8. 单击**应用**。

具有 Endpoint Agent 组件的主机表的显示得到配置。

查看有关主机的信息

要查看有关具有 Endpoint Agent 组件的主机的信息：

1. 在应用程序 Web 界面窗口中选择“**资产**”部分。
2. 转到“**Endpoint Agent**”选项卡。
3. 选择您想查看信息的主机。

这将打开一个窗口，其中包含有关主机的信息。

该窗口包含以下信息：

- 推荐组：
  - 单击**警报**链接将打开包含选定主机的筛选条件的**警报**部分。
  - 单击**事件**链接将打开包含选定主机的搜索条件的**威胁搜索**部分。
  - 单击**受防止规则影响的事件**链接将打开包含选定主机和**阻止的应用程序 (防止规则)**事件类型的搜索条件的**威胁搜索**部分。

  如果您仅使用 KATA 功能（KATA 键），则只有“**警报**”链接显示在建议部分。

- 在**详细信息**选项卡上，**主机**部分显示以下信息：
  - **名称**是具有 Endpoint Agent 组件的主机的名称。
  - **IP**是安装 Endpoint Agent 组件的主机的 IP 地址。
  - **操作系统** — 安装了 Endpoint Agent 组件的主机上的操作系统版本。
- 在**详细信息**选项卡上，**Endpoint Agent**部分显示以下信息：
  - **版本** — 安装的 Endpoint Agent 组件的版本。
- **活动**是Endpoint Agent 组件的活动指示器。可能值：
  - **正常活动**用于最近从其收到最新数据的主机。
  - **警告**用于长久以前从其收到最新数据的主机。
  - **严重不活动**用于很久很久以前从其收到最新数据的主机。
- **服务器** — SCN 或 PCN 服务器的名称。仅在分布式解决方案和多租户模式下显示。
- **已连接到服务器** — Central Node 服务器的名称。
- **最后一次连接** — 上次连接到 Central Node、SCN 或 PCN 服务器的时间。
- **授权许可密钥状态** — 例如，“OK”。
- 在**防护规则**选项卡上，您可以查看被阻止在主机上运行或打开的文件的 MD5 或 SHA256 哈希值。将显示以下信息：
  - **名称** — 文件的名称。
  - **状态** — 防护规则的状态。
  - **哈希** — 哈希算法。

  如果您仅使用 KATA 功能（KATA 键），则不显示“**防护规则**”选项卡。

- 在**任务**选项卡上，您可以查看主机上运行了哪些任务。将显示以下信息：
  - **创建时间** – 任务创建日期和时间。
  - **名称** – 任务名称。
  - **详细信息** – 为其创建了任务的文件或数据流的完整路径。
  - **状态** – 任务完成状态。

> 如果您仅使用 KATA 功能（KATA 键），则不显示"**任务**"选项卡。

单击具有主机名的链接将打开一个列表，您可以从其中选择以下操作之一：

- 运行以下任务：
  - **杀死进程**。
  - **删除文件**。
  - **获取文件**。
  - **进行取证**。
  - **隔离文件**。
  - **运行应用程序**。
- **新的防止规则**。
- **从网络隔离**。
- **查找事件**。
- **查找警报**。
- **按照此值进行过滤**。
- **从过滤器中排除**。
- **复制值到剪贴板**。

> 可用操作列表取决于 Endpoint Agent 组件的类型：适用于 Windows、Linux 或 Mac（有关详细信息，请参阅"*应用程序的操作原则*"部分）。

单击具有 IP 的链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **复制值到剪贴板**。

如果您仅使用 KATA 功能（KATA 键），则在单击主机名和 IP 地址链接后显示的列表中，您可以执行以下操作：

- **查找警报**。
- **复制值到剪贴板**。

按主机名筛选和搜索具有 Endpoint Agent 组件的主机

要按主机名筛选或搜索具有 Endpoint Agent 组件的主机：

1. 在应用程序 Web 界面窗口中选择“**资产**”部分。
2. 转到“**Endpoint Agent**”选项卡。
   这将打开主机表。
3. 单击**主机**链接以打开筛选配置窗口。
4. 如果您只想显示隔离的主机，请选择**仅显示隔离的 Endpoint Agent**复选框。
5. 在下拉列表中，选择以下筛选运算符之一：
   - **包含**
   - **不包含**
6. 在输入字段中，指定主机名的一个或多个字符。
7. 要使用不同条件添加筛选条件，请单击 + 并指定筛选条件。
8. 如果要删除筛选条件，请单击该字段右侧的 按钮。
9. 单击**应用**。

筛选配置窗口关闭。

表格将仅显示与您设置的筛选条件相匹配的主机。

您可以同时使用多个筛选器。

根据已与网络隔离的 Endpoint Agent 组件筛选和搜索主机

要筛选或搜索与网络隔离的具有 Endpoint Agent 组件的主机：

1. 在应用程序 Web 界面窗口中选择“**资产**”部分。
2. 转到“**Endpoint Agent**”选项卡。
   这将打开主机表。

3. 单击**主机**链接以打开筛选配置窗口。

4. 选择**仅显示隔离的 Endpoint Agent**复选框。

5. 单击**应用**。

筛选配置窗口关闭。

表格将仅显示与您设置的筛选条件相匹配的主机。

您可以同时使用多个筛选器。

按 PCN 和 SCN 服务器名称筛选和搜索具有 Endpoint Agent 组件的主机

如果使用分布式解决方案和多租户模式，您可以根据主机所连接的 PCN 和 SCN 服务器的名称筛选或查找具有 Kaspersky Endpoint Agent 组件的主机。

要按 PCN 和 SCN 服务器的名称筛选或搜索具有 Endpoint Agent 组件的主机：

1. 在应用程序 Web 界面窗口中选择“**资产**”部分。

2. 转到“**Endpoint Agent**”选项卡。
这将打开主机表。

3. 单击**服务器**链接以打开筛选配置窗口。

4. 选择想要按其筛选或搜索具有 Endpoint Agent 组件的主机的服务器名称旁边的复选框。

5. 单击**应用**。

筛选配置窗口关闭。

表格将仅显示与您设置的筛选条件相匹配的主机。

您可以同时使用多个筛选器。

按计算机 IP 地址筛选和搜索具有 Endpoint Agent 组件的主机

要按在其上安装应用程序的计算机的 IP 地址筛选或搜索具有 Endpoint Agent 组件的主机：

1. 在应用程序 Web 界面窗口中选择“**资产**”部分。
2. 转到“**Endpoint Agent**”选项卡。
   这将打开主机表。
3. 单击 **IP** 链接以打开筛选配置窗口。
4. 在下拉列表中，选择以下筛选运算符之一：
   - **包含**
   - **不包含**
5. 在输入字段中，指定计算机 IP 地址的一个或多个字符。您可以输入 IPv4 格式的 IP 地址或子网掩码（例如，`192.0.0.1` 或 `192.0.0.0/16`）。
6. 要使用不同条件添加筛选条件，请单击 + 并指定筛选条件。
7. 如果要删除筛选条件，请单击该字段右侧的 按钮。
8. 单击**应用**。

筛选配置窗口关闭。

表格将仅显示与您设置的筛选条件相匹配的主机。

您可以同时使用多个筛选器。

按计算机上的操作系统版本筛选和搜索具有 Endpoint Agent 组件的主机

要根据安装在计算机上的操作系统版本筛选或搜索具有 Endpoint Agent 组件的主机：

1. 在应用程序 Web 界面窗口中选择“**资产**”部分。
2. 转到“**Endpoint Agent**”选项卡。
   这将打开主机表。
3. 单击**操作系统**链接以打开筛选设置窗口。

4. 在下拉列表中，选择以下筛选运算符之一：

   - **包含**
   - **不包含**

5. 在输入字段中，指定操作系统版本的一个或多个字符。

6. 要使用不同条件添加筛选条件，请单击 + 并指定筛选条件。

7. 如果要删除筛选条件，请单击该字段右侧的 按钮。

8. 单击**应用**。

   筛选配置窗口关闭。

   表格将仅显示与您设置的筛选条件相匹配的主机。

您可以同时使用多个筛选器。

按组件版本筛选和搜索具有 Endpoint Agent 组件的主机

您可以按 Endpoint Agent 组件的角色中使用的应用程序版本筛选主机。

要按组件版本筛选或搜索具有 Endpoint Agent 组件的主机：

1. 在应用程序 Web 界面窗口中选择“**资产**”部分。

2. 转到“**Endpoint Agent**”选项卡。
   这将打开主机表。

3. 单击**版本**链接以打开筛选设置窗口。

4. 在下拉列表中，选择以下筛选运算符之一：

   - **包含**
   - **不包含**

5. 在输入字段中，指定用作 Endpoint Agent 组件的应用程序版本的一个或多个字符。

6. 要使用不同条件添加筛选条件，请单击 + 并指定筛选条件。

7. 如果要删除筛选条件，请单击该字段右侧的 按钮。

8. 单击**应用**。

   筛选配置窗口关闭。

表格将仅显示与您设置的筛选条件相匹配的主机。

您可以同时使用多个筛选器。

按活动筛选和搜索具有 Endpoint Agent 组件的主机

要按其活动筛选或搜索具有 Endpoint Agent 组件的主机：

1. 在应用程序 Web 界面窗口中选择“**资产**”部分。
2. 转到“**Endpoint Agent**”选项卡。
   这将打开主机表。
3. 单击**活动**链接以打开筛选配置窗口。
   选择一个或多个活动指示器旁边的复选框：
   - **正常活动**，如果您想查找最近从其中接收到最后数据的主机。
   - **警告**，如果您想查找前段时间从其中接收到最后数据的主机。
   - **严重不活动**，如果您想查找很久以前从其中接收到最后数据的主机。
4. 单击**应用**。

筛选配置窗口关闭。

表格将仅显示与您设置的筛选条件相匹配的主机。

您可以同时使用多个筛选器。

为具有 Endpoint Agent 组件的主机快速创建筛选器

要为具有 Endpoint Agent 组件的主机快速创建筛选器：

1. 在应用程序 Web 界面窗口中选择“**资产**”部分。
2. 转到“**Endpoint Agent**”选项卡。
   这将打开主机表。
3. 执行以下操作以便将筛选条件快速添加到正在创建的筛选器中：
   a. 将鼠标光标置于包含您希望将其作为筛选条件添加的表列值的链接上。
   b. 左键单击。
      这将打开要对值执行的操作列表。

c. 在打开的列表中，选择以下操作之一：

- **按照此值进行过滤**，如果您想将该值包含在筛选条件中。
- **从过滤器中排除**，如果您想从筛选条件中排除该值。

4. 如果您想添加多个筛选条件到正在创建的筛选器中，请执行操作以将每个筛选条件快速添加到正在创建的筛选器。

表格将仅显示与您设置的筛选条件相匹配的主机。

为具有 Endpoint Agent 组件的主机重置筛选器

要清除一个或多个筛选条件的 Endpoint Agent 主机筛选器：

1. 在应用程序 Web 界面窗口中选择“**资产**”部分。
2. 转到“**Endpoint Agent**”选项卡。
3. 单击您想清除其筛选条件的表列标题右侧的。

如果要清除多个筛选条件，请执行必要的操作以清除每个筛选条件。

选定筛选器将被清除。

表格将仅显示与您设置的筛选条件相匹配的主机。

删除具有 Endpoint Agent 组件的主机

从**Endpoint Agent**表中删除一台或多台主机：

1. 在应用程序 Web 界面窗口中选择“**资产**”部分。
2. 转到“**Endpoint Agent**”选项卡。
3. 选择要删除的一台或多台主机旁边的复选框。您可以通过选择包含列标题的行中的复选框来选择所有主机。
   控制面板出现在窗口的下部。
4. 单击**删除**。
5. 这将打开操作确认窗口；在该窗口中，单击**是**。

选定的主机将被从**Endpoint Agent**表中移除。

主机被移除后，Kaspersky Anti Targeted Attack Platform 的 Web 界面会发生以下更改：

- 您无法为已移除的主机创建任务、防止规则或网络隔离规则。
- 如果之前为主机创建了防止规则，则其在规则窗口中的名称（**防止于**字段）在主机被移除后隐藏。该规则继续适用。

  如果该主机重新连接到 Central Node 服务器，主机名将在**防止于**字段中被恢复，防护规则将再次对其应用。
- 如果之前为主机创建了网络隔离规则，则该规则将继续应用，直到规则中指定的时间到期。

  当该主机重新连接到 Central Node 时，该规则将被重新应用于该主机。
- 远程主机上被隔离的对象的元数据将被从 Kaspersky Anti Targeted Attack Platform 隔离区中删除。

  当该主机重新连接到 Central Node 服务器时，Kaspersky Anti Targeted Attack Platform 隔离区中对象的元数据**不会**恢复。您可以通过在命令行或 Kaspersky Security Center 中清除主机上的隔离区来避免填满隔离区。有关详细信息，请参阅您在 Endpoint Agent 组件角色中使用的应用程序的帮助。
- 如果对象仅在一台主机上被**隔离文件**任务隔离且该主机已被移除，任务窗口中的**恢复所有**按钮将处于非活动状态，因为文件无法在已移除的主机上恢复。

按被移除主机的名称进行事件搜索仍然可用。

支持的解释器和进程

Kaspersky Endpoint Agent 应用程序通过以下解释器监控脚本的执行：

- cmd.exe
- reg.exe
- regedit.exe
- regedt32.exe
- cscript.exe
- wscript.exe
- mmc.exe
- msiexec.exe
- mshta.exe
- rundll32.exe
- runlegacycplelevated.exe
- control.exe
- explorer.exe
- regsvr32.exe

- wwahost.exe
- powershell.exe
- java.exe 和 javaw.exe（仅当使用 –jar 选项启动时）
- InstallUtil.exe
- msdt.exe
- python.exe
- ruby.exe
- rubyw.exe

有关被 Kaspersky Endpoint Agent 应用程序监控的进程的信息，请参见下表。

进程及其打开的文件扩展名

进程	文件扩展名
winword.exe	rtf doc dot docm docx dotx dotm docb
excel.exe	xls xlt xlm xlsx xlsm xltx xltm xlsb xla xlam xll xlw
powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm
acrord32.exe	pdf

进程	文件扩展名
wordpad.exe	docx pdf
chrome.exe	pdf
MicrosoftEdge.exe	pdf

使用 Endpoint Agent 组件对主机进行网络隔离

在响应威胁时，具有“**高级安全官**”角色的用户可以在事件调查期间隔离包含带有风险的检测对象的主机。

网络隔离本身不是威胁响应操作。当主机的网络隔离处于活动状态时，安全管理人员应自行采取措施调查事件。您可以在创建网络隔离规则时配置主机网络隔离的时长。

如果您使用 Kaspersky Endpoint Agent for Windows 作为 Endpoint Agent 组件，则具有 Kaspersky Endpoint Agent 应用程序版本 3.8 及更高版本的主机可以使用网络隔离。

为确保隔离主机的正常运行，建议满足以下条件：

- 在启用网络隔离规则之前，在主机上创建本地管理员账户或将域账户数据保存到缓存。
- 启用网络隔离规则时，请勿使用 Central Node 组件更改服务器的证书和 IP 地址。

隔离的主机可以通过网络访问以下资源：

- 具有 Central Node 组件的服务器。
- 应用程序数据库更新源（卡巴斯基更新服务器或自定义源）。
- KSN 服务的服务器。
- 主机添加到网络隔离规则排除项。

如果主机上的 Endpoint Agent 组件关闭，以及在打开该组件或使用该组件重新启动计算机后的一段时间内，主机的网络隔离可能会处于非活动状态。

如有必要，您可以通过以下方式之一禁用网络隔离：

- 使用 KEDR API 请求。
- 通过在 Kaspersky Anti Targeted Attack Platform Web 界面中删除网络隔离规则。
- 通过命令行。
  有关通过命令行禁用网络隔离的更多信息，请参阅 Kaspersky Endpoint Security for Windows 帮助。

应用网络隔离时请考虑一些限制。

创建一个网络隔离规则

要创建一个网络隔离规则：

1. 在应用程序 Web 界面窗口中选择“**资产**”部分。
2. 转到“**Endpoint Agent**”选项卡。
   这将打开主机表。
3. 选择您要启用或禁用网络隔离规则的主机。
   这将打开一个窗口，其中包含有关主机的信息。
4. 单击**隔离**。
5. 在**此时间后禁用隔离**字段中，输入以小时为单位的时间（1 到 9999），在此期间主机的网络隔离将处于活动状态。
6. 在**主机隔离规则排除项**设置组中的**流量方向**列表中，选择必须放行的网络流量方向：
   - **传入/传出**。
   - **传入**。
   - **传出**。
7. 在**IP**字段，输入必须放行的网络流量的 IP 地址。

   如果您使用 Kaspersky Endpoint Agent 充当 Endpoint Agent 组件，则可以使用代理服务器将 Kaspersky Endpoint Agent for Windows 与 Kaspersky Anti Targeted Attack Platform 进行连接。当您将此代理服务器添加到排除项时，可通过代理服务器访问的网络资源也被添加到排除项。如果通过代理服务器访问的网络资源已被添加到排除项，但代理服务器本身未被添加到排除项，则此类排除项不起作用。

8. 如果您选择了**传入**或**传出**，请在**端口**字段中输入连接端口。
9. 如果您想添加多个排除项，请单击**添加**并重复上述步骤填写**流量方向**、IP和**端口**字段。
10. 单击**保存**。

    将主机与网络隔离。

您还可以通过在**事件信息**和警报信息中单击隔离<主机名称>链接来创建一个网络隔离规则。

具有**安全审计员**和**安全官**角色的用户无法创建网络隔离规则。

网络隔离功能不适用于使用 Kaspersky Endpoint Security 11.4 for Linux 作为 Endpoint Agent 组件的主机。

添加网络隔离规则中的排除项

要将排除添加到先前创建的网络隔离规则：

1. 在应用程序 Web 界面窗口中选择“**资产**”部分。
2. 转到“**Endpoint Agent**”选项卡。
   这将打开主机表。
3. 从网络隔离规则中选择要为其创建排除项的被隔离主机。
   这将打开一个窗口，其中包含有关主机的信息。
4. 单击**添加到排除项**链接以展开**主机隔离规则排除项**设置组。
5. 选择不得阻止的网络流量方向：
   - **传入/传出**。
   - **传入**。
   - **传出**。
6. 在**IP**字段，输入必须放行的网络流量的 IP 地址。
7. 如果您选择了**传入**或**传出**，请在**端口**字段中输入连接端口。
8. 如果您想添加多个排除项，请单击**添加**并重复上述步骤填写**流量方向**、IP和**端口**字段。单击**保存**。

将添加网络隔离规则排除。

如果您使用 Kaspersky Endpoint Agent for Windows 充当 Endpoint Agent 组件，则可以使用代理服务器将 Kaspersky Endpoint Agent 与 Kaspersky Anti Targeted Attack Platform 进行连接。当您将此代理服务器添加到排除项时，可通过代理服务器访问的网络资源也被添加到排除项。如果通过代理服务器访问的网络资源已被添加到排除项，但代理服务器本身未被添加到排除项，则此类排除项不起作用。

具有**安全审计员**和**安全官**角色的用户无法创建网络隔离规则的排除项。

删除网络隔离规则

要删除网络隔离规则：

1. 在应用程序 Web 界面窗口中选择“**资产**”部分。
2. 转到“**Endpoint Agent**”选项卡。
   这将打开主机表。

3. 单击要删除网络隔离规则的主机的名称以打开该主机的操作菜单。
4. 选择**删除主机隔离规则**操作。
   这将打开操作确认窗口。
5. 单击**是**。

主机的网络隔离规则被删除。

具有**安全审计员**和**安全官**角色的用户无法删除网络隔离规则。

与网络隔离相关的限制

使用网络隔离时存在一些限制：

- 在主机上启用网络隔离规则时，将断开所有当前连接，并且VPN连接将不可用。
- 如果在启用网络隔离规则时应用程序管理员使用 Central Node 组件替换服务器的证书，则无法禁用该规则。
- 该应用程序阻止隔离主机与活动目录服务器的连接。如果操作系统设置需要连接到活动目录服务以进行授权，则隔离主机的用户将无法登录系统。

根据 Kaspersky TAA (IOA) 规则自动从 Kaspersky Endpoint Agent 主机发送文件以供 Sandbox 组件扫描

如果启用了此功能，应用程序可以自动从具有 Endpoint Agent 组件的主机发送文件，以便根据 Kaspersky TAA (IOA) 规则使用 Sandbox 组件进行扫描。文件发送按照以下原则：

1. Kaspersky Anti Targeted Attack Platform 检查事件数据库并标记与 TAA (IOA) 规则匹配的事件。
2. 如果在 TAA (IOA) 规则中找到相关条件，Kaspersky Anti Targeted Attack Platform 将发送文件供 Sandbox 组件进行扫描。

   Sandbox 组件扫描文件的请求不会显示在 Kaspersky Anti Targeted Attack Platform Web 界面中。

3. 根据扫描结果，应用程序可能会创建警报。
   您可以通过按照**详细信息**–**自动发送到 Sandbox**属性筛选警报来查看以此方式创建的警报。

如果启用了自动发送供 Sandbox 组件扫描的文件，组件处理的流量会变得非常大。如果 Sandbox 组件服务器无法支持增加的负载，处理请求队列中的某些对象将被替换为被自动发送进行扫描的处理文件请求。

为了避免从处理请求队列中掉落对象，您可以：

- 部署额外的 Sandbox 服务器。
- 禁用自动发送要由 Sandbox 组件扫描的文件。
- 将最常导致 Kaspersky Anti Targeted Attack Platform 发送文件以供 Sandbox 组件进行扫描的 TAA (IOA) 规则添加到排除项中。

  有关 Kaspersky Anti Targeted Attack Platform发送文件以供 Sandbox 组件进行扫描的最常用规则的信息显示在**按 TAA 规则发送到 Sandbox**小组件中。您可以将此小组件添加到当前布局中。

  > 当您将文件添加到排除项时，根据此规则的事件标记和警报创建也会停止。

下表列出了可以自动发送供 Sandbox 组件进行扫描的文件。

可以自动发送供 Sandbox 组件进行扫描的文件列表

事件类型	文件类型
进程已启动	已启动进程的文件及其父进程的文件。
模块已加载	已加载模块的文件及其父进程的文件。
到远程主机的连接	父进程文件。
阻止的应用程序 (防止规则)	被阻止运行的应用程序的文件及其父进程的文件。
文件已阻止	被阻止运行的文档的文件及其父进程的文件。
文件已更改	已创建、删除或修改的文件和父进程的文件。
系统事件日志	进程文件（仅适用于 Linux）。
注册表已修改	父进程文件。
监听的端口	父进程文件。
驱动程序已加载	加载的驱动程序的文件。
检测	检测到的文件及其父进程的文件（如果有）。
检测处理结果	检测到的文件及其父进程的文件（如果有）。
AMSI 扫描	进程的文件。
进程: 解释文件运行	已启动的文件及其父进程的文件。
进程: 控制台交互式输入	父进程文件。

> 有关被发送供 Sandbox 组件进行扫描的文件的信息不显示在 Kaspersky Anti Targeted Attack Platform Web 界面中。

启用和禁用从具有 Endpoint Agent 组件的主机自动发送文件以供 Sandbox 组件扫描

要启用或禁用自动发送文件以供 Sandbox 组件根据 Kaspersky TAA (IOA) 规则进行扫描：

1. 在应用程序 Web 界面的窗口中，选择**设置**部分的**Endpoint Agent**子部分。
2. 在**自动将文件发送到 Sandbox**下面：
   - 设置“**发送文件**”切换开关至“**已启用**”，如果您想启用文件自动发送功能。
     默认情况下启用此功能。
   - 设置“**发送文件**”切换开关至“**已禁用**”，如果您想禁用文件自动发送功能。
     禁用此功能不会影响 TAA (IOA) 规则的运行；仅自动发送文件会被禁用。
3. 单击**应用**。

根据 Kaspersky TAA (IOA) 规则自动发送要由 Sandbox 组件扫描的文件被启用或禁用。

在分布式解决方案和多租户模式下，根据 PCN 服务器上配置的 Kaspersky TAA (IOA) 规则自动发送文件供 Sandbox 组件扫描的设置也适用于连接到该 PCN 服务器的 SCN 服务器。如有必要，您可以单独启用或禁用每个选定 SCN 服务器上的文件自动发送。

选择扫描 Sandbox 中的对象时要使用的操作系统

具有**高级安全官**角色的用户可以选择一组操作系统作为创建由 Sandbox 组件扫描对象的任务的基础。Sandbox 服务器必须安装与所选集匹配的虚拟机。

您可以查看服务器上部署的 Sandbox 服务器和虚拟机的列表。

具有**安全审计员**角色的用户可以查看Sandbox 服务器列表以及一组操作系统的设置。具有**安全官**角色的用户无法查看此部分。

查看具有 Sandbox 组件的服务器表

具有**安全官**角色无法查看具有 Sandbox 组件的服务器表。

具有**高级安全官**角色可以查看具有 Sandbox 组件的服务器表。

要查看具有 Sandbox 组件的服务器表：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**Sandbox 服务器**子部分。
2. 单击**服务器**选项卡。

一个表格将显示，其中包含 Sandbox 服务器列表。

表包含以下信息：

- **IP 和名称** — 具有 Sandbox 组件的服务器的 IP 地址或完全限定域名。
- **授权** — 连接到 Sandbox 组件的请求的状态。
- **状态** — 与 Sandbox 组件的连接状态。
- **证书指纹** — 具有 Sandbox 组件的服务器的证书指纹。
- **虚拟机** — 在服务器上创建的虚拟机列表。

选择扫描 Sandbox 中的对象时要使用的操作系统

要选择操作系统集：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**Sandbox 服务器**子部分。
2. 前往**设置**选项卡。
3. 在**操作系统集合**下面，选择以下选项之一：
   - **Windows 7、Windows 10**。
   - **CentOS 7.8、Windows 7、Windows 10**。
   - **Astra Linux 1.7、Windows 7、Windows 10**。
   - **自定义**。
4. 如果您选择了**自定义**， 在**集合组成**下面，选择要包含在该集合中的操作系统旁边的复选框。

   如果 Sandbox 服务器上安装了具有这些操作系统的虚拟机，则自定义操作系统将显示在列表中。预设操作系统始终显示在列表中，但如果未部署运行这些操作系统的虚拟机，则**未知**状态会显示在操作系统名称旁边。

Kaspersky Anti Targeted Attack Platform 将根据选定的集合创建扫描 Sandbox 中对象的任务。

如果 Sandbox 服务器上安装的操作系统集与 Central Node 服务器上选择的操作系统集不匹配，则该 Sandbox 服务器不会发送对象以进行扫描。如果有多个 Sandbox 服务器连接到 Central Node 服务器，则应用程序会将对象发送到其安装的操作系统与 Central Node 上选择的集合相匹配的 Sandbox 服务器。

您可以在使用应用程序的过程中更改操作系统集。在这种情况下，您需要确保 Sandbox 服务器的配置满足硬件要求。

在分布式解决方案和多租户模式下，PCN 服务器上配置的操作系统集的设置不会被应用于连接到该 PCN 服务器的 SCN 服务器。您可以单独为每个 PCN 和 SCN 服务器选择操作系统集。

管理任务

在服务器上创建任务、具有**高级安全官**角色的用户对具有连接到服务器的 Endpoint Agent 组件的所有主机有无限制的（root）访问权限。

在应用程序的 Web 界面中，具有**高级安全官**角色的用户可以通过创建和删除任务来管理主机上的文件和应用程序。

在分布式解决方案和多租户模式下，**杀死进程**、**进行取证**、**获取注册表键**、**启动 YARA 扫描**、**管理服务**、**运行应用程序**、**删除文件**、**从隔离区恢复文件**、**隔离文件**任务可以具有以下类型之一：

- **全球** – 在 PCN 服务器上创建。这些任务适用于连接到此 PCN 服务器的主机以及连接到此 PCN 服务器的所有 SCN 服务器。任务属于用户为其使用 Web 界面管理程序的租户。
- **本地**–在 SCN 服务器上创建。这些任务仅适用于连接到此 SCN 服务器的主机。任务属于用户为其使用 Web 界面管理程序的租户。

获取文件、**获取进程内存转储**、**获取 NTFS 图元文件**、**获取磁盘镜像**、**获取内存转储**任务仅在指定主机上运行，无论应用程序运行模式如何。

最长任务执行时间为 24 小时。如果此时任务未完成，则执行暂停。

具有**高级安全官**角色的用户可以管理他们有权访问其数据的租户的所有任务。

具有**安全官**角色的用户无权访问任务。

具有**安全审计员**角色的用户可以查看任务表以及有关所选任务的信息。

查看任务表

任务表包含已创建任务的列表，位于程序 Web 界面窗口的**任务**部分。您可以查看所有任务或仅查看您（当前用户）创建的任务。

您可以显示或隐藏您使用位于窗口右上角的**仅我的**切换开关创建的任务。默认启用显示当前用户创建的任务。

任务表包含以下信息：

- **时间** – 任务创建日期和时间。
- **类型**是任务的类型，具体取决于应用程序的操作模式和在其上创建任务的服务器。

任务可以是以下类型之一：

- **全球** – 在 PCN 服务器上创建。这些任务适用于连接到此 PCN 服务器的主机以及连接到此 PCN 服务器的所有 SCN 服务器。任务属于用户为其使用 Web 界面管理程序的租户。
- **本地**–在 SCN 服务器上创建。这些任务仅适用于连接到此 SCN 服务器的主机。任务属于用户为其使用 Web 界面管理程序的租户。

- **名称** – 任务名称。

  单击具有任务类型名称的链接将打开一个列表，您可以从其中选择以下操作之一：

  - **按照此值进行过滤**。
  - **从过滤器中排除**。
  - **复制值到剪贴板**。

- **详细信息** – 为其创建任务的文件或数据流的完整路径，或共享网络资源的路径。

  单击包含有关文件或数据流路径的信息的链接将打开一个列表，您可以在其中选择以下操作之一：

  - **按照此值进行过滤**。
  - **从过滤器中排除**。
  - **复制值到剪贴板**。

- **服务器** – 具有 PCN 或 SCN 角色的服务器的名称，任务在该服务器上运行。

  如果您使用分布式解决方案和多租户模式，则此字段会显示。

- **主机** – 在其上执行任务的主机名称。

  仅当您使用独立的 Central Node 服务器时才会显示此字段。

- **创建者** – 创建任务的用户名称。

  > 如果只显示当前用户创建的任务，则不显示该列。

- **状态** – 任务完成状态。

  任务可以具有以下状态之一：

  - **等待**。
  - **进行中**。
  - **已完成**。

查看有关任务的信息

查看任务详细信息：

1. 在应用程序 Web 界面窗口中选择**任务**部分。
   这将打开任务表。
2. 选择您想查看信息的任务。

这将打开一个窗口，其中包含有关任务的信息。

根据任务类型，窗口可以包含以下信息：

- **状态** – 任务完成状态。
- **描述**是任务描述。
- **文件路径** – 文件或数据流的路径。
- **信息类型** – 所收集数据的类型。
- **注册表键** – 您想要获取的注册表项的路径。
- **进程 ID** – 进程标识符。
- **掩码** – 数据列表中包含的文件的掩码。
- **图元文件** – 您想要获取的 NTFS 元文件。
- **卷** – 您要从中接收元文件、磁盘镜像或内存转储的驱动器的名称。
- **分享路径**– 共享网络资源的路径。
- **存储的文件** – 因为任务执行收到的文件的链接。
- **最大嵌套级别** – 应用程序搜索文件的文件夹的最大嵌套级别。
- **排除项** – 禁止在其中搜索和扫描文件的文件夹。
- **扫描范围** – 按照 YARA 规则扫描的文件夹。
- **操作** – 为服务执行的操作。
  该应用程序支持以下服务操作：
  - **开始**。
  - **停止**。
  - **暂停**。
  - **恢复**。

- **删除**。
- **修改启动类型**。

- **最大扫描持续时间** – 最大任务执行时间，之后扫描将停止。
- **SHA256** – 要接收的文件的 SHA256 哈希。
- **运行身份** – 使用本地系统名称运行应用程序的选项。
- **创建者** – 创建任务的用户名称。
- **租户**– 租户姓名。仅当使用分布式方案和多租户模式时显示。
- **创建时间** – 创建任务的时间。
- **完成时间** – 任务完成时间。
- **报告** – 选定主机上的任务结果。

创建获取文件任务

您可以从具有 Endpoint Agent 组件的主机检索文件。为此，您必须创建一个获取文件任务。

要下载的文件不得超过 100 MB。如果文件超过 100 MB，任务将结束并出现错误。

要创建获取文件任务：

1. 在应用程序 Web 界面窗口中选择**任务**部分。
   这将打开任务表。
2. 单击**添加**按钮并在**获取数据**下拉列表中选择**文件**。
   这将打开任务创建窗口。
3. 配置以下设置：
   a. **文件路径** – 您想接收的文件的路径。
      如果请求的文件已链接到其他 NTFS 数据流，则运行该任务将生成请求的文件链接到的 NTFS 数据流的所有文件。
      您还可以指定此文件的备用数据流的路径。在这种情况下，您仅接收指定流的文件。

      创建任务时，应用程序不会检查您要接收的文件的指定路径是否有效。

   b. **MD5/SHA256** – 要接收的文件的 MD5- 或 SHA256 哈希。该字段是可选的。
   c. 如果您不想扫描文件，则清除**发送以进行扫描**复选框。
      默认情况下已选择该复选框。
   d. **描述**是任务描述。该字段是可选的。

e. **主机**是主机的名称或 IP 地址。
您只能指定一台主机。

4. 单击**添加**。

将创建获取文件任务。任务创建后自动运行。

通过此任务接收的文件将被放入存储中。如果获取文件任务成功完成，则可以将接收到的文件下载到本地计算机。

如果您使用分布式解决方案和多租户模式，则存档将被放置在 Central Node 服务器的存储中，在**主机**字段中指定的主机已连接该 Central Node 服务器。

您也可以从任务报告窗口下载该文件。

要从任务报告窗口下载文件：

1. 在应用程序 Web 界面窗口中选择**任务**部分。
这将打开任务表。
2. 打开您想复制的获取文件任务。
3. 在**报告**部分，单击主机的名称或 IP 地址。
这将打开一个窗口，其中包含有关文件的信息。
4. 单击**下载**。

该文件将被保存到浏览器下载文件夹中的本地计算机。

具有**安全审计员**角色的用户无法创建获取文件任务。

具有**安全官**角色的用户无权访问任务。

创建取证收集任务

您可以从选定的 Endpoint Agent 主机获取文件、进程和自动运行点的列表。为此，您必须创建取证收集任务。

要创建取证收集任务：

1. 在应用程序 Web 界面窗口中选择**任务**部分。
这将打开任务表。
2. 单击**添加**按钮并在**获取数据**下拉列表中选择**取证**。
这将打开任务创建窗口。

3. 配置以下设置：

a. **信息类型**是所收集数据的类型。选择一项、多项或所有设置旁边的复选框：

- **进程列表**，如果您想获取任务执行时主机上运行的进程列表。
- **自动运行点列表**，如果您想获取自动运行点的列表。

  自动运行点列表包括有关添加到启动文件夹或在注册表的 Run 键中注册的应用程序的信息，以及在带有 Endpoint Agent 组件的主机启动时以及用户登录指定主机上的操作系统时自动运行的应用程序的信息。

  支持的自动运行点列表

  Kaspersky Endpoint Agent 支持收集以下自动运行点的数据：

  - Logon。
  - Run。
  - Explorer。
  - Shell。
  - Office。
  - Internet Explorer®。
  - Tasks。
  - Services。
  - Drivers。
  - Telephony。
  - Cryptography。
  - Debuggers。
  - COM。
  - Session Manager。
  - Network。
  - LSA。
  - Applications。
  - Codecs。
  - Shellex。
  - WMI。
  - Unspecified。

Kaspersky Endpoint Security 支持收集上述自动运行点以及以下内容：

- BootLog
- Browsers
- DriverLog
- EfiLoader
- GroupPolicy
- 登录
- OsLoader
- OsUpdate
- Printer
- Process
- Scheduler

- **文件列表**，如果您想获取任务执行时存储在所选文件夹或所有主机文件夹中的文件列表。

b. 如果您选择了**文件列表**复选框，在**源类型**设置组中选择以下选项之一：

- **所有本地磁盘**，如果您希望文件列表包含任务执行时存储在本地磁盘上所有文件夹中的文件。
- **目录**如果，您希望文件列表包含任务运行时存储在指定文件夹及其子文件夹中的文件。

c. 如果您选择了**目录**，请在**启动目录**字段中指定文件搜索应从其开始的文件夹路径。

您可以使用以下前缀：

- 系统环境变量。
- 用户定义的环境变量。

  使用用户定义的环境变量时，文件列表包含有关设置了指定环境变量的所有用户的文件夹中的文件的信息。如果用户定义的环境变量覆盖系统环境变量，则文件列表将根据系统环境变量的值包含有关文件夹中文件的信息。

d. 在**主机**字段中，输入要向其分配任务的主机的 IP 地址或名称。

您可以指定多个主机。

如果您使用 Kaspersky Endpoint Agent 充当 Endpoint Agent 组件，则取证收集任务只能分配给运行 Kaspersky Endpoint Agent for Windows 版本 3.10 及更高版本的主机。仅具有 Kaspersky Endpoint Agent for Windows 3.12 及更高版本的主机支持获取自动运行点列表。

如有必要，您可以为文件夹中的文件指定以下搜索条件：

- **掩码**是要包含在文件列表中的文件的掩码。
- **备用数据流**是启用在文件列表中记录有关备用数据流的信息的复选框。
  如果请求的文件已链接到其他 NTFS 数据流，则运行该任务将生成请求的文件链接到的 NTFS 数据流的所有文件。
  默认情况下已选择该复选框。
- **最大嵌套级别**是应用程序在其中搜索文件的文件夹的最大嵌套级别。
- **排除项**是要禁止在其中搜索文件信息的文件夹的路径。
- **描述**是任务描述。

4. 单击**添加**。

取证收集任务已创建。任务创建后自动运行。

作为任务的结果，应用程序将 ZIP 存档放置在存储中；存档包含包含所选数据的文件。如果任务成功完成，您可以将存档下载到本地计算机。

具有**安全审计员**角色的用户无法创建取证收集任务。

具有**安全官**角色的用户无权访问任务。

创建注册表项检索任务

您可以从所选具有 Endpoint Agent 组件的主机检索注册表项。为此，您必须创建注册表项检索任务。

要创建注册表项检索任务：

1. 在应用程序 Web 界面窗口中选择**任务**部分。
   这将打开任务表。
2. 单击**添加**按钮并在**获取数据**下拉列表中选择**注册表键**。
   这将打开任务创建窗口。
3. 配置以下设置：
   a. **注册表键** — 您想要获取的注册表项。
      您可以采用以下格式之一输入注册表项：
      - 相对于根密钥。
        例如，\REGISTRY\MACHINE\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator。
      - 相对于根密钥的全名。
        例如，HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator。

- 相对于用缩写代替根密钥的全名。
  例如，HKLM\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator。

  如果要从 HKEY_CURRENT_USER 获取数据，您必须指定 HKEY_USERS 和用户的 SID：HKEY_USERS\<SID of the user>。

b. **描述**是任务描述。该字段是可选的。

c. 在**主机**字段中，输入要向其分配任务的主机的名称或 IP 地址。
   您可以指定多个主机。

   如果您使用 Kaspersky Endpoint Agent 充当 Endpoint Agent 组件，则注册表项检索任务只能分配给运行 Kaspersky Endpoint Agent for Windows 版本 3.13 及更高版本的主机。

4. 单击**添加**。

注册表项检索任务已创建。任务创建后自动运行。

作为任务的结果，应用程序将 ZIP 存档放置在存储中；该存档包含一个 .reg 文件，其中包含所有注册表项以及创建任务时指定的项下的值的列表。您可以将存档下载到本地计算机。

如果任务导致错误，存档文件将包含错误的描述。

具有**安全审计员**角色的用户无法创建此任务。

具有**安全官**角色的用户无权访问任务。

创建 NTFS 元文件检索任务

您可以从所选具有 Endpoint Agent 组件的主机检索 NTFS 元文件。为此，您必须创建 NTFS 元文件检索任务。

要创建 NTFS 元文件检索任务：

1. 在应用程序 Web 界面窗口中选择**任务**部分。
   这将打开任务表。

2. 单击**添加**按钮并在**获取数据**下拉列表中选择**NTFS 元文件**。
   这将打开任务创建窗口。

3. 配置以下设置：

   a. **图元文件**是您可以使用该任务获取的元文件列表。通过选择相应的复选框来选择相关元文件。
      您可以选择多个元文件。

b. **卷**是您要从中获取元文件的磁盘的名称。

默认指定系统盘。您可以以`<drive letter>:`格式输入不同磁盘的路径。

c. **描述**是任务描述。该字段是可选的。

d. **主机**是要向其分配任务的主机的名称或 IP 地址。

您只能指定一台主机。

> 如果您使用 Kaspersky Endpoint Agent 充当 Endpoint Agent 组件，则 NTFS 元文件检索任务只能分配给运行 Kaspersky Endpoint Agent for Windows 版本 3.13 及更高版本的主机。

4. 单击**添加**。

NTFS 元文件创建任务已创建。任务创建后自动运行。

任务完成后，应用程序会将包含所选元文件的 ZIP 存档放置在存储中。您可以将存档下载到本地计算机。

如果任务导致错误，存档文件将包含错误的描述。

如果您使用分布式解决方案和多租户模式，则存档将被放置在 Central Node 服务器的存储中，在**主机**字段中指定的主机已连接该 Central Node 服务器。

> 如果下载选定的图元文件耗尽了存储容量，则存储中的对象将被轮换。如果某图元文件大于总存储容量，则不会下载它。

> 具有**安全审计员**角色的用户无法创建此任务。具有**安全官**角色的用户无权访问任务。

创建进程内存转储检索任务

您可以从所选具有 Endpoint Agent 组件的主机检索进程内存转储。为此，您必须创建进程内存转储检索任务。

创建进程内存转储检索任务：

1. 在应用程序 Web 界面窗口中选择**任务**部分。

这将打开任务表。

2. 单击**添加**按钮并在**获取数据**下拉列表中选择**进程内存转储**。

这将打开任务创建窗口。

3. 配置以下设置：

a. **进程 ID**是要获取其内存转储的进程的 ID。

b. **MD5/SHA256**是要获取其内存转储的进程的文件的 MD5 或 SHA256 哈希值。该字段是可选的。

c. **描述** — 任务描述。该字段是可选的。

d. **主机**是要向其分配任务的主机的名称或 IP 地址。

您只能指定一台主机。

> 如果您使用 Kaspersky Endpoint Agent 充当 Endpoint Agent 组件，则进程内存转储检索任务只能分配给运行 Kaspersky Endpoint Agent for Windows 版本 3.13 及更高版本的主机。

4. 单击**添加**。

创建进程内存转储检索任务。任务创建后自动运行。

该任务会在存储中创建一个 ZIP 存档，其中包含一个包含进程信息的文件和一个进程内存转储文件。您可以将存档下载到本地计算机。

如果任务导致错误，存档文件将包含错误的描述。

如果您使用分布式解决方案和多租户模式，则存档将被放置在 Central Node 服务器的存储中，在**主机**字段中指定的主机已连接该 Central Node 服务器。

> 具有**安全审计员**角色的用户无法创建此任务。

> 具有**安全官**角色的用户无权访问任务。

创建磁盘镜像检索任务

您可以从选定的 Kaspersky Endpoint Agent for Windows 主机检索磁盘镜像。为此，您必须创建 NTFS 磁盘镜像检索任务。

生成的文件只能被保存到共享网络资源。

创建磁盘镜像检索任务：

1. 在应用程序 Web 界面窗口中选择**任务**部分。

这将打开任务表。

2. 单击**添加**按钮并在**获取数据**下拉列表中选择**磁盘镜像**。

这将打开任务创建窗口。

3. 配置以下设置：

a. **分享路径** — 共享网络资源的路径。

您需要以通用命名约定 (UNC) 格式指定路径：`\\server\share\path`。

如果具有指定名称的最后一个文件夹不存在， Kaspersky Endpoint Agent 将创建一个。如果创建不成功，Kaspersky Anti Targeted Attack Platform 的 Web 界面中将显示错误。

b. **用户名称** — 用于访问共享网络资源的账户的用户名。

c. **密码** — 用于访问共享网络资源的账户的密码。

d. 在**磁盘类型**下面，选择以下选项之一：

- **逻辑**。
- **物理的**。

e. 如果您选择了**逻辑**，请输入`% SystemDrive%`变量或驱动器字母，**卷**字段中没有冒号和斜线。

f. 如果您选择了**物理的**，请在**物理驱动器**字段中输入磁盘号。

g. 如果您希望在保存时将文件分为多个部分，请选择**将文件拆分为多个部分**复选框。

h. 如果您选择了该复选框，请在**部分大小，GB**字段中指定已保存文件的一部分的最小大小。
最小部分大小必须大于 1 GB。

i. **描述**是任务描述。该字段是可选的。

j. **主机** — 您想要向其分配任务的主机的 IP 地址或名称。

4. 单击**添加**。

磁盘镜像检索任务将创建。任务创建后自动运行。

应用程序会将包含一个或多个 EWF 或 RAW 格式文件的存档放置在网络共享中。您可以将文件从 RAW 格式转换为 EWF 格式。

如果您使用 Kaspersky Endpoint Agent 充当 Endpoint Agent 组件，则任务只能分配给运行 Kaspersky Endpoint Agent for Windows 版本 3.14 及更高版本的主机。

具有**安全审计员**角色的用户无法创建任务。

具有**安全官**角色的用户无权访问任务。

将文件从 RAW 转换为 EWF 格式

Kaspersky Endpoint Security 以 RAW 格式保存磁盘镜像。文件也可以被压缩到存档中。特殊的 Python 脚本允许将文件从 RAW 格式转换为 EWF 格式。该脚本不断在指定文件夹中查找 RAW 文件。如果检测到此类文件，脚本会自动将文件转换为 EWF 格式。

Convert_to_ewf_monitor.py 脚本

为了使脚本正常工作，计算机上必须安装以下软件：

- 用于访问专家见证压缩格式 (EWF) 文件的 libewf 库。
  libewf 库是开源软件。
  建议将库文件和脚本文件放在同一文件夹中。
- Python 解释器。

要启用磁盘镜像文件的转换：

1. 启动命令行解释器。
2. 更改为脚本所在的文件夹。
3. 运行以下命令：

   ```
   py Convert_to_ewf_monitor.py --source <源文件文件夹的完整路径> [其他设置]
   ```

EWF 转换脚本参数

参数	描述
`--source <文件夹的完整路径>`	脚本在其中查找源文件的文件夹的完整路径。该脚本还会在指定路径的子文件夹中查找文件。这是一个强制参数。
`--destination <文件夹的完整路径>`	脚本在其中保存转换后的文件的文件夹的完整路径。文件夹结构被保留。默认情况下，脚本将转换后的文件保存在 `source` 参数中指定的文件夹中。
`--delete`	转换成功后删除源文件。如果转换失败，脚本会跳过删除源文件，您可以重试。
`--ewftool <文件夹的完整路径>`	ewfacquirestream.exe 文件的完整路径。路径必须包含文件名。默认情况下，脚本尝试在脚本所在的文件夹中查找 ewfacquirestream.exe 文件。
`--name_mask <正则表达式>`	用于查找要转换的源文件的正则表达式。如果您需要转换单个文件，可以使用此选项。默认情况下，该脚本使用 `^diskdump_` 正则表达式查找文件。
`--convert_single_dump`	找到要转换的单个文件。成功转换单个文件后，脚本退出。
`--workers_num <文件数量>`	脚本可以同时转换的源文件的最大数量。您可以使用此设置来优化脚本的性能。默认情况下，该脚本一次最多可以转换四个文件。
`--log_level <日志级别>`	记录级别。默认情况下，脚本使用 DEBUG 日志记录级别。
`--log_path <文件夹的完整路径>`	保存日志文件的完整路径。该路径必须包含日志文件的文件名。默认情况下，脚本在解释器控制台上显示事件。

示例：

```
PS D:\Folder\Script\> py convert_to_ewf_monitor.py --source E:/Folder --destination E:/EWF --delete --log_path
E:/Folder/Logs.txt
```

创建 RAM 转储检索任务

您可以从所选具有 Endpoint Agent 组件的主机检索 RAM 转储。为此，您必须创建内存转储检索任务。

生成的文件只能被保存到共享网络资源。

要创建内存转储检索任务：

1. 在应用程序 Web 界面窗口中选择**任务**部分。
   这将打开任务表。
2. 单击**添加**按钮并在**获取数据**下拉列表中选择**内存转储**。
   这将打开任务创建窗口。
3. 配置以下设置：

   a. **分享路径** — 共享网络资源的路径。
      您需要以通用命名约定 (UNC) 格式指定路径：`\\server\share\path`。

如果具有指定名称的最后一个文件夹不存在， Kaspersky Endpoint Agent 将创建一个。如果创建不成功，Kaspersky Anti Targeted Attack Platform 的 Web 界面中将显示错误。

b. **用户名称** — 用于访问共享网络资源的账户的用户名。

c. **密码** — 用于访问共享网络资源的账户的密码。

d. **描述**是任务描述。该字段是可选的。

e. **主机** — 您想要向其分配任务的主机的 IP 地址或名称。

4. 单击**添加**。

RAM 转储检索任务已创建。任务创建后自动运行。

结果，应用程序会将 RAW 文件或包含 RAW 文件的存档放置在共享网络资源上。

如果您使用 Kaspersky Endpoint Agent 充当 Endpoint Agent 组件，则任务只能分配给运行 Kaspersky Endpoint Agent for Windows 版本 3.14 及更高版本的主机。

具有**安全审计员**角色的用户无法创建任务。

具有**安全官**角色的用户无权访问任务。

创建进程终止任务

如果您认为在计算机上运行的进程可能威胁到计算机或企业 LAN 的安全，您可以终止该进程。

要创建进程终止任务：

1. 在应用程序 Web 界面窗口中选择**任务**部分。
   这将打开任务表。

2. 单击**添加**并选择**杀死进程**。
   这将打开任务创建窗口。

3. 配置以下设置：

   a. **文件路径** — 您想终止的进程文件的路径。
   您还可以指定此文件的备用数据流的路径。在这种情况下，只会终止指定数据流的进程。将执行此文件的其他流的进程。

   b. **MD5/SHA256** — 要终止的进程文件的 MD5- 或 SHA256 哈希。该字段是可选的。

   c. **描述** — 任务描述。该字段是可选的。

d. **任务所有者** – 任务范围：

- 如果您想运行所有服务器上的任务，请选择**所有主机**选项。
- 如果要在选定的服务器上运行任务，请选择**指定服务器**选项并在**服务器**参数名称的右侧选择要在其上运行任务的服务器名称旁边的复选框。

  仅当启用分布式解决方案和多租户模式时，此选项才可用。
- 如果您想运行选定主机上的任务，请选择**指定主机**选项并在**主机**字段中列出这些主机。

4. 单击**添加**。

将创建进程终止任务。任务创建后自动运行。

具有**安全审计员**角色的用户无法创建进程终止任务。

具有**安全官**角色的用户无权访问任务。

创建任务以使用 YARA 规则扫描主机

您可以使用 YARA 规则扫描具有 Endpoint Agent 组件的主机。为此，您必须创建一个**启动 YARA 扫描**任务。您可以创建任务：

- 在**任务**部分。

  在这种情况下，在创建任务时，您必须选择要用于扫描主机的 YARA 规则。
- 在**自定义规则**部分，**YARA**子部分。

  在这种情况下，将创建一个任务来使用选定的 YARA 规则扫描主机。

*要使用 YARA 规则创建扫描具有 Kaspersky Endpoint Agent 组件的主机的任务，请在**任务**部分：*

1. 在应用程序 Web 界面窗口中选择**任务**部分。

   这将打开任务表。
2. 单击**添加**并选择**启动 YARA 扫描**。

   这将打开任务创建窗口。
3. 配置以下设置：

   a. **选择规则**是规则的名称。您可以输入规则名称或规则名称中的字符序列，然后在列表中选择规则。

   您可以添加多个规则。

   b. **扫描**是扫描范围。您可以选择以下选项之一：

   - **内存**，如果您想扫描任务执行时正在运行的进程。

     应用程序不扫描低优先级的进程。

- **自动运行点**，如果您想扫描从**进行取证**任务获取的自动运行点。

  如果您使用 Kaspersky Endpoint Agent 作为 Endpoint Agent 组件，则此功能仅在与 Kaspersky Endpoint Agent 3.13 或更高版本集成时可用。

  要扫描自动运行点，您必须指定之前为其运行过**进行取证**的主机。

- **指定目录**，如果您想要扫描在任务执行时位于指定文件夹及其所有嵌套文件夹中的文件。
- **所有本地磁盘**，如果您希望扫描任务执行时存储在本地磁盘上所有文件夹中的文件。

  扫描所有本地磁盘可能会导致主机负载过高。

c. 如果您选择了**内存**，必要时请执行以下操作：

- 在**进程**字段中，输入要扫描的进程的短名称或文件掩码。

  应用程序扫描主机上运行的所有具有相同名称的进程。

  如果**进程**字段留空，应用程序将扫描任务执行时正在运行的所有进程，除了 PID 小于 10 的进程和**排除项**字段中所列的进程。

- 在**排除项**字段中，输入要从扫描中排除的进程的完整名称或文件掩码。

  如果主机上正在运行多个具有相同名称的进程，应用程序将从扫描中排除所有此类进程。

d. 如果您选择了**自动运行点**，在**扫描类型**字段中，选择扫描类型：

- **快速**。

  在这种情况下，将扫描除 COM 对象之外的所有自动运行点。

- **全盘**。

  在这种情况下，将扫描所有自动运行点以及与其相关的文件。

如果您使用 Kaspersky Endpoint Security for Windows 作为 Endpoint Agent 组件，则无论选择的设置如何，都会执行完整扫描。

e. 如果您选择了**指定目录**：

- 在**指定目录**字段中，以 C:\<目录名称>* 格式指定目录路径。
- 在**排除项**字段中，以 C:\<目录名称>* 格式指定目录路径。

f. **最大扫描持续时间**是最大扫描持续时间。

当该时间过去后，即使未应用某些规则来扫描主机，扫描也会停止。任务报告包含扫描停止时的最新结果。

g. **描述**是任务描述。该字段是可选的。

h. **任务所有者**是任务范围：

- 如果您想运行所有服务器上的任务，请选择**所有主机**选项。
- 如果要在选定的服务器上运行任务，请选择**指定服务器**选项并在**服务器**参数名称的右侧选择要在其上运行任务的服务器名称旁边的复选框。

  仅当启用分布式解决方案和多租户模式时，此选项才可用。
- 如果您想运行选定主机上的任务，请选择**指定主机**选项并在**主机**字段中列出这些主机。

  如果您使用 Kaspersky Endpoint Agent 充当 Endpoint Agent 组件，则使用 YARA 规则扫描 Kaspersky Endpoint Agent 主机的任务只能分配给运行 Kaspersky Endpoint Agent for Windows 版本 3.12 及更高版本的主机。如果您同时将任务分配给装有 Kaspersky Endpoint Agent 3.12 和早期版本应用程序的主机，则该任务仅在装有 Kaspersky Endpoint Agent 3.12 的主机上执行。

*若要创建使用 YARA 规则在**自定义规则**部分的**YARA**子部分中扫描 Kaspersky Endpoint Agent for Windows 主机的任务：*

1. 在应用程序 Web 界面窗口中，选择**自定义规则**部分的**YARA**子部分。
2. 选择扫描主机时要使用的规则左侧的复选框。

   控制面板出现在窗口的下部。
3. 单击**启动 YARA 扫描**。
4. 执行上述说明的步骤 3。

任务创建完成。任务创建后自动运行。

如果扫描检测到任何威胁，Kaspersky Anti Targeted Attack Platform 会创建相应的警报。

具有**安全审计员**角色的用户无法创建使用 YARA 规则扫描主机的任务。

具有**安全官**角色的用户无权访问任务。

创建服务管理任务

您可以在具有 Endpoint Agent 组件的所选主机上远程启动、停止、暂停或恢复服务，以及删除服务或更改启动类型。为此，您必须创建服务管理任务。

创建服务管理任务：

1. 在应用程序 Web 界面窗口中选择**任务**部分。

   这将打开任务表。
2. 单击**添加**并选择**管理服务**。

   这将打开任务创建窗口。

3. 配置以下设置：

a. 在**服务名称**字段中，输入服务名称。

b. 在**MD5/SHA256**字段中，输入服务的 MD5 或 SHA256 哈希值。该字段是可选的。

如果您输入从 DLL 加载的服务的哈希值，Kaspersky Anti Targeted Attack Platform 会同时将指定的哈希值与服务 DLL 的哈希值和 svchost 进程的哈希值进行比较。

c. 在**操作**字段中，选择您要对服务执行的操作。

该应用程序支持以下服务操作：

- **开始**。
- **停止**。
- **暂停**。
- **恢复**。
- **删除**。
- **修改启动类型**。

当您删除某个服务时，该服务启动的进程将继续运行，直到系统重新启动或该进程终止。

d. 如果您选择了“**修改启动类型**”， 请在“**启动类型**”中选择服务的启动类型。

e. **描述**是任务描述。该字段是可选的。

f. **任务所有者**是任务范围：

- 如果您想运行所有服务器上的任务，请选择**所有主机**选项。
- 如果要在选定的服务器上运行任务，请选择**指定服务器**选项并在**服务器**参数名称的右侧选择要在其上运行任务的服务器名称旁边的复选框。

  仅当启用分布式解决方案和多租户模式时，此选项才可用。
- 如果您想运行选定主机上的任务，请选择**指定主机**选项并在**主机**字段中列出这些主机。

如果您使用 Kaspersky Endpoint Agent 作为 Endpoint Agent 组件，则任务只能分配给运行 Kaspersky Endpoint Agent for Windows 版本 3.12 及更高版本的主机。运行早期版本 Kaspersky Endpoint Agent for Windows 的主机显示在主机列表中，但无法被选择。

4. 单击**添加**。

服务管理任务已创建。任务创建后自动运行。

强烈建议不要停止、暂停、删除服务或更改影响主机功能的服务启动类型。

不建议管理的服务列表

- AVP*。
- BFE。
- CertPropSvc。
- CoreMessagingRegistrar。
- CryptSvc。
- DcomLaunch。
- Dhcp。
- DispBrokerDesktopSvc。
- EventLog。
- EventSystem。
- LanmanServer。
- LanmanWorkstation。
- LSM。
- mpssvc。
- Netlogon。
- Netman。
- PlugPlay。
- PolicyAgent。
- Power。
- ProfSvc。
- RasMan。
- RpcEptMapper。
- RpcS。
- SamSs。
- SCardSvr。
- SecurityHealthService。
- SessionEnv。
- Spooler。
- SstpSvc。
- TermService。
- UmRdpService。
- UserManager。
- UsoSvc。
- VaultSvc。
- W32Time。
- WebClient。
- Winmgmt。
- WlanSvc。
- wscsvc。

具有**安全审计员**角色的用户无法创建服务管理任务。

具有**安全官**角色的用户无权访问任务。

创建应用程序执行任务

您可以创建应用程序运行任务或命令执行任务。

如果在运行任务时标准输出文件或错误输出文件的大小达到 100 KB，则会从文件中删除一些数据。该文件不包含所有数据。

要创建运行应用程序或执行命令的任务：

1. 在应用程序 Web 界面窗口中选择**任务**部分。
   这将打开任务表。
2. 单击**添加**并选择**运行应用程序**。
   这将打开任务创建窗口。
3. 配置以下设置：
   a. 在**文件路径**和**工作目录**字段中，通过以下方式之一输入值：
      - 在**文件路径**字段中，输入可执行文件的完整路径（例如，`C:\Windows\System32\ipconfig.exe`）。留下**工作目录**字段为空。

        创建任务时，应用程序不会检查指定的可执行文件路径是否有效。

      - 在**文件路径**字段中，输入可执行文件的名称和扩展名（例如 `ipconfig.exe`）。在**工作目录**字段中，输入工作目录（例如 `C:\Windows\System32\`）。

   b. 在**参数**字段中，输入用于运行文件或任务的其他选项（例如 `/all` 参数）。

   c. 在**描述**字段中，输入任务描述。该字段是可选的。

d. 配置**任务所有者**设置，即任务范围：

- 如果您想运行所有服务器上的任务，请选择**所有主机**选项。
- 如果要在选定的服务器上运行任务，请选择**指定服务器**选项并在**服务器**参数名称的右侧选择要在其上运行任务的服务器名称旁边的复选框。

  仅当启用分布式解决方案和多租户模式时，此选项才可用。
- 如果您想运行选定主机上的任务，请选择**指定主机**选项并在**主机**字段中列出这些主机。

4. 单击**添加**。

应用程序运行任务或命令执行任务已创建。任务创建后自动运行。

示例：

要在 IP 地址为 `10.10.10.1` 的主机上运行 `ipconfig /all` 命令：

1. 在应用程序 Web 界面窗口中选择**任务**部分。
   这将打开任务表。
2. 单击**添加**并选择**运行应用程序**。
   这将打开任务创建窗口。
3. 配置以下设置：
   a. 在**文件路径**和**工作目录**字段中，通过以下方式之一输入值：
      - 在**文件路径**字段中，输入 `C:\Windows\System32\ipconfig.exe`。留下**工作目录**字段为空。
      - 在**文件路径**字段中，输入 `ipconfig.exe`。在**工作目录**字段中，输入 `C:\Windows\System32\`。

   b. 在**参数**字段中，输入 `/all`。
   c. 在**描述**字段中，输入任务描述。
   d. 选择**指定主机**任务范围。
   e. 在**主机**字段中，开始输入 IP 地址 `10.10.10.1` 的字符，当下面的搜索结果下拉列表中显示该 IP 地址时，选择它。
4. 单击**添加**。

具有**安全审计员**角色的用户不能创建应用程序运行任务或命令执行任务。

具有**安全官**角色的用户无权访问任务。

创建文件删除任务

要创建文件删除任务：

1. 在应用程序 Web 界面窗口中选择**任务**部分。
   这将打开任务表。

2. 单击**添加**并选择**删除文件**。

   这将打开任务创建窗口。

3. 配置以下设置：

   a. **文件路径** — 您想删除的文件的路径。

      您还可以指定此文件的备用数据流的路径。在这种情况下，只会删除指定的数据流。此文件的其他数据流将保持不变。

   b. **MD5/SHA256** — 要删除的文件的 MD5 或 SHA256 哈希。该字段是可选的。

   c. **描述** — 任务描述。该字段是可选的。

   d. **任务所有者** — 任务范围：

      - 如果您想运行所有服务器上的任务，请选择**所有主机**选项。
      - 如果要在选定的服务器上运行任务，请选择**指定服务器**选项并在**服务器**参数名称的右侧选择要在其上运行任务的服务器名称旁边的复选框。

        仅当启用分布式解决方案和多租户模式时，此选项才可用。
      - 如果您想运行选定主机上的任务，请选择**指定主机**选项并在**主机**字段中列出这些主机。

4. 单击**添加**。

将创建文件删除任务。任务创建后自动运行。

如果该文件已被另一个进程阻止，则该任务将显示为*已完成*状态，但该文件仅在主机重新启动后才会删除。建议在主机重新启动后检查文件是否成功删除。

不支持从映射的网络驱动器中删除文件。

具有**安全审计员**角色的用户无法创建文件删除任务。

具有**安全官**角色的用户无权访问任务。

创建文件隔离任务

如果您认为具有 Endpoint Agent 组件的计算机上存在感染文件或疑似感染文件，可以通过将其放入隔离区中将其隔离。

要创建文件隔离任务：

1. 在应用程序 Web 界面窗口中选择**任务**部分。

   这将打开任务表。

2. 单击**添加**并选择**隔离文件**。
   这将打开任务创建窗口。

3. 配置以下设置：

   a. 在**文件路径**字段中，输入要隔离的文件的路径。

   b. 在**MD5/SHA256**字段中，输入要隔离的文件的 MD5 或 SHA256 哈希值。该字段是可选的。

   c. **描述** — 任务描述。该字段是可选的。

   d. 在**主机**字段中，输入要向其分配任务的主机的名称或 IP 地址。
   您可以指定多个主机。

   e. 单击**添加**。

文件隔离任务已创建。任务创建后自动运行。
作为任务结果：

- 文件将被从其所在计算机的文件夹中删除，并移动到同一计算机上的隔离目录，该目录是在配置用作 Endpoint Agent 组件的应用程序期间指定的。
- 在应用程序 Web 界面中**任务**部分的任务列表中，会显示有关任务的执行信息。
- 在**存储**部分、**隔离区**子部分的文件列表中，会显示有关被隔离文件的信息。

如果该文件已被另一个进程阻止，则该任务将显示为*已完成*状态，但该文件仅在主机重新启动后才会被放置在隔离区中。建议在主机重新启动后检查任务是否成功完成。

如果您尝试隔离可执行文件并且该文件当前正在运行，文件隔离任务可以完成但会有**拒绝访问**错误。

要解决此问题，请为此文件创建进程终止任务，然后尝试再次创建文件隔离任务。

具有**安全审计员**角色的用户无法创建文件隔离任务。

具有**安全官**角色的用户无权访问任务。

创建隔离文件恢复任务

如果您认为以前隔离的文件是安全的，则可以将其从隔离区还原到主机。

要从隔离区创建恢复文件的任务：

1. 在应用程序 Web 界面窗口中选择**任务**部分。
   这将打开任务表。
2. 单击**添加**并选择**从隔离区恢复文件**。
   这将打开任务创建窗口。
3. 配置以下设置：
   a. **描述**是任务描述。该字段是可选的。
   b. **文件搜索** — 隔离区中文件的名称。
4. 单击**添加**。

从隔离区恢复文件的任务已创建。任务创建后自动运行。

将文件从隔离区恢复到主机后，有关该文件的元数据将保留在存储区中的对象表中。

在分布式解决方案和多租户模式下，被在 SCN 服务器上隔离的文件无法在 PCN 服务器上恢复。您可以在创建隔离文件任务的 SCN 服务器上恢复文件。

具有**安全审计员**角色的用户无法创建从隔离区恢复文件的任务。

具有**安全官**角色的用户无权访问任务。

创建任务副本

要复制任务：

1. 在应用程序 Web 界面窗口中选择**任务**部分。
   这将打开任务表。
2. 打开您想复制的任务。
3. 单击**复制**。
   这将打开任务创建窗口。将复制所有任务设置。

4. 如果您想要修改任务设置，请根据正在被复制的任务类型编辑一项或多项设置。
5. 单击**添加**。

   将创建选定任务的副本。

具有**安全审计员**角色的用户无法复制任务。

具有**安全官**角色的用户无权访问任务。

删除任务

如果您在任务运行时将其删除，则可能不会保存任务结果。

如果您删除成功完成的文件下载任务，则该文件也将被删除。

要删除任务：

1. 在应用程序 Web 界面窗口中选择**任务**部分。
   这将打开任务表。
2. 打开您想删除的任务。
3. 单击**删除**。
   这将打开操作确认窗口。
4. 单击**是**。

   该任务将被删除。

删除全部或多个任务：

1. 在应用程序 Web 界面窗口中选择**任务**部分。
   这将打开任务表。
2. 选择要删除的任务旁边的复选框。
   您可以通过选择包含列标题的行中的复选框来选择所有任务。

3. 在窗口下部显示的窗格中，单击**删除**。
   这将打开操作确认窗口。
4. 单击**是**。

选定的任务被删除。

具有**安全审计员**角色的用户无法删除任务。

具有**安全官**角色的用户无权访问任务。

按创建时间筛选任务

要按创建时间筛选任务：

1. 在应用程序 Web 界面窗口中选择**任务**部分。
   这将打开任务表。
2. 单击**时间**链接以打开任务筛选菜单。
3. 选择以下任务显示时段之一：
   - **所有**，如果您希望应用程序显示表中创建的所有任务。
   - **上一个小时**，如果您希望应用程序显示表中最后一小时创建的任务。
   - **最后一天**，如果您希望应用程序显示表中最后一天创建的任务。
   - **自定义范围**，如果您希望应用程序显示表中指定期间创建的任务。
4. 如果您选择了**自定义范围**任务显示时段：
   a. 这将打开日历；在日历中，指定任务显示期间的开始日期和结束日期。
   b. 单击**应用**。

日历关闭。

任务表将仅显示与您设置的筛选条件相匹配的任务。

您可以同时使用多个筛选器。

按类型筛选任务

如果您使用分布式解决方案和多租户模式，您可以按任务类型筛选任务。

要按类型筛选任务：

1. 在应用程序 Web 界面窗口中选择**任务**部分。
   这将打开任务表。
2. 单击**类型**链接以打开任务筛选菜单。
3. 选择以下任务显示选项之一：
   - **所有**，如果您想显示所有任务，无论其类型如何。
   - **全球**，如果您只想显示在 PCN 服务器上创建的任务。这些任务适用于连接到此 PCN 服务器的主机以及连接到此 PCN 服务器的所有 SCN 服务器。任务属于用户为其使用 Web 界面管理程序的租户。
   - **本地**，如果您只想显示在 SCN 服务器上创建的任务。这些任务仅适用于连接到此 SCN 服务器的主机。任务属于用户为其使用 Web 界面管理程序的租户。

任务表将仅显示与您设置的筛选条件相匹配的任务。

您可以同时使用多个筛选器。

按名称筛选任务

要按名称筛选任务：

1. 在应用程序 Web 界面窗口中选择**任务**部分。
   这将打开任务表。
2. 单击**名称**链接以打开任务筛选菜单。
3. 选择一个或多个复选框：
   - **杀死进程**。
   - **运行应用程序**。
   - **进行取证**。
   - **启动 YARA 扫描**。
   - **管理服务**。
   - **获取文件**。

- **删除文件**。
- **隔离文件**。
- **恢复文件**。

4. 单击**应用**。

任务表将仅显示与您设置的筛选条件相匹配的任务。

> 您可以同时使用多个筛选器。

按文件名和路径筛选任务

您可以根据**详细信息**条件 – 文件或数据流的名称和路径来筛选任务。

要按照文件或数据流的名称和路径筛选任务：

1. 在应用程序 Web 界面窗口中选择**任务**部分。
   这将打开任务表。
2. 单击**详细信息**链接以打开任务筛选配置窗口。
3. 在右侧的下拉列表中，选择**详细信息**。
4. 在左侧下拉列表中，选择以下筛选运算符任务之一：
   - **包含**。
   - **不包含**。
   - **等于**。
   - **不等于**。
5. 在输入字段中，指定文件名或路径的一个或多个字符。
6. 要使用不同条件添加筛选条件，请单击 + 并指定筛选条件。
7. 单击**应用**。

任务表将仅显示与您设置的筛选条件相匹配的任务。

> 您可以同时使用多个筛选器。

按描述筛选任务

您可以通过**描述**条件、即创建任务时添加的任务描述来筛选任务。

要按描述筛选任务：

1. 在应用程序 Web 界面窗口中选择**任务**部分。
   这将打开任务表。
2. 单击**详细信息**链接以打开任务筛选配置窗口。
3. 在左侧的下拉列表中，选择**描述**。
4. 在右侧的下拉列表中，选择以下任务筛选运算符之一：
   - **包含**。
   - **不包含**。
   - **等于**。
   - **不等于**。
5. 在输入字段中，指定文件名或路径的一个或多个字符。
6. 要使用不同条件添加筛选条件，请单击 + 并指定筛选条件。
7. 单击**应用**。

   任务表将仅显示与您设置的筛选条件相匹配的任务。

> 您可以同时使用多个筛选器。

按服务器名称筛选任务

如果您使用分布式解决方案和多租户模式，您可以根据应用任务的服务器来筛选任务。

要按应用任务的服务器筛选任务：

1. 在应用程序 Web 界面窗口中选择**任务**部分。
   这将打开任务表。

2. 单击**服务器**链接以打开任务筛选菜单。
3. 选择要显示其任务的服务器名称旁边的复选框。

任务表将仅显示与您设置的筛选条件相匹配的任务。

> 您可以同时使用多个筛选器。

根据创建任务的用户的名称筛选任务

要根据创建任务的用户名筛选任务，必须显示所有任务。如果只显示当前用户创建的任务，则无法按用户名筛选任务。

按照创建任务的用户的名称筛选任务：

1. 在应用程序 Web 界面窗口中选择**任务**部分。
   这将打开任务表。
2. 单击**创建者**链接以打开任务筛选菜单。
3. 在下拉列表中，选择以下任务筛选运算符之一：
   - **包含**
   - **不包含**
4. 在输入字段中，指定用户名称的一个或多个字符。
5. 要使用不同条件添加筛选条件，请单击 + 并指定筛选条件。
6. 单击**应用**。

任务表将仅显示与您设置的筛选条件相匹配的任务。

> 您可以同时使用多个筛选器。

按处理状态筛选任务

要根据用户处理任务的状态筛选任务：

1. 在应用程序 Web 界面窗口中选择**任务**部分。
   这将打开任务表。
2. 单击**状态**链接以打开任务筛选菜单。

3. 选择一个或多个复选框：

   - **等待**。
   - **进行中**。
   - **已完成**。

4. 单击**应用**。

任务表将仅显示与您设置的筛选条件相匹配的任务。

您可以同时使用多个筛选器。

清除任务筛选器

要清除一个或多个筛选条件的任务筛选器：

1. 在应用程序 Web 界面窗口中选择**任务**部分。
   这将打开任务表。
2. 单击您想清除其筛选条件的表列标题右侧的  。

   如果要清除多个筛选条件，请执行必要的操作以清除每个筛选条件。

选定筛选器将被清除。

任务表将仅显示与您设置的筛选条件相匹配的任务。

管理策略（防止规则）

在应用程序 Web 界面中工作时，具有**高级安全官**角色的用户可以管理选定主机上文件和进程的防止规则。例如，您可以阻止运行您认为在具有 Endpoint Agent 组件的选定主机上使用不安全的应用程序。该应用程序通过使用 MD5 和 SHA256 哈希算法基于文件哈希识别文件。您可以创建、启用、禁用、删除和修改防止规则。此外，您还可以单击防止规则表中带有哈希算法名称的链接来查找触发了防止规则的对象、事件或警报，例如"**查找事件**"、"**查找警报**"、"**在 Kaspersky TIP 上查找**"或"**在 virustotal.com 上查找**"。

在分布式解决方案和多租户模式下，防止规则可以有以下类型：

- **全球** — 在 PCN 上创建。这些防止规则适用于连接到此 PCN 服务器的主机以及连接到此 PCN 服务器的所有 SCN 服务器。防止规则属于用户在应用程序 Web 界面中管理的租户。
- **本地** — 在 SCN 服务器上创建。这些防止规则仅适用于连接到此 SCN 服务器的主机。防止规则属于用户在应用程序 Web 界面中管理的租户。

具有**高级安全官**角色的用户可以为他们有权访问其数据的租户创建、编辑、删除、启用、禁用和导入防止规则。

具有**安全官**角色的用户无权访问策略。

具有**安全审计员**角色的用户可以查看文件运行防止规则和进程运行防止规则表，以及所选防止规则的信息，但不能编辑规则。

在与选定主机建立授权连接之后，所有防止规则更改都会应用到主机上。如果与主机没有连接，则旧的防止规则将继续应用于主机。对防止规则的更改不会影响已在运行的进程。

防止规则可以根据默认添加的预设策略（以下也称为"预设"）自动创建。打开预设时，防止规则将根据 Sandbox 组件的中度或高严重性警报创建。这样创建的防止规则会根据文件的 MD5 哈希值来阻止运行该文件。具有**高级安全官**角色的用户可以启用和禁用预设。

分布式解决方案和多租户模式不支持预设。

对于自动创建或导入的防止规则，可以应用与手动创建的规则相同的操作。

您只能为每个文件哈希创建一条防止规则。

系统中支持的最大防止规则数量为 50000 条。

仅当 Endpoint Agent 组件在主机上运行时才会强制执行防止规则。如果在启动组件之前或在主机上关闭组件之后尝试运行文件，则该文件不会被阻止运行。

仅当 Endpoint Agent 组件与 Central Node 服务器集成时，您才可以使用策略管理选定主机上的文件和进程运行阻止规则；为此，您必须使用 Kaspersky Anti Targeted Attack Platform 的 Web 界面。

如果您使用 Kaspersky Endpoint Security for Windows 作为 Endpoint Agent 组件，则必须考虑到该应用程序支持阻止运行具有某些扩展名的 Office 格式文件和某些脚本解释器。

查看防止规则表

防止规则表位于应用程序 Web 界面窗口的**防止**部分。

表包含以下信息：

1. **类型**是规则的类型，具体取决于应用程序的操作模式和生成规则的服务器的角色：
   - **全球** — 在 PCN 上创建。这些防止规则适用于连接到此 PCN 服务器的主机以及连接到此 PCN 服务器的所有 SCN 服务器。防止规则属于用户在应用程序 Web 界面中管理的租户。
   - **本地** — 在 SCN 服务器上创建。这些防止规则仅适用于连接到此 SCN 服务器的主机。防止规则属于用户在应用程序 Web 界面中管理的租户。
2. **名称** — 防护规则的名称。

3. **创建者** – 其账户被用于创建规则的用户的名称。

4. **文件哈希值** – 应用于识别文件的哈希算法。
   可以基于以下哈希算法之一识别文件：

   - **MD5**。
   - **SHA256**。

   单击具有哈希算法名称的链接将打开一个列表，您可以查看文件哈希并从其中选择以下操作之一：

   - **按照此值进行过滤**。
   - **从过滤器中排除**。
   - **在 Kaspersky TIP 上查找**。
   - **在 virustotal.com 上查找**（适用于 SHA256）。
   - **查找事件**。
     执行此操作时，将打开**威胁搜索**部分，其中具有根据您选定的哈希已经筛选的事件。
   - **查找警报**。
     执行此操作时，**警报**部分将打开，其中具有根据您选定的哈希已经筛选的警报。
   - **启用防止规则**。
   - **禁用防止规则**。
   - **删除防止规则**。
   - **复制值到剪贴板**。

5. **服务器**是服务器的名称，具有对其应用防止规则的 PCN 或 SCN 角色。
   如果您使用分布式解决方案和多租户模式，则此字段会显示。

6. **主机**是对其主机应用了防止规则且具有 Central Node 组件的服务器的名称。
   仅当您使用独立的 Central Node 服务器时才会显示此字段。

7. **状态**是防止规则的当前状态。
   防止规则可具有以下状态之一：

   - **已启用**。
   - **已禁用**。

配置防止规则表显示

您可以显示或隐藏列以及更改防止规则表中列的顺序。

要配置防止规则表显示：

1. 在应用程序 Web 界面窗口中选择**防止**部分。
   这将打开防御规则表
2. 在表格的标题部分，单击 。
   这将打开**定制表格**窗口。
3. 如果要在表中显示列，请选择要在表中显示的参数名称旁边的复选框。
   如果要隐藏表中的参数，请清除该复选框。

   > 必须选择至少一个复选框。

4. 如果要更改表格中列的顺序，请将鼠标光标移动到具有相关参数的行，单击 并将该行移动到新位置。
5. 如果要恢复默认表格显示设置，请单击**默认**。
6. 单击**应用**。

防止规则表显示已配置。

查看防止规则

查看防止规则：

1. 在应用程序 Web 界面窗口中选择**防止**部分。
   这将打开防止规则表
2. 选择要查看的规则规则。

防止规则包含以下信息：

- **事件**链接将打开包含选定防止规则的搜索条件的**威胁搜索**部分。
- **状态**是防止规则的当前状态。
  防止规则可具有以下状态之一：
  - **已启用。**
  - **已禁用。**
- **详细信息**选项卡包含以下信息：
  - **MD5/SHA256**是被阻止运行的文件的哈希。
    单击 **MD5/SHA256** 链接将打开一个列表，您可以从其中选择以下操作之一：
    - **在 Kaspersky TIP 上查找**。
    - **查找事件**。

- **查找警报**。
- **复制值到剪贴板**。

- **名称**是被阻止运行的防止规则或文件的名称。
- **类型**是规则的类型，具体取决于应用程序的操作模式和生成规则的服务器的角色：
  - **全球** — 在 PCN 上创建。这些防止规则适用于连接到此 PCN 服务器的主机以及连接到此 PCN 服务器的所有 SCN 服务器。防止规则属于用户在应用程序 Web 界面中管理的租户。
  - **本地** — 在 SCN 服务器上创建。这些防止规则仅适用于连接到此 SCN 服务器的主机。防止规则属于用户在应用程序 Web 界面中管理的租户。
- **通知**是**通知用户阻止文件执行**设置的状态。
- **防止于**是应用防止规则的主机列表。
  如果防御在所有主机上生效，则显示**所有主机**部分。

- **更改日志**选项卡包含对防御做出的更改列表：更改时间、更改防御的用户名，以及对防御采取的操作。

创建防止规则

为系统文件创建防护规则时，阻止文件运行的主机可能无法正常工作。Kaspersky Anti Targeted Attack Platform 不检查为哪种类型的文件创建防护规则。

要创建防止规则：

1. 在应用程序 Web 界面窗口中选择**防止**部分。
   这将打开防止规则表
2. 单击**添加**。
3. 选择**创建规则**。
   这将打开防止规则创建窗口。
4. 配置以下设置：
   a. **状态**是防护规则的状态：
      - 如果要启用防护规则，请将切换开关设置为**开启**。
      - 如果要禁用防护规则，请将切换开关设置为**关闭**。
   b. **MD5/SHA256** — 要阻止启动的文件或数据流的 MD5 或 SHA256 哈希。
   c. **名称**是防护规则的名称。

d. 如果您希望应用程序向应用防御的计算机用户显示防护规则触发通知，请选择**通知用户阻止文件执行**复选框。

如果您选择了**通知用户阻止文件执行**复选框并尝试执行被阻止运行的文件，则用户会被通知该文件触发了执行阻止规则。

e. **防止于**是防止规则范围：

- 如果您想在所有服务器的所有主机上应用防御，请选择**所有主机**。
- 如果要在选定的服务器上应用防防护规则，请选择**指定服务器**选项并在**服务器**参数名称的右侧选择要在其上应用防护规则的服务器名称旁边的复选框。

  仅当启用分布式解决方案和多租户模式时，此选项才可用。
- 如果您想在选定主机上应用防护规则，请选择**指定主机**选项并在**主机**字段中列出这些主机。

如果您使用的是版本早于 12.2 的 Kaspersky Endpoint Security for Linux 作为 Endpoint Agent 组件，则防护规则创建功能不可用。创建防御规则时，如果您选择装有 Kaspersky Endpoint Security for Linux 的主机或所有主机作为规则范围，则该规则不会应用或仅应用于装有 Kaspersky Endpoint Agent for Windows 和 Kaspersky Endpoint Security for Windows 的主机。

5. 单击**添加**。

将创建文件启动阻止。

您还可以导入防止规则。

具有**安全审计员**角色的用户无法创建文件启动阻止规则。

具有**安全官**角色的用户无法访问防止规则。

导入防止规则

对于要阻止运行的文件，您可以导入具有 MD5 和 SHA256 哈希值的文件。对于每个哈希值，Kaspersky Anti Targeted Attack Platform 会创建单独的防止规则。

导入文件的最大大小为 10 MB。每行只允许一个哈希。

要导入防止规则：

1. 在应用程序 Web 界面窗口中选择**防止**部分。

   这将打开防止规则表
2. 单击**添加**。

3. 选择**导入规则**。
   这将打开防止规则导入窗口。

4. 配置以下设置：

   a. **状态**是防护规则的状态：

      - 如果要启用所有导入的防止规则，请将切换开关设置为**开启**。
      - 如果要禁用所有导入的防止规则，请将切换开关设置为**关闭**。

   b. 如果您希望应用程序向应用防御的计算机用户显示防止规则触发通知，请选择**通知用户阻止文件执行**复选框。

   防止于字段无法编辑。默认情况下，在 PCN 服务器上创建的防止规则将被应用于连接到该 PCN 服务器的所有主机以及连接到该 PCN 服务器的所有 SCN 服务器（如果您使用的是分布式解决方案和多租户模式）。

5. 单击**浏览**上传包含要为其创建防止规则的文件哈希的文件。
   这将打开文件选择窗口。

6. 选择您想上传的文件，然后单击**打开**。
   这将关闭文件选择窗口。

7. 单击**添加**。

规则已导入。

具有**安全审计员**角色的用户无法导入文件启动阻止规则。

具有**安全官**角色的用户无法访问防止规则。

启用和禁用防止规则

要启用或禁用防止规则：

1. 在应用程序 Web 界面窗口中选择**防止**部分。
   这将打开防止规则表

2. 在包含要启用或禁用的防止规则的行中，在**状态**列中执行以下操作之一：

   - 如果要启用防止规则，请将切换开关设置为**已启用**。
     将启用您选定的防止规则。

- 如果要禁用防止规则，请将切换开关设置为**已禁用**。
  将禁用您选定的防止规则。

具有**安全审计员**角色的用户无法启用或禁用防止规则。

具有**安全官**角色的用户无权访问使用策略在选定主机上启动文件和进程的防止规则。

启用和禁用预设

要启用或禁用预设：

1. 在应用程序 Web 界面窗口中选择**防止**部分。
   这将打开防止规则表
2. 选择**预设**选项卡。
3. 在要启用或禁用的预设行中，在**状态**列中，将切换开关设置为**已启用**或者**已禁用**。

   预设被启用或禁用。禁用预设后，之前自动创建的所有防止规则都不会被删除。

删除防止规则

您可以删除单个防止规则或多个防止规则，或同时删除所有防止规则。

删除单个防止规则：

1. 在应用程序 Web 界面窗口中选择**防止**部分。
   这将打开防止规则表
2. 单击您想删除的防止规则。
   这将打开防止规则详情窗口。
3. 单击**删除**。
   这将打开操作确认窗口。
4. 单击**是**。

   防止规则被删除。

删除全部或多个防止规则：

1. 在应用程序 Web 界面窗口中选择**防止**部分。
   这将打开防止规则表
2. 选择要删除的防止规则旁边的复选框。
   您可以通过选择包含列标题的行中的复选框来选择所有防止规则。

3. 在窗口下部显示的窗格中，单击**删除**。
   这将打开操作确认窗口。
4. 单击**是**。

选定的防止规则将被删除。

具有**安全审计员**角色的用户无法删除防止规则。

具有**安全官**角色的用户无权访问使用策略在选定主机上启动文件和进程的防止规则。

按名称筛选防止规则

要按名称筛选防止规则：

1. 在应用程序 Web 界面窗口中选择**防止**部分。
   这将打开防止规则表
2. 单击**名称**链接以打开防御筛选菜单。
3. 在下拉列表中，选择以下防御筛选运算符之一：
   - **包含**
   - **不包含**
4. 在文本框中输入防止规则名称的一个或多个字符。
5. 要使用不同条件添加筛选条件，请单击 + 并指定筛选条件。
6. 单击**应用**。

防止规则表仅显示与您设置的筛选条件相匹配的防止规则。

您可以同时使用多个筛选器。

按类型筛选防止规则

如果您使用分布式解决方案和多租户模式，则可以按类型筛选防止规则。

按类型筛选防止规则：

1. 在应用程序 Web 界面窗口中选择**防止**部分。
   这将打开防止规则表

2. 单击**类型**链接以打开防止规则筛选菜单。

3. 选择以下选项之一来显示防止规则：

   - **所有**，如果您想显示所有防止规则（无论其类型如何）。
   - **全球**，如果您只想显示在 PCN 上创建的防止规则。这些防止规则适用于连接到此 PCN 服务器的主机以及连接到此 PCN 服务器的所有 SCN 服务器。防止规则属于用户在应用程序 Web 界面中管理的租户。
   - **本地**，如果您只想显示在 SCN 服务器上创建的防止规则。这些防止规则仅适用于连接到此 SCN 服务器的主机。防止规则属于用户在应用程序 Web 界面中管理的租户。

防止规则表仅显示与您设置的筛选条件相匹配的防止规则。

您可以同时使用多个筛选器。

按文件哈希筛选防止规则

要按文件哈希来筛选防止规则：

1. 在应用程序 Web 界面窗口中选择**防止**部分。
   这将打开防止规则表

2. 单击**文件哈希值**链接以打开防止规则筛选菜单。

3. 在下拉列表中，选择以下防御筛选运算符之一：

   - **包含**
   - **不包含**

4. 在文本框中，输入文件哈希的一个或多个字符。

5. 要使用不同条件添加筛选条件，请单击 + 并指定筛选条件。

6. 单击**应用**。

防止规则表仅显示与您设置的筛选条件相匹配的防止规则。

您可以同时使用多个筛选器。

按服务器名称筛选防止规则

如果您使用的是分布式解决方案和多租户模式，您可以根据防止规则应用的服务器来筛选防止规则。

要按服务器名称筛选防止规则：

1. 在应用程序 Web 界面窗口中选择**防止**部分。
   这将打开防止规则表
2. 单击**服务器**链接以打开防止规则筛选菜单。
3. 选择要用于筛选防止规则的服务器旁边的复选框。
4. 单击**应用**。

防止规则表仅显示与您设置的筛选条件相匹配的防止规则。

您可以同时使用多个筛选器。

清除防止规则筛选器

要清除一个或多个筛选条件的防止规则筛选器：

1. 在应用程序 Web 界面窗口中选择**防止**部分。
   这将打开防止规则表
2. 单击您想清除其筛选条件的防止规则表列标题右侧的  。

   如果要清除多个筛选条件，请执行必要的操作以清除每个筛选条件。

选定筛选器将被清除。

防止规则表仅显示与您设置的筛选条件相匹配的防止规则。

管理用户定义的规则

为了进一步保护企业 IT 基础设施，您可以配置 TAA、IDS、IOC 和 YARA 自定义规则。

具有**高级安全官**角色的用户可以使用自定义**TAA**、**IDS**、**IOC**和**YARA**规则：加载和删除规则文件、查看规则列表以及编辑选定的规则。

具有**安全审计员**角色的用户可以查看自定义**TAA**、**IDS**、**IOC**和**YARA**规则列表以及所选规则的属性，但无法编辑。

具有**安全官**角色的用户可以查看自定义**TAA**、**IOC**和**YARA**规则列表和所选规则的属性，但无法编辑。

使用入侵指标 (IOC) 和攻击指标 (IOA) 进行威胁搜索

Kaspersky Anti Targeted Attack Platform 使用两种类型的指示器进行威胁搜索：*IOC*（入侵指标）和*IOA*（攻击指标）。

IOC 是有关恶意对象或恶意活动的一组数据。Kaspersky Anti Targeted Attack Platform 使用符合 OpenIOC 标准的 IOC 文件，该标准是描述入侵指标的开放标准。IOC 文件包含一组与事件指标进行比较的指标。如果比较的指标匹配，应用程序将该事件视为检测并创建警报。如果扫描检测到对象数据与多个 IOC 文件之间的精确匹配，则警报的可能性会增加。

IOA（也称为"TAA (IOA) 规则"）是包含系统中可疑活动描述的规则，该活动可能是针对性攻击的迹象。Kaspersky Anti Targeted Attack Platform 扫描应用程序的事件数据库，并标记与 TAA (IOA) 规则描述的行为相匹配的事件或事件链。使用*流式扫描*技术，对从受保护设备接收到的事件进行连续实时扫描。

由卡巴斯基专家创建的 TAA (IOA) 规则得到 TAA（针对性攻击分析器）技术的使用，与应用程序数据库一起更新。它们不会显示在应用程序的界面中，并且无法编辑。

您可以使用 OpenIOC 格式的 IOC 文件添加用户定义的 IOC和TAA (IOA) 规则，以及基于事件数据库搜索条件创建 TAA (IOA) 规则。

下表包含入侵指标 (IOC) 和攻击指标 (IOA) 的比较分析。

IOC 和 IOA 指标对比

特征	用户定义的 IOC 规则中的 IOC	用户定义的 TAA (IOA) 规则中的 IOA	卡巴斯基专家创建的 TAA (IOA) 规则中的 IOA
扫描范围	具有 Endpoint Agent 组件的计算机	应用程序事件数据库	应用程序事件数据库
扫描机制	定期扫描	流式扫描	流式扫描
可以被添加到扫描排除项	无。	不需要。 具有**高级安全官**角色的用户可以根据需要编辑自定义 TAA (IOA) 规则中的指标文本。	是。

如果使用的是分布式解决方案和多租户模式，此部分将显示所选租户的信息。

管理用户定义的 TAA (IOA) 规则

自定义 TAA (IOA) 规则是根据事件数据库搜索条件创建的。例如，当您认为不安全的应用程序在带有 Endpoint Agent 组件的计算机上启动时，您希望 Kaspersky Anti Targeted Attack Platform 生成事件警报，您可以：

1. 手动向事件数据库生成搜索查询，或者上传带有入侵指标的 IOC 文件或带有 Sigma 规则的 YAML 文件来检测此应用程序。

   创建 IOC 文件时，请在"**威胁搜索**"部分查看可用于搜索事件的 IOC 术语列表。您可以通过从下面的链接下载文件来查看受支持的 IOC 术语列表。

   在"**威胁搜索**"部分搜索事件的 IOC 术语

2. 根据事件搜索条件创建自定义 TAA (IOA) 规则。

   当 Central Node 服务器收到与创建的 TAA (IOA) 规则匹配的事件时，Kaspersky Anti Targeted Attack Platform 会生成警报。

您还可以根据已加载的 IOC 文件中的条件创建 TAA (IOA) 规则。为此：

1. 查找与所选文件的条件相对应的事件。
2. 根据所选文件中的事件搜索条件创建 TAA (IOA) 规则。

在分布式解决方案和多租户模式下，TAA（IOA）规则可以有以下类型之一：

- **全球** – 在 PCN 服务器上创建。这些规则用于扫描此 PCN 服务器以及连接到此 PCN 服务器的所有 SCN 服务器上的事件。扫描的事件属于用户在应用程序 Web 界面中管理的租户。
- **本地** – 在 SCN 服务器上创建。这些规则用于扫描此 SCN 服务器上的事件。扫描的事件属于用户在应用程序 Web 界面中管理的租户。

下表总结了用户规则和卡巴斯基规则之间的差异。

TAA（IOA）规则对比

特征	用户定义的 TAA (IOA) 规则	Kaspersky TAA (IOA) 规则
关于响应事件的建议	否	是 您可以在警报信息中查看推荐
与MITRE ATT&CK 数据库中的技术对应	否	是 您可以根据 MITRE 数据库在警报信息中查看技术描述
在TAA（IOA）规则表中显示	是	否
能够禁用此规则的数据库查找	禁用规则	将规则添加到 TAA 排除项
能够删除或添加规则	您可以在应用程序的 Web 界面中删除或添加规则	规则与应用程序数据库一起更新 并且不能被用户删除
搜索其中触发了 TAA (IOA) 规则的警报和事件	使用TAA (IOA) 规则信息窗口中的**警报**和**事件**链接	使用警报信息窗口中的**警报**和**事件**链接

具有**高级安全官**角色的用户可以创建、导入、删除、启用或禁用TAA (IOA) 规则，以及从扫描中排除 Kaspersky TAA (IOA) 规则。具有**安全官**或者**安全审计员**角色的用户可以使用 TAA（IOA）规则在事件和警报数据库中搜索针对性攻击迹象、受感染和可能受感染的对象，并查看 TAA（IOA）规则表和TAA（IOA）规则信息。

查看TAA（IOA）规则表

如果您使用分布式解决方案和多租户模式，请使用要为其配置参数的 PCN 或 SCN 服务器的 Web 界面。

用户定义的 TAA (IOA) 规则表包含有关用于扫描事件和创建警报的 TAA (IOA) 规则的信息；该表位于应用程序 Web 界面窗口的**自定义规则**部分，**TAA**子部分。

表包含以下信息：

1. – 分配给使用此 TAA (IOA) 规则生成的警报的重要性级别。

重要性级别可以采用以下值之一：

- – **低**。
- – **中**。
-  – **高**。

2. **类型**是规则的类型，具体取决于应用程序的操作模式和生成规则的服务器的角色：
   - **全球** – 在 PCN 服务器上创建。这些规则用于扫描此 PCN 服务器以及连接到此 PCN 服务器的所有 SCN 服务器上的事件。扫描的事件属于用户在应用程序 Web 界面中管理的租户。
   - **本地** – 在 SCN 服务器上创建。这些规则用于扫描此 SCN 服务器上的事件。扫描的事件属于用户在应用程序 Web 界面中管理的租户。
3. **置信** – 置信度取决于规则引起误报的可能性：
   - **高**。
   - **中**。
   - **低**。

   置信度越高，误报的可能性就越低。
4. **名称** – 规则的名称。
5. **服务器**是服务器的名称，具有对其应用规则的 PCN 或 SCN 角色。
   如果您使用的是分布式解决方案和多租户模式，则会显示此列。
6. **警报** – 要求根据数据库中的事件与规则条件的匹配来存储警报信息。
   - **已启用** – 使用指定的针对性攻击分析器 (TAA) 技术在警报表中为该事件创建一条记录。
   - **已禁用** – 不显示在警报表中。
7. **状态** – 事件扫描中规则的使用状态：
   - **已启用** – 规则正在被使用。
   - **已禁用**– 该规则未被使用。

根据事件搜索条件创建 TAA (IOA) 规则

根据事件搜索条件创建 TAA (IOA) 规则：

1. 选择程序 Web 界面窗口中的**威胁搜索**部分。
   这将打开事件搜索表单。
2. 使用构建器模式或源代码模式执行事件搜索。

3. 单击**另存为 TAA (IOA) 规则**。
   这将打开**新 TAA (IOA) 规则**窗口。

4. 在**名称**字段中，输入规则的名称。

5. 单击**保存**。

事件搜索条件将被保存。在**自定义规则**部分的 TAA（IOA）规则表中，在 Web 界面的**TAA**子部分中，新规则将以指定名称显示。

如果要将事件搜索条件保存为用户定义的 TAA (IOA) 规则，请避免使用以下字段：

- IOAd。
- IOATag。
- IOATechnique。
- IOATactics。
- IOAImportance。
- IOAConfidence。

保存用户定义的 TAA (IOA) 规则时，应用程序可能没有任何包含这些字段数据的事件。当出现具有此数据的事件时，您之前创建的用户定义字段将无法按这些字段标记事件。

具有**安全审计员**和**安全官**角色的用户无法根据事件搜索条件创建 TAA (IOA) 规则。

导入 TAA (IOA) 规则

您可以从 IOC 文件或具有 Sigma 规则的 YAML 文件导入 TAA (IOA) 规则，并使用这些规则扫描事件并生成针对性攻击分析器警报。

要导入 TAA (IOA) 规则：

1. 在应用程序 Web 界面的窗口中，选择**自定义规则**部分，**TAA**子部分。
   这将打开 TAA (IOA) 规则表。

2. 单击**导入**。
   这将在您的本地计算机上打开文件选择窗口。

3. 选择您想上传的文件，然后单击**打开**。
   这将打开**新 TAA (IOA) 规则**窗口。

4. 如果要启用扫描事件数据库的规则，将**状态**切换开关设置为**已启用**。

5. 在**详细信息**选项卡上的**名称**字段中，输入规则的名称。

6. 在**描述**字段中，输入有关规则的任何附加信息。

7. 在**重要级别**下拉列表中，选择要分配给使用此 TAA (IOA) 规则生成的警报的重要性级别。
   - **低**。
   - **中**。
   - **高**。
8. 在**置信**下拉列表中，根据您的估计选择此规则的置信度：
   - **低**。
   - **中**。
   - **高**。
9. 在**应用到**下面，选择与要对其应用规则的服务器对应的复选框。
10. **查询**选项卡上，验证定义的搜索条件。如有必要，请进行更改。
11. 单击**保存**。

    用户定义的 TAA (IOA) 规则被导入到应用程序中。

您还可以通过将事件数据库搜索条件保存在**威胁搜索**部分中来添加 TAA (IOA) 规则。

查看自定义 TAA (IOA) 规则详细信息

要显示有关 TAA (IOA) 规则的信息：

1. 在应用程序 Web 界面的窗口中，选择**自定义规则**部分，**TAA**子部分。

   这将打开 TAA (IOA) 规则表。
2. 选择您想查看信息的规则。

这将打开一个窗口，其中包含有关规则的信息。

该窗口包含以下信息：

- 单击**警报**链接即可在新的浏览器选项卡中显示警报表。警报将根据针对性攻击分析器技术和您正在处理的TAA (IOA) 规则的名称进行筛选。
- 单击**查找事件**链接以在新的浏览器选项卡中显示事件表。该表按规则名称筛选。
- 单击**运行查询**链接以在新的浏览器选项卡中显示事件表。该表按规则名称筛选。事件搜索条件将使用您正在处理的 TAA (IOA) 规则中的信息进行填充。例如，`EventType=进程已启动 AND FileName CONTAINS <您正在处理的规则的名称>`。您可以编辑事件搜索查询。

- 单击**IOA ID**链接显示应用程序分配给每个规则的 ID。
  ID 无法修改。您可以单击**复制值到剪贴板**按钮复制 ID。
- **状态**– 在事件数据库扫描中使用规则。

详细信息选项卡包含以下信息：

- **名称**是您在添加规则时指定的规则的名称。
- **描述**是有关您指定的规则的任何附加信息。
- **重要级别**是对添加规则时用户指定的事件对计算机或公司 LAN 安全的可能影响的估计。
- **置信**是取决于添加规则时用户定义的误报可能性的置信度。
- **类型**是规则的类型，取决于生成它的服务器的角色：
  - **全球** — 在 PCN 服务器上创建。这些规则用于扫描此 PCN 服务器以及连接到此 PCN 服务器的所有 SCN 服务器上的事件。扫描的事件属于用户在应用程序 Web 界面中管理的租户。
  - **本地** — 在 SCN 服务器上创建。这些规则用于扫描此 SCN 服务器上的事件。扫描的事件属于用户在应用程序 Web 界面中管理的租户。
- **应用到**– 服务器的名称，包含在其上应用规则的 Central Node 组件。

查询选项卡显示正在被检查的查询的源代码。单击窗口上部的**运行查询**链接可转到**威胁搜索**部分并运行事件搜索查询。

搜索其中触发了 TAA (IOA) 规则的警报和事件

要搜索并显示由用户定义的 TAA (IOA) 规则触发创建的警报和事件：

1. 在应用程序 Web 界面的窗口中，选择**自定义规则**部分，**TAA**子部分。
   这将打开 TAA (IOA) 规则表。
2. 选择您要查看触发结果的规则。
   这将打开一个窗口，其中包含有关规则的信息。
3. 执行以下操作之一：
   - 如果您想查看TAA（IOA）规则触发生成的警报，请单击**警报**转至警报数据库。
     警报表将在新的浏览器选项卡中打开。
   - 如果您想查看TAA（IOA）规则触发生成的事件，请单击**事件**转至事件数据库。
     事件表将在新的浏览器选项卡中打开。

要搜索并显示由用户定义的 TAA (IOA) 规则触发创建的警报和事件：

要搜索并显示由 Kaspersky TAA (IOA) 规则触发创建的警报和事件：

1. 在应用程序 Web 界面窗口中选择**警报**部分。
   这将打开警报表。

2. 单击**技术**列中的链接打开筛选器配置窗口。

3. 在左侧的下拉列表中，选择**包含**。

4. 在右侧的下拉列表中，选择**（TAA）针对性攻击分析器**技术。

5. 单击**应用**。
   该表显示 TAA 技术根据 TAA (IOA) 规则生成的警报。

6. 选择一个警报，**检测到**列为其显示相关规则的名称。
   这将打开一个窗口，其中包含有关警报的信息。

7. 在**扫描结果**下面，单击带有规则名称的链接以打开规则信息窗口。

8. 执行以下操作之一：

   - 如果您想查看TAA（IOA）规则触发生成的警报，请单击**警报**转至警报数据库。
     警报表将在新的浏览器选项卡中打开。
   - 如果您想查看TAA（IOA）规则触发生成的事件，请单击**事件**转至事件数据库。
     事件表将在新的浏览器选项卡中打开。

要搜索并显示由 Kaspersky TAA (IOA) 规则触发创建的警报和事件：

筛选和搜索 TAA (IOA) 规则

要按所需条件筛选或搜索 TAA (IOA) 规则：

1. 在应用程序 Web 界面的窗口中，选择**自定义规则**部分，**TAA**子部分。
   这将打开 TAA (IOA) 规则表。

2. 根据筛选条件，执行以下操作：

   - **按重要性**

     a. 单击图标以打开 IOA 规则筛选配置窗口。

     b. 选择要包含在筛选条件中的重要性级别旁边的复选框：

     - **低**。
     - **中**。
     - **高**。

     c. 单击**应用**。

- **按规则类型**

  a. 单击**类型**链接以打开筛选配置窗口。

  b. 选择以下选项之一：

  - **所有** – 所有规则。
  - **全球** – 在 PCN 服务器上创建的规则。这些规则用于扫描此 PCN 服务器以及连接到此 PCN 服务器的所有 SCN 服务器上的事件。扫描的事件属于用户在应用程序 Web 界面中管理的租户。
  - **本地** – 在 SCN 服务器上创建的规则。这些规则用于扫描此 SCN 服务器上的事件。扫描的事件属于用户在应用程序 Web 界面中管理的租户。

- **按置信度**

  a. 单击**置信**链接以打开筛选配置窗口。

  b. 选择要添加到筛选条件的置信度旁边的复选框。

  - **低**。
  - **中**。
  - **高**。

  c. 单击**应用**。

- **按规则名称**

  a. 单击**IOA 标记**链接以打开筛选配置窗口。

  b. 输入 IOA 规则名称的一个或多个字符。

  c. 单击**应用**。

- **按服务器名称**

  a. 单击**服务器**链接以打开筛选配置窗口。

  b. 选择要包含在筛选条件中的租户或租户中的服务器旁边的复选框。

  c. 单击**应用**。

- **通过基于规则的警报生成**

  a. 单击**警报**链接以展开筛选器设置列表。

  b. 选择以下选项之一：

  - **所有。**
  - **已启用。**
  - **已禁用。**

- **按规则状态**

  a. 单击**状态**展开筛选器设置列表。

  b. 选择以下选项之一：

  - **所有。**
  - **已启用。**
  - **已禁用。**

该表仅显示与指定条件匹配的规则。

> 您可以同时使用多个筛选器。

重置 TAA (IOA) 规则筛选器

要根据一个或多个筛选条件清除 TAA (IOA) 规则筛选器：

1. 在应用程序 Web 界面的窗口中，选择**自定义规则**部分，**TAA**子部分。
   这将打开 TAA (IOA) 规则表。
2. 单击要为其清除筛选条件的规则表的列标题右侧的  。

   > 如果要清除多个筛选条件，请执行必要的操作以清除每个筛选条件。

   选定筛选器将被清除。

   该表仅显示与指定条件匹配的规则。

启用和禁用 TAA (IOA) 规则

具有**高级安全官**角色的用户可以启用或禁用一个或多个规则，也可以同时启用或禁用所有规则。

要在扫描事件时启用或禁用 TAA (IOA) 规则的使用：

1. 在应用程序 Web 界面的窗口中，选择**自定义规则**部分，**TAA**子部分。
   这将打开 TAA (IOA) 规则表。
2. 在具有相关规则的行中，选择或清除**状态**列中的复选框。

扫描事件时使用规则被启用或禁用。

要在扫描事件时启用或禁用所有或多个 TAA (IOA) 规则：

1. 在应用程序 Web 界面的窗口中，选择**自定义规则**部分，**TAA**子部分。
   这将打开 TAA (IOA) 规则表。
2. 选择要启用或禁用其使用的规则左侧的复选框。
   您可以通过选择包含列标题的行中的复选框来选择所有规则。
   控制面板出现在窗口的下部。
3. 单击**启用**或者**禁用**启用或禁用所有规则。

扫描事件时使用所选规则被启用或禁用。

在分布式解决方案和多租户模式下，您只能在 PCN 服务器上管理全局 TAA（IOA）规则。您可以在有权访问的租户的 SCN 服务器上管理本地 TAA (IOA) 规则。

具有**安全审计员**和**安全官**角色的用户无法启用或禁用 TAA (IOA) 规则。

修改 TAA (IOA) 规则

具有**高级安全官**角色的用户可以修改自定义 TAA (IOA) 规则。卡巴斯基创建的规则无法编辑。

在分布式解决方案和多租户模式下，您只能编辑在当前服务器上创建的 TAA (IOA) 规则。因此，在 PCN 的 Web 界面中，您只能编辑在 PCN 上创建的规则。在 SCN 的 Web 界面中，您只能编辑在 SCN 上创建的规则。

要编辑 TAA (IOA) 规则：

1. 在应用程序 Web 界面的窗口中，选择**自定义规则**部分，**TAA**子部分。
   这将打开 TAA (IOA) 规则表。
2. 选择要修改的规则。
   这将打开一个窗口，其中包含有关规则的信息。
3. 进行相关更改。
4. 单击**保存**。

规则设置已修改。

具有**安全审计员**和**安全官**角色的用户无法根据事件搜索条件修改 TAA (IOA) 规则。

删除 TAA (IOA) 规则

具有**高级安全官**角色的用户可以删除一条或多条 TAA (IOA) 规则，或同时删除所有规则。

在分布式解决方案和多租户模式下，您只能删除在当前服务器上创建的 TAA (IOA) 规则。因此，在 PCN 的 Web 界面中，您只能删除在 PCN 上创建的规则。在 SCN 的 Web 界面中，您只能删除在 SCN 上创建的规则。

要删除自定义 TAA (IOA) 规则：

1. 在应用程序 Web 界面的窗口中，选择**自定义规则**部分，**TAA**子部分。
   这将打开 TAA (IOA) 规则表。
2. 选择您想删除的规则。
   这将打开一个窗口，其中包含有关规则的信息。
3. 单击**删除**。
   这将打开操作确认窗口。
4. 单击**是**。

规则被删除。

要删除全部或多个自定义 TAA (IOA) 规则：

1. 在应用程序 Web 界面的窗口中，选择**自定义规则**部分，**TAA**子部分。
   这将打开 TAA (IOA) 规则表。
2. 选择您要删除的规则左侧的复选框。
   您可以通过选择包含列标题的行中的复选框来选择所有规则。
   控制面板出现在窗口的下部。
3. 单击**删除**。
   这将打开操作确认窗口。
4. 单击**是**。

所选文件将被删除。

您无法删除卡巴斯基定义的 TAA (IOA) 规则。如果您不想使用 Kaspersky TAA (IOA) 规则进行扫描，请将其添加到排除项。

具有**安全审计员**和**安全官**角色的用户无法根据事件搜索条件修改 TAA (IOA) 规则。

管理用户定义的 IOC 规则

您可以使用 IOC 文件在事件数据库和具有 Endpoint Agent 组件的计算机上搜索入侵指标。例如，如果您收到了有关当前正在传播的恶意软件的第三方信息，您可以：

1. 创建一个包含恶意软件入侵指标的 IOC 文件，并将其上传到 Kaspersky Anti Targeted Attack Platform 的 Web 界面。
2. 查找与所选 IOC 文件的条件相对应的事件。

   您可以查看此类事件，并且如果您希望 Kaspersky Anti Targeted Attack Platform 为选定事件生成警报，您可以创建 TAA (IOA) 规则。
3. 启用自动使用选定的 IOC 文件来搜索具有 Endpoint Agent 组件的计算机上的入侵指标。
4. 如果在扫描计算机时 Endpoint Agent 组件检测到入侵指标，Kaspersky Anti Targeted Attack Platform 会生成警报。

   您可以通过按技术名称过滤在警报表中找到这些警报。
5. 配置在具有 Endpoint Agent 组件的计算机上使用 IOC 文件搜索入侵指标的计划。

在分布式解决方案和多租户模式下，IOC 文件可以有以下类型：

- **本地** — 上传到 SCN 服务器的 IOC 文件。这些 IOC 文件用于搜索连接到 SCN 服务器的 Kaspersky Endpoint Agent 主机上的入侵指标。
- **全球** — 上传到 PCN 服务器的 IOC文件。这些 IOC 文件用于搜索连接到 PCN 服务器的 Kaspersky Endpoint Agent 主机以及连接到 PCN 服务器的所有 SCN 服务器上的入侵指标。

IOC 文件是以 .ioc 扩展名保存的文本文件。创建 IOC 文件时，请查看您在 Endpoint Agent 角色中使用的应用程序支持的 IOC 术语列表。您可以通过从下面的链接下载文件来查看受支持的 IOC 术语列表。

Kaspersky Endpoint Agent for Windows 和 Kaspersky Endpoint Security for Windows

Kaspersky Endpoint Security 12 for Linux

Kaspersky Endpoint Security 11.4 for Linux 和 Kaspersky Endpoint Security for Mac 不支持 IOC 文件。

通过哈希查找文件的 IOC 文件示例

```
<?xml version="1.0" encoding="us-ascii"?>

<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xmlns:xsd="http://www.w3.org/2001/XMLSchema"

id="UUID 格式的唯一 ID" last-modified="规则最后修改日期，格式为 YYYY-MM-DDT hh:mm:ss"
xmlns="http://schemas.mandiant.com/2010/ioc">

<short_description>规则名称</short_description>
```

```
<authored_by>规则名称</authored_by>

<authored_date>文件创建日期，格式为 YYYY-MM-DDThh:mm:ss</authored_date>

<links />

<definition>

<Indicator operator="OR" id="UUID 格式的唯一 ID">

<IndicatorItem id="UUID 格式的唯一 ID" condition="is">

<Context document="FileItem" search="FileItem/Md5sum" type="mir" />

<Content type="md5">文件的 MD5 哈希</Content>

</IndicatorItem>

</Indicator>

</definition>

</ioc>
```

每个 IOC 文件只能包含一条规则。规则可以具有任意复杂度。

具有**高级安全官**角色的用户可以将IOC 文件导入、删除或下载到计算机上，启用或禁用使用 IOC 文件搜索入侵指标，以及配置在装有 Endpoint Agent 组件的计算机上搜索入侵指标的计划。

具有**安全官**和**安全审计员**角色的用户可以查看 IOC 文件列表和有关所选文件的信息，并将IOC 文件导出到计算机。

查看 IOC 文件表

如果您使用分布式解决方案和多租户模式，请使用要为其配置参数的 PCN 或 SCN 服务器的 Web 界面。

IOC 文件表包含有关用于在安装了 Endpoint Agent 组件的计算机上进行扫描的 IOC 文件的信息；您可以在应用程序 Web 界面窗口**自定义规则**部分的**IOC**子部分中找到该表。

IOC 文件表包含以下信息：

1. — 将分配给使用此 IOC 文件生成的警报的重要性级别。
   重要性级别可以采用以下值之一：
   - — 低重要性。
   - — 中重要性。
   - — 高重要性。

2. **类型** – IOC 文件的类型，取决于应用程序操作模式和 IOC 文件上传到的服务器：

   - **本地** – 上传到 SCN 服务器的 IOC 文件。这些 IOC 文件用于搜索主机上的入侵指标，这些主机具有连接到 SCN 服务器的 Endpoint Agent 组件。
   - **全球** – 上传到 PCN 服务器的 IOC文件。这些 IOC 文件用于搜索具有连接到 PCN 服务器的 Endpoint Agent 组件的主机上以及连接到 PCN 服务器的所有 SCN 服务器上的入侵指标。

3. **名称** – IOC 文件的名称。
4. **服务器**是服务器的名称，具有对其应用规则的 PCN 或 SCN 角色。

   如果您使用的是分布式解决方案和多租户模式，则会显示此列。
5. **自动扫描** – 自动扫描具有 Endpoint Agent 组件的主机时使用 IOC 文件。

   使用此 IOC 文件扫描主机可能具有以下状态之一：

   - **已启用。**
   - **已禁用。**

查看有关 IOC 文件的信息

要查看 IOC 文件详细信息：

1. 在应用程序 Web 界面的窗口中，选择**自定义规则**部分，**IOC**子部分。

   这将打开 IOC 文件表。
2. 选择您想查看信息的 IOC 文件。

这将打开一个窗口，其中包含有关 IOC 文件的信息。

该窗口包含以下信息：

- 单击**查找警报**链接可打开**警报**部分，其中包含填充了所选 IOC 文件名称的筛选条件。
- 单击**查找事件**链接可打开**威胁搜索**部分，其中包含填充了所选 IOC 文件的入侵指标的搜索条件。
- 单击**下载**链接将打开 IOC 文件下载窗口。
- **自动扫描** – 自动扫描具有 Endpoint Agent 组件的主机时使用 IOC 文件。
- **名称** – IOC 文件的名称。
- **重要级别** – 必须分配给使用此 IOC 文件生成的警报的重要性级别。

  重要性级别可以采用以下值之一：

  - – 低重要性。
  - – 中重要性。
  - – 高重要性。

- **应用到** – 显示租户名称以及与基于此 IOC 文件扫描的事件关联的服务器名称（在分布式解决方案和多租户模式下）。
- **XML** – 以 XML 格式显示 IOC 文件内容。

上传 IOC 文件

不支持具有用于域用户的 UserItem 属性的 IOC 文件。

要上传 IOC 文件：

1. 在程序 Web 界面窗口中，选择**自定义规则**部分的**IOC**子部分。
   这将打开 IOC 文件表。
2. 单击**导入**。
   这将在您的本地计算机上打开文件选择窗口。
3. 选择您想上传的文件，然后单击**打开**。
4. 指定以下参数：
   a. **自动扫描** – 自动扫描具有 Endpoint Agent 组件的主机时使用 IOC 文件：
      - **已启用。**
      - **已禁用。**
   b. **名称** – IOC 文件的名称。
   c. **重要级别** – 必须分配给使用此 IOC 文件生成的警报的重要性级别：
      - **低。**
      - **中。**
      - **高。**
   d. **应用到** – 租户名称以及想要使用此 IOC 文件扫描的服务器名称（在分布式解决方案和多租户模式下）。
5. 单击**保存**。

IOC 文件将以 XML 格式上传。

下载 IOC 文件到计算机

您可以将之前上传的 IOC 文件下载到计算机上。

要下载 IOC 文件：

1. 在程序 Web 界面窗口中，选择**自定义规则**部分的**IOC**子部分。
   这将打开 IOC 文件表。
2. 选择您想下载的 IOC 文件。
   这将打开一个窗口，其中包含有关 IOC 文件的信息。
3. 根据您的浏览器设置，单击**下载**链接将文件保存到默认文件夹或指定保存文件的文件夹。

该 IOC 文件将被保存到浏览器下载文件夹中的计算机。

扫描主机时启用和禁用 IOC 文件的自动使用

您可以启用或禁用自动使用 IOC 文件来搜索具有 Endpoint Agent 组件的主机上的入侵指标。

要启用或禁用自动使用 IOC 文件来搜索具有 Endpoint Agent 组件的主机上的入侵指标：

1. 在程序 Web 界面窗口中，选择**自定义规则**部分的**IOC**子部分。
   这将打开 IOC 文件表。
2. 在包含要启用或禁用其使用的 IOC 文件的行中，在**状态**列中，将切换开关设置为以下位置之一：
   - **已启用。**
   - **已禁用。**

自动使用 IOC 文件来搜索具有 Endpoint Agent 组件的主机上的入侵指标被启用或禁用。

具有**安全审计员**和**安全官**角色的用户无法启用或禁用自动应用 IOC 文件。

删除 IOC 文件

要删除 IOC 文件：

1. 在程序 Web 界面窗口中，选择**自定义规则**部分的**IOC**子部分。
   这将打开 IOC 文件表。
2. 选择您想删除的 IOC 文件。
   这将打开一个窗口，其中包含有关 IOC 文件的信息。
3. 单击**删除**。

IOC 文件将被删除。

具有**安全审计员**和**安全官**角色的用户无法删除 IOC 文件。

在 IOC 扫描结果中搜索警报

要查找并查看所选 IOC 文件的扫描结果：

1. 在程序 Web 界面窗口中，选择**自定义规则**部分的**IOC**子部分。
   这将打开 IOC 文件表。
2. 选择您想查看扫描结果的 IOC 文件。
   这将打开一个窗口，其中包含有关 IOC 文件的信息。
3. 单击**查找警报**转至警报数据库。
   警报表将在新的浏览器选项卡中打开。

您还可以通过按技术名称筛选警报来查看所有 IOC 文件的扫描结果。

使用 IOC 文件搜索事件

要查看使用 IOC 文件找到的事件：

1. 在程序 Web 界面窗口中，选择**自定义规则**部分的**IOC**子部分。
   这将打开 IOC 文件表。
2. 选择用于在事件数据库中搜索事件的 IOC 文件。
   这将打开一个窗口，其中包含有关 IOC 文件的信息。
3. 单击**查找事件**转至事件数据库。
   事件表将在新的浏览器选项卡中打开。

筛选和搜索 IOC 文件

要按要求的条件筛选或搜索 IOC 文件：

1. 在程序 Web 界面窗口中，选择**自定义规则**部分的**IOC**子部分。
2. 这将打开 IOC 文件表。根据筛选条件，执行以下操作：

- **按重要性**

  a. 单击图标打开 IOC 文件的筛选配置窗口。

  b. 选择一个或多个以下重要性级别：

  - **低**。
  - **中**。
  - **高**。

  c. 单击**应用**。

- **按文件名**

  a. 单击**名称**链接以打开 IOC 文件筛选配置窗口。

  b. 输入 IOC 文件名的一个或多个字符。

  c. 单击**应用**。

- **按自动扫描的状态（已启用/禁用）**

  a. 单击**自动扫描**链接以打开 IOC 文件的筛选配置窗口。

  b. 选择以下选项之一：

  - **已启用。**
  - **已禁用。**

IOC 文件表将仅显示与您设置的筛选条件相匹配的 IOC 文件。

> 您可以同时使用多个筛选器。

清除 IOC 文件筛选器

要清除一个或多个筛选条件的 IOC 文件筛选器：

1. 在程序 Web 界面窗口中，选择**自定义规则**部分的**IOC**子部分。
2. 这将打开 IOC 文件表。单击您想清除其筛选条件的 IOC 文件表列标题右侧的。

   如果要清除多个筛选条件，请执行必要的操作以清除每个筛选条件。

   选定筛选器将被清除。

   IOC 文件表将仅显示与您设置的筛选条件相匹配的 IOC 文件。

配置 IOC 扫描时间表

您可以配置在具有 Endpoint Agent 组件的主机上使用 IOC 文件搜索入侵指标的计划。

具有**安全审计员**和**安全官**角色的用户无法配置使用 IOC 文件搜索入侵指标的计划。

要配置在具有 Endpoint Agent 组件的主机上使用 IOC 文件搜索入侵指标的计划：

1. 在应用程序 Web 界面的窗口中，选择**设置**部分，**Endpoint Agent**子部分，**IOC 扫描计划**设置组。
2. 在**启动时间**下拉列表中，选择搜索入侵指标的开始时间。该时间是在您正在执行配置的 Central Node 服务器的时区中指定的。

   如果 Endpoint Agent 获取新的扫描计划的时间晚于“**IOC 扫描计划**”中指定的时间，下一次扫描将于第二天的指定时间启动。
3. 在**最大扫描持续时间**下拉列表中，选择完成入侵指标搜索的时间限制。
4. 单击**应用**。

   保存更改后，使用具有 Endpoint Agent 组件的主机上的 IOC 文件搜索入侵指标的新计划立即生效。入侵指标搜索结果显示在警报表中。

管理使用 IOC 文件搜索入侵指标仅限于 Kaspersky Anti Targeted Attack Platform Web 界面提供的功能。没有提供管理入侵指标搜索的替代方法。

如果您以 Endpoint Agent 组件的角色使用 Kaspersky Endpoint Security for Windows，请确保 IOC 文件符合要求。您还必须考虑到，将 RegistryItem 数据类型添加到 IOC 搜索范围时，应用程序仅分析某些注册表项。

有关 IOC 文件和被扫描注册表项要求的更多详细信息，请参阅 Kaspersky Endpoint Security for Windows 在线帮助：

- 注册表中的 IOC 扫描范围（RegistryItem）。
- IOC 文件要求。

管理用户定义的入侵检测规则

为了检测网络流量中的入侵，您可以使用入侵检测规则和使用内置算法的其他入侵检测方法。当在流量中检测到攻击指标时，Kaspersky Anti Targeted Attack Platform 会记录*入侵检测*技术事件。

需要有效的 KATA 或 KATA + NDR 授权许可密钥来管理用户定义的入侵检测规则。

*入侵检测规则*描述可能表示网络攻击的流量异常。规则包含入侵检测系统用于分析流量的条件。

如果启用了基于规则的入侵检测方法，则应用入侵检测规则。您可以启用或禁用方法。

您可以使用以下类型的规则集：

- 系统规则集。这些规则集由卡巴斯基提供，用于检测最常见攻击或不必要的网络活动的指标。系统规则集在安装应用程序后立即可用。您可以通过安装更新来更新系统规则集。
- 用户定义的规则集。这些是您自己上传的规则集。您上传的文件必须包含定义入侵检测规则的数据结构。您要上传的文件必须都位于同一目录中，并且必须具有 .rules 扩展名。自定义规则集的名称与从其上传规则集的文件的名称相匹配。

  用户定义的入侵检测规则集显示在“**自定义规则→入侵检测**”部分。

该应用程序支持所有上传的规则集中总共最多 50000 条规则。您最多可以上传 100 个规则集。

从用户自定义规则集加载的规则可能包含流量分析条件，导致应用程序注册过多的规则触发事件。在这种情况下，您必须记住，注册过多事件会影响入侵检测系统的性能。

可以启用或禁用入侵检测规则集。如果启用了基于规则的入侵检测方法，则在流量分析期间将应用已启用规则集中的规则。如果禁用某个规则集，则不会应用该规则集中的规则。

上传规则集时，应用程序会检查其中包含的规则。如果在规则中发现任何错误，应用程序将阻止此类规则并且不会应用它们。如果在规则集的所有规则中发现错误或规则集不包含任何规则，则应用程序将禁用此规则集。

当在流量中检测到已启用集的规则中指定的条件时，应用程序会注册规则触发事件。使用系统事件类型进行注册，其代码如下：

- 4000003000 – 对于涉及系统规则集中的规则被触发的事件
- 4000003001 – 对于涉及用户定义规则集中的规则被触发的事件

用户定义的规则集可以包含从其他入侵检测和防护系统获得的规则。当处理这些规则时，应用程序不执行应用于网络数据包的指定操作（例如，丢弃和拒绝操作）。当入侵检测规则触发时，Kaspersky Anti Targeted Attack Platform 仅记录一个事件。

Kaspersky Anti Targeted Attack Platform 事件分数的数值与入侵检测规则中的优先级值相对应（见下表）。

规则优先级与事件分数的对应关系

入侵检测规则中的优先级值	Kaspersky Anti Targeted Attack Platform 事件分数
四个或以上	2.5
3	4.5
2	6.5
1	9

您可以在“**设置→事件类型**”下配置注册入侵检测事件的设置。

您可以在已注册事件表中查看入侵检测事件。

拥有“**高级安全官**”角色的用户可以上传、启用和禁用用户定义的入侵检测规则集。拥有“**安全审计员**”角色的用户可以查看用户定义的检测规则集。拥有“**安全官**”角色的用户无权访问用户定义的入侵检测规则集。

入侵检测规则

*入侵检测规则*描述可能表示网络攻击的流量异常。规则包含入侵检测系统用于分析流量的条件。

如果启用了基于规则的入侵检测方法，则应用入侵检测规则。您可以启用或禁用方法。

您可以使用以下类型的规则集：

- 系统规则集。这些规则集由卡巴斯基提供，用于检测最常见攻击或不必要的网络活动的指标。系统规则集在安装应用程序后立即可用。您可以通过安装更新来更新系统规则集。
- 用户定义的规则集。这些是您自己上传的规则集。您上传的文件必须包含定义入侵检测规则的数据结构。您要上传的文件必须都位于同一目录中，并且必须具有 .rules 扩展名。自定义规则集的名称与从其上传规则集的文件的名称相匹配。

该应用程序支持所有上传的规则集中总共最多 50000 条规则。您最多可以上传 100 个规则集。

从用户自定义规则集加载的规则可能包含流量分析条件，导致应用程序注册过多的规则触发事件。在这种情况下，您必须记住，注册过多事件会影响入侵检测系统的性能。

可以启用或禁用入侵检测规则集。如果启用了基于规则的入侵检测方法，则在流量分析期间将应用已启用规则集中的规则。如果禁用某个规则集，则不会应用该规则集中的规则。

上传规则集时，应用程序会检查其中包含的规则。如果在规则中发现任何错误，应用程序将阻止此类规则并且不会应用它们。如果在规则集的所有规则中发现错误或规则集不包含任何规则，则应用程序将禁用此规则集。

当在流量中检测到已启用集的规则中指定的条件时，应用程序会注册规则触发事件。使用系统事件类型进行注册，其代码如下：

- 4000003000 – 对于涉及系统规则集中的规则被触发的事件
- 4000003001 – 对于涉及用户定义规则集中的规则被触发的事件

用户定义的规则集可以包含从其他入侵检测和防护系统获得的规则。当处理这些规则时，应用程序不执行应用于网络数据包的指定操作（例如，丢弃和拒绝操作）。当入侵检测规则触发时，Kaspersky Anti Targeted Attack Platform 仅记录一个事件。

Kaspersky Anti Targeted Attack Platform 事件分数的数值与入侵检测规则中的优先级值相对应（见下表）。

规则优先级与事件分数的对应关系

入侵检测规则中的优先级值	Kaspersky Anti Targeted Attack Platform 事件分数
四个或以上	2.5
3	4.5
2	6.5
1	9

其他入侵检测方法

为了检测入侵，您可以使用以下附加方法：

- 检测 ARP 数据包中伪造地址的迹象（ARP 欺骗）。

  如果启用了 ARP 欺骗检测，Kaspersky Anti Targeted Attack Platform 会检查 ARP 数据包中指定的地址并检测低级中间人 (MITM) 攻击的指标。在使用 ARP 协议的网络中，这种类型的攻击表现为在流量中发现虚假 ARP 消息。

  当检测到 ARP 欺骗指标时，应用程序会注册入侵检测技术事件。使用系统事件类型进行注册，其代码如下：

  - 4000004001 用于检测与 ARP 请求无关的多个 ARP 响应的事件。
  - 4000004002 用于检测从同一 MAC 地址到不同收件人的多个 ARP 请求的事件。

- TCP 协议异常检测。

  如果启用了 TCP 协议异常检测，Kaspersky Anti Targeted Attack Platform 将扫描受支持的应用程序层协议中数据流的 TCP 段。

  当 Kaspersky Anti Targeted Attack Platform 检测到包含不同内容的重叠 TCP 段的数据包时，它会记录入侵检测技术事件。事件注册的系统事件类型代码为 4000002701。

- IP 协议异常检测。

  如果启用了 IP 协议异常检测，Kaspersky Anti Targeted Attack Platform 将扫描碎片化的 IP 数据包。

  当检测到 IP 数据包组装错误时，应用程序会注册入侵检测技术事件。使用系统事件类型进行注册，其代码如下：

  - 4000005100 用于在 IP 数据包组装过程中检测数据冲突的事件（IP 片段重叠）
  - 4000005101 用于检测超过最大允许大小的 IP 数据包的事件（IP 片段溢出）
  - 4000005102 用于检测初始片段小于预期（IP 片段太小）的 IP 数据包的事件
  - 4000005103 用于检测 IP 数据包片段的误关联事件（误关联片段）

- 暴力攻击和扫描检测。

  启用暴力攻击和扫描检测后，Kaspersky Anti Targeted Attack Platform 会检查网络活动统计数据，以检测暴力攻击、拒绝服务攻击、扫描、网络服务欺骗和其他异常的指标。

  此方法使用内置规则。当触发规则时，应用程序会注册入侵检测技术事件。这些事件使用被分配了代码 4000003002 的系统事件类型进行注册。

您可以启用或禁用方法。无论入侵检测规则是否存在或是否启用，都可以应用其他入侵检测方法。其他检测方法使用内置算法。

启用和禁用入侵检测规则集

入侵检测规则集可以*启用*或*禁用*。如果禁用某个规则集，则该规则集中的任何规则都不会用于入侵检测。

启用或禁用选定的规则集时，入侵检测系统将在安装了应用程序组件（Central Node 和 Sensor）的所有计算机上重新启动。必须重新启动才能应用更改。

只有拥有"**高级安全官**"角色的用户可以改变入侵检测规则集的状态。

要更改入侵检测规则集的状态：

1. 在应用程序 Web 界面的窗口中，选择"**自定义规则**"部分，"**入侵检测**"子部分。
2. 选中要更改其状态的规则集旁边的复选框。
3. 右键单击以打开上下文菜单。
4. 在上下文菜单中，选择以下命令之一：
   - 如果要启用所选规则集中所有已禁用的规则集，**启用**。
   - 如果要禁用所选规则集中所有已启用的规则集，**禁用**。
   - 如果要反转所有选定规则集的状态，**更改选定规则集的状态**。此选项允许您在安装了应用程序组件的所有计算机上快速启用和禁用具有不同状态的选定规则集：要应用更改，您只需在这些计算机上重新启动一次入侵检测系统。
5. 在确认窗口中，单击"**确定**"。

入侵检测规则集的状态发生改变。

加载和替换用户定义的入侵检测规则集

您可以将入侵检测规则集从文件上传到应用程序中。要上传到应用程序，具有入侵检测规则描述的文件必须位于同一文件夹中并具有 .rules 扩展名。文件名不能包含以下字符：`\ / : * ? , " < > |`

从文件上传的入侵检测规则作为用户定义的规则集保存在应用程序中。规则集的名称与上传规则集的文件的名称相同。

> 从文件上传规则集时，当前用户自定义规则集将从表中删除并替换为新规则集。

只有拥有"**高级安全官**"角色的用户可以上传用户定义的入侵检测规则集。

要上传和替换用户定义的入侵检测规则集：

1. 在应用程序 Web 界面的窗口中，选择"**自定义规则**"部分，"**入侵检测**"子部分。
2. 在工具栏中，单击"**替换所有用户定义的规则**"按钮。

3. 在确认窗口中，单击“**确定**”。

   这将打开文件上传窗口。

4. 选择包含所需文件的文件夹，然后单击按钮从该文件夹上传文件。

   规则集表显示新的用户自定义规则集。所有没有错误的规则集均已启用。

5. 检查上传的规则集是否有错误。

   有关检测到的错误的信息显示在“**规则**”列中。如果没有错误，则会显示“*正常*”状态。如果规则集包含错误，您可以点击“**详细信息**”查看有关它们的详细信息。

6. 如有必要，启用或禁用规则集（包括状态为“*一些规则有错误*”的规则集）。

用户自定义的入侵检测规则集被上传。

删除用户定义的入侵检测规则集

您可以删除从文件上传到应用程序中的所有用户定义的入侵检测规则集。无法选择要删除的用户自定义规则集。如果您只想使用应用程序中当前的某些规则集，可以将包含这些规则集的文件复制到单独的文件夹中，用该文件夹中的规则集替换所有用户定义的规则集。

只有拥有“**高级安全官**”角色的用户可以删除用户定义的入侵检测规则集。

要删除用户自定义的入侵检测规则集：

1. 在应用程序 Web 界面的窗口中，选择“**自定义规则**”部分，“**入侵检测**”子部分。

2. 在工具栏中，单击“**删除所有用户定义的规则**”按钮。

3. 在确认窗口中，单击“**确定**”。

   这将打开一个窗口，用于选择包含入侵检测规则文件的文件夹。

所有用户定义的入侵检测规则集都将从表中删除。

管理用户定义的 YARA 规则

您可以使用 YARA 规则作为 YARA 模块数据库来扫描在 Central Node 接收的文件和对象，并扫描安装有 Endpoint Agent 组件的主机。

在分布式解决方案和多租户模式下，自定义 YARA 规则可以具有以下类型之一：

- **全球** — 在 PCN 服务器上创建。这些规则被用于扫描在 PCN 服务器以及连接到该 PCN 服务器的所有 SCN 服务器上收到的文件和对象。扫描的文件和对象属于用户在应用程序 Web 界面中管理的租户。
- **本地** — 在 SCN 服务器上创建。这些规则被用于扫描在 SCN 服务器上收到的文件和对象。扫描的文件和对象属于用户在应用程序 Web 界面中管理的租户。

在管理应用程序 Web 界面时，具有**高级安全官**角色的用户可以使用应用程序 Web 界面将 YARA 规则文件导入 Kaspersky Anti Targeted Attack Platform。

具有**安全审计员**和**安全官**角色的用户只能查看 YARA 规则。

查看 YARA 规则表

用户定义的 YARA 规则表包含有关用于扫描文件和对象以及创建警报的 YARA 规则的信息；该表显示在应用程序 Web 界面窗口的**自定义规则**部分，**YARA**子部分。

表包含以下信息：

- **已创建**是规则创建时间。
- — 根据卡巴斯基的经验，对于 Kaspersky Anti Targeted Attack Platform 用户而言，警报重要性取决于此警报可能对计算机或企业 LAN 安全造成的影响。

  默认情况下，通过上传的 YARA 规则扫描生成的警报被分配高重要性。
- **类型**是规则的类型，具体取决于应用程序的操作模式和生成规则的服务器的角色：
  - **全球** — 在 PCN 服务器上创建。这些规则被用于扫描在 PCN 服务器以及连接到该 PCN 服务器的所有 SCN 服务器上收到的文件和对象。扫描的文件和对象属于用户在应用程序 Web 界面中管理的租户。
  - **本地** — 在 SCN 服务器上创建。这些规则被用于扫描在 SCN 服务器上收到的文件和对象。扫描的文件和对象属于用户在应用程序 Web 界面中管理的租户。
- **名称** — 规则的名称。
- **文件名**是从中导入规则的文件的名称。
- **创建者**是用于导入规则的账户的用户的名称。
- **服务器**是服务器的名称，具有对其应用规则的 PCN 或 SCN 角色。

  如果您使用的是分布式解决方案和多租户模式，则会显示此列。
- **流量扫描**流扫描文件和对象到达 Central Node 时规则的使用情况：
  - **已启用**– 规则正在被使用。
  - **已禁用**– 该规则未被使用。

配置 YARA 规则表显示

您可以显示或隐藏列并更改表中列的顺序。

要配置表格显示：

1. 在应用程序 Web 界面窗口中，选择**自定义规则**部分的**YARA**子部分。

   这将打开 YARA 规则表。
2. 在表格的标题部分，单击 。

   这将打开**定制表格**窗口。
3. 如果要在表中显示列，请选择要在表中显示的参数名称旁边的复选框。

如果要隐藏表中的参数，请清除该复选框。

> 必须选择至少一个复选框。

4. 如果要更改表格中列的顺序，请将鼠标光标移动到具有相关参数的行，单击 ⠿ 并将该行移动到新位置。
5. 如果要恢复默认表格显示设置，请单击**默认**。
6. 单击**应用**。

表格显示已配置。

导入 YARA 规则

要导入 YARA 规则：

1. 在程序 Web 界面窗口中，选择**自定义规则**部分的**YARA**子部分。
2. 单击**上传**。
   这将打开文件选择窗口。
3. 选择您想上传的 YARA 规则文件，然后单击“**打开**”。
   这将关闭文件选择窗口并打开**导入 YARA 规则**窗口。

> 上传文件的最大允许大小为 20 MB。

报告显示在窗口的下部。报告包含以下信息：

- 可以成功导入的规则数量。
- 不导入的规则数量（如果有）。
  对于每条无法导入的规则，都会列出其名称。

4. 选择**流量扫描**，如果要使用导入的规则对在 Central Node 接收的对象和数据进行流式扫描。
5. 如有必要，请在**描述**字段中输入任何附加信息。

> **重要级别**字段无法编辑。默认情况下，由上传的 YARA 规则生成的警报被分配高重要性级别。

6. 在**应用到**下面，选择与要对其应用规则的服务器对应的复选框。
   仅当您使用分布式方案和多租户模式时，才会显示该字段。
7. 单击**保存**。

导入的规则显示在 YARA 规则表中。

查看 YARA 规则详细信息

要查看 YARA 规则详细信息：

1. 在应用程序 Web 界面窗口中，选择**自定义规则**部分的**YARA**子部分。
   这将打开 YARA 规则表。
2. 选择您想查看信息的规则。

这将打开一个窗口，其中包含有关规则的信息。

该窗口包含以下信息：

- 单击**警报**链接即可在新的浏览器选项卡中显示警报表。警报将根据针对性攻击分析器技术和您正在处理的TAA (IOA) 规则的名称进行筛选。
- **启动 YARA 扫描**链接将打开任务创建窗口。
- **下载**链接可让您下载包含 YARA 规则的文件。
- **规则名称**是文件中指定的规则的名称。
- **流量扫描**流扫描文件和对象到达 Central Node 时规则的使用情况：
- **类型**是规则的类型，取决于生成它的服务器的角色：
  - **全球** — 在 PCN 服务器上创建。这些规则被用于扫描在 PCN 服务器以及连接到该 PCN 服务器的所有 SCN 服务器上收到的文件和对象。扫描的文件和对象属于用户在应用程序 Web 界面中管理的租户。
  - **本地** — 在 SCN 服务器上创建。这些规则被用于扫描在 SCN 服务器上收到的文件和对象。扫描的文件和对象属于用户在应用程序 Web 界面中管理的租户。
- **重要级别**是分配给根据此规则扫描而创建的警报的重要性级别。
  默认情况下，通过上传的 YARA 规则扫描生成的警报被分配高重要性。
- **描述**是有关您指定的规则的任何附加信息。
- **应用到**– 服务器的名称，包含在其上应用规则的 Central Node 组件。

筛选和搜索 YARA 规则

要按所需条件筛选或搜索 YARA 规则：

1. 在应用程序 Web 界面窗口中，选择**自定义规则**部分的**YARA**子部分。
   这将打开 YARA 规则表。

2. 根据筛选条件，执行以下操作：

- **按创建时间**

  a. 单击**已创建**链接以打开筛选设置窗口。

  b. 选择以下选项之一：

  - **任何时候**如果您希望表显示任何时间创建的规则。
  - **上一个小时**，如果您希望应用程序显示表中最后一小时创建的规则。
  - **最后一天**，如果您希望应用程序显示表中最后一天创建的规则。
  - **自定义范围**，如果您希望应用程序显示表中在指定时段内创建的规则。

  c. 如果您选择了**自定义范围**，请选择该期间的开始日期和结束日期，然后单击**应用**。

- **按规则名称**

  a. 单击**规则名称**链接以打开筛选菜单。

  b. 在下拉列表中，选择以下筛选运算符之一：

  - **包含**
  - **不包含**

  c. 在文本框中，键入规则名称或规则名称中的字符序列。

  d. 单击**应用**。

- **按文件名**

  a. 单击**文件名**链接以打开筛选菜单。

  b. 在下拉列表中，选择以下筛选运算符之一：

  - **包含**
  - **不包含**

  c. 在输入字段中，键入文件名或文件名中的字符序列。

  d. 单击**应用**。

- **按上传规则文件的用户名**

  a. 单击**创建者**链接以打开筛选菜单。

  b. 在下拉列表中，选择以下筛选运算符之一：

  - **包含**
  - **不包含**

c. 在文本框中，键入用户名或用户名中的字符序列。

d. 单击**应用**。

- **按规则状态**

  a. 单击**流量扫描**链接以展开筛选器设置列表。

  b. 选择以下选项之一：

  - **所有。**
  - **已启用。**
  - **已禁用。**

该表仅显示与指定条件匹配的规则。

您可以同时使用多个筛选器。

清除 YARA 规则筛选器

要清除 YARA 规则筛选器的一个或多个筛选条件：

1. 在应用程序 Web 界面窗口中，选择**自定义规则**部分的**YARA**子部分。
   这将打开 YARA 规则表。
2. 单击要为其清除筛选条件的规则表的列标题右侧的。
   如果要清除多个筛选条件，请采取步骤单独清除每个筛选条件。

选定筛选器将被清除。

该表仅显示与指定条件匹配的规则。

启用和禁用 YARA 规则

具有**高级安全官**角色的用户可以启用或禁用一个或多个规则，也可以同时启用或禁用所有规则。

在分布式解决方案和多租户模式下工作时，您只能启用或禁用在当前服务器上创建的 YARA 规则。这意味着在 PCN 的 Web 界面中，您只能启用或禁用在 PCN 服务器上创建的规则。在 SCN 的 Web 界面中，您只能启用或禁用在 SCN 服务器上创建的规则。

如果在 PCN 和 SCN 服务器上启用了同名的 YARA 规则，则扫描文件和对象时 PCN 规则优先于 SCN 规则。

要启用或禁用用于流扫描到达 Central Node 的文件和对象的 YARA 规则：

1. 在应用程序 Web 界面窗口中，选择**自定义规则**部分的**YARA**子部分。
   这将打开 YARA 规则表。
2. 在具有相关规则的行中，选择或清除**流量扫描**列。

该规则针对到达 Central Node 的流扫描文件和对象启用或禁用。

要启用或禁用所有或多个 YARA 规则以流扫描到达 Central Node 的文件和对象：

1. 在程序 Web 界面窗口中，选择**自定义规则**部分的**YARA**子部分。
2. 选择要启用或禁用其使用的规则左侧的复选框。
   您可以通过选择包含列标题的行中的复选框来选择所有规则。
   控制面板出现在窗口的下部。
3. 单击**启用**或者**禁用**启用或禁用所有规则。

所选规则针对到达 Central Node 的流扫描文件和对象启用或禁用。

删除 YARA 规则

要删除 YARA 规则:

1. 在应用程序 Web 界面窗口中，选择**自定义规则**部分的**YARA**子部分。
   这将打开 YARA 规则表。
2. 选择您想删除的规则。
   这将打开一个窗口，其中包含有关规则的信息。
3. 单击**删除**。
4. 这将打开操作确认窗口；在该窗口中，单击**是**。

规则被删除。

要删除全部或多个 YARA 规则：

1. 在应用程序 Web 界面窗口中，选择**自定义规则**部分的**YARA**子部分。
   这将打开 YARA 规则表。
2. 选择您要删除的规则左侧的复选框。
   您可以通过选择包含列标题的行中的复选框来选择所有规则。
   控制面板出现在窗口的下部。

3. 单击**删除**。

4. 这将打开操作确认窗口；在该窗口中，单击**是**。

所选文件将被删除。

具有**安全审计员**和**安全官**角色的用户无法删除 YARA 规则。

管理存储和隔离区中的对象

存储区被用于存储必须被发送进行扫描的文件以及运行任务所获得的文件：**获取文件**，**从隔离区恢复文件**，**进行取证**，**获取 NTFS 图元文件**，**获取注册表键**，**获取进程内存转储**。

存储位于 Central Node 服务器上。

您可以按照以下方式管理存储中的对象：删除、下载、上传和发送待扫描的对象，以及过滤对象列表。

Kaspersky Anti Targeted Attack Platform 将存储中的对象显示为对象表。

如果您使用分布式解决方案和多租户模式，存储位于 PCN 和 SCN 服务器上。PCN 服务器的 Web 界面显示有关用户有权访问的租户的所有已连接 SCN 的存储信息。

具有**高级安全官**角色的用户可以使用任务将对象副本放入存储，或者使用 PCN 或 SCN 服务器（用于管理用户有权访问的租户）上的 Kaspersky Anti Targeted Attack Platform Web 界面将对象上传到存储。

具有**安全官**角色的用户只能处理作为同一用户在 PCN 或 SCN 服务器上创建的任务的一部分收到的文件，该服务器用于管理用户有权访问的租户。

如果您认为某个文件具有威胁，可以使用 Endpoint Agent 组件将其在计算机上隔离。被隔离文件的元数据显示在 Kaspersky Anti Targeted Attack Platform Web 界面的**存储**部分，**隔离区**子部分。

*Kaspersky Anti Targeted Attack Platform 服务器上的隔离区*是 Kaspersky Anti Targeted Attack Platform 解决方案服务器部分的存储区域，用于存储在 Endpoint Agent 计算机上隔离的对象的元数据，位于 Kaspersky Anti Targeted Attack Platform Web 界面的**存储**部分，**隔离区**子部分。

您可以管理被隔离的对象：从隔离区恢复对象和将 Endpoint Agent 计算机上隔离的对象的副本上传到 Kaspersky Anti Targeted Attack Platform 的存储。

Kaspersky Anti Targeted Attack Platform 以表格形式显示有关隔离对象的信息。

存储的最大容量是在配置应用程序大小时确定的。一旦超过此阈值，应用程序就开始从存储区中移除最早的对象副本。当占用的空间量再次低于阈值时，应用程序停止从存储区中删除对象的副本。

可以放置在存储中的对象的最大大小为 1 GB。

由于从隔离区恢复对象所需的元数据，对象的实际大小可能大于对象的表观大小。隔离对象时，会考虑其实际大小。加密文件可能以解密形式发送（取决于加密设置），压缩文件按原样发送。

查看放入存储中的对象表

放入备份区中的对象表位于应用程序 Web 界面窗口的**存储**部分，**文件**子部分。

放入存储区中的对象表包含以下信息：

1. **类型**是将对象放入存储区的方法。
   可以采用以下方法：
   - – 该对象通过以下方式之一放置在存储中：
     - **获取文件**任务已运行。
     - 收到了在带有 Endpoint Agent 组件的主机上被隔离的对象的副本（在**存储**部分，**隔离区**子部分，在菜单中选择了对具有对象目录的链接的**从隔离区获取文件**操作）。
   - – 该对象通过以下方式之一放置在存储中：
     - **进行取证**任务已运行。
     - **获取进程内存转储**任务已运行。
     - **获取注册表键**任务已运行。
     - **获取 NTFS 图元文件**任务已运行。
   - – 对象是由用户在**存储**部分的**文件**子部分中手动下载的。
2. **对象** – 有关该对象的信息。例如，文件名或文件路径。
3. **扫描结果** – 对象扫描结果。
   扫描结果显示为以下值之一：
   - **未检测到** – 扫描的结果是，应用程序未检测到针对性攻击、疑似感染对象或可疑活动的迹象。
   - **错误** – 对象扫描以错误结束。
   - **进行中** – 对象扫描尚未开始。
   - **未扫描** – 对象未被发送以进行扫描。
   - **检测到** – 扫描的结果是，应用程序检测到针对性攻击、疑似感染对象或可疑活动的迹象。
4. **服务器**是具有 PCN 或 SCN 角色的服务器的名称。从中接收对象的主机连接到此服务器。
   如果您使用的是分布式解决方案和多租户模式，则会显示此列。
5. **源** – 从中接收对象的主机的 IP 地址或名称，或上载对象的用户账户的名称。
6. **存储时间** – 对象放入存储区中的日期和时间。

7. **操作** – 可以对对象执行的操作。如下操作可用：

   - – 删除存储区中的对象。
   - – 将对象发送到存储中，以便通过反恶意软件引擎、YARA 和 Sandbox 技术进行扫描。
   - – 将对象从存储下载到您的计算机。

单击具有文件名称或文件路径的链接将打开一个列表，您可以在其中选择以下操作之一：

- **按照此值进行过滤**。
- **从过滤器中排除**。
- **下载**。
- **发送文件进行扫描**。
- **查找事件**：
  - **文件路径**。
  - **MD5**。
  - **SHA256**。
- **查找警报**：
  - **文件路径**。
  - **MD5**。
  - **SHA256**。
- **复制值到剪贴板**。

单击具有主机名的链接将打开一个列表，您可以从其中选择以下操作之一：

- **按照此值进行过滤**。
- **从过滤器中排除**。
- **查找事件**。
- **查找警报**。
- **复制值到剪贴板**。

使用 Web 界面查看有关手动放置在存储中的对象的信息

要查看被手动放置在存储中的对象的信息：

1. 在应用程序 Web 界面窗口中，选择**存储**部分，**文件**子部分。
   这将打开对象表。
2. 在表中，选择带有您要查看其信息的↥图标的对象。
   这将打开对象详细信息窗口。

该窗口包含以下信息：

- **文件名** – 文件的名称。
- **大小** – 文件的大小。
- **MD5** – 文件的 MD5 哈希。
- **SHA256** – 文件的 SHA256 哈希。
- **上传时间** – 上传用户手动上传对象的时间。
- **用户名称** –手动将对象上传到存储区的用户账户名称。
- **扫描结果**– 应用程序的对象扫描结果。

在 Kaspersky TIP 上查找按钮允许在 Kaspersky Threat Intelligence Portal 上查找文件。

单击**创建防止规则**以阻止文件运行。

您可以单击**下载**将文件下载到计算机的硬盘上。

单击具有文件名称的链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **复制值到剪贴板**。

单击具有“**MD5**”的链接将打开一个列表，您可以从其中选择以下操作之一：

- **在 Kaspersky TIP 上查找**。
- **查找事件**。
- **查找警报**。
- **创建防止规则**。
- **复制值到剪贴板**。

单击具有 **SHA256** 的链接将打开一个列表，您可以从其中选择以下操作之一：

- **在 Kaspersky TIP 上查找**。
- **在 virustotal.com 上查找**。
- **查找事件**。
- **查找警报**。
- **创建防止规则**。
- **复制值到剪贴板**。

查看有关通过获取文件任务放置在存储中的对象的信息

*查看有关被**获取文件**或者**从隔离区获取文件**任务放置在存储中的对象的信息：*

1. 在应用程序 Web 界面窗口中，选择**存储**部分，**文件**子部分。
   这将打开对象表。
2. 在表中，选择带有您要查看其信息的图标的对象。
   这将打开对象详细信息窗口。

该窗口包含以下信息：

- 推荐组。以下建议可以显示：
  - “**任务**”链接打开将对象放入存储的任务。
  - “**警报**”链接可打开警报，其中包含被放置在存储中的对象。
  - “**隔离的对象**”链接打开隔离对象的元数据。
- **对象**— 文件名或路径。
- **大小** — 文件的大小。
- **MD5** — 文件的 MD5 哈希。
- **SHA256** — 文件的 SHA256 哈希。
- **存储时间** — 对象放入存储区中的时间。
- **租户** — Central Node、PCN 或 SCN 服务器所属租户的名称。
- **服务器** — Central Node、PCN 或 SCN 服务器的名称。从中接收对象的主机连接到此服务器。
- **主机** — 接收对象的主机的名称。
- **扫描结果**— 应用程序的对象扫描结果。

点击“**Sandbox 检测**”显示文件行为分析结果的详细信息。

只有当 Sandbox 检测该文件时，才会显示文件行为分析结果。如果文件上传到系统，然后在 Sandbox 中扫描，但组件没有检测到威胁，则不会显示结果。

在 Kaspersky TIP 上查找按钮允许在 Kaspersky Threat Intelligence Portal 上查找文件。

单击**创建防止规则**以阻止文件运行。

您可以单击**下载**将文件下载到计算机的硬盘上。

单击具有文件名称的链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **复制值到剪贴板**。

单击具有“**MD5**”的链接将打开一个列表，您可以从其中选择以下操作之一：

- **在 Kaspersky TIP 上查找**。
- **查找事件**。
- **查找警报**。
- **创建防止规则**。
- **复制值到剪贴板**。

单击具有 **SHA256** 的链接将打开一个列表，您可以从其中选择以下操作之一：

- **在 Kaspersky TIP 上查找**。
- **在 virustotal.com 上查找**。
- **查找事件**。
- **查找警报**。
- **创建防止规则**。
- **复制值到剪贴板**。

查看有关通过获取数据任务放置在存储中的对象的信息

*查看有关被**进行取证**、**获取进程内存转储**、**获取注册表键**、**获取 NTFS 图元文件**任务放置在存储中的对象的信息：*

1. 在应用程序 Web 界面窗口中，选择**存储**部分，**文件**子部分。

   这将打开对象表。

2. 在表中，选择带有您要查看其信息的图标的对象。
   这将打开对象详细信息窗口。

该窗口包含以下信息：

- **对象**是文件名或路径。
- **大小** — 文件的大小。
- **MD5** — 文件的 MD5 哈希。
- **SHA256** — 文件的 SHA256 哈希。
- **存储时间** — 对象放入存储区中的时间。
- **主机** — 接收对象的主机的名称。

您可以单击**下载**将文件下载到计算机的硬盘上。

单击具有文件名称的链接将打开一个列表，您可以从其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **复制值到剪贴板**。

单击具有“**MD5**”的链接将打开一个列表，您可以从其中选择以下操作之一：

- **在 Kaspersky TIP 上查找**。
- **查找事件**。
- **查找警报**。
- **创建防止规则**。
- **复制值到剪贴板**。

单击具有 **SHA256** 的链接将打开一个列表，您可以从其中选择以下操作之一：

- **在 Kaspersky TIP 上查找**。
- **在 virustotal.com 上查找**。
- **查找事件**。
- **查找警报**。
- **创建防止规则**。
- **复制值到剪贴板**。

从存储下载对象

如果您认为存储区中的某个对象是安全的，可以将它下载到本地计算机。

下载受感染对象可能会对本地计算机的安全构成威胁。

要下载存储区中的对象：

1. 在应用程序 Web 界面窗口中，选择**存储**部分，**文件**子部分。
   这将打开对象表。
2. 在包含要下载的对象名称的行的右侧部分，单击。

该对象将保存到浏览器下载文件夹中的本地计算机。文件以 ZIP 存档形式下载，并受密码“infected”保护。

将对象上传到存储

如果需要扫描特定对象，可以将此对象上载到存储并发送以进行扫描。

要上传对象到存储区中：

1. 在应用程序 Web 界面窗口中，选择**存储**部分，**文件**子部分。
   这将打开对象表。
2. 在窗口的右上角，单击**上传**。
   这将打开文件选择窗口。
3. 选择您想上传到存储的对象。
4. 如果要将扩展名为 .Lnk 的文件上传到存储：
   a. 在**文件名**字段中，输入 *.Lnk 并按**Enter**。
   b. 选择对象。
5. 单击**打开**。

对象将被上传到存储并显示在对象表中。

具有**安全审计员**角色的用户无法将对象上传到存储。

发送存储中的对象进行扫描

您可以使用反恶意软件引擎和 YARA 技术对包含 Central Node 组件以及 Sandbox 组件的存储区对象进行扫描。

在以下情况下，建议从存储区中发送要扫描的对象：

- 放入存储区时扫描对象已被禁用。
- 应用程序数据库已更新。
- 手动将对象上传到存储区。

要从存储发送对象进行扫描：

1. 在应用程序 Web 界面窗口中，选择**存储**部分，**文件**子部分。
   这将打开对象表。
2. 单击您想扫描的对象。
   这将打开对象详细信息窗口。
3. 单击**扫描**。
   对象扫描将开始。
   对象扫描完成后，其状态将显示在对象表中。

您还可以通过单击被放置在存储中的对象表中的对象信息行的右侧部分的发送存储中的对象进行扫描。

具有**安全审计员**角色的用户无法扫描存储中的对象。

删除存储中的对象

要删除存储区中的对象：

1. 在应用程序 Web 界面窗口中，选择**存储**部分，**文件**子部分。
   这将打开对象表。
2. 单击您想删除的对象。
   这将打开对象详细信息窗口。
3. 单击**删除**。
   这将打开操作确认窗口。
4. 单击**是**。

该对象将从存储区中删除。

您还可以通过单击被放置在存储中的对象表中的对象信息行的右侧部分的删除存储中的对象。

要从存储中删除所有或多个对象：

1. 在应用程序 Web 界面窗口中，选择**存储**部分，**文件**子部分。
   这将打开对象表。
2. 选择要从存储中删除的对象旁边的复选框。
   您可以通过选择包含列标题的行中的复选框来选择所有对象。
3. 在窗口下部显示的窗格中，单击**删除**。
   这将打开操作确认窗口。
4. 单击**是**。

选定的对象将从存储中删除。

具有**安全审计员**角色的用户无法删除存储中的对象。

按对象类型筛选存储中的对象

要按类型筛选存储区中的对象：

1. 在应用程序 Web 界面窗口中，选择**存储**部分，**文件**子部分。
   这将打开对象表。
2. 单击**类型**链接以打开对象筛选菜单。
3. 选择一个或多个复选框：
   - **由“获取文件”任务上传**，如果您希望表显示被**获取文件**和**从隔离区恢复文件**任务放置在存储中的对象。
   - **通过 Web 界面上传**，如果您希望表显示用户使用 Kaspersky Anti Targeted Attack Platform Web 界面上传的对象。
   - **由“获取数据”任务上传**，如果您希望表显示被**进行取证**、**获取 NTFS 图元文件**、**获取注册表键**、**获取进程内存转储**任务放置在存储中的对象。
4. 单击**应用**。

对象表将仅显示与您设置的筛选条件相匹配的对象。

您可以同时使用多个筛选器。

按对象描述筛选存储中的对象

要按对象描述筛选存储中的对象：

1. 在应用程序 Web 界面窗口中，选择**存储**部分，**文件**子部分。
   这将打开对象表。
2. 单击**对象**链接以打开对象筛选菜单。
3. 在下拉列表中，选择以下选项之一：
   - **文件路径**
   - **MD5**
   - **SHA256**
4. 在下拉列表中，选择以下对象筛选运算符之一：
   - **包含。**
   - **不包含。**
   - **等于。**
   - **不等于**
   - **匹配**
   - **不匹配**
5. 在输入字段中，指定对象描述的一个或多个字符。
6. 要使用不同条件添加筛选条件，请单击 + 并指定筛选条件。
7. 单击**应用。**

   对象表将仅显示与您设置的筛选条件相匹配的对象。

> 您可以同时使用多个筛选器。

根据扫描结果筛选存储中的对象

要按这些对象的扫描结果筛选存储中的对象：

1. 在应用程序 Web 界面窗口中，选择**存储**部分，**文件**子部分。
   这将打开对象表。

2. 单击**扫描结果**链接以打开对象筛选菜单。
3. 选择一个或多个复选框：
   - **未检测到**。
   - **错误**。
   - **进行中**。
   - **未扫描**。
   - **检测到**。
4. 单击**应用**。

   对象表将仅显示与您设置的筛选条件相匹配的对象。

> 您可以同时使用多个筛选器。

根据 Central Node、PCN 或 SCN 服务器的名称筛选存储中的对象

要按 Central Node、PCN 或 SCN 服务器的名称筛选存储中的对象：

1. 在应用程序 Web 界面窗口中，选择**存储**部分，**文件**子部分。
   这将打开对象表。
2. 单击**服务器**链接以打开对象筛选菜单。
3. 选择要在存储中筛选对象的服务器对面的一个或多个复选框。
4. 单击**应用**。

   对象表将仅显示与您设置的筛选条件相匹配的对象。

> 您可以同时使用多个筛选器。

按对象源筛选存储中的对象

要按从中接收对象的来源筛选存储区中的对象：

1. 在应用程序 Web 界面窗口中，选择**存储**部分，**文件**子部分。
   这将打开对象表。

2. 单击**源**链接以打开对象筛选菜单。

3. 在下拉列表中，选择以下对象筛选运算符之一：

   - **包含**
   - **不包含**

4. 在输入字段中，指定手动上传对象的用户账户的 IP 地址、主机名或名称的一个或多个字符。

5. 要使用不同条件添加筛选条件，请单击 + 并指定筛选条件。

6. 单击**应用**。

对象表将仅显示与您设置的筛选条件相匹配的对象。

> 您可以同时使用多个筛选器。

根据放入存储中的时间筛选对象

要按对象被放入存储时的时间筛选对象：

1. 在应用程序 Web 界面窗口中，选择**存储**部分，**文件**子部分。
   这将打开对象表。

2. 单击**存储时间**链接以打开对象筛选菜单。

3. 选择以下对象显示时段之一：

   - **所有**，如果您希望表格显示放入存储区中的所有对象。
   - **上一个小时**，如果您希望表格显示在最后一个小时内放入存储区中的对象。
   - **最后一天**，如果您希望表格显示在最后一天内放入存储区中的对象。
   - **自定义范围**，如果您希望表格显示在指定时段内放入存储区中的对象。

4. 如果您选择了**自定义范围**对象显示时段：

   a. 在打开的日历中，指定对象显示时段的开始和结束日期。

   b. 单击**应用**。

对象表将仅显示与您设置的筛选条件相匹配的对象。

> 您可以同时使用多个筛选器。

清除存储对象筛选器

要清除一个或多个筛选条件的存储对象筛选器：

1. 在应用程序 Web 界面窗口中，选择**存储**部分，**文件**子部分。
   这将打开对象表。
2. 单击您想清除其筛选条件的存储对象表列标题右侧的。

   如果要清除多个筛选条件，请执行必要的操作以清除每个筛选条件。

选定筛选器将被清除。

对象表将仅显示与您设置的筛选条件相匹配的对象。

查看在具有 Kaspersky Endpoint Agent 组件的计算机上被隔离的对象表

可以在应用程序 Web 界面的**存储**部分、**隔离区**子部分中找到具有 Endpoint Agent 组件的计算机上的被隔离对象表。

Kaspersky Anti Targeted Attack Platform 服务器可存储在具有 Endpoint Agent 组件的计算机上被隔离的对象的元数据。这些对象本身被保存在检测到威胁对象的每台计算机上的特殊存储中。

在具有 Endpoint Agent 组件的计算机上被隔离的对象表包含以下信息：

1. **对象** — 有关该对象的信息。例如，文件名或文件路径。
2. **源** — 对象被隔离的的具有 Endpoint Agent 组件的计算机的 IP 地址或主机名。
3. **存储时间** — 对象被隔离的日期和时间。
4. **状态** — 对象的状态。

对象信息行的右侧部分包含按钮：

- 您可以单击删除 Kaspersky Anti Targeted Attack Platform 服务器上对象的元数据。
- 您可以单击在具有 Endpoint Agent 组件的计算机上从隔离区恢复对象。
- 您可以单击将对象从具有 Endpoint Agent 组件的计算机上的隔离区复制到 Kaspersky Anti Targeted Attack Platform 服务器。

单击具有文件名称或文件路径的链接将打开一个列表，您可以在其中选择以下操作之一：

- **按照此值进行过滤**。
- **从过滤器中排除**。
- **下载**。
- **发送文件进行扫描**。
- **查找事件**：
  - **文件路径**。
  - **MD5**。
  - **SHA256**。
- **查找警报**：
  - **文件路径**。
  - **MD5**。
  - **SHA256**。
- **复制值到剪贴板**。

单击具有主机名的链接将打开一个列表，您可以从其中选择以下操作之一：

- **按照此值进行过滤**。
- **从过滤器中排除**。
- **查找事件**。
- **查找警报**。
- **复制值到剪贴板**。

查看被隔离对象的信息

要查看在具有 Endpoint Agent 组件的计算机上被隔离的对象的信息：

1. 在应用程序 Web 界面窗口中，选择**存储**部分，**隔离区**子部分。
   这将打开对象表。
2. 在表格中，选择要查看其信息的对象。
   这将打开对象详细信息窗口。

该窗口包含以下信息：

- 推荐组。**任务**推荐可以显示，这是一个可打开**任务**部分的链接；这是隔离了对象的任务。
- **类型**是悲隔离对象的类型。
  可以使用以下类型的对象：
  - – 文件。
  - – 进程内存转储。
- **对象** – 文件名或路径。
- **状态**是文件的状态（文件是否可以从隔离区恢复）。
- **源**是在其上隔离对象、具有 Endpoint Agent 组件的计算机的名称。
- **记录时间**是对象被隔离的日期和时间。
- **操作**是文件的状态（文件是否可以从隔离区恢复）。
  如下操作可用：
  - – 从隔离区中删除文件。
  - – 获取 Kaspersky Anti Targeted Attack Platform 服务器上的文件副本。

单击具有文件名称或文件路径的链接将打开一个列表，您可以在其中选择以下操作之一：

- **查找事件**。
- **查找警报**。
- **复制值到剪贴板**。

从隔离中恢复对象

要在具有 Endpoint Agent 组件的计算机上从隔离区恢复对象：

1. 在应用程序 Web 界面窗口中，选择**存储**部分，**隔离区**子部分。
   这将打开对象表。
2. 在表中，选择要在具有 Endpoint Agent 组件的计算机上从隔离区恢复的对象。
   这将打开对象详细信息窗口。
3. 单击窗口下部的**恢复**。
   这将打开**任务**部分和**从隔离区恢复文件**任务。
4. 在**描述**字段中，输入任务描述。
5. 单击**添加**。

文件被从隔离区恢复。

您还可以单击在带有 Endpoint Agent 组件的计算机上被隔离的对象表的对象信息行的右侧部分的，运行任务以从隔离区恢复文件。

在分布式解决方案和多租户模式下，被在 SCN 服务器上隔离的文件无法在 PCN 服务器上恢复。您可以在创建隔离文件任务的 SCN 服务器上恢复文件。

具有**安全审计员**角色的用户无法从隔离区恢复对象。

获取 Kaspersky Anti Targeted Attack Platform 服务器上被隔离对象的副本

您要下载其副本的对象不得超过 100 MB。如果对象超过 100 MB，任务将结束并出现错误。

要将在具有 Kaspersky Endpoint Agent 组件的计算机上被隔离的对象复制到 Kaspersky Anti Targeted Attack Platform 服务器：

1. 在应用程序 Web 界面窗口中，选择**存储**部分，**隔离区**子部分。

   这将打开对象表。

2. 在表中，选择要在具有 Endpoint Agent 组件的计算机上从隔离区恢复的对象。

   这将打开对象详细信息窗口。

3. 单击窗口下部的**获取文件**。

   这将创建一个任务，用于获取在具有 Endpoint Agent 组件的计算机上被隔离的对象的副本。如果任务成功完成，对象的副本将被上传到 Kaspersky Anti Targeted Attack Platform 服务器。对象会显示在应用程序 Web 界面的**存储**部分、**文件**子部分，位于放置在存储的对象表中。

   已创建任务的信息显示在 Web 界面的**任务**部分。

您还可以将具有 Endpoint Agent 组件的计算机上的隔离对象复制到 Kaspersky Anti Targeted Attack Platform 服务器，方法是单击具有Endpoint Agent组件的计算机上的隔离对象表中对象信息行的右侧部分中的。

具有**安全审计员**角色的用户无法从隔离区获取对象的副本。

从表中删除有关隔离对象的信息

要从 Kaspersky Anti Targeted Attack Platform表中删除在具有 Kaspersky Endpoint Agent 组件的计算机上被隔离的对象的信息：

1. 在应用程序 Web 界面窗口中，选择**存储**部分，**隔离区**子部分。

   这将打开对象表。

2. 单击要从表中删除其信息的对象。
   这将打开对象详细信息窗口。
3. 单击**删除**。
   这将打开操作确认窗口。
4. 单击**是**。

有关在具有 Endpoint Agent 组件的计算机上被隔离的对象的信息将被从表中删除。

您还可以从表中删除具有 Endpoint Agent 组件的计算机上的被隔离对象的信息，方法是单击隔离对象表中对象信息行的右侧部分中的。

具有**安全审计员**角色的用户无法从表中删除有关隔离对象的信息。

按对象类型筛选有关隔离对象的信息

要按对象类型筛选被隔离对象的详细信息：

1. 在应用程序 Web 界面窗口中，选择**存储**部分，**隔离区**子部分。
   这将打开对象表。
2. 单击**类型**链接以打开对象筛选菜单。
3. 选择一个或多个复选框：
   - **文件**，如果您希望表显示被隔离对象的元数据。
   - **进程内存转储**，如果您希望表显示被隔离转储的元数据。
4. 单击**应用**。

对象表将仅显示与您设置的筛选条件相匹配的对象。

您可以同时使用多个筛选器。

按对象描述筛选有关隔离对象的信息

要按对象描述筛选被隔离对象的详细信息：

1. 在应用程序 Web 界面窗口中，选择**存储**部分，**隔离区**子部分。
   这将打开对象表。
2. 单击**对象**链接以打开对象筛选菜单。

3. 在下拉列表中，选择以下对象筛选运算符之一：

   - **包含**
   - **不包含**

4. 在输入字段中，指定对象描述的一个或多个字符。

5. 要使用不同条件添加筛选条件，请单击 + 并指定筛选条件。

6. 单击**应用**。

   对象表将仅显示与您设置的筛选条件相匹配的对象。

> 您可以同时使用多个筛选器。

按主机名筛选有关隔离对象的信息

要按隔离对象的主机名称筛选被隔离对象的详细信息：

1. 在应用程序 Web 界面窗口中，选择**存储**部分，**隔离区**子部分。
   这将打开对象表。

2. 单击**源**链接以打开对象筛选菜单。

3. 在下拉列表中，选择以下对象筛选运算符之一：

   - **包含**
   - **不包含**

4. 在输入字段中，指定主机名的一个或多个字符。

5. 要使用不同条件添加筛选条件，请单击 + 并指定筛选条件。

6. 单击**应用**。

   对象表将仅显示与您设置的筛选条件相匹配的对象。

> 您可以同时使用多个筛选器。

按时间筛选有关隔离对象的信息

要按对象被隔离时的时间筛选被隔离对象的详细信息：

1. 在应用程序 Web 界面窗口中，选择**存储**部分，**隔离区**子部分。
   这将打开对象表。
2. 单击**存储时间**链接以打开对象筛选菜单。
3. 选择以下对象显示时段之一：
   - **所有**，如果您希望表格显示所有对象。
   - **上一个小时**，如果您希望表格显示在最后一个小时内被隔离的对象。
   - **最后一天**，如果您希望表格显示在最后一天内被隔离的对象。
   - **自定义范围**，如果您希望表格显示在指定时段内被隔离的对象。
4. 如果您选择了**自定义范围**对象显示时段：
   a. 在打开的日历中，指定对象显示时段的开始和结束日期。
   b. 单击**应用**。

对象表将仅显示与您设置的筛选条件相匹配的对象。

> 您可以同时使用多个筛选器。

重置有关隔离对象信息的筛选器

要清除一个或多个筛选条件的筛选器：

1. 在应用程序 Web 界面窗口中，选择**存储**部分，**隔离区**子部分。
   这将打开对象表。
2. 单击您想重设其筛选条件的隔离对象表列标题右侧的  。

> 如果要清除多个筛选条件，请执行必要的操作以清除每个筛选条件。

选定筛选器将被清除。

对象表将仅显示与您设置的筛选条件相匹配的对象。

管理报告

具有“**高级安全官**”角色的用户可以使用 Kaspersky Anti Targeted Attack Platform 管理有关应用程序警报的报告：创建报告模板、基于模板创建报告、查看和删除报告和报告模板。

具有**安全审计员**角色的用户可以查看报告和报告模板并从模板创建报告。

可以使用以下类型的报告：

- 一般报告。这些报告的模板可在“**报告**”部分，“**模板**”子部分找到。您可以在“**报告**”部分，“**生成的报告**”字部份管理生成的报告。

  您可以根据您的授权许可管理应用程序的所有模式下的报告模板和报告。报告根据指定时间段内的警报选择生成。如果您使用分布式解决方案和多租户模式，则选择还可以基于租户和该租户的服务器。

- NDR 功能报告。可在“**报告**”部分，“**报告(NDR)**”子部分找到。

  如果您添加 KATA+NDR 授权许可密钥，则可以管理报告模板和报告。根据生成报告的节点的数据，根据指定时间段内的警报选择生成报告。

管理常见报告

在管理应用程序 Web 界面时，具有“**高级安全官**”角色的用户可以管理有关应用程序警报的 KATA 报告：创建报告模板、基于模板创建报告、查看和删除报告和报告模板。

具有“**安全审计员**”角色的用户可以查看 KATA 报告和报告模板以及从模板创建报告。

要创建 KATA 报告：

1. **创建报告模板。**
2. **根据模板创建报告。**

查看模板和报告的表格

模板和报告显示在应用程序 Web 界面窗口的**报告**部分中。

“**生成的报告**”子部分包含一个报告表。表包含以下信息：

- **创建时间** – 报告创建的日期和时间。
- **报告名称** – 根据模板创建的报告的名称。
- **时期** – 报告生成的时段。
- **服务器**是服务器的名称，具有对其应用规则的 PCN 或 SCN 角色。

  如果您使用的是分布式解决方案和多租户模式，则会显示此列。

- **创建者** – 创建报告的用户的名称。
- **状态** – 报告状态（文件是否可以下载）。

模板子部分显示模板表。表包含以下信息：

- **创建时间** – 创建模板的日期和时间。
- **更新时间** – 上次修改模板的日期和时间。
- **报告名称** – 模板的名称。
- **创建者** – 创建模板的用户的名称。

创建模板

创建报告模板时，您需要指定要在报告中显示的所有信息：报告名称，其描述，表格、图表或镜像的可用性。您还可以选择要在报告中显示的数据并定义报告元素的位置。

在界面的“报告”部分、“**生成的报告**”子部分中**创建报告**时，您只能选择用于创建报告的模板和数据显示周期。

为每个数据样本创建了一个新的报告模板。

要创建模板：

1. 在应用程序 Web 界面窗口中，选择**报告**部分，**模板**选项卡。

   这将打开模板表。

2. 单击**添加**。

   这将打开模板创建窗口。该窗口在浮动窗口中包含报告正文和报告构建器。您可以将报告构建器移动到 Web 界面窗口的工作区上。

3. 在窗口右上角的**模板名称**字段中，键入要分配给从此模板创建的报告的名称。例如，**技术警报**。

   当在该模板中创建所有报告时，该名称显示在“**报告**”部分、“**生成的报告**”子部分的表中。

4. 代替**报告标题**文本，输入创建报告后将在报告中显示的报告名称。如果您不想添加报告名称，可以删除**报告标题**文本并将此报告部分留空。

   您可以使用模板构建器中“**文本**”部分的按钮来设计文本的格式。

5. 代替**报告说明**文本，输入创建报告后将在报告中显示的报告描述。如果您不想添加报告描述，可以删除**报告说明**文本并将此报告部分留空。

   您可以使用模板设计器中“**文本**”部分的按钮来设计文本的格式。

6. 使用报告构建器添加一个或多个报告元素：

   - **表**。
   - **饼状图**。
   - **图片**。

7. 如果您选择添加镜像，**图片**窗口将打开。执行以下操作：

   a. 单击**上传**。

   b. 上传图像。例如，您可以上传公司徽标。

   c. 在上传按钮右侧的列表中，选择报告页面上图像的对齐方式：**左边**、**权限**或者**中心**。

   d. 单击**应用**。

8. 如果您选择添加饼图，**警报属性饼图**窗口将打开。执行以下操作：

   a. 在**名称**字段中，输入饼图的名称。例如，**按技术排列的前 5 名警报**。您也可以将该字段留空。

   b. 在**数据源**列表中，选择要为其创建饼图的警报属性。例如：**技术**。

   c. 在**片数**字段中，指定饼图的最大扇区数。

      创建报告时，应用程序会选择最常遇到的数据。例如，如果您指定了 5 个扇区并希望按技术创建饼图，则应用程序将显示生成警报数量最多的 5 种技术的饼图。产生较少警报的技术未包含在图表中。

   d. 单击**应用**。

9. 如果您选择添加表格，**警报表**窗口将打开。执行以下操作：

   a. 在**可用列**字段中，双击以选择要添加到报告表中的警报属性。

      选定的属性将被移至**选定的列**字段。您可以在**可用列**和**选定的列**字段之间拖动列名称，并更改报告表中的列顺序。

      例如，如果您将**技术**、**检测到**和**创建时间**属性移到**选定的列**字段，已创建报告的表格将显示生成警报的技术、检测到的对象列表以及警报生成的时间。

   b. 如果您想按**状态**属性筛选警报，请选择要在报告中显示其数据的警报处理状态旁边的复选框。

   c. 如果您想按**技术**属性筛选警报，请选择要在报告中显示其数据的应用程序模块和组件名称旁边的复选框。

   d. 如果您想按**重要级别**属性筛选警报，请选择要在报告中显示其数据的警报重要性级别旁边的复选框。

   e. 如果您想按**VIP 状态**筛选警报， 请在列表中选择**VIP**。报告中仅显示具有 VIP 身份的警报。

   f. 单击**应用**。

10. 单击窗口右上部的**保存**按钮。

一个新模板将被创建。

具有**安全审计员**和**安全官**角色的用户无法创建报告模板。

根据模板创建报告

要基于模板创建报告：

1. 在程序 Web 界面窗口中，选择“**报告**”部分，“**生成的报告**”子部分。
   这将打开报告表。
2. 单击**添加**。
   这将打开**新报告**窗口。
3. 执行以下操作：
   a. 在**模板**下拉列表中，选择以下模板之一创建报告。
   b. 在**时期**下面，选择以下选项之一：
   - **上一个小时**，如果您希望报告包含最近一小时内应用程序运行的信息。
   - **最后一天**，如果您希望报告包含最后一天内应用程序运行的信息。
   - **过去 7 天**，如果您希望报告包含最近一周内应用程序运行的信息。
   - **过去 30 天**，如果您希望报告包含最近一月内系统运行的信息。
   - **自定义**，如果您希望报告包含指定时段内系统运行的信息。
4. 如果您已选择**自定义**显示时段以获取有关应用程序运行的信息：
   a. 在打开的日历中，指定将生成报告的时段的开始和结束日期。
   b. 单击**应用**。
5. 如果您使用分布式解决方案和多租户模式，请在**服务器**设置组中选择要将其数据包含在报告中的租户和服务器旁边的复选框。
6. 单击**创建**。

创建的报告显示在报告表中。您可以下载报告以便在计算机上查看。

具有**安全官**角色的用户无法创建报告模板。

查看报告

要查看报告：

1. 在程序 Web 界面窗口中，选择“**报告**”部分，“**生成的报告**”子部分。
   这将打开报告表。
2. 选择要查看的报告。

该报告将在浏览器的新选项卡中打开。

将报告下载到本地计算机

要将报告下载到您的计算机：

1. 在程序 Web 界面窗口中，选择“**报告**”部分，“**生成的报告**”子部分。
   这将打开报告表。
2. 在包含要查看的报告的行中，单击 图标。
   报告以 HTML 格式保存到本地计算机上您指定的文件夹中。
   要查看报告，您可以使用任何允许您查看 HTML 文件的应用程序（例如浏览器）。

编辑模板

编辑模板：

1. 在应用程序 Web 界面窗口中，选择**报告**部分，**模板**选项卡。
2. 这将打开模板表。选择您想要编辑的模板。
   这将打开模板编辑窗口。
3. 您可以编辑以下设置：

   - “**模板名称**”是基于此模板创建所有报告时显示在“**报告**”部分、“**生成的报告**”子部分中的表中的报告名称。
   - **报告标题**是创建报告后显示在报告中的报告名称。
     您可以使用模板构建器中“**文本**”部分的按钮来设计文本的格式。
   - **报告说明**是创建报告后显示在报告中的报告描述。
     您可以使用模板构建器中“**文本**”部分的按钮来设计文本的格式。
   - **图片**。您可以上传或删除镜像。

- **饼状图**。您可以更改以下饼图设置：
  - **名称**。
  - **数据源**。
  - **片数**。

  单击**应用**。
- **表**。您可以更改以下表设置：
  - **选定的列**。您可以在**可用列**和**选定的列**字段之间拖动列名称，并更改报告表中的列顺序。
  - **状态**。
  - **技术**。
  - **重要级别**。
  - **VIP 状态**。

4. 选择以下方法之一来保存模板：
   - 如果您想将更改应用于当前模板，请单击**保存**按钮。
     模板已修改。
   - 如果要创建新模板，请输入模板名称，然后单击**另存为**。

     > 新模板的名称不能与已有模板的名称相同。

     新模板将被保存。

> 具有**安全审计员**和**安全官**角色的用户无法编辑模板。

按名称筛选模板

要按名称筛选模板：

1. 在应用程序 Web 界面窗口中，选择**报告**部分，**模板**选项卡。
2. 这将打开模板表。单击**报告名称**链接以打开模板筛选菜单。
3. 在下拉列表中，选择以下模板筛选运算符之一：
   - **包含**
   - **不包含**
4. 输入模板名称的一个或多个字符。

5. 如果您想为筛选器添加筛选条件，请单击筛选运算符列表下的 + 按钮并重复指定筛选条件的序列。

6. 单击**应用**。

模板表将仅显示与您设置的筛选条件相匹配的模板。

根据创建模板的用户的名称筛选模板

要按照创建该模板的用户的名称筛选模板：

1. 在应用程序 Web 界面窗口中，选择**报告**部分，**模板**选项卡。

2. 这将打开模板表。单击**创建者**链接以打开用于筛选模板的菜单。

3. 在下拉列表中，选择以下模板筛选运算符之一：

   - **包含**
   - **不包含**

4. 输入用户名的一个或多个字符。

5. 如果您想为筛选器添加筛选条件，请单击筛选运算符列表下的 + 按钮并重复指定筛选条件的序列。

6. 单击**应用**。

模板表将仅显示与您设置的筛选条件相匹配的模板。

按创建时间筛选模板

要按创建时间筛选报告模板：

1. 在应用程序 Web 界面窗口中，选择**报告**部分，**模板**选项卡。

2. 这将打开模板表。单击**创建时间**链接以打开用于筛选模板的菜单。

3. 选择以下模板显示时段之一：

   - **所有**，如果您希望应用程序显示表中创建的所有模板。
   - **上一个小时**，如果您希望应用程序显示表中最后一小时创建的模板。
   - **最后一天**，如果您希望应用程序显示表中最后一天创建的模板。
   - **自定义范围**，如果您希望应用程序显示表中在指定时段内创建的模板。

4. 如果您选择了**自定义范围**模板显示时段：

   a. 这将打开日历；在日历中，指定模板显示期间的开始日期和结束日期。

   b. 单击**应用**。

模板表将仅显示与您设置的筛选条件相匹配的模板。

清除模板筛选器

要清除一个或多个筛选条件的模板筛选器：

1. 在应用程序 Web 界面窗口中，选择**报告**部分，**模板**选项卡。
2. 这将打开模板表。单击要为其清除筛选条件的模板表列标题右侧的。

> 如果要清除多个筛选条件，请执行必要的操作以清除每个筛选条件。

选定筛选器将被清除。

模板表将仅显示与您设置的筛选条件相匹配的模板。

删除模板

要删除模板：

1. 在应用程序 Web 界面窗口中，选择**报告**部分，**模板**选项卡。
2. 这将打开模板表。选择包含您想删除的模板的行中的复选框。
3. 单击**删除**。
   这将打开操作确认窗口。
4. 单击**是**。

您选定的模板将被删除。

> 具有**安全审计员**和**安全官**角色的用户无法删除模板。

按创建时间筛选报告

要按创建时间筛选报告：

1. 在程序 Web 界面窗口中，选择“**报告**”部分，“**生成的报告**”子部分。
   这将打开报告表。
2. 单击**创建时间**链接以打开报告筛选菜单。
3. 选择以下报告显示时段之一：
   - **所有**，如果您希望应用程序显示表中创建的所有报告。
   - **上一个小时**，如果您希望应用程序显示表中最后一小时创建的报告。
   - **最后一天**，如果您希望应用程序显示表中最后一天创建的报告。
   - **自定义范围**，如果您希望应用程序显示表中在指定时段内创建的报告。
4. 如果您选择了**自定义范围**报告显示时段：
   a. 在打开的日历中，指定报告显示时段的开始和结束日期。
   b. 单击**应用**。

报告表将仅显示与您设置的筛选条件相匹配的报告。

按名称筛选报告

要按名称筛选报告：

1. 在程序 Web 界面窗口中，选择“**报告**”部分，“**生成的报告**”子部分。
   这将打开报告表。
2. 单击**报告名称**链接以打开报告筛选菜单。
3. 在下拉列表中，选择以下报告筛选运算符之一：
   - **包含**
   - **不包含**
4. 在文本框中输入报告名称的一个或多个字符。
5. 如果您想为筛选器添加筛选条件，请单击筛选运算符列表下的 + 按钮并重复指定筛选条件的序列。
6. 单击**应用**。

报告表将仅显示与您设置的筛选条件相匹配的报告。

按具有 Central Node 组件的服务器名称筛选报告

要按具有 Central Node 组件的服务器名称筛选报告：

1. 在程序 Web 界面窗口中，选择“**报告**”部分，“**生成的报告**”子部分。
   这将打开报告表。
2. 单击**服务器**链接以打开报告筛选菜单。
3. 选择要用于筛选报告的服务器对面的复选框。
4. 单击**应用**。

报告表将仅显示与您设置的筛选条件相匹配的报告。

根据创建报告的用户的名称筛选报告

要按照创建该报告的用户的名称筛选报告：

1. 在程序 Web 界面窗口中，选择“**报告**”部分，“**生成的报告**”子部分。
   这将打开报告表。
2. 单击**创建者**链接以打开报告筛选菜单。
3. 在下拉列表中，选择以下报告筛选运算符之一：
   - **包含**
   - **不包含**
4. 输入用户名的一个或多个字符。
5. 如果您想为筛选器添加筛选条件，请单击筛选运算符列表下的 + 按钮并重复指定筛选条件的序列。

报告表将仅显示与您设置的筛选条件相匹配的报告。

清除报告筛选器

要清除一个或多个筛选条件的报告筛选器：

1. 在程序 Web 界面窗口中，选择“**报告**”部分，“**生成的报告**”子部分。
   这将打开报告表。

2. 单击要为其清除筛选条件的报告表列标题右侧的。

> 如果要清除多个筛选条件，请执行必要的操作以清除每个筛选条件。

选定筛选器将被清除。

报告表将仅显示与您设置的筛选条件相匹配的报告。

删除报告

要删除应用程序操作报告：

1. 在程序 Web 界面窗口中，选择“**报告**”部分，“**生成的报告**”子部分。
   这将打开报告表。
2. 选择包含您想删除的报告的行中的复选框。
3. 单击**删除**。
   这将打开操作确认窗口。
4. 单击**是**。

选定的报告将被删除。

> 具有**安全审计员**和**安全官**角色的用户无法删除报告。

管理 NDR 报告

您可以使用 Kaspersky Anti Targeted Attack Platform 获取包含应用程序保存的各种信息的报告。Kaspersky Anti Targeted Attack Platform 以 PDF 文件形式生成报告。应用程序可以将报告文件发送至电子邮件地址。

您可以查看有关生成的报告的信息并在“**报告**”部分，“**报告(NDR)**”子部分，“**生成的报告**”选项卡上将其导出到文件。

可能有以下类型的 NDR 报告模板：

- 系统模板，在应用程序安装期间自动创建。在报告模板表中，系统模板显示为图标。您不能删除系统模板。

  Kaspersky Anti Targeted Attack Platform 支持以下系统报告模板：

  - 清查报告。
    包含有关设备、系统命令的信息，以及设备上使用的协议和检测到的风险。
  - 系统安全报告。
    包含有关设备的安全状态、注册的事件、检测到的风险以及与外部网络上的设备交互的信息。

- 执行摘要。

  包含有关设备和系统安全状态的简要信息。

- 完整报告。

  包含有关设备和系统安全状态的完整信息。

- 自定义模板，通过复制模板手动创建。您可以复制系统或自定义模板。只有具有高级安全官角色的用户才能复制报告模板。

报告中的信息以单独的信息块呈现。每份 Kaspersky Anti Targeted Attack Platform 报告均包含一组固定的信息块，这些信息块按固定顺序排列。报告中使用的信息块及其描述如下表所列。

在报告中使用信息块

信息块的名称	清查报告	系统安全报告	执行摘要	完整报告
设备类别	✓	–	✓	✓
设备供应商	✓	–	✓	✓
设备操作系统	✓	–	✓	✓
拥有最多风险的设备。	✓	✓	–	✓
态势感知	–	✓	✓	✓
网络中的新设备	✓	–	–	✓
流量最大的协议	✓	–	–	✓
与其他节点连接最多的设备	✓	–	–	✓
网络流量	✓	–	✓	✓
通用协议	✓	–	✓	✓
设备安全状态	–	✓	✓	✓
按状态划分的设备分布	–	✓	–	✓
事件统计	–	✓	–	✓
按检测技术分布的事件	–	✓	–	✓
发生事件最多的设备	–	✓	–	✓
最关键的事件	–	✓	–	✓
最常触发的恶意活动检测规则	–	✓	–	✓
带有访问公共资源标志的设备	–	✓	–	✓
通过远程控制协议的连接	–	✓	–	✓
活动风险	–	✓	✓	✓

查看 NDR 报告模板表

您可以在应用程序的 Web 界面中查看报告模板表，在“**报告**”部分，“**报告(NDR)**”子部分，“**报告模板**”选项卡上。

报告模板设置显示在表格以下列中：

- **名称**。

  报告模板名称。 图标显示在系统报告模板名称旁边。

- **计划**。

  有关 Kaspersky Anti Targeted Attack Platform 基于模板自动生成报告所使用的时间表的信息。如果具有“**高级安全官**”角色的用户在报告模板中配置了计划则显示计划信息。如果未配置计划，则该列显示“**已禁用**”。

- **类型/用途**。

  上次修改报告模板的用户的姓名。对于具有默认设置的系统模板，会显示“**系统**”。

- **最后报告**。

  上次根据报告模板生成报告的时间。

- **目的地**。

  表示已配置电子邮件报告收件人的图标。以下图标具有以下含义：

  - – 定义了报告接收者。
  - – 未定义报告接收者。

查看 NDR 报告模板详细信息

要查看报告模板信息：

在“**报告**”部分，“**报告(NDR)**”子部分，“**报告模板**”选项卡上，选择相关模板。

详细信息区域显示在 Web 界面窗口的右侧。详细信息区域显示所有指定的详细信息。

报告模板的详细信息包括以下字段：

- “**名称**”是报告模板的名称。
- “**类型/用户**”是最后修改报告模板的用户的名称。对于具有默认设置的系统模板，会显示“**系统**”。
- “**期限**”是卡 Kaspersky Anti Targeted Attack Platform 根据模板生成的报告涵盖的时间段。
- “**修改时间**”是模板最近一次更改的时间。
- “**上次报告**”是根据模板生成上次报告的时间。
- “**下次开始（当地时间）**”是根据模板开始生成下一个报告的时间。如果为报告模板配置了计划，则会显示此设置。
- “**计划**”显示有关 Kaspersky Anti Targeted Attack Platform 用于根据模板自动生成报告的计划的信息。如果为报告模板配置了计划，则会显示此设置。

“**收件人地址**”是 Kaspersky Anti Targeted Attack Platform 向其发送生成的报告的电子邮件地址。如果为报告模板配置了收件人地址，则会显示此设置。

查看 NDR 报告表

您可以在应用程序的 Web 界面中查看报告表，在“**报告**”部分，“**报告(NDR)**”子部分，“**生成的报告**”选项卡上。

报告设置显示在表格以下列中：

- **ID**。
  报告的唯一 ID。
- **报告名称**。
  生成的报告的名称。
- **模板名称**。
  用于生成报告的模板的名称。
- **开始**。
  报告生成开始的日期和时间。
- **状态**。
  报告状态。报告可以具有以下状态之一：
  待处理。该报告正在排队等待生成。当同时生成多个报告时，一份报告可能处于*“待处理”*状态。
  进行中。报告正在生成。
  错误。生成报告时出现错误。
  完成。报告已成功生成。
  正在取消。正在取消报告生成。
  已取消。报告生成已取消。
- **用户**。
  启动报告生成或配置基于模板运行报告的计划的用户的名称。
- **运行类型**。
  报告生成类型：手动或计划。
- **完全的**。
  报告生成结束的日期和时间。

根据模板手动生成 NDR 报告

您可以根据模板手动开始生成报告。

要开始生成报告：

1. 选择“**报告**”部分，然后“**报告(NDR)**”子部份。
2. 在“**报告模板**”选项卡，选择要用于生成报告的一个或多个模板。
   当选择多个模板时，应用程序将同时根据这些模板生成报告。您最多可以选择 10 个模板。

3. 在报告模板表上方的工具栏中，单击“**获取报告**”。

   Kaspersky Anti Targeted Attack Platform 开始生成报告。

   您将被带到“**生成的报告**”选项卡，显示正在生成的报告的状态。报告生成后，Kaspersky Anti Targeted Attack Platform 会将 PDF 格式的报告文件发送至报告模板中指定的电子邮件地址。如果报告模板中未定义电子邮件地址，您可以在“**生成的报告**”选项卡上单独手动将生成的报告导出到文件。报告文件的最大大小为 10 MB。

如果有必要，您可以取消报告的生成。

复制 NDR 报告模板

您可以通过复制现有的报告模板来创建自定义模板。您可以复制系统模板或自定义模板。复制模板时，您无法选择要在报告中包含哪些信息块或重新排列它们。

应用程序中的最大模板数量为 5000 个。

要复制报告模板：

1. 选择“**报告**”部分，然后“**报告(NDR)**”子部份。
2. 在“**报告模板**”选项卡，选择相关模板。

   详细信息区域显示在 Web 界面窗口的右侧。
3. 单击“**创建新模板**”。
4. 在“**名称**”字段中，编辑报告模板的名称。

   您可以使用拉丁字母和西里尔字母、数字、空格字符以及 -、–、_ 字符。

   报告模板的名称必须满足以下要求：

   - 不要重复使用另一个报告模板的名称（不区分大小写）。
   - 最多包含 100 个字符。

   从更新后的模板生成的报告的名称将反映模板的新名称。
5. 在“**数据周期**”下拉列表中，选择您想要在报告中获取系统信息的时间段。

   您可以使用应用程序在过去 24 小时、7 天、30 天、去年或手动配置的时间范围内收到的信息生成报告。
6. 如果需要按计划生成报告，请打开“**按计划生成报告**”切换开关并设置计划：

   a. 在“**频率**”下拉列表中，选择生成报告的频率：**每小时**、**每天**、**每周**或**每月**。

   b. 根据所选的选项，指定设置值以优化报告生成开始时间。
7. 如有必要，请使用“**收件人地址**”字段输入要向其发送生成的报告的电子邮件地址。如果需要指定报告的其他收件人，请点击“**添加收件人地址**”并输入电子邮件地址。

   报告收件人的最大数量为 20。
8. 单击“**保存**”。

新报告将添加到报告模板表中。

编辑 NDR 报告模板

要编辑报告模板的设置：

1. 选择“**报告**”部分，然后“**报告(NDR)**”子部份。
2. 在“**报告模板**”选项卡，选择相关模板。
   详细信息区域显示在 Web 界面窗口的右侧。
3. 单击**“编辑”**。
4. 在“**名称**”字段中，编辑报告模板的名称。
   您可以使用拉丁字母和西里尔字母、数字、空格字符以及 -、–、_ 字符。
   报告模板的名称必须满足以下要求：
   - 不要重复使用另一个报告模板的名称（不区分大小写）。
   - 最多包含 100 个字符。

   从更新后的模板生成的报告的名称将反映模板的新名称。
5. 在“**数据周期**”下拉列表中，选择您想要在报告中获取系统信息的时间段。
   您可以使用应用程序在过去 24 小时、7 天、30 天、去年或手动配置的时间范围内收到的信息生成报告。
6. 如果需要按计划生成报告，请打开“**按计划生成报告**”切换开关并设置计划：
   a. 在“**频率**”下拉列表中，选择生成报告的频率：**每小时**、**每天**、**每周**或**每月**。
   b. 根据所选的选项，指定设置值以优化报告生成开始时间。
7. 如有必要，请使用“**收件人地址**”字段输入要向其发送生成的报告的电子邮件地址。如果需要指定报告的其他收件人，请点击“**添加收件人地址**”并输入电子邮件地址。
   报告收件人的最大数量为 20。
8. 单击“**保存**”。

更改将显示在报告模板表的相应列中。

将 NDR 报告导出到文件

您可以将生成的报告导出为 PDF 文件。

要将报告导出到文件：

1. 在“**报告**”部分，选择“**报告(NDR)**”子部分。
2. 在“**生成的报告**”选项卡上，选择相关报告。
   这些报告按当前服务器连接会话中最后启动的报告的 ID 进行过滤。要显示所有生成的报告，请单击“**默认过滤器**”重置过滤器设置。如果有必要，您可以按您选择的时间段配置过滤。

详细信息区域显示在 Web 界面窗口的右侧。

3. 单击“**导出**”。

浏览器保存报告文件。默认情况下，报告文件的名称为“<报告名称>_<生成报告的日期和时间>”格式。根据您的浏览器的设置，屏幕上可能会显示一个窗口，您可以在其中指定下载文件的路径和名称。

删除 NDR 报告模板

只能删除自定义报告模板。

要删除报告模板：

1. 选择“**报告**”部分，然后“**报告(NDR)**”子部份。
2. 在“**报告模板**”选项卡上，选择一个或多个要删除的报告模板。
3. 单击“**删除**”。
   系统模板不能被删除。在报告模板表中，系统模板显示为 图标。
4. 在显示的提示窗口中，确认删除报告模板。

删除 NDR 报告

要删除报告：

1. 选择“**报告**”部分，然后“**报告(NDR)**”子部份。
2. 在“**生成的报告**”选项卡上，选择一个或多个要删除的报告。
   报告表中的报告按当前服务器连接会话中最后启动的报告的 ID 进行过滤。要显示所有生成的报告，请单击“**默认过滤器**”重置过滤器设置。如果有必要，您可以按您选择的时间段配置过滤。
   详细信息区域显示在 Web 界面窗口的右侧。
3. 单击“**删除**”。
4. 在显示的提示窗口中，确认删除报告。

取消 NDR 报告生成

您只能取消处于**“进行中”**状态的报告的生成。

要取消报告生成：

1. 选择“**报告**”部分，然后“**报告(NDR)**”子部份。
2. 在“**生成的报告**”选项卡上，选择要取消的、状态为**“进行中”**的报告。
   详细信息区域显示在 Web 界面窗口的右侧。
3. 单击**“取消”**。
4. 在弹出的提示窗口中，确认取消报告。

此请求完成后，报告状态更改为“**已取消**”。

管理存储报告文件的设置

您可以更改存储的报告文件的最大总大小限制。

要编辑报告文件存储设置：

1. 使用应用程序管理员账户登录 Web 界面。
2. 选择“**Sensor 服务器**”部分。
3. 选择本地主机（IP 地址 0.0.0.0）的卡。
   详细信息区域显示在 Web 界面窗口的右侧。
4. 单击**“编辑”**。
   在详细信息区域，会显示选项卡，您可以在其中管理服务器的设置。
5. 在**“常规”**选项卡上的**“报告”**下，使用**“最大卷”**设置为存储的报告文件设置大小限制。
   您可以选择大小限制的计量单位：**MB** 或 **GB**。
   编辑值时，还需要考虑到所有大小限制的总和不得超过节点指定的最大存储容量。
6. 如有必要，使用“**存储时间（天）**”设置来限制报告文件的存储时间，并以天为单位指定时间。
7. 单击**“保存”**。

管理将 VIP 身份分配给警报的规则

具有**高级安全官**角色的用户可以创建、删除、修改、导入和导出用于向警报分配 VIP 身份的规则列表。

您可以创建以下类型的规则：

- **IP**。VIP 身份将分配给与计算机的此 IP 地址关联的新警报。
- **主机名称**。VIP 身份将分配给与该主机名关联的新警报。
- **电子邮件地址**。VIP 身份将分配给与此电子邮件地址关联的新警报。

具有**安全审计员**角色的用户可以查看和导出用于将 VIP 身份分配给警报的规则列表。

具有**安全官**角色的用户无法查看为警报分配 VIP 身份的规则列表。

查看 VIP 身份分配规则表

用于分配 VIP 身份的规则表位于应用程序 Web 界面的**设置**部分，**VIP 状态**子部分。

表包含以下信息：

- **标准** – 将条目添加到规则列表的条件。
- **值** – 条件的值。
- **描述** – 创建规则时指定的附加信息。

创建 VIP 身份分配规则

要添加用于将 VIP 身份分配给警报的规则：

1. 在应用程序 Web 界面的主窗口中，选择**设置**选项卡，**VIP 状态**部分。
2. 在应用程序 Web 界面窗口的右上角，单击**添加**。
   这将打开添加规则的窗口。
3. 在**标准**下拉列表中，选择以下规则类型之一：
   - **IP**，如果您想为计算机 IP 地址添加规则。
   - **主机**，如果您想添加主机名规则。
   - **电子邮件地址**，如果您想为电子邮件地址添加规则。
4. **值**字段中输入必要的值。
   例如，如果在**标准**下面您选择了**电子邮件地址**，请在**值**字段中输入您要添加的电子邮件地址。
5. 在**描述**字段中，根据需要输入其他信息。
6. 单击**添加**。

规则已添加。VIP 身份将被分配给与添加的 IP 地址、主机名或电子邮件地址关联的新警报。

具有**安全审计员**角色的用户无法创建 VIP 身份分配规则。

具有**安全官**角色的用户无法查看为警报分配 VIP 身份的规则列表。

删除 VIP 身份分配规则

要删除为警报分配 VIP 身份的规则：

1. 在应用程序 Web 界面的主窗口中，选择**设置**选项卡，**VIP 状态**部分。
2. 选择您想从列表中移除的每条规则左侧的复选框。
3. 如果您想删除所有规则，请选择列表上方的复选框。
4. 在应用程序 Web 界面窗口的右上角，单击**删除**。
   操作确认窗口将显示。
5. 单击**是**。

所选文件将被删除。

具有**安全审计员**角色的用户无法删除 VIP 身份分配规则。

具有**安全官**角色的用户无法查看为警报分配 VIP 身份的规则列表。

修改 VIP 身份分配规则

要修改为警报分配 VIP 身份的规则：

1. 在应用程序 Web 界面的主窗口中，选择**设置**选项卡，**VIP 状态**部分。
2. 选择要修改的规则。
   这将打开规则编辑窗口。
3. 对**标准**、**值**和**描述**字段进行必要的更改。
4. 单击**保存**。

规则已修改。

具有**安全审计员**角色的用户无法修改 VIP 身份分配规则。

具有**安全官**角色的用户无法查看为警报分配 VIP 身份的规则列表。

导入 VIP 身份分配规则列表

要导入用于向警报分配 VIP 身份的规则列表：

1. 在应用程序 Web 界面的主窗口中，选择**设置**选项卡，**VIP 状态**部分。
2. 单击**导入**。
   系统将提示您确认列表导入。

   导入的用于将 VIP 身份分配给警报的规则列表将替换当前的 VIP 身份警报分配规则列表。

3. 单击**是**。
   这将打开文件选择窗口。
4. 选择包含要导入的规则列表的 JSON 文件，然后单击**打开**。
   这将关闭文件选择窗口。

列表已导入。

导出从扫描中排除的数据列表

要导出扫描排除项列表：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**排除项**子部分。
2. 前往**扫描**选项卡。
3. 在应用程序 Web 界面窗口的右上角，单击**导出**。

包含导出的扫描排除项列表的 JSON 文件被保存在计算机上的浏览器下载文件夹中。

按 VIP 身份分配规则类型筛选和搜索

要按规则类型筛选或搜索 VIP 身份分配规则：

1. 在应用程序 Web 界面的主窗口中，选择**设置**选项卡，**VIP 状态**部分。
2. 单击**标准**链接以打开筛选配置窗口。

3. 选择规则类型旁边的一个或多个复选框：

   - **IP**。
   - **主机**。
   - **电子邮件地址**。

4. 单击**应用**。

   筛选配置窗口关闭。

   表将仅显示与您设置的筛选条件相匹配的规则。

> 您可以同时使用多个筛选器。

按 VIP 身份规则的值筛选和搜索

要按规则值筛选或搜索 VIP 身份分配规则：

1. 在应用程序 Web 界面的主窗口中，选择**设置**选项卡，**VIP 状态**部分。
2. 单击**值**链接以打开筛选配置窗口。
3. 输入规则值的一个或多个字符。
4. 单击**应用**。

   筛选配置窗口关闭。

   表将仅显示与您设置的筛选条件相匹配的规则。

> 您可以同时使用多个筛选器。

按 VIP 身份分配规则描述筛选和搜索

要按描述筛选或搜索 VIP 身份分配规则：

1. 在应用程序 Web 界面的主窗口中，选择**设置**选项卡，**VIP 状态**部分。
2. 单击**描述**链接以打开筛选配置窗口。

3. 输入描述的一个或多个字符。

4. 单击**应用**。

筛选配置窗口关闭。

表将仅显示与您设置的筛选条件相匹配的规则。

> 您可以同时使用多个筛选器。

清除 VIP 身份分配规则筛选器

要清除一个或多个筛选条件的 VIP 身份分配规则筛选器：

1. 在应用程序 Web 界面的主窗口中，选择**设置**选项卡，**VIP 状态**部分。

2. 单击您想清除其筛选条件的表列标题右侧的。

> 如果要清除多个筛选条件，请执行必要的操作以清除每个筛选条件。

选定筛选器将被清除。

表将仅显示与您设置的筛选条件相匹配的规则。

管理 NDR 事件的允许规则

Kaspersky Anti Targeted Attack Platform 可以监控设备之间的网络交互。*允许规则*用于配置已授权和未授权的网络交互。所有符合活动允许规则的网络交互都被视为允许。当检测到允许的交互时，应用程序不会记录 NDR 事件或生成警报。

您可以查看、创建、复制、修改、删除、启用或禁用允许规则。

查看允许规则表格

要查看允许规则表：

1. 在应用程序 Web 界面窗口中选择“**设置**”部分。

2. 转到“**允许规则**”选项卡。
允许规则表将显示。

表包含以下信息：

- **规则 ID** 是该规则的唯一标识。
- **状态**（◐ 图标）表示规则的当前状态（*已启用*或*已禁用*）。
- **规则类型**：对于禁用事件注册的规则，指定 EVT 类型。
- **协议/命令**定义了一组协议。
- **面 1** 是网络交互一端的设备名称/地址信息。您可以使用以下设置启用或禁用地址信息中地址和端口的显示：**MAC 地址**、**IP 地址**和**端口号**。如果向应用程序添加了其他地址空间，您可以使用以下设置启用或禁用地址空间名称的显示：
  - **MAC 地址的 AS**：包含规则中的 MAC 地址的地址空间。只有当地址空间具有**数据链 (L2)** 被选为 OSI 层的地址空间规则时，此设置才能包含地址空间的名称。
  - **IP 地址的 AS**：包含规则中的 IP 地址的地址空间。只有当地址空间具有**网络 (L3)** 被选为 OSI 层的地址空间规则时，此设置才能包含地址空间的名称。
- **面 1** 是网络交互的另一端的设备名称/地址信息。地址信息的显示可以按照与**面 1** 列相同的方式配置。
- **评论**可让您提供有关规则的其他信息。
- **创建日期**是规则创建的日期和时间。
- **更改日期**是规则最后修改的日期和时间。
- **监控点**是事件中要指定的监控点的名称。
- **事件类型**是事件类型的 ID 和标题。
- **源**提供有关规则来源的信息。
- "**系统 IDS 规则的 SID**"是系统 IDS 规则的 ID。如果在创建允许规则时未指定 ID，则会显示"*所有规则*"。

使用空白设置或模板中的设置创建允许规则

要使用空白设置或模板中的设置创建允许规则：

1. 在应用程序 Web 界面窗口中选择"**设置**"部分。
2. 转到"**允许规则**"选项卡。
3. 单击"**添加规则**"。
4. 如果要使用模板中的设置，请在详细信息区域中单击"**使用模板**"，在打开的窗口中选择必要的模板，然后单击"**应用**"。
5. 在"**协议**"字段中，指定用于设备之间交互的协议。

   选择**"协议"**字段将打开窗口，其中以协议堆栈树的形式显示支持的协议表。您可以使用包含下一层协议的协议名称旁边的 **+** 和 **-** 按钮来控制树节点的显示。

   如有必要，请使用表格上方的搜索栏查找所需的协议。

要指定协议：

a. 在协议表中，选择要为规则指定的协议。要选择协议，请单击协议表左列中的按钮。

b. 单击“**确定**”。

如果您选择应用程序可以通过网络数据包的内容检测的协议，则“**协议**”字段下会显示相应的警告。

6. 如果必要，请在“**注释**”字段中输入有关该规则的其他信息。

7. 在“**面 1**”和“**面 2**”下，指定网络交互各方的可编辑地址信息。根据所选的协议（或协议集），地址信息可能包含 MAC 地址、IP 地址和/或端口号。如果已向应用程序添加了额外的地址空间，您可以为地址指定地址空间的名称。

   为了自动填写网络交互端的地址信息，您可以选择应用程序已知的设备。为此：

   a. 单击“**指定设备地址**”打开设备选择窗口。

   b. 在设备选择窗口中，选中要使用的设备旁边的复选框。

      设备选择窗口包含一个表，您可以在其中配置列的布局和顺序，还可以像“**资产**”部分中的设备表一样进行过滤、搜索和排序。

   c. 在设备选择窗口中单击“**确定**”。

8. 在“**事件类型**”字段中，指定事件中指示其数字代码的事件类型。

   选择“**事件类型**”字段将打开一个窗口，其中包含允许规则中可能指定的事件类型列表。如有必要，请使用列表上方的搜索栏查找所需的事件类型。要指定事件类型，请在列表中选择它并单击“**应用**”。

9. 在“**监控点**”字段中指定事件中指示的监控点名称。

   选择“**监控点**”字段将打开一个窗口，其中包含已安装应用程序组件的所有节点上的所有监控点的列表。如有必要，请使用列表上方的搜索栏查找所需的监控点名称。要指定监控点名称，请在列表中选择它并单击“**应用**”。

10. 如果您不希望应用程序使用选定的系统 IDS 规则扫描符合此允许规则的条件的网络连接，请在“**系统 IDS 规则的 SID**”字段中指定此规则的 ID。您可以在 IDS 警报的详细信息中查看系统 IDS 规则的 SID。

    如果未指定 SID，应用程序将禁用所有系统 IDS 规则对符合此允许规则的条件的网络交互的扫描。

11. 在详细信息区域中，单击“**保存**”。

该规则被添加到允许规则表中。

从已注册事件创建允许规则

要从已注册事件创建允许规则：

1. 在“**网络流量事件**”部分的事件表中，选择您要基于其创建事件允许规则的事件。
2. 在详细信息区域中，单击“**创建允许规则**”。

   这将在浏览器窗口中打开“**允许规则**”部分。在 Web 界面窗口的右侧，规则设置编辑模式中显示详细信息区域。新规则的设置使用已保存的事件详细信息中的值进行初始化。
3. 如有必要，编辑新规则的设置。为此，请按照创建最初为空白的设置的规则的步骤 4 至 12 进行操作。如果不需要编辑新规则的设置，请单击“**保存**”来保存该规则。

根据已注册的事件创建允许规则。

复制允许规则

要从现有交互控制规则创建交互控制规则：

1. 在应用程序 Web 界面窗口中选择“**设置**”部分。
2. 转到“**允许规则**”选项卡。
3. 选择新规则所基于的规则。
4. 右键单击以打开上下文菜单。
5. 在上下文菜单中，选择“**复制规则**”。

   在 Web 界面窗口的右侧，规则设置编辑模式中显示详细信息区域。新规则的设置使用已保存的事件设置的值进行初始化。
6. 根据需要编辑设置。为此，请按照创建规则的过程中描述的步骤 4 至 12 进行操作。

允许规则被复制。

编辑允许规则的设置

您可以编辑已启用的允许规则的设置。禁用的规则不可编辑。

要编辑允许规则的设置：

1. 在应用程序 Web 界面窗口中选择“**设置**”部分。
2. 转到“**允许规则**”选项卡。
3. 选择要编辑其设置的规则。

   详细信息区域显示在 Web 界面窗口的右侧。

4. 单击**"编辑"**。

5. 根据需要编辑设置。为此，请按照创建规则的过程中描述的步骤 4 至 12 进行操作。

6. 单击"**保存**"。

规则设置已修改。

启用或禁用允许规则

允许规则可以具有*已启用*或*已禁用*状态。默认情况下，规则在创建后处于启用状态。

要更改允许规则的状态：

1. 在应用程序 Web 界面窗口中选择"**设置**"部分。

2. 转到"**允许规则**"选项卡。

3. 在规则表中，选择要更改其状态的规则。

4. 单击"**启用**"或"**禁用**"可启用或禁用规则。每个按钮都显示所选的规则，其中包括可应用相应操作的规则。

所选规则的状态已改变。

删除允许规则

您可以有选择地删除一个或更多允许规则。

要删除允许规则：

1. 在应用程序 Web 界面窗口中选择"**设置**"部分。

2. 转到"**允许规则**"选项卡。

3. 在规则表中，选择要删除的允许规则。

4. 单击"**删除**"。

这将打开一个确认提示窗口。根据所选规则的状态，提示提供以下选项：

- 如果所有选定的规则都已启用，应用程序将提示您删除选定的规则、禁用它们或取消操作。如果选择了所有匹配当前过滤和搜索条件的规则，且选定规则的数量超过 1000 条，则不会检查此条件。

- 如果选定的规则包含已禁用的规则或选择了所有满足当前过滤和搜索条件的规则，且选定的规则数量超过 1000 条，应用程序将提示您删除选定的规则或取消操作。

5. 在提示窗口中，确认删除规则。

所选文件将被删除。

管理扫描排除项列表

具有**高级安全官**角色的用户可以创建、导入和导出*扫描排除项*列表，即 Kaspersky Anti Targeted Attack Platform 视为安全且不会在警报表中显示的数据列表。您可以为以下数据创建扫描排除规则：

- **MD5**。
- **格式**。
- URL **掩码**。
- **电子邮件收件人**。
- **电子邮件发送者**。
- **源 IP 或子网**。
- **目标 IP 或子网**。
- **用户代理**。

具有**安全审计员**和**安全官**角色的用户可以查看扫描排除规则列表并将其导出。

查看从扫描中排除的数据表

要查看包含从扫描中排除的数据的表：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**排除项**子部分。
2. 前往**扫描**选项卡。

   这将打开一个表格，其中包含 Kaspersky Anti Targeted Attack Platform 将视为安全且不会为其创建警报的数据列表。您可以通过单击列标题中的链接来筛选规则。

表包含以下信息：

- **标准** – 将条目添加到允许对象列表的条件。
- **值** – 条件的值。

添加扫描排除规则

要添加到扫描排除项：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**排除项**子部分。
2. 前往**扫描**选项卡。
3. 在应用程序 Web 界面窗口的右上角，单击**添加**。
   这将打开**新规则**窗口。
4. 在**标准**下拉列表中，选择以下条件之一将规则添加到扫描排除项列表中：
   - **MD5**。
   - **格式**。
   - **URL 掩码**。
   - **电子邮件收件人**。
   - **电子邮件发送者**。
   - **源 IP 或子网**。
   - **目标 IP 或子网**。
   - **用户代理**。
5. 如果选择了**格式**，则从**值**下拉列表中选择要添加的文件格式。
   例如，您可以选择 **MSOfficeDoc** 格式。
6. 如果您选择了**MD5**、**URL 掩码**、**电子邮件收件人**、**电子邮件发送者**、**源 IP 或子网**、**目标 IP 或子网** 或者**用户代理**， 请在**值**字段中输入要添加到扫描排除项列表的相关条件的值：
   - 如果您选择了**MD5**，请在**值**字段中中输入文件的 MD5 哈希值。
   - 如果您选择了**URL 掩码**，请在**值**字段中输入 URL 掩码。
     您可以在掩码中使用以下特殊字符：
     * – 任何字符序列。

     示例：
     如果您输入 `*abc*` 作为掩码，应用程序会将包含序列 `abc` 的任何 URL 视为安全。例如，`www.example.com/download_virusabc`

     ? – 任意单个字符。

     示例：
     如果您输入 `example_123?.com` 作为掩码，应用程序会将包含给定字符序列以及任何 3 之后的字符的 URL 视为安全。例如，`example_1234.com`

     如果 * 或 ? 字符是要添加到扫描排除项列表的完整 URL 的一部分，请在输入 URL 时使用 \ 字符来转义单个 *、 ? 或其后的 \ 字符。

示例：
您需要添加以下 URL 作为受信任地址： `www.example.com/download_virus/virus.dll?virus_name=`
您不想应用程序将 `?` 作为特殊掩码字符处理，因此您可以在 `?` 之前添加 `\` 字符。
添加到扫描排除项列表的 URL 如下所示： `www.example.com/download_virus/virus.dll\?virus_name=`

- 如果您选择了**电子邮件收件人**或者**电子邮件发送者**，请在**值**字段中输入电子邮件地址。
- 如果您选择了**用户代理**，请在**值**字段中输入包含浏览器信息的**HTTP 请求的用户代理标头**。
- 如果您选择了**源 IP 或子网**或者**目标 IP 或子网**，请在**值**字段中输入地址或子网（例如 255.255.255.0）。

在**URL 掩码**、**电子邮件收件人**和**电子邮件发送者**字段中，您可以输入包含西里尔字符的域名。在这种情况下，地址将被转换为 Punycode 并根据应用程序设置进行处理。

7. 单击**添加**。

该规则将被添加到扫描排除项列表中。

具有**安全审计员**和**安全官**角色的用户无法添加扫描排除规则。

删除扫描排除规则

要从扫描排除项中删除一条或多条规则：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**排除项**子部分。
2. 前往**扫描**选项卡。
3. 选择您想从扫描排除项列表中移除的每条规则左侧的复选框。
   如果您想删除所有规则，请选中列表上方的复选框。
4. 在窗口的下部，单击**删除**。
   操作确认窗口将显示。
5. 单击**是**。

选定的规则将被从扫描排除项列表中删除。

具有**安全审计员**和**安全官**角色的用户无法从扫描排除项列表中删除条目。

编辑添加到扫描排除项的规则

要编辑扫描排除项列表中的规则：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**排除项**子部分。
2. 前往**扫描**选项卡。
3. 选择要修改的规则。
   这将打开**编辑规则**窗口。
4. 对**标准**和**值**字段进行必要的更改。
5. 单击**保存**。

规则已修改。

具有**安全审计员**和**安全官**角色的用户无法编辑扫描排除项列表中的规则。

导出从扫描中排除的数据列表

要导出扫描排除项列表：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**排除项**子部分。
2. 前往**扫描**选项卡。
3. 在应用程序 Web 界面窗口的右上角，单击**导出**。

包含导出的扫描排除项列表的 JSON 文件被保存在计算机上的浏览器下载文件夹中。

按条件筛选扫描排除项列表中的规则

要按规则类型筛选扫描排除项列表条目：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**排除项**子部分。
2. 前往**扫描**选项卡。
3. 单击**标准**链接以打开筛选配置窗口。

4. 选择您要根据其筛选规则的条件旁边的一个或多个复选框：

   - **MD5**。
   - **格式**。
   - **URL 掩码**。
   - **电子邮件收件人**。
   - **电子邮件发送者**。
   - **源 IP 或子网**。
   - **目标 IP 或子网**。
   - **用户代理**。

5. 单击**应用**。

   筛选配置窗口关闭。

   扫描排除项列表仅显示符合您条件的规则。

> 您可以同时使用多个筛选器。

按值搜索扫描排除项列表中的规则

要按值搜索扫描排除项列表中的规则：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**排除项**子部分。
2. 前往**扫描**选项卡。
3. 单击**值**链接以打开筛选配置窗口。
4. 输入值字符。
5. 单击**应用**。

   扫描排除项列表仅显示符合您条件的规则。

> 您可以同时使用多个筛选器。

重置扫描排除项列表中的规则筛选器

要按一个或多个筛选条件清除排除项列表记录筛选器：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**排除项**子部分。
2. 前往**扫描**选项卡。
3. 单击要为其清除筛选条件的扫描排除项列表条目表中列标题右侧的。

> 如果要清除多个筛选条件，请执行必要的操作以清除每个筛选条件。

选定筛选器将被清除。

扫描排除项列表仅显示符合您条件的规则。

管理入侵检测规则排除项

具有“高级安全官”角色的用户可以添加卡巴斯基入侵检测规则来扫描排除项。Kaspersky Anti Targeted Attack Platform 在通过排除的入侵检测规则进行扫描时不会创建警报。

> 您只能添加卡巴斯基制定的入侵检测规则到排除项。如果您不想在扫描时应用用户定义的入侵检测规则，可以禁用或删除该规则。

如果要配置单一排除（例如，针对特定源地址），您可以：

1. 打开您想要创建单一异常的 IDS 警报的警报详情。
2. 复制 Suricata 格式的 IDS 警报数据并以您认为方便的任何方式保存。
3. 将生成警报的卡巴斯基入侵检测规则添加到扫描排除项中。

4. 通过以下方式之一将基于排除的卡巴斯基规则的属性的新规则添加到用户定义的入侵检测规则列表：

   - 如果系统已有用户定义的入侵检测规则，请导出包含规则的文件，然后向该文件添加新规则，其中包含使用 Suricata 语法缩小规则范围的条件。下面是创建用户定义的入侵检测规则的示例。
   - 如果系统中尚不存在用户定义的入侵检测规则，请创建一个文本文件并使用 Suricata 语法向其中添加具有限定条件的规则。下面是创建用户定义的入侵检测规则的示例。

5. 导入包含已添加规则的文件。

> 我们不建议定期使用上述创建单一排除项的方法，因为大量用户定义的入侵检测规则可能会失控并降低企业 LAN 的保护级别。我们强烈推荐监控所创建的排除项的结果。我们还强烈推荐在导入之前在测试环境中测试用户定义的规则。用户定义的入侵检测规则可能会导致性能问题，在这种情况下无法保证 Kaspersky Anti Targeted Attack Platform 的稳定运行。

具有“安全审计员”角色的用户可以查看添加到排除项的入侵检测规则列表，并查看所选规则的属性。

具有“安全官”角色的用户无法查看添加到排除项的入侵检测规则列表。

根据排除的卡巴斯基规则的属性创建用户定义的入侵检测规则的示例

如果您不希望一个或多个源地址和/或目标地址反映在 IDS 警报中，则可以使用 ! (NOT) 运算符。

示例：
对于包含数据的 IDS 警报：

- header: alert ip any any -> any any.
- flow: established.
- content: example.
- sid: 10000000.

您可以创建以下具有单一排除项的用户定义的入侵检测规则：

- alert ip !10.10.0.22 any -> any any (msg:"Example"; flow:established; content:"example"; sid:1000001;)
  如果建立了连接 (flow:established) 并且有效负载包含字符串“example”，则此规则将针对除 IP 地址 10.10.0.22 之外的所有源触发。
- alert ip ![10.10.0.22,10.10.0.23] any -> any any (msg:"Example"; flow:established; content:"example"; sid:1000002;)
  如果建立了连接 (flow:established) 并且有效负载包含字符串“example”，则此规则将针对除 IP 地址 10.10.0.22 和 10.10.0.23 之外的所有源触发。
- alert ip any any -> ![10.10.0.22,10.10.0.23] any (msg:"Example"; flow:established; content:"example"; sid:1000003;)
  如果建立了连接 (flow:established) 并且有效负载包含字符串“example”，则此规则将针对除 IP 地址 10.10.0.22 和 10.10.0.23 之外的所有目标触发。
- alert ip any any -> ![10.10.0.22,10.10.0.23] ![8080,8085] (msg:"Example"; flow:established; content:"example"; sid:1000004;)
  如果建立了连接 (flow:established) 并且有效负载包含字符串“example”，则此规则将针对除具有特定端口的 IP 地址 10.10.0.22 和 10.10.0.23 之外的所有目标触发。
- alert ip ![10.10.0.22,10.10.0.23] ![8080,8085] -> ![10.80.0.1,10.80.0.2,10.80.0.3] ![8080,8085,8090] (msg:"Example"; flow:established; content:"example"; sid:1000005;)
  如果源 IP 地址和目标 IP 地址不在排除项列表（包括端口）上，如果建立了连接 (flow:established) 并且有效负载包含字符串“example”，则会触发此规则。
- alert ip ![10.10.0.22/24,10.10.0.23/16] any -> any any (msg:"Example"; flow:established; content:"example"; sid:1000006;)
  如果建立了连接 (flow:established) 并且有效负载包含字符串“example”，则此规则将针对除具有特定端口的子网 10.10.0.22/24 和 10.10.0.23/16 之外的所有源触发。
- alert ip ![10.10.0.22/24,10.10.0.23/16] any -> ![10.80.0.1/12,10.80.0.2/8] ![8080,8085] (msg:"Example"; flow:established; content:"example"; sid:1000007;)
  如果未排除源子网和目标子网、目标端口不是 8080 或 8085、建立了连接 (flow:established) 并且有效负载包含字符串“example”，则会触发此规则。

查看添加到排除项的入侵检测规则表

要查看添加到排除项的入侵检测规则表：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**排除项**子部分。
2. 前往**IDS**选项卡。

被排除的 IDS 规则表将显示。您可以通过单击列标题中的链接来筛选规则。

表包含以下信息：

- **创建时间** — 入侵检测规则被添加到排除项的日期和时间。
- **规则名称** — 入侵检测规则的名称。
- **规则 ID** — Suricata 格式的入侵检测规则的 ID (SID 或签名 ID)。

- **描述** – 入侵检测规则描述。
- **创建者** – 账户被用于将入侵检测规则添加到排除项的用户名。

将入侵检测规则添加到排除项

您可以从事件扫描中排除具有中等或高度重要性警报的卡巴斯基入侵检测规则。

您只能排除卡巴斯基入侵检测规则。如果您不想在扫描事件时应用用户定义的入侵检测规则，可以禁用或删除该规则。

要将入侵检测规则添加到排除项：

1. 在应用程序 Web 界面窗口中选择**警报**部分。
   这将打开警报表。
2. 单击**技术**列中的链接打开筛选器配置窗口。
3. 在左侧的下拉列表中，选择**包含**。
4. 在右侧的下拉列表中，选择**（IDS）入侵检测系统**技术。
5. 单击**应用**。
6. 如果您想筛选检测，请单击展开筛选参数列表并选择所需的筛选器。
7. 选择一个警报，“**检测到**”列显示相关入侵检测规则的名称。
   这将打开一个窗口，其中包含有关警报的信息。
8. 在窗口的右侧的**建议**部分、**分类**子部分，单击**添加到排除项**。
   这将打开**将 IDS 规则添加到排除项**窗口。
9. 在**描述**字段中，输入入侵检测规则的描述。
10. 单击**添加**。

入侵检测规则将被添加到排除项中，并显示在应用程序 Web 界面中的“**设置**”部分，“**排除项**”子部分，“IDS”选项卡上的排除项列表中。此规则不再被用于创建警报。

具有**安全审计员**角色的用户无法修改允许对象列表中的条目。

具有“**安全官**”角色的用户无权访问添加到排除项的入侵检测规则列表。

编辑添加到排除项的入侵检测规则的描述

*要编辑被排除的入侵检测规则的描述，请在“**警报**”部分：*

1. 在应用程序 Web 界面窗口中选择**警报**部分。
   这将打开警报表。
2. 单击**技术**列中的链接打开筛选器配置窗口。
3. 在左侧的下拉列表中，选择**包含**。
4. 在右侧的下拉列表中，选择**（IDS）入侵检测系统**技术。
5. 单击**应用**。
6. 如果您想筛选检测，请单击展开筛选参数列表并选择所需的筛选器。
7. 选择一个警报，“**检测到**”列显示相关入侵检测规则的名称。
   这将打开一个窗口，其中包含有关警报的信息。
8. 在窗口的右侧的**建议**部分、**分类**子部分，单击**编辑 IDS 排除项**。
   这将打开**编辑 IDS 排除**窗口。
   在**描述**字段中，编辑规则描述。
   单击**保存**。

被排除的入侵检测规则的描述被修改。此规则不再被用于创建警报。

具有“**安全审计员**”角色的用户无法编辑入侵检测规则描述。

具有“**安全官**”角色的用户无权访问添加到排除项的入侵检测规则列表。

从排除项中删除入侵检测规则

您可以从排除项中删除单个入侵检测规则、多个规则或同时删除所有规则。

要将入侵检测规则从排除项中删除：

1. 在应用程序 Web 界面窗口中，选择“**设置**” → “**排除项**”部分并转到“**IDS**”选项卡。
2. 显示排除的入侵检测规则的列表。
3. 选择要从排除项中删除的规则。
   这将打开一个窗口，其中包含有关规则的信息。

4. 单击**删除**。
   这将打开操作确认窗口。
5. 单击**是**。

该规则已被从排除项中删除。此规则用于创建警报。

要从排除项中删除所有或多个 IDS 规则：

1. 在应用程序 Web 界面窗口中，选择“**设置**” → “**排除项**”部分并转到“**IDS**”选项卡。
2. 显示排除的入侵检测规则的列表。
3. 选中要从排除项中删除的规则旁边的复选框。
   您可以通过选择包含列标题的行中的复选框来选择所有规则。
4. 在窗口下部显示的窗格中，单击**删除**。
   这将打开操作确认窗口。
5. 单击**是**。

选定的规则将被从排除项中删除。这些规则用于创建警报。

具有“**安全审计员**”角色的用户无法从排除项中删除入侵检测规则。

拥有“**安全官**”角色的用户无权访问入侵检测规则的排除项列表。

管理 TAA 排除项

由卡巴斯基专家创建的TAA (IOA) 规则包含企业 IT 基础架构中对象可疑行为的指标。Kaspersky Anti Targeted Attack Platform 可扫描应用程序的事件数据库，并为与 TAA (IOA) 规则描述的行为相匹配的事件创建警报。如果您不希望应用程序为作为组织正常的主机活动的一部分生成的事件创建警报，您可以将 TAA (IOA) 规则添加到排除项。

被添加到排除项的 TAA (IOA) 规则模式可以在以下模式下工作：

- 规则始终被排除在外。
  在这种情况下，Kaspersky Anti Targeted Attack Platform 不会将事件标记为与 TAA (IOA) 规则匹配，也不会根据该规则创建警报。
- 规则由条件补充。
  在这种情况下，TAA（IOA）规则由条件以搜索查询形式补充。Kaspersky Anti Targeted Attack Platform 不会将符合指定条件的事件标记为符合 TAA (IOA) 规则。对于与 TAA (IOA) 规则匹配但不满足应用的排除条件的事件，应用程序会标记事件并创建警报。

如果您使用分布式解决方案和多租户模式，TAA 排除项可以有以下类型：

- **本地** – 在 SCN 服务器上创建。这些排除项仅适用于连接到此 SCN 服务器的主机。排除项属于用户在应用程序 Web 界面中管理的租户。
- **全球** – 在 PCN 服务器上创建。排除项适用于连接到此 PCN 服务器的主机以及连接到此 PCN 服务器的所有 SCN 服务器。排除项属于用户在应用程序 Web 界面中管理的租户。

具有**高级安全官**角色的用户可以为其有权访问数据的租户创建、编辑和删除排除项。

具有**安全审计员**和**安全官**角色的用户只能查看 TAA 排除项列表以及所选排除项的属性。

对于每条 TAA (IOA) 规则，您只能创建一个本地或全局排除项。

如果一条 TAA (IOA) 规则在 SCN 服务器和 PCN 服务器上都创建了排除项，Kaspersky Anti Targeted Attack Platform 将根据 PCN 服务器上的排除设置处理事件。

查看添加到排除项的 TAA (IOA) 规则表

要查看被添加到排除项的 TAA (IOA) 规则表：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**排除项**子部分。
2. 单击**TAA**选项卡。

被排除的 TAA (IOA) 规则表将显示。您可以通过单击列标题中的链接来筛选规则。

表包含以下信息：

- 是根据此 TAA (IOA) 规则扫描而生成的警报的重要性。
  重要性级别可以采用以下值之一：
  - – **低**。
  - – **中**。
  - – **高**。
- **类型**是规则的类型，取决于生成它的服务器的角色：
  - **本地** – 在 SCN 服务器上创建。这些排除项仅适用于连接到此 SCN 服务器的主机。排除项属于用户在应用程序 Web 界面中管理的租户。
  - **全球** – 在 PCN 服务器上创建。排除项适用于连接到此 PCN 服务器的主机以及连接到此 PCN 服务器的所有 SCN 服务器。排除项属于用户在应用程序 Web 界面中管理的租户。

- **置信** – 置信度取决于规则引起误报的可能性：
  - **高**。
  - **中**。
  - **低**。

  置信度越高，误报的可能性就越低。
- **排除规则**是添加到排除项的规则的操作模式。
  - **总是**意味着该规则始终被排除。在这种情况下，Kaspersky Anti Targeted Attack Platform 不会将事件标记为与 TAA (IOA) 规则匹配，也不会根据该规则创建警报。
  - **根据条件**表示如果添加了条件则排除该规则。在这种情况下，TAA（IOA）规则由条件以搜索查询形式补充。Kaspersky Anti Targeted Attack Platform 不会将符合指定条件的事件标记为符合 TAA (IOA) 规则。对于与 TAA (IOA) 规则匹配但不满足应用的排除条件的事件，程序会标记事件并创建警报。
- **名称**是规则的名称。

将 TAA (IOA) 规则添加到排除项

您只能排除卡巴斯基 TAA (IOA) 规则。如果您不想应用用户定义的 TAA (IOA) 规则进行扫描事件，您可以禁用该规则或将其删除。

*要从**警报**部分将 TAA (IOA) 规则添加到排除项：*

1. 在应用程序 Web 界面窗口中选择**警报**部分。
   这将打开警报表。
2. 单击**技术**列中的链接打开筛选器配置窗口。
3. 在左侧的下拉列表中，选择**包含**。
4. 在右侧的下拉列表中，选择**（TAA）针对性攻击分析器**技术。
5. 单击**应用**。
   该表显示 TAA 技术根据 TAA (IOA) 规则生成的警报。
6. 选择一个警报，**检测到**列为其显示相关规则的名称。
   这将打开一个窗口，其中包含有关警报的信息。
7. 在**扫描结果**下面，单击带有规则名称的链接以打开规则信息窗口。
8. 在**TAA 排除项**设置名称右侧，单击**添加到排除项**。
   这将打开一个窗口，允许您将 TAA (IOA) 规则添加到排除项。

9. 在**排除规则**字段中，选择排除操作模式：

   - **总是**，如果您不希望应用程序为与所选 TAA (IOA) 规则匹配的事件创建警报。
   - **根据条件**，如果您不希望应用程序只为符合指定条件的事件创建事件。将为与 TAA (IOA) 规则匹配的事件创建警报，并考虑了配置的排除条件。

     如果您选择了**根据条件**：

     a. 单击**配置附加条件**打开事件搜索表单。

     b. 如果您使用的是分布式解决方案和多租户模式，并且希望为所有租户启用事件显示，请开启**在所有租户中搜索**切换开关。

     c. 在构建器模式下执行事件搜索。

     一个表格将显示，其中包含与给定指定排除条件的 TAA (IOA) 规则相匹配的事件。

     如果您使用分布式解决方案和多租户模式，则找到的事件将按层分组：服务器 – 租户名称 – 服务器名称。

     d. 单击要查看其事件的服务器的名称。

     所选服务器的主机表将显示。事件分组级别显示在表格上方。

     > 如有必要，您可以更改事件搜索条件。

     e. 单击**添加排除项**。

10. 如果您使用分布式解决方案和多租户模式，请在**应用到服务器***字段中选择必须对其应用规则的租户和服务器的复选框。

11. 单击**添加**。

TAA (IOA) 规则将被添加到排除项中，并显示在应用程序 Web 界面中排除项列表的**设置**部分、**排除项**子部分、**TAA**选项卡上。此规则不再被用于创建检测。

*要从**威胁搜索**部分将 TAA (IOA) 规则添加到排除项：*

1. 选择程序 Web 界面窗口中的**威胁搜索**部分。

   这将打开事件搜索表单。

2. 定义搜索条件并单击**搜索**按钮。例如，您可以在构建器模式下在**TAA 属性**组中选择事件搜索条件。

   满足搜索条件的事件表将显示。

3. 选择一个事件。

4. 在**IOA 标记**设置右侧，单击规则名称。

   这将打开一个窗口，其中包含有关规则的信息。

5. 在**TAA 排除项**设置名称右侧，单击**添加到排除项**。

   这将打开一个窗口，允许您将 TAA (IOA) 规则添加到排除项。

6. 在**排除规则**字段中，选择排除操作模式：

- **总是**，如果您不希望应用程序为与所选 TAA (IOA) 规则匹配的事件创建警报。
- **根据条件**，如果您不希望应用程序只为符合指定条件的事件创建事件。将为与 TAA (IOA) 规则匹配的事件创建警报，并考虑了配置的排除条件。

  如果您选择了**根据条件**：

  a. 单击**配置附加条件**打开事件搜索表单。

  b. 如果您使用的是分布式解决方案和多租户模式，并且希望为所有租户启用事件显示，请开启**在所有租户中搜索**切换开关。

  c. 在构建器模式下执行事件搜索。

  一个表格将显示，其中包含与给定指定排除条件的 TAA (IOA) 规则相匹配的事件。

  如果您使用分布式解决方案和多租户模式，则找到的事件将按层分组：服务器 – 租户名称 – 服务器名称。

  d. 单击要查看其事件的服务器的名称。

  所选服务器的主机表将显示。事件分组级别显示在表格上方。

  > 如有必要，您可以更改事件搜索条件。

  e. 单击**添加排除项**。

7. 单击**添加**。

TAA (IOA) 规则将被添加到排除项中，并显示在应用程序 Web 界面中排除项列表的**设置**部分、**排除项**子部分、**TAA**选项卡上。扫描事件时不再应用此规则。

创建要保存为排除条件的搜索查询时，请避免使用以下字段：

- IOAd。
- IOATag。
- IOATechnique。
- IOATactics。
- IOAImportance。
- IOAConfidence。

仅当 Kaspersky Anti Targeted Attack Platform 将事件标记为匹配 TAA (IOA) 规则后，这些字段才会显示。

> 具有**安全审计员**和**安全官**角色的用户无法将 TAA (IOA) 规则添加到排除项。

查看添加到排除项的 TAA (IOA) 规则

要查看添加到排除项的 TAA (IOA) 规则：

1. 在应用程序 Web 界面窗口中，选择**设置**部分、**排除项**子部分并转到**TAA**选项卡。
   被排除的 TAA (IOA) 规则表将显示。
2. 选择要查看的规则。

这将打开一个窗口，其中包含有关规则的信息。

该窗口包含以下信息：

- **TAA (IOA) 规则**：单击此链接可打开一个窗口，其中包含与此规则对应的 MITRE 技术的描述、关于响应事件的建议以及有关误报可能性的信息。
- **ID**是应用程序分配给每个规则的 ID。
- **名称**是您在添加规则时指定的规则的名称。
- **重要级别**是卡巴斯基专家评估的该事件对计算机或企业 LAN 安全可能影响的估计。
- **置信**是取决于卡巴斯基专家估计的误报概率的置信水平。
- **排除规则**是添加到排除项的规则的操作模式。
  - **总是**意味着该规则始终被排除。在这种情况下，Kaspersky Anti Targeted Attack Platform 不会将事件标记为与 TAA (IOA) 规则匹配，也不会根据该规则创建警报。
  - **根据条件**表示如果添加了条件则排除该规则。在这种情况下，TAA（IOA）规则由条件以搜索查询形式补充。Kaspersky Anti Targeted Attack Platform 不会将符合指定条件的事件标记为符合 TAA (IOA) 规则。对于与 TAA (IOA) 规则匹配但不满足应用的排除条件的事件，程序会标记事件并创建警报。
- **配置附加条件**：单击此链接可打开带有搜索条件的事件搜索表单。
  如果在将 TAA (IOA) 规则添加到排除项时您选择了**根据条件**模式并配置了一些搜索条件，则显示此字段。
- 搜索条件以`<IOA ID> AND NOT <`搜索条件`>`格式配置。
  如果在将 TAA (IOA) 规则添加到排除项时您选择了**根据条件**模式并配置了一些搜索条件，则显示搜索条件。
- **应用到服务器***是排除项对其应用的主机。
  该字段在分布式解决方案和多租户模式下显示。

从排除项中删除 TAA (IOA) 规则

您可以从排除项中删除单个 TAA (IOA) 规则、多个规则或同时删除所有规则。

要从排除项中删除 TAA (IOA) 规则：

1. 在应用程序 Web 界面窗口中，选择**设置**部分、**排除项**子部分并转到**TAA**选项卡。
   被排除的 TAA (IOA) 规则表将显示。
2. 选择要从排除项中删除的规则。
   这将打开一个窗口，其中包含有关规则的信息。
3. 单击**删除**。
   这将打开操作确认窗口。
4. 单击**是**。

该规则已被从排除项中删除。创建警报或扫描事件时应用该规则。

要从排除项中删除全部或多个 TAA (IOA) 规则：

1. 在应用程序 Web 界面窗口中，选择**设置**部分、**排除项**子部分并转到**TAA**选项卡。
2. 被排除的 TAA (IOA) 规则表将显示。
3. 选中要从排除项中删除的规则旁边的复选框。
   您可以通过选择包含列标题的行中的复选框来选择所有规则。
4. 在窗口下部显示的窗格中，单击**删除**。
   这将打开操作确认窗口。
5. 单击**是**。

选定的规则将被从排除项中删除。创建警报或扫描事件时将应用这些规则。

具有**安全审计员**和**安全官**角色的用户无法从排除项中删除 TAA (IOA) 规则。

管理 ICAP 排除项

具有**高级安全官**的用户可以创建 ICAP 排除项列表，即 Kaspersky Anti Targeted Attack Platform 不得扫描的数据列表。您可以为以下数据创建 ICAP 排除规则：

- **格式**。
- **用户代理**。
- **MD5**。
- **URL 掩码**。
- **源 IP 或子网**。

具有**安全审计员**和**安全官**角色的用户可以查看 ICAP 排除规则列表。

在分布式解决方案模式下，在 SCN 上创建的 ICAP 排除项适用于连接到该 SCN 的所有 Sensor 组件。在 PCN 上创建的 ICAP 排除项适用于安装在与 PCN 相同的设备上的 SCN 以及连接到该 SCN 的所有 Sensor 组件。

查看 ICAP 排除表

要查看 ICAP 排除表：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**排除项**子部分。
2. 打开**ICAP**选项卡。

   Kaspersky Anti Targeted Attack Platform 不得扫描的数据表将显示。您可以通过单击列标题中的链接来筛选规则。

表列包含以下信息：

- **值** – 条件的值。
- **标准** – 将条目添加到允许对象列表的条件。
- **状态**是规则的状态。

将规则添加到 ICAP 排除项

如果数据规则之前尚未被添加到扫描排除规则中，则 ICAP 排除规则将得到处理。

要将规则添加到 ICAP 排除项：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**排除项**子部分。
2. 打开**ICAP**选项卡。
3. 在应用程序 Web 界面窗口的右上角，单击**添加**。
   这将打开**新规则**窗口。
4. 移动**状态**切换开关到您需要的位置。
   默认情况下，切换开关位于**已启用**位置。
5. 在**标准**下拉列表中，选择以下条件之一将规则添加到 ICAP 排除项列表中：
   - **格式**。
   - **用户代理**。

- **MD5**。
- **URL 掩码**。
- **源 IP 或子网**。

6. 根据所选条件，在**值**字段中指定以下信息：

- 如果选择了**格式**，则从下拉列表中选择要添加的文件格式。

  > 按格式添加 ICAP 排除规则时，无需扫描即可加载相应格式的网页内容，且不影响网页显示。

- 如果您选择了**用户代理**，请输入包含浏览器信息的HTTP 请求的用户代理标头。
- 如果您选择了**MD5**，请输入文件的 MD5 哈希值。
- 如果您选择了**URL 掩码**，请输入 URL 掩码。
  您可以在掩码中使用以下特殊字符：
  * – 任何**字符**序列。

  示例：
  如果您输入`*abc*`作为掩码，应用程序不会扫描任何包含序列`abc`的 URL。例如，
  `www.example.com/download_virusabc`

  ? – 任意单个**字符**。

  示例：
  如果您输入`example_123?.com`作为掩码，应用程序不会扫描任何包含给定字符序列以及任何`3`之后的字符的 URL。例如，`example_1234.com`

  如果 * 或 ? 字符是要添加到扫描排除项列表中的完整 URL 的一部分，请在输入 URL 时使用 \ 字符来转义单个 *、 ? 或其后的 **\字符**。

  示例：
  您需要添加以下 URL 作为受信任地址：`www.example.com/download_virus/virus.dll?virus_name=`
  您不想应用程序将 ? 作为特殊掩码字符处理，因此您可以在 ? 之前添加 \ 字符。
  添加到扫描排除项列表的 URL 如下所示：`www.example.com/download_virus/virus.dll\?virus_name=`

  > 在**URL 掩码**字段中，您可以输入包含西里尔字符的域名。在这种情况下，地址将被转换为 Punycode 并根据应用程序设置进行处理。

- 如果您选择了**源 IP 或子网**，请输入地址或子网（例如 255.255.255.0）。

7. 单击**添加**。

该规则将被添加到 ICAP 排除项列表中。

> 具有**安全审计员**和**安全官**角色的用户无法添加 ICAP 排除规则。

从 ICAP 排除项中删除规则

要从 ICAP 排除项中删除一条或多条规则：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**排除项**子部分。
2. 打开**ICAP**选项卡。
3. 选择您想从 ICAP 排除项列表中移除的每条规则左侧的复选框。
   如果您想删除所有规则，请选中列表上方的复选框。
4. 在窗口的下部，单击**删除**。
5. 这会打开一个窗口；在该窗口中，单击**是**确认删除规则。

选定的规则将被从 ICAP 排除项列表中删除。之前在 ICAP 排除规则中列出的数据现在由Kaspersky Anti Targeted Attack Platform 进行扫描。

具有**安全审计员**和**安全官**角色的用户无法从 ICAP 排除项列表中删除条目。

编辑或禁用 ICAP 排除项列表中的规则

要编辑 ICAP 排除项列表中的规则：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**排除项**子部分。
2. 打开**ICAP**选项卡。
3. 选择要修改的规则。
   这将打开**编辑规则**窗口。
4. 对**状态**、**标准**和**值**字段进行必要的更改。
5. 单击**保存**。

规则已修改。

要禁用 ICAP 排除项列表中的规则：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**排除项**子部分。
2. 打开**ICAP**选项卡。

3. 在 ICAP 排除项列表中要禁用的规则的右侧，在**状态**列中，将切换开关移至**已禁用**位置。

4. 这会打开一个窗口；在该窗口中，单击**是**确认禁用规则。

该规则被禁用。

具有**安全审计员**和**安全官**角色的用户无法编辑或禁用 ICAP 排除项列表中的规则。

按条件筛选 ICAP 排除项列表中的规则

要按条件筛选 ICAP 排除项列表中的规则：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**排除项**子部分。

2. 打开**ICAP**选项卡。

3. 单击**标准**链接以打开筛选配置窗口。

4. 选择您要根据其筛选规则的条件旁边的一个或多个复选框：

   - **格式**。
   - **用户代理**。
   - **MD5**。
   - **URL 掩码**。
   - **源 IP 或子网**。

5. 单击**应用**。
   筛选配置窗口关闭。

ICAP 排除项列表仅显示与指定筛选条件匹配的规则。您可以按**值**和**状态**列同时进行筛选。

按值筛选 ICAP 排除项列表中的规则

要按值筛选 ICAP 排除项列表中的规则：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**排除项**子部分。

2. 打开**ICAP**选项卡。

3. 单击**值**链接以打开筛选配置窗口。

4. 输入一个值。

5. 单击**应用**。

ICAP 排除项列表仅显示与指定搜索条件匹配的规则。您可以按**标准**和**状态**列同时进行筛选。

按状态筛选 ICAP 排除项列表中的规则

要按状态筛选 ICAP 排除项列表中的规则：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**排除项**子部分。

2. 打开**ICAP**选项卡。

3. 单击**状态**链接以打开筛选配置窗口。

4. 选择某个值旁边的复选框：

   - **已启用。**
   - **已禁用。**

5. 单击**应用**。

ICAP 排除项列表仅显示与指定搜索条件匹配的规则。您可以按**标准**和**值**列同时进行筛选。

重置 ICAP 排除项列表中的规则筛选条件

要清除 ICAP 排除项列表中规则的筛选条件：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**排除项**子部分。

2. 打开**ICAP**选项卡。

3. 单击表中要为其重置筛选条件的**值**、**标准**或者**状态**列的标题右侧的。
   如果要清除多个筛选条件，请执行必要的操作以清除每个筛选条件。

选定筛选条件将被清除。ICAP 排除项列表仅显示与指定条件匹配的规则。

管理 SPAN 端口的镜像流量

管理 Web 界面时，具有“**高级安全官**”角色的用户可以从 Sensor 组件服务器的 SPAN 端口下载 PCAP 格式的镜像流量转储，并进行调查以检测可疑活动。

如果您使用分布式解决方案和多租户模式，请在带有 Sensor 组件的服务器所连接的 PCN 或 SCN 服务器上执行相关步骤。

要从 SPAN 端口下载镜像流量：

1. 在应用程序 Web 界面窗口中选择**Sensor 服务器**部分。
2. 单击相关 Sensor 组件的卡片。

   这将打开一个窗口，其中包含有关组件的信息。
3. 单击“**下载流量**”。

   显示下载选项窗口。

   在“**内部存储**”部分，“**最旧的数据包**”字段显示内部存储中第一次保存的转储的日期和时间。在“**已使用/最大**”字段中，第一个数字表示内部存储的已占用空间，第二个数字表示内部存储的总大小。“**外部存储**”部分显示存储状态：“**已连接**”或“**未连接**”。
4. 执行以下操作：

   - 在“**要下载的流量周期**”中，设置要下载流量转储的期限范围。

     如果您选择的时间段内不存在记录的流量，则当您单击“**下载流量**”时，Kaspersky Anti Targeted Attack Platform 会建议选择从第一次记录的网络流量转储到最后一次记录的时间段。如果根本不存在记录的转储，则会显示一条警告，指示指定时间段内缺少数据。

   - 在“**下载量限制**”字段中，您可以指定要下载的最大流量。

     如果下载的流量超过指定的限制，则会丢弃最新的流量。

   - 如果需要，请在**“按监控点过滤”**下启用过滤，并指定要从中获取流量的监控点。

   - 如有必要，请在“**使用 BPF 过滤**”部分启用过滤，并输入使用 Berkeley Packet Filter (BPF) 技术的过滤表达式。BPF 过滤表达式的写入格式为 libpcap。有关语法的更多详细信息，请参阅 pcap-filter 手册页。

     过滤表达式的示例：
     ```
     tcp port 102 or tcp port 502
     ```

   - 如有必要，请在“**使用正则表达式过滤**”部分启用过滤，并输入基于流量中的有效负载数据进行过滤的表达式。

     过滤表达式示例：
     ```
     ^test.+xABxCD
     ```
5. 单击“**下载流量**”。

来自 SPAN 端口的镜像流量转储以 PCAP 格式下载。

顺序流量下载请求的建议

我们建议在发送新的流量下载请求时考虑处理之前的流量下载请求所需的时间。

如果下一个流量下载请求在前一个流量下载请求完成之前到达，则转储文件下载可能会失败，并且不会出现任何错误消息。

请求处理时间取决于各种因素：搜索范围、要下载的流量大小以及 Sensor、服务器和客户端计算机之间的连接速度。

要下载的流量大小取决于客户的要求；少量流量可以在几秒钟内下载。如果用户尝试下载所有可用流量，则下载速度限制为 50 Mbps。这个限制可以保护系统不因下载大量流量而导致过载。在 50 Mbps 的速度下，下载 1 GB 的流量大约需要 20 秒，下载 1 TB 的流量大约需要 5.5 小时。

创建存档的密码列表

该应用程序不扫描受密码保护的存档。您可以为在组织内交换文件时使用的存档创建最常遇到的密码列表。如果这样做，应用程序将在扫描存档时尝试列表中的密码。如果其中一个密码匹配，则将解锁并扫描存档。

应用程序设置中设置的密码列表也会传输到具有 Sandbox 组件的服务器。

要创建存档密码列表：

1. 在应用程序 Web 界面窗口中，选择**设置**部分的**存档密码**子部分。
2. 在**存档密码**字段中，输入应用程序用于密码保护存档的密码。

   在新行上输入每个密码。您最多可以输入50个密码。
3. 单击**应用**。

将创建存档的密码列表。扫描受密码保护的 PDF 文件以及 Microsoft Word、Excel® 和 PowerPoint® 文件时，应用程序将使用定义列表中的密码。

具有**安全审计员**角色的用户可以查看存档的密码列表，但无法编辑它。

管理 Central Node 或 Sensor 服务器信息

拥有“**安全审计员**”角色的用户可以查看有关具有 Central Node 和 Sensor 组件的服务器的信息。

有关带有 Central Node 或 Sensor 组件的服务器的信息显示在应用程序 Web 界面窗口的“**Sensor 服务器**”区域。

此部分显示组件的卡（左侧）和在这些组件上检测到的网络接口卡（每个组件的右侧）。

Sensor 组件卡片上方是该 Sensor 所连接的 Central Node 组件卡片。

如果 Central Node 组件部署了嵌入式 Sensor，则该 Sensor 组件的名称将在卡上显示为嵌入式 Sensor。

网络接口卡显示以下信息：

- 网络接口名称
- 网络接口的 MAC 地址
- 网络接口的 IP 地址
- 网络接口频宽

如果网络接口已经添加了监控点，则网络接口的卡片中将显示该监控点的以下信息：

- 监控点名称。
- **技术模式**是技术继承功能的状态。它可以是**已启用**或者**已禁用**。

您可以查看 Central Node 和 Sensor 组件以及在这些组件上发现的网络接口的详细信息。

要查看组件或者网络接口详细信息：

单击其卡片。

Central Node 和 Sensor 组件的**"设置"**选项卡显示以下信息：

- "**状态**"是通过图标和文本描述指示的组件的当前状态。
- **节点类型**表示应用程序组件：**Server**（Central Node 组件）或者**Sensor**（Sensor组件）。
- **应用程序当前使用的磁盘空间**是应用程序文件占用的磁盘空间。包括已安装的文件和应用程序在运行过程中创建的文件。
- **应用程序可使用的最大磁盘空间**就是应用程序文件可占用的磁盘空间。包括已安装的文件和数据存储规则中配置的所有空间限制的总和。该值不得超过可用磁盘空间量。
- "**磁盘占用**"是所有文件使用的磁盘空间。包括应用程序文件、操作系统文件和其他应用程序的文件。该空间是根据包含组件文件系统中 /var 目录的磁盘来计算的。
- "**可用磁盘空间**"是未被文件使用的磁盘空间。该空间是根据包含组件文件系统中 /var 目录的磁盘来计算的。
- "**总磁盘空间**"是包含组件文件系统中 /var 目录的驱动器上的磁盘空间总量。
- "**BPF 过滤**"指示是否启用或禁用使用基于网络数据包中的地址参数的 Berkley Packet Filter (BPF) 技术进行过滤。
- **流量转储文件的外部存储**指示外部存储的连接状态。可能显示以下状态：**已连接**、**未连接**。
- "**保留规则**"指示应用程序数据的大小、项目数量和存储期限的当前值和最大值。

对于 Sensor 组件，除了**"设置"**选项卡之外，还会显示**"外部存储"**、**"其他"**、**"ICAP 集成"**、**"POP3 集成"**和**"SMTP 集成"**选项卡。

- "**外部存储**"选项卡显示有关镜像 SPAN 流量的外部存储配置的信息。
- 在**"其他"**选项卡上，显示以下信息：
  - 扫描文件的最大大小是组件当前能够扫描的文件大小的限制。
  - 转储 HTTP 正文指示是否启用或禁用 HTTP 正文内容转储。
- "**ICAP 集成**"选项卡显示通过 ICAP 与代理服务器集成的设置。
- "**POP3 集成**"选项卡显示 POP3 邮件服务器集成设置。
- "**SMTP 集成**"选项卡显示 SMTP 邮件服务器集成设置。

对于未添加监控点的网络接口，详细信息区中显示以下信息：

- “**网络接口**”是操作系统中网络接口的名称。
- “**连接**”是表示网线已连接到网络接口的以太网端口的图标：
  - – 网线已连接。
  - – 网线已断开连接。

  启用以太网端口指示模式时，图标闪烁。
- **MAC 地址**是网络接口的 MAC 地址。
- **IP 地址**是网络接口的 IP 地址。如果网络接口上发现多个 IP 地址，则详细信息区域中最多显示 16 个 IP 地址。

如果网络接口上已经添加了监控点，则网络接口的卡片中会显示以下信息：

- “**状态**”是监控点当前的状态，用图标和文字描述表示：
  - *正常*。监测点可用。
  - *切换*。监控点运行模式正在改变。
  - *错误*。切换监控点操作模式时检测到错误。
- “**连接**”是表示网线已连接到网络接口的以太网端口的图标：
  - – 网线已连接。
  - – 网线已断开连接。

  启用以太网端口指示模式时，图标闪烁。
- “**网络接口**”是操作系统中网络接口的名称。
- “**模式**”是监控点当前的模式：
  - *已启用*。
  - *已禁用*。
- 在**“设置”**选项卡上：
  - “**技术继承**”指示是否为服务器启用或禁用技术继承。
  - **MAC 地址**是网络接口的 MAC 地址。
  - **IP 地址**是网络接口的 IP 地址。

查看服务器设置

具有**安全审计员**角色的用户可以查看分布式解决方案和多租户模式下的 Central Node 服务器和 PCN 设置。

服务器设置位于 Web 界面窗口的**设置**部分。在此部分中，您可以查看以下信息：

- **用户** — 应用程序 Web 界面用户的用户账户列表。
- **常规设置** — 服务器的常规设置。
  - **数据库更新** — 数据库更新。
  - **监控** — Central Node 和 Sensor 服务器允许的最大硬盘空间使用量。
  - SNMP — SNMP 连接设置。
- **身份验证策略** — 密码策略设置。
- **证书** — 服务器证书和具有 Endpoint Agent 组件的计算机的状态。
- **日期和时间** — 服务器日期和时间设置。
- Endpoint Agent — 与 Endpoint Agent 组件集成时可用的程序功能。
  - IOC **扫描计划** — IOC 扫描计划的设置。
  - **自动将文件发送到** Sandbox — 自动发送要由 Sandbox 组件扫描的文件。
  - **活动指标** — Endpoint Agent 组件的活动指示器。
  - **自动删除不活动的主机** — 自动从 Endpoint Agent 表中删除不活动的主机。
  - **手动将文件从主机发送到** Sandbox **进行分析** — 手动发送要由 Sandbox 组件扫描的文件。
  - **对事件链使用** TAA (IOA) **规则** — 使用 TAA（IOA）规则扫描事件链。默认情况下禁用此功能。
- ICAP **流量扫描** — 通过 ICAP 与代理服务器集成的设置。
- **连接服务器** — 作为 Endpoint Agent 组件的集成服务器的服务器。
- **连接器** — 连接器设置。
- Secret — Secret 的设置。
- **事件类型** — 事件类型的设置。
- **风险类型** — 风险类型的设置。
- KSN/KPSN **和** MDR — 参与卡巴斯基安全网络和卡巴斯基私人安全网络的设置。
- KPSN **信誉数据库** — 使用 KPSN 信誉数据库的设置。
- SIEM **系统** — 与 SIEM 系统集成的设置。
- **通知**—通知设置。
- VIP **状态** — 将 VIP 身份分配给警报的规则列表。
- **排除项** — TAA 和 IDS 规则允许的对象列表和排除项列表。

- **网络设置** – 网络接口参数的设置。
- **允许规则** – 控制网络上设备交互的规则。
- **存档密码** – 存档密码列表。
- **授权许可** – 授权许可密钥的状态。

查看具有 Sandbox 组件的服务器表

具有**安全审计员**角色的用户可以查看具有Sandbox 组件的服务器表。

具有 Sandbox 组件的服务器表位于程序 Web 界面窗口的**Sandbox 服务器**部分的**服务器**选项卡上。

证书指纹字段显示 Central Node 服务器的 TLS 证书的指纹。

服务器列表表包含以下信息：

- **IP 和名称** – 具有 Sandbox 组件的服务器的 IP 地址或完全限定域名。
- **证书指纹** – 具有 Sandbox 组件的服务器的证书指纹。
- **授权** – 连接到 Sandbox 组件的请求的状态。
- **状态** – 与 Sandbox 组件的连接状态。

具有**安全官**角色无法查看具有 Sandbox 组件的服务器表。

查看用于扫描 Sandbox 中对象的操作系统集的设置

具有**安全审计员**角色的用户可以查看操作系统集的设置，这些设置被用作 Sandbox 组件创建扫描对象任务的基础。Sandbox 服务器必须安装与所选集匹配的虚拟机。

有关用于在 Sandbox 中扫描对象的操作系统集设置的信息位于应用程序 Web 界面窗口**Sandbox 服务器**部分的**设置**选项卡上。

Sandbox 组件可以在其上扫描对象的操作系统集显示在**操作系统集合**下面。

属于所选集的操作系统显示在**集合组成**下面。

查看外部系统表

具有**安全审计员**角色的用户可以查看外部系统表。

外部系统表位于应用程序 Web 界面窗口的**外部系统**部分。

证书指纹字段显示 Central Node 服务器的 TLS 证书的指纹。

服务器列表表包含以下信息：

- **Sensor** — 外部系统服务器的 IP 地址或域名。
- **类型** — 外部系统的类型（邮件传感器或其他系统）。
- **名称** — 不是邮件传感器的集成外部系统的名称。
  邮件传感器的此列中显示破折号。
- **ID** — 外部系统的 ID。
- **证书指纹** — 服务器的 TLS 证书的指纹，外部系统用于与 Central Node 服务器建立加密连接。

  具有 Central Node 组件的服务器的证书指纹显示在**证书指纹**字段中窗口的上部。
- **状态** — 集成请求的状态。

具有**高级安全官**和**安全官**角色的用户无法查看外部系统表。

管理用户定义的 Sandbox 规则

用户自定义的文件和 URL 扫描 Sandbox 规则允许将对象发送到自定义虚拟机进行扫描。如果未添加任何规则，则不会在自定义虚拟机中扫描对象。若要在预设虚拟机中发送要扫描的对象，您不需要创建任何规则。默认情况下，Kaspersky Anti Targeted Attack Platform 会发送需要扫描的对象进行扫描。

仅当存在自定义虚拟机时，规则创建才可用。

具有**高级安全官**和**管理员**角色的用户可以创建扫描文件和 URL 的规则，编辑、删除、启用或禁用规则。文件扫描规则也可以被导入和导出。

在分布式解决方案模式下，您必须在要从中发送文件进行扫描的每个 PCN 和 SCN 服务器上创建用于在自定义虚拟机中扫描文件的规则。

具有**安全审计员**角色的用户可以查看规则列表。具有**安全官**角色的用户无法查看此部分。

查看用户定义的 Sandbox 规则表

要查看用户定义的 Sandbox 规则表：

1. 在应用程序 Web 界面窗口中，选择**自定义规则**部分的**Sandbox**小节。
2. 打开**文件**或者**URL**选项卡。

   用户定义的文件或 URL 扫描 Sandbox 规则表将显示。

用户定义的文件扫描规则表包含以下信息：

- **已创建**是规则创建时间。
- **虚拟机**是文件被发送到进行扫描的虚拟机的名称。
- **掩码**是被发送进行扫描的文件的掩码。
- **掩码排除项**是被从扫描中排除的文件的掩码。
- **文件类别**是被发送用于扫描的文件类别。
- **状态**是规则的状态。它可以具有值**已启用**和**已禁用**。

用户定义的 URL 扫描规则表包含以下信息：

- **已创建**是规则创建时间。
- **虚拟机**是文件被发送到进行扫描的虚拟机的名称。
- **状态**是规则的状态。它可以具有值**已启用**和**已禁用**。

配置 Sandbox 规则表显示

您可以显示或隐藏列并更改表中列的顺序。

要配置表格显示：

1. 在应用程序 Web 界面窗口中，选择**自定义规则**部分的**Sandbox**小节。
2. 打开**文件**或者**URL**选项卡。
   用户定义的文件或 URL 扫描 Sandbox 规则表将显示。
3. 在表格的标题部分，单击  。
   这将打开**定制表格**窗口。
4. 如果要在表中显示列，请选择要在表中显示的参数名称旁边的复选框。
   如果要隐藏表中的参数，请清除该复选框。

   > 必须选择至少一个复选框。

5. 如果要更改表格中列的顺序，请将鼠标光标移动到具有相关参数的行，单击  并将该行移动到新位置。
6. 如果要恢复默认表格显示设置，请单击**默认**。
7. 单击**应用**。

规则表显示已配置。

筛选和搜索 Sandbox 规则

要按所需条件筛选或搜索 Sandbox 规则：

1. 在应用程序 Web 界面窗口中，选择**自定义规则**部分的**Sandbox**小节。
2. 打开**文件**或者**URL**选项卡。
3. 根据筛选条件，执行以下操作：

   - **按创建时间**

     a. 单击**已创建**链接以打开筛选设置窗口。

     b. 选择以下选项之一：

     - **任何时候**如果您希望表显示任何时间创建的规则。
     - **上一个小时**，如果您希望应用程序显示表中最后一小时创建的规则。

- **最后一天**，如果您希望应用程序显示表中最后一天创建的规则。
- **自定义范围**，如果您希望应用程序显示表中在指定时段内创建的规则。

c. 如果您选择了**自定义范围**，请选择该期间的开始日期和结束日期，然后单击**应用**。

- **按虚拟机名称**

a. 单击**虚拟机**打开筛选设置窗口。

b. 输入虚拟机名称的一个或多个字符。

c. 单击**应用**。

该表仅显示与指定条件匹配的规则。

您可以同时使用多个筛选器。

清除 Sandbox 规则筛选器

要清除 Sandbox 规则筛选器的一个或多个筛选条件：

1. 在应用程序 Web 界面窗口中，选择**自定义规则**部分的**Sandbox**小节。
2. 打开**文件**或者**URL**选项卡。
3. 单击要为其清除筛选条件的规则表的列标题右侧的。
   如果要清除多个筛选条件，请采取步骤单独清除每个筛选条件。

选定筛选器将被清除。

该表仅显示与指定条件匹配的规则。

查看用户定义的 Sandbox 规则信息

要查看用户定义的 Sandbox 规则信息：

1. 在应用程序 Web 界面窗口中，选择**自定义规则**部分的**Sandbox**小节。
2. 打开**文件**或者**URL**选项卡。
3. 选择您想查看信息的规则。

这将打开一个窗口，其中包含有关规则的信息。

有关用户定义的文件扫描规则的信息窗口包含以下信息：

- **状态**是防护规则的状态。
- **虚拟机**是在其上根据此规则扫描文件的虚拟机。
- **掩码**是被发送进行扫描的文件的掩码。
- **掩码排除项**是被从扫描中排除的文件的掩码。
- **文件类别**是被发送用于扫描的文件类别。
- **文件大小**是正在被扫描的文件的大小。

有关用户定义的 URL 扫描规则的信息窗口包含以下信息：

- **虚拟机**是扫描 URL 的虚拟机。
- **状态**是防止规则的状态。

创建用户定义的文件扫描 Sandbox 规则

添加用户定义的文件扫描 Sandbox 规则：

1. 在应用程序 Web 界面窗口中，选择**自定义规则**部分的**Sandbox**小节。
2. 打开**文件**选项卡。
3. 单击**添加**。
4. 选择**创建规则**。
   这将打开规则创建窗口。
5. 配置以下设置：
   a. **状态**是防止规则的状态。如果您想要启用该规则，请选择该复选框。
   b. **虚拟机**是根据此规则扫描文件的虚拟机。
   只能选择具有自定义操作系统镜像的虚拟机。这些虚拟机必须属于在 Central Node 上选择的操作系统集。
   c. 至少指定以下值之一：掩码或文件类别。如果填写所有字段，则会针对与类别和大小条件或掩码和大小条件匹配且不是排除项的文件触发规则。
      - **掩码**是您要发送进行扫描的文件的掩码。您可以指定多个值。
      要指定掩码，您可以使用 * 和 ? 通配符。其他通配符不受支持。
      - **掩码排除项**是必须从扫描中排除的文件的掩码。您可以指定多个值。
      要指定排除掩码，您可以使用 * 和 ? 通配符。其他通配符不受支持。
      - **文件类别**是您要发送进行扫描的文件类别。您可以指定多个类别。
      您可以在文件类别的扩展名列表部分中查看每个类别的扩展名的完整列表。

- **文件大小**是正在被扫描的文件的大小。
- 如果要设置多个范围，请单击**添加文件大小**。

6. 单击**添加**。

规则已创建。

如果要发送存档进行扫描，则必须考虑扫描存档时涉及的特殊注意事项。

档案扫描如下：

1. Kaspersky Anti Targeted Attack Platform 解压缩存档。
2. 存档中与规则匹配的文件将被发送以进行扫描。

具有 MSI 扩展名的文件的扫描方式与存档相同。

创建用户定义的 URL 扫描 Sandbox 规则

添加用户定义的 URL 扫描 Sandbox 规则：

1. 在应用程序 Web 界面窗口中，选择**自定义规则**部分的**Sandbox**小节。
2. 打开**URL**选项卡。
3. 单击**添加**。
4. 选择**创建规则**。
   这将打开规则创建窗口。
5. 配置以下设置：
   a. **虚拟机**是将扫描 URL 的虚拟机。
      只能选择具有自定义操作系统镜像的虚拟机。这些虚拟机必须属于在 Central Node 上选择的操作系统集。
   b. **状态**是防止规则的状态。如果您想要启用该规则，请选择该复选框。
6. 单击**添加**。

规则已创建。

复制用户定义的 Sandbox 规则

复制用户定义的 Sandbox 规则：

1. 在应用程序 Web 界面窗口中，选择**自定义规则**部分的**Sandbox**小节。
2. 打开**文件**或者**URL**选项卡。
3. 选择相关规则。
4. 在规则窗口中，单击**复制**。

   规则将与所有设置一起复制。如有必要，您可以更改设置的值。

导入用户定义的文件扫描 Sandbox 规则

要导入用户定义的文件扫描 Sandbox 规则：

1. 在应用程序 Web 界面窗口中，选择**自定义规则**部分的**Sandbox**小节。
2. 打开**文件**选项卡。
3. 单击**添加**。
4. 选择**导入规则**。
5. 这将打开文件上传窗口。
6. 选择您想导入的文件。
7. 单击**打开**。

   文件已导入。

编辑用户定义的 Sandbox 规则

编辑用户定义的 Sandbox 规则：

1. 在应用程序 Web 界面窗口中，选择**自定义规则**部分的**Sandbox**小节。
2. 打开**文件**或者**URL**选项卡。
   用户定义的文件或 URL 扫描 Sandbox 规则表将显示。
3. 选择一个规则。

   这将打开规则编辑窗口。

您可以编辑以下字段：

- 在用户定义的文件扫描 Sandbox 规则中：
  - **状态**是防止规则的状态。如果您想要启用该规则，请选择该复选框。
  - **虚拟机**是根据此规则扫描文件的虚拟机。
    只能选择具有自定义操作系统镜像的虚拟机。这些虚拟机必须属于在 Central Node 上选择的操作系统集。
  - 至少指定以下值之一：掩码或文件类别。如果填写所有字段，则会针对与类别和大小条件或掩码和大小条件匹配且不是排除项的文件触发规则。
    - **掩码**是您要发送进行扫描的文件的掩码。您可以指定多个值。
      要指定掩码，您可以使用 * 和 ? 通配符。其他通配符不受支持。
    - **掩码排除项**是必须从扫描中排除的文件的掩码。您可以指定多个值。
      要指定排除掩码，您可以使用 * 和 ? 通配符。其他通配符不受支持。
    - **文件类别**是您要发送进行扫描的文件类别。您可以指定多个类别。
      您可以在文件类别的扩展名列表部分中查看每个类别的扩展名的完整列表。
    - **文件大小**是正在被扫描的文件的大小。
      如果要设置多个范围，请单击**添加文件大小**。
- 在用户定义的 URL 扫描 Sandbox 规则中：
  - **虚拟机**是将扫描 URL 的虚拟机。
    只能选择具有自定义操作系统镜像的虚拟机。这些虚拟机必须属于在 Central Node 上选择的操作系统集。
  - **状态**是防止规则的状态。如果您想要启用该规则，请选择该复选框。

启用或禁用用户禁用 Sandbox 规则

要启用或禁用 Sandbox 规则：

1. 在应用程序 Web 界面窗口中，选择**自定义规则**部分的**Sandbox**小节。
2. 打开**文件**或者**URL**选项卡。
   用户定义的文件或 URL 扫描 Sandbox 规则表将显示。
3. 在具有相关规则的行中，选择或清除**状态**列中的复选框。

规则被启用或禁用。

要启用或禁用所有或多个 Sandbox 规则的使用：

1. 在应用程序 Web 界面窗口中，选择**自定义规则**部分的**Sandbox**小节。
2. 打开**文件**或者**URL**选项卡。
   用户定义的文件或 URL 扫描 Sandbox 规则表将显示。

3. 选择要启用或禁用其使用的规则左侧的复选框。
   您可以通过选择包含列标题的行中的复选框来选择所有规则。
   控制面板出现在窗口的下部。
4. 单击**启用**或者**禁用**启用或禁用选定的规则。

选定的规则被启用或禁用。

导出用户定义的文件扫描 Sandbox 规则

要导出用户定义的 Sandbox 规则以进行对象扫描：

1. 在应用程序 Web 界面窗口中，选择**自定义规则**部分的**Sandbox**小节。
2. 打开**文件**选项卡。
3. 单击**导出**。

规则文件被保存到本地计算机。该文件以 JSON 格式下载。

删除用户定义的 Sandbox 规则

具有**高级安全官**角色的用户可以删除一个或多个用户定义的 Sandbox 规则，或同时删除所有规则。

要删除用户定义的 Sandbox 规则：

1. 在应用程序 Web 界面窗口中，选择**自定义规则**部分的**Sandbox**小节。
2. 打开**文件**或者**URL**选项卡。
   用户定义的文件或 URL 扫描 Sandbox 规则表将显示。
3. 选择您想删除的规则。
   这将打开一个窗口，其中包含有关规则的信息。
4. 单击**删除**。
   这将打开操作确认窗口。
5. 单击**是**。

规则被删除。

要删除所有或多个用户定义的 Sandbox 规则：

1. 在应用程序 Web 界面窗口中，选择**自定义规则**部分的**Sandbox**小节。
2. 打开**文件**或者**URL**选项卡。
   用户定义的文件或 URL 扫描 Sandbox 规则表将显示。

3. 选择您要删除的规则左侧的复选框。

   您可以通过选择包含列标题的行中的复选框来选择所有规则。

   控制面板出现在窗口的下部。

4. 单击**删除**。

   这将打开操作确认窗口。

5. 单击**是**。

所选文件将被删除。

文件类别的扩展名列表

下表列出了文件类别的扩展名。

文件类别的扩展名

类别	
1C	.epf、.ert、.erf、.cf、.dt、.deb、.bsl、.os、.ertx、.xls、.xml、.html、.txt、.cfu、.rptdesign、.xdt、.xslt、.wsdl
Adobe Flash Player	.swf、.fla、.flv、.f4v、.f4p、.f4a、.f4b、.mxml、.as、.asc、.ascs、.asv、.fxp、.fxpl、.xfl、.swc、.cfx、.spl、.dcr、.dir、.dxr、.aam、.s
Java	.jar、.class、.war、.ear、.jad、.jnlp、.ser、.jsp、.jspx、.properties、.policy
Html	.html、.htm、.shtml、.xhtml、.xml、.svg、.mathml、.rss、.atom、.json、.mht、.mhtml、.webarchive
网络包	.pcap、.pcapng、.cap、.netcap、.etl、.erf、.pkts、.pkt、.tcpdump、.snoop、.ngc、.dump、.cat、.smb、.vpcap、.dmp、.shb、.npl、
SAP	.abap、.adt、.bak、.cct、.cdp、.cpf、.dsc、.erd、.glo、.grc、.lis、.log、.lsa、.msg、.olap、.pgm、.prd、.sap、.sd、.se、.so、.spf、.t
XML	.xml、.xsl、.xslt、.rdf、.rss、.opf、.svg、.wsdl、.xhtml、.xjb、.xmi、.xpl、.xsl-fo、.xquery、.xsd、.dtd、.xht、.atom、.mathml、.mml、.
存档	.snb、.apk、.mht、.crx、.dd、.r01、.mpkg、.pup、.tbz、.ace、.arj、.bin、.cab、.cbr、.deb、.exe、.gzip、.one、.pak、.pkg、.ppt、.rpm
音频	.a52、.adt、.dct、.dss、.dvf、.iklax、.ivs、.rm、.rmvb、.8svx、.amb、.avr、.cdda、.cvs、.cvsd、.cvu、.dts、.dvms、.fap、.fssd、.gsr
视频	.drc、.f4a、.f4b、.f4p、.gifv、.mng、.mp2、.mpe、.mpv、.nsv、.roq、.svi、.3gp2、.3gpp2、.asx、.bin、.dat、.drv、.gtp、.moov、.spl
文档	.sxi、.odg、.svg、.vsd、.eps、.cwk、.wp、.ott、.asp、.cdd、.cpp、.dotm、.gpx、.indd、.kdc、.kml、.mdb、.mdf、.mso、.one、.pkg、
镜像	.dib、.pdf、.mrw、.icns、.wdp、.fig、.epsf、.cur、.erf、.fts、.heif、.jfif、.jpe、.jps、.mng、.pam、.pbm、.pes、.pfm、.picon、.pnm、
Android 可执行文件	.apk、.aab、.dex、.so、.jar、.aar、.class、.obb、.odex、.vdex、.vmx、.vmem、.img
Windows 可执行文件	.cgi、.ds、.air、.cpp、.gadget、.hta、.jar、.msu、.paf.exe、.pwz、.thm、.vbs、.exe、.msi、.bat、.cmd、.com、.pif、.scr、.vb、.vbe、
可执行文件	.rc、.p、.d、.asc、.bas、.cbl、.vbp、.iwb、.pb、.yml、.pika、.s19、.xt、.suo、.fsproj、.pbj、.pbxuser、.pyw、.xq、.cd、.sb、.sb2、.ise
磁盘映像	.img、.cue、.dsk、.vmdk、.vhd、.vhdx、.tc、.crypt、.dmgpart、.sparsebundle、.xva、.cif、.pqi、.udf、.fvd、.arc、.fcd、.gi、.giz、.im
Windows 事件日志	.evt、.evtx、.log、.txt、.xml
Windows 注册表文件	.reg、.dat、.pol、.hiv、.srd
字体	.bin、.ps、.sfd、.fnt、.afm、.ttf、.otf、.woff、.woff2、.eot、.svg、.dfont、.pfa、.pfb、.pfm、.fon、.suit、.bdf、.pcf、.snf、.ufo、.lib
数据库文件	.bup、.csv、.json、.xml、.myi、.sqlplan、.abs、.abx、.ac、.accdb、.accdc、.accde、.accdr、.accdt、.accdw、.accft、.adb、.ade、.a wal、.db2、.db3、.dbc、.dbf、.dbs、.dbt、.dbv、.dbx、.dcb、.dct、.dcx、.ddl、.dlis、.dp1、.dqy、.dsk、.dsn、.dtsx、.dxl、.eco、.ecx

发送通知

具有**管理员**、**高级安全官**或者**安全官**角色的用户可以配置将通知转发到一个或多个电子邮件地址。

您可以创建有关警报和系统运行状况的通知。

通知包含应用程序 Web 界面的链接。确保分配给中心节点服务器以供 DNS 服务器使用的名称正确，并且可以由 DNS 服务器进行解析。如果名称不正确或 DNS 服务器无法对其进行解析，则通知中的 Web 界面链接将不起作用。

具有**安全审计员**角色的用户可以查看用于发送通知的规则列表、所选规则的属性以及邮件服务器连接设置，但无法编辑它们。

为了将通知正确发送到电子邮件地址，您必须首先配置与邮件服务器的连接。连接必须由**管理员**进行配置。

查看发送通知的规则表

发送通知的规则显示在应用程序 Web 界面窗口的**设置**部分，**通知**子部分中。

用于发送通知的规则表包含以下信息：

- **类型**是用于发送通知的规则类型。
  以下类型的规则是可能的：
  - **检测**是用于发送有关检测的通知的规则。
  - **组件健康**是一个用于发送有关应用程序组件操作的通知的规则。
- **主题** – 包含通知的消息的主题。
- **到** – 发送通知的电子邮件地址。
- **状态** – 发送通知的规则的状态。

创建发送有关检测的通知的规则

要创建发送有关警报的通知的规则：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**通知**子部分。
2. 前往**通知规则**选项卡。
3. 单击**添加**。
   这将打开**新规则**窗口。

4. 在**到**字段中，输入您想要向其转发通知的一个或多个电子邮件地址。
   如果用逗号分隔，可以输入多个电子邮件地址。
5. 在**主题**字段中，输入通知消息的主题。
6. 如果您要让应用程序将警报重要性插入邮件主题，请将 `%importance%` 宏添加到**主题**字段中。
7. 在“**通知类型**”字段中，选择“**检测**”。
8. 在**检测重要性**下拉列表中，选择您想要发送通知的最低警报重要性。
   例如，您可以配置仅转发其警报具有高度重要性，或其警报具有中度或高度重要性的通知。
9. 如果要发送有关与特定源或目标 IP 地址或子网地址关联的警报的通知，请在**源或目的地**字段中输入 IP 地址和网络掩码。
10. 如果要发送有关与特定电子邮件发送人或收件人地址关联的警报的通知，请在**电子邮件**字段中输入电子邮件地址。
11. 如果您想要发送有关特定技术生成的警报的通知，请在**组件**下面选择一种或多种技术名称旁边的复选框。
12. 单击**添加**。

发送有关警报通知的规则将被添加到规则列表中。要将通知发送到指定的电子邮件地址，您必须启用通知规则。通知将被发送到为此规则配置的每个电子邮件地址一次。

具有**管理员**和**安全审计员**角色的用户无法创建发送警报通知的规则。

在分布式解决方案模式下，您必须为每个下级服务器（*从属 Central Node*，*SCN*）单独创建通知。

创建用于发送有关应用程序组件操作的通知的规则

要创建用于发送有关应用程序组件操作的通知的规则：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**通知**子部分。
2. 前往**通知规则**选项卡。
3. 单击**添加**。
   这将打开**新规则**窗口。
4. 在**到**字段中，输入您想要向其转发通知的一个或多个电子邮件地址。
   如果用逗号分隔，可以输入多个电子邮件地址。
5. 在**主题**字段中，输入通知消息的主题。
6. 如果您要让应用程序将警报重要性插入邮件主题，请将 `%importance%` 宏添加到**主题**字段中。
7. 在“**通知类型**”字段中，选择“**组件健康**”。

8. 在**组件**下面，选择您想要接收通知的应用程序功能区域名称旁边的复选框。

9. 单击**添加**。

发送有关应用程序组件运行通知的规则被添加到规则列表中。要将通知发送到指定的电子邮件地址，您必须启用通知规则。通知将被发送到为此规则配置的每个电子邮件地址一次。

具有**安全审计员**角色的用户无法创建用于发送有关应用程序操作的通知的规则。

在分布式解决方案模式下，通知是为每个下级服务器（*从属 Central Node，SCN*）单独配置的。

启用和禁用发送通知的规则

要启用或禁用发送有关警报的通知的规则：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**通知**子部分。

2. 前往**通知规则**选项卡。

3. 在**状态**列中，使用规则旁边的切换开关启用或禁用发送通知的规则。

发送有关警报通知的规则的状态将被修改。

具有**安全审计员**角色的用户无法启用或禁用通知规则。

修改发送通知的规则

要编辑发送通知的规则：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**通知**子部分。

2. 前往**通知规则**选项卡。

3. 在发送通知的规则列表中，选择您要修改的规则。

这将打开**编辑规则**窗口。

4. 进行相关更改。

5. 单击**保存**。

发送通知的规则将被修改。

具有**安全审计员**角色的用户无法编辑发送通知的规则。

删除发送通知的规则

要删除发送通知的规则：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**通知**子部分。

2. 前往**通知规则**选项卡。

3. 选择您要删除的每个规则的名称左侧的复选框。
如果您想删除所有规则，请选择列表上方的复选框。

4. 单击窗口下部的**删除**。

5. 在确认窗口中，单击**是**。

所选文件将被删除。

具有**安全审计员**角色的用户无法删除发送通知的规则。

按规则类型筛选和搜索通知转发规则

要按规则类型筛选或搜索通知规则：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**通知**子部分。

2. 前往**通知规则**选项卡。

3. 单击规则表中的⬚图标以发送通知。
这将打开筛选配置窗口。

4. 选择以下选项之一：

   - **所有**。
   - **警报**。
   - **组件健康**。

   通知转发规则表格将仅显示与您设置的筛选条件相匹配的规则。

> 您可以同时使用多个筛选器。

根据通知主题筛选和搜索通知转发规则

要按通知主题筛选或搜索通知规则：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**通知**子部分。
2. 前往**通知规则**选项卡。
3. 单击**主题**链接以打开筛选配置窗口。
4. 输入通知主题的一个或多个字符。
5. 单击**应用**。

   筛选配置窗口关闭。

   通知转发规则表格将仅显示与您设置的筛选条件相匹配的规则。

> 您可以同时使用多个筛选器。

按电子邮件地址筛选和搜索通知转发规则

要按目标电子邮件地址筛选或搜索通知规则：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**通知**子部分。
2. 前往**通知规则**选项卡。
3. 单击**到**链接以打开筛选配置窗口。

4. 输入电子邮件底子的一个或多个字符。

5. 单击**应用**。

通知转发规则表格将仅显示与您设置的筛选条件相匹配的规则。

> 您可以同时使用多个筛选器。

根据状态筛选和搜索通知转发规则

要按状态筛选或搜索通知规则：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**通知**子部分。

2. 前往**通知规则**选项卡。

3. 单击**状态**链接以打开筛选配置窗口。

4. 选择状态值旁边的一个或多个复选框：

   - **已启用。**
   - **已禁用。**

5. 单击**应用**。

筛选配置窗口关闭。

通知转发规则表格将仅显示与您设置的筛选条件相匹配的规则。

> 您可以同时使用多个筛选器。

清除通知转发规则筛选器

要清除一个或多个筛选条件的通知规则筛选器：

1. 在应用程序 Web 界面的主窗口中，选择**设置**部分的**通知**子部分。

2. 前往**通知规则**选项卡。

3. 单击您想清除其筛选条件的通知转发规则表列标题右侧的。

> 如果要清除多个筛选条件，请执行必要的操作以清除每个筛选条件。

选定筛选器将被清除。

通知转发规则表格将仅显示与您设置的筛选条件相匹配的规则。

管理日志

本节包含有关管理 Kaspersky Anti Targeted Attack Platform 日志的信息。

在 Kaspersky Anti Targeted Attack Platform Web 界面中，您可以管理以下日志：

- 用户活动日志。具有“**管理员**”角色的用户可以管理日志。具有“**安全审计员**”角色的用户可以下载日志。
- NDR 功能的用户活动日志。具有“**管理员**”角色的用户可以管理日志。具有“**安全审计员**”角色的用户可以查看日志。

管理活动日志

应用程序 Web 界面中的某些用户操作可能会导致Kaspersky Anti Targeted Attack Platform 运行错误。您可以在应用程序 Web 界面中启用用户操作信息的记录，并在必要时通过下载日志文件查看信息。

启用和禁用在活动日志中记录信息

要启用或禁用将 Kaspersky Anti Targeted Attack Platform Web 界面中的用户操作信息记录到活动日志中：

1. 选择应用程序 Web 界面中的“**日志**”部分的“**用户活动**”子部分。
2. 执行以下操作之一：
   - 如果您想要启用记录有关用户在应用程序 Web 界面中的操作的信息，请设置“**事件记录**”切换开关至“**已启用**”位置。
   - 如果您想要禁用记录有关用户在应用程序 Web 界面中的操作的信息，请设置“**事件记录**”切换开关至“**已禁用**”位置。

     默认情况下启用此功能。

有关用户操作的信息记录在 user_actions.log 文件中，该文件存储在 Central Node 服务器的 /data/storage/volumes/siem_proxy/log-user-actions/ 目录中。默认情况下，此文件中的记录将保留 90 天，之后将被删除。

要查看活动日志记录，您需要下载 user_actions.log 文件。

您可以配置将应用程序 Web 界面中的用户活动信息记录到远程日志。远程日志被保存到安装了 SIEM 系统的服务器上。必须配置与 SIEM 系统的集成设置 以写入到远程日志。

在分布式解决方案模式中，有关应用程序 Web 界面中的用户操作的信息记录在用户管理 Web 界面的同一服务器的日志中。有关影响 SCN 服务器设置的 PCN 服务器用户操作的信息记录在 PCN 服务器日志中。

具有**安全审计员**角色的用户只能查看用于将信息记录到活动日志的设置。

下载活动日志文件

要下载活动日志文件：

1. 选择应用程序 Web 界面中的“**日志**”部分的“**用户活动**”子部分。
2. 单击**下载**。

该文件将被保存到您本地计算机的浏览器下载文件夹中。文件以 ZIP 存档形式下载。

在分布式解决方案模式下，您只能下载您在其 Web 界面中管理的服务器的日志文件。

有关 Web 界面中用户活动的 CEF 消息的内容和属性

每条消息的标头包含以下信息：

- 格式化版本。
  当前版本号：`0`。当前字段值：`CEF:0`。
- 供应商。
  当前字段值：`AO Kaspersky Lab`。
- 应用程序名称。
  当前字段值：`Kaspersky Anti Targeted Attack Platform`。
- 应用程序版本
  当前字段值：7.0.1-500。
- 事件类型。
  见下表。
- 活动名称。
  见下表。
- 事件重要性。
  当前字段值：低。

  示例：
  ```
  CEF:0|AO Kaspersky Lab|Kaspersky Anti Targeted Attack Platform|7.0.1-500|任务|管理任务|低|
  ```

CEF 消息的所有字段都具有“<密钥>=<值>”格式。密钥以及消息中包含的值显示在下表中。

事件类型	事件名称和说明	关键及其价值描述
sensors	管理 Sensor 组件 将 Sensor 组件连接到 Central Node 服务器，修改组件设置。	• dvs = <服务器的 IP 地址>。 • eventId = <事件 ID>。 • rt = <事件日期和时间>。 • src = <用户的 IP 地址>。 • 用户 = <用户名>。 • cs1 = <事件类型>。
sb	配置与 Sandbox 组件的集成 将 Sandbox 组件连接到 Central Node 服务器。	• dvs = <服务器的 IP 地址>。 • eventId = <事件 ID>。 • rt = <事件日期和时间>。 • src = <用户的 IP 地址>。 • 用户 = <用户名>。 • cs1 = <事件类型>。
ex_integration	配置与外部系统的集成 配置与外部系统的集成。	• dvs = <服务器的 IP 地址>。 • eventId = <事件 ID>。 • rt = <事件日期和时间>。 • src = <用户的 IP 地址>。 • 用户 = <用户名>。 • cs1 = <事件类型>。
ksn_kpsn_mdr	参与 KSN、KPSN 和 MDR 配置参与卡巴斯基安全网络、启用或禁用卡巴斯基私人安全网络的使用以及配置与 Kaspersky Managed Detection and Response 的集成。	• dvs = <服务器的 IP 地址>。 • eventId = <事件 ID>。 • rt = <事件日期和时间>。 • src = <用户的 IP 地址>。 • 用户 = <用户名>。 • cs1 = <事件类型>。
yara	管理 YARA 规则 YARA 规则操作。	• dvs = <服务器的 IP 地址>。 • eventId = <事件 ID>。 • rt = <事件日期和时间>。 • src = <用户的 IP 地址>。 • 用户 = <用户名>。 • cs1 = <事件类型>。 • 设备外部 ID =<分布式方案模式下的主机 ID>。 • cs1label = <被上传文件的名称>。
ioc	管理入侵指标 IOC 规则操作。	• dvs = <服务器的 IP 地址>。 • eventId = <事件 ID>。 • rt = <事件日期和时间>。 • src = <用户的 IP 地址>。 • 用户 = <用户名>。 • cs1 = <事件类型>。 • deviceExternalID =<分布式方案模式下主机的标识符>。
ids	管理 IDS 规则 IDS 规则操作。	• dvs = <服务器的 IP 地址>。 • eventId = <事件 ID>。 • rt = <事件日期和时间>。 • src = <用户的 IP 地址>。 • 用户 = <用户名>。 • cs1 = <事件类型>。 • deviceExternalID =<分布式方案模式下主机的标识符>。
taa	管理 TAA 规则 TAA (IOA) 规则操作。	• dvs = <服务器的 IP 地址>。 • eventId = <事件 ID>。 • rt = <事件日期和时间>。 • src = <用户的 IP 地址>。 • 用户 = <用户名>。 • cs1 = <事件类型>。
sb rules	管理 Sandbox 规则 Sandbox 规则操作。	• dvs = <服务器的 IP 地址>。 • eventId = <事件 ID>。 • rt = <事件日期和时间>。 • src = <用户的 IP 地址>。 • 用户 = <用户名>。 • cs1 = <事件类型>。
prevention	管理防护规则 防御规则操作。	• dvs = <服务器的 IP 地址>。 • eventId = <事件 ID>。 • rt = <事件日期和时间>。

事件类型	事件名称和说明	关键及其价值描述
		• src = <用户的 IP 地址>。 • 用户 = <用户名>。 • cs1 = <事件类型>。
exclusions	管理扫描排除项 扫描排除规则操作。	• dvs = <服务器的 IP 地址>。 • eventId = <事件 ID>。 • rt = <事件日期和时间>。 • src = <用户的 IP 地址>。 • 用户 = <用户名>。 • cs1 = <事件类型>。
endpoint_agents	管理 Endpoint Agent 主机 对安装了 Endpoint Agent 组件的主机进行的操作。	• dvs = <服务器的 IP 地址>。 • eventId = <事件 ID>。 • rt = <事件日期和时间>。 • src = <用户的 IP 地址>。 • 用户 = <用户名>。 • cs1 = <事件类型>。
tasks	管理任务 任务操作。	• dvs = <服务器的 IP 地址>。 • eventId = <事件 ID>。 • rt = <事件日期和时间>。 • src = <用户的 IP 地址>。 • 用户 = <用户名>。 • cs1 = <事件类型>。
network_isolation	Endpoint Agent 主机的网络隔离 Endpoint Agent 主机的网络隔离。	• dvs = <服务器的 IP 地址>。 • eventId = <事件 ID>。 • rt = <事件日期和时间>。 • src = <用户的 IP 地址>。 • 用户 = <用户名>。 • cs1 = <事件类型>。
settings	设置 修改 Central Node 服务器设置。	• dvs = <服务器的 IP 地址>。 • eventId = <事件 ID>。 • rt = <事件日期和时间>。 • src = <用户的 IP 地址>。 • 用户 = <用户名>。 • cs1 = <事件类型>。
mt	管理 CN、PCN 和 SCN 服务器 修改分布式解决方案和多租户模式下主 Central Node 和从属 Central Node 服务器的设置。	• dvs = <服务器的 IP 地址>。 • eventId = <事件 ID>。 • rt = <事件日期和时间>。 • src = <用户的 IP 地址>。 • 用户 = <用户名>。 • cs1 = <事件类型>。
user_account	管理用户账户 对户账户的操作。	• dvs = <服务器的 IP 地址>。 • eventId = <事件 ID>。 • rt = <事件日期和时间>。 • src = <用户的 IP 地址>。 • 用户 = <用户名>。 • cs1 = <事件类型>。
notifications	发送通知 配置电子邮件通知。	• dvs = <服务器的 IP 地址>。 • eventId = <事件 ID>。 • rt = <事件日期和时间>。 • src = <用户的 IP 地址>。 • 用户 = <用户名>。 • cs1 = <事件类型>。
license	授权许可 管理授权许可密钥。	• dvs = <服务器的 IP 地址>。 • eventId = <事件 ID>。 • rt = <事件日期和时间>。 • src = <用户的 IP 地址>。 • 用户 = <用户名>。 • cs1 = <事件类型>。

如果同时对超过 30 个对象执行某项操作，则仅记录该操作的一项。该条目包括有关操作的信息以及执行该操作的对象的数量。

管理 NDR 用户活动日志

本节包含有关管理 NDR 功能日志的信息。

具有“**管理员**”角色的用户可以管理日志。具有“**安全审计员**”角色的用户可以查看日志。

使用任何类型的 Kaspersky Anti Targeted Attack Platform 授权许可密钥时均可使用日志。

管理日志存储设置

您可以编辑 Central Node 数据库中日志记录存储的设置。

要更改日志存储设置：

1. 使用应用程序管理员账户登录 Web 界面。
2. 选择“**Sensor 服务器**”部分。
3. 选择 Central Node 服务器的卡。
   详细信息区域显示在 Web 界面窗口的右侧。
4. 单击**“编辑”**。
   在详细信息区域，会显示选项卡，您可以在其中管理服务器的设置。
5. 在“**常规**”选项卡上，在“**事件**”、“**审计条目**”和“**应用程序消息**”部分配置以下设置：
   a. 使用“**最大卷**”设置来设置存储记录的大小限制。您可以选择该值的计量单位：**MB** 或 **GB**。
      编辑此设置时，请记住指定卷的预计最大记录数。您还需要考虑到所有大小限制的总和不得超过节点指定的最大存储容量。
   b. 如有必要，使用“**存储时间（天）**”设置来限制记录的存储时间，并以天为单位指定时间。
6. 单击“**保存**”。

日志存储已配置。

启用和禁用用户活动审计

您可以启用或禁用 NDR 功能的用户活动审计。

用户活动审计默认启用。

要启用或禁用用户活动审计：

1. 使用 Web 界面连接到 Central Node 服务器。
2. 选择“**日志**”部分，“**审计**”字部份。

3. 使用工具栏中的**用户活动审计**开关启用或禁用用户活动审计。

4. 等待更改得到应用。直到转换至另一状态完成之后，开关才会再次可用。

查看用户活动审计记录

Kaspersky Anti Targeted Attack Platform 可以保存有关 NDR 功能用户执行的操作的信息。如果启用了用户活动审计，信息将保存在审计日志中。

您可以在使用 Web 界面连接到 Central Node 服务器时查看审计记录。如果需要，您还可以配置审计记录通过连接器发送到第三方系统。

只有具有管理员角色的用户才能查看审计记录。

要查看审计记录：

1. 使用 Web 界面连接到 Central Node 服务器。

2. 选择“**日志**”部分，“**审计**”字部份。

   该表显示符合指定过滤和搜索条件的审计记录。

审计记录设置显示在表格以下列中：

- **日期和时间**。
  记录用户活动信息的日期和时间。
- **操作**。
  已注册的用户执行的操作。
- **结果**。
  已注册操作的结果（成功或不成功）。
- **用户**。
  执行注册操作的用户的名称。
- **用户节点**。
  执行注册操作的节点的 IP 地址。
- **描述**。
  有关注册操作的其他信息。

查看审计记录表时，您可以使用配置、过滤、搜索和排序功能。

设置跟踪日志的最大存储空间限制

有关 NDR 功能性能的信息记录在跟踪日志中。您可以限制这些日志占用的存储空间。在这种情况下，当达到限制时，旧的跟踪日记文件将被从 `/var/log/kaspersky` 目录中删除。

具有**管理员**角色的用户可以管理日志存储。具有"**安全审计员**"角色的用户可以查看这些设置。

要限制跟踪日志占用的空间量：

1. 使用应用程序管理员账户登录 Web 界面。
2. 在应用程序 Web 界面窗口中选择**Sensor 服务器**部分。
3. 单击相关 Sensor 组件的卡片。
4. 这将打开一个窗口，其中包含有关组件的信息。
5. 单击**"编辑"**。
6. 转到"**常规**"选项卡。
7. 在**跟踪数据**字段中，使用**最大容量**设置来配置日志可以占用的最大空间。您可以选择该值的计量单位：**MB** 或 **GB**。

跟踪日志占用的空间有限。

设置跟踪日志的最大存储空间限制

统计日志记录 NDR 功能的指标，例如接收到的网络数据包的数量。您可以限制这些日志占用的存储空间。在这种情况下，当达到限制时，旧的统计日志文件将被从 `/var/log/kaspersky` 目录中删除。

具有**管理员**角色的用户可以管理日志存储。具有"**安全审计员**"角色的用户可以查看这些设置。

要限制统计日志占用的空间量：

1. 使用应用程序管理员账户登录 Web 界面。
2. 在应用程序 Web 界面窗口中选择**Sensor 服务器**部分。
3. 单击相关 Sensor 组件的卡片。
4. 这将打开一个窗口，其中包含有关组件的信息。
5. 单击**"编辑"**。

6. 转到“**常规**”选项卡。

7. 在**统计数据**字段中，使用**最大容量**设置来配置日志可以占用的最大空间。您可以选择该值的计量单位：**MB** 或 **GB**。

统计日志占用的空间有限。

下载 Kaspersky Anti Targeted Attack Platform 日志

如果需要，您可以下载 Kaspersky Anti Targeted Attack Platform 的系统日志文件。为此，您必须使用 kata-collect 脚本获取有关应用程序操作的信息。

使用 kata-collect 脚本获取有关应用程序操作的信息。

1. 登录到您要通过 SSH 或终端获取信息的服务器的管理控制台。

   如果您在分布式解决方案和多租户模式下使用 Kaspersky Anti Targeted Attack Platform，则需要在每个 Central Node 服务器上执行这些步骤。如果您组织的基础架构已单独安装了 Sensor 组件，您还必须在具有此组件的服务器上执行以下步骤。如果应用程序作为集群部署，则必须在 Docker swarm 中具有“管理者”角色的服务器之一上执行这些步骤。要查看服务器角色，请使用 `$ docker node ls` 命令。

2. 系统提示时，输入管理员用户名和安装组件期间指定的密码。

   显示应用程序组件管理员菜单。

3. 在应用程序管理员菜单部分的列表中，选择**“技术支持模式”**部分。

4. 按下“**Enter**”。

   这将打开技术支持模式确认窗口。

5. 确认您想要在技术支持模式下管理应用程序。为此，请选择**是**并按**Enter**。

6. 通过执行以下命令来运行脚本：

   ```
   sudo kata-run.sh kata-collect --output-dir <路径>
   ```

您还可以为此命令指定一个或多个参数（请参阅下表）。

kata-collect 实用程序的参数

必需的参数	参数	描述
是	`--output-dir <路径>`	在指定路径创建目录， 其中<路径>是您要保存包含下载数据的存档的目录的绝对路径或相对路径。 如果不指定路径，数据存档默认保存在 /tmp/collect 目录中。
否	`--no-prometheus`	跳过准备和转储 prometheus 数据库。 此参数显著加快了脚本的速度。
否	`--no-siem-logs`	跳过下载写入 SIEM 系统的数据。
否	`--siem-logs-range-start <YYYY-MM-DD-HH>`	下载从该日期（含）开始写入 SIEM 系统的数据。
否	`--siem-logs-range-end <YYYY-MM-DD-HH>`	下载以此日期（含）结束的写入 SIEM 系统的数据。

示例：

使用按日期过滤的 SIEM 系统数据且不使用 prometheus 数据库来获取有关应用程序操作的信息的命令：

```
sudo kata-run.sh kata-collect --output-dir <路径> --no-prometheus --siem-logs-range-start <YYYY-MM-DD-HH> --siem-logs-range-end <YYYY-MM-DD-HH>
```

脚本完成后，collect--<存档下载日期>.tar.gz 存档被保存到指定目录。该存档包含应用程序的系统日志文件。

查看应用程序消息

应用程序的消息日志存储有关 NDR 功能的错误以及 Kaspersky Anti Targeted Attack Platform 的系统进程执行的操作的信息。

您可以在 Web 界面中查看应用程序消息。如果需要，您还可以配置应用程序消息通过连接器发送到第三方系统。

具有以下角色的用户可以查看应用程序消息：**管理员**、**安全审计员**、**安全官**或**高级安全官**。

要查看应用程序消息：

1. 使用应用程序管理员账户登录 Web 界面。
2. 选择“**设置**”部分，“**应用程序消息**”字部份。

   表格显示符合指定过滤和搜索条件的应用程序消息。

应用程序消息设置显示在表格的以下列中：

- **日期和时间**。
  注册应用程序消息的日期和时间。
- **状态**。
  消息状态的名称。消息可以具有以下状态之一：
  - 信息性消息的*正常操作*。
  - 有关非关键应用程序错误的消息包括“*未知*”、“*故障*”。
  - 有关应用程序故障的消息包括“*中度故障*、*严重故障*”、“*致命故障*”。
- **节点**。
  消息到达的节点的名称或 IP 地址。
- **系统进程**。
  导致消息被注册的应用程序进程。
- **信息**。
  消息的数字标识符和文本。

查看应用程序消息表时，您可以使用过滤、搜索和排序功能。

查看已发送至 Kaspersky Anti Targeted Attack Platform 进行扫描的文件的信息

如果有必要，您可以查看该文件是否已在 Kaspersky Anti Targeted Attack Platform 中扫描，以及扫描结果是什么。为此，您必须使用 kata-collect 脚本获取有关应用程序操作的信息。

要使用 kata-collect 脚本获取有关应用程序性能的信息：

按照“*下载 Kaspersky Anti Targeted Attack Platform 日志*”部分给出的说明的步骤进行操作。

完成说明的步骤后，包含 Kaspersky Anti Targeted Attack Platform 日志文件的 collect--<存档下载日期>.tar.gz 存档被放置在指定目录中。接收并扫描的文件信息包含在日志中，该日志位于此存档内的 /logs/kaspersky/siem/log-history/ 目录中。如果某个文件被排除在扫描之外，则有关该文件的信息也会反映在日志中。

您可以通过名称或 MD5 哈希值找到任何文件。

如果该文件是由 Sensor 组件获取的，您可以通过以下字段找到它：

- 文件源信息：
  - 如果文件是从流量中获取的，则为源 IP 地址和目标 IP 地址。
  - 如果文件是通过电子邮件收到的，则为发件人电子邮件地址和收件人电子邮件地址。
  - 如果文件是从外部系统接收的，则为外部系统的 IP 地址和 ID。
  - 如果文件是从 Endpoint Agent 主机接收的，则为主机的 IP 地址和名称。
  - 如果文件是手动上传至 Kaspersky Anti Targeted Attack Platform 的，则为用户账户名称。
- 源类型：span、smtp、icap、pop3、external（外部系统）、endpoint（Endpoint Agent 主机）、upload（手动上传的文件）。
- 对于电子邮件消息，会记录 Message-ID 字段。

文件信息日志记录的特殊注意事项

在日志中搜索文件信息时，请牢记以下有关文件信息日志记录的特殊注意事项：

- 文件信息被记录两次：从流量中获取文件时和扫描文件时。如果 Sensor 组件与您的基础设施中的 Central Node 分开安装，则文件接收记录将转到 Sensor 组件的日志，而文件扫描记录将转到 Sensor 连接的 Central Node 组件的日志。如果 Central Node 组件和 Sensor 安装在同一台服务器上，则两个记录都会写入 Central Node 日志。
- 对于复合文件（例如，存档或电子邮件），如果子文件被 Kaspersky Anti Targeted Attack Platform 技术之一扫描，则会记录父文件的哈希值以及子文件的名称和哈希值。

文件 MD5 哈希值的 apt-history 日志记录示例

下表列出了文件 MD5 哈希值的 apt-history 日志记录示例。

文件 MD5 哈希值的 apt-history 日志记录示例

日志记录	值
2024-06-11 02:37:03.645586 info apt-history: f0429d4845208857cd303df968ef545e enqueued am, priority: normal	该文件已被接收并利用反恶意软件引擎技术进行处理。
2024-06-11 02:37:03.647434 info apt-history: external KSMG sensor with ip 10.0.0.0 provide file with name: File_Name 2024/2025, md5: f0429d4845208857cd303df968ef545e, msg_id: <87c13e55e789aa966089b6bf2e8c453b@localhost.localdomain>	从 Kaspersky Secure Mail Gateway 和 Kaspersky Security for Linux Mail Server 接收并在 Kaspersky Anti Targeted Attack Platform 中处理的对象的字符串。 值得关注的信息： • 外部 KSMG 传感器，IP 为 10.0.0.0 — Kaspersky Secure Mail Gateway 服务器的 IP 地址 • File_Name 2024/2025 — 文件名 • md5 — 正在扫描的文件的 MD5 哈希值 • msg_id — 消息 ID
2024-06-11 02:37:03.847696 info apt-history: f0429d4845208857cd303df968ef545e engine am result {verdict: CLEAN, bases_version: 202406071010, detect_time: 2024-06-11 02:37:03.841275, rescan_priority: 3, sb_hash: 77f5b6276dd9b1c534b6c9adcff86845, multitask_details: {priority: background, tasks: {pdf: 1}}, scanEngines: [sb]}	使用反恶意软件引擎技术处理对象的结果。包括扫描后分配给对象的状态 (CLEAN) 以及有关将用于额外扫描对象的技术的信息 ("scanEngines: [sb]")。 值得关注的信息： • multitask_details — 扫描任务的详细信息 • priority — 扫描的优先级 可能的值是 "background"、"must" • scanEngines — 扫描技术 可能的值是 [yr]（代表 YARA）和 [sb]（代表 Sandbox）。
2024-06-11 02:37:03.886784 info apt-history: f0429d4845208857cd303df968ef545e enqueued sb: {pdf: 1}, priority: low, sb_priority: background	该任务已发送到 Sandbox 组件进行处理。 值得关注的信息： • {pdf: 1} — 发送以扫描的对象数量和类型 • low — 处理优先级 可能的处理优先级值为 "low"、"medium"、"high"。 • background — Sandbox 组件处理的队列类型。 可能的值是 "background"、"must"
2024-06-11 02:37:04.179597 info apt-history: f0429d4845208857cd303df968ef545e delivered to sb, sb_hash: 77f5b6276dd9b1c534b6c9adcff86845, node: Server_Name, mtask_id: 900	该任务已发送到 Sandbox 组件进行处理。 值得关注的信息： • node:Server_Name — 具有 Sandbox 组件的服务器的名称 • mtask_id: 900 — 任务 ID
2024-06-11 02:38:44.515070 info apt-history: f0429d4845208857cd303df968ef545e sb result received, sb_hash: 77f5b6276dd9b1c534b6c9adcff86845, node: Server_Name, mtask_id: 900, priority: low	已收到 Sandbox 组件处理对象的结果。

2024-06-11 02:38:44.783370 info apt-history: f0429d4845208857cd303df968ef545e engine sb result {bases_version: 202406102122, detect_time: 2024-06-11 02:38:44.776655, verdict: SILENT, hidden: True, details: [{file: //[From WCR <test@mail.com>][Date 11 Jun 2024 03:51:21][Subj Company_Name 2024/2025]/WCR-form.pdf, images: [{verdicts_info: {ScannerVersion: 1.22.3.34, ...}, hidden: True, verdict: SILENT, sb_id: fb15ec106318b0d54babce2379d956f7, image: Win7_x64, task_id: task0, file: //[From WCR <test@mail.com>][Date 11 Jun 2024 03:51:21][Subj Company_Name 2024/2025]/WCR-form.pdf, file_id: 1, filesize: 445856, md5: 0d87eebc9676214f35046a482150e537, tracing_mode: all_events, store_artifacts: False, bases_version: 202406102122, ids_bases_version: 202406101817, version: 1.22.3.34, suspicious_log: [], network_activity: {http: [], dns: []}}], verdict: SILENT, hidden: True, priority: 150}], md5_list: [], file_list: [], sb_hash: 77f5b6276dd9b1c534b6c9adcff86845, sb_names_map: {0: {md5: , name: }, 1: {md5: 0d87eebc9676214f35046a482150e537, name: //[From WCR <test@mail.com>][Date 11 Jun 2024 03:51:21][Subj Company_Name 2024/2025]/WCR-form.pdf}, 2: {md5: 71072dd9a36d7ce560cebc533ecb3cad, name: }}}

Sandbox 组件对所有虚拟机上的对象进行处理的结果。

值得关注的信息：

- verdict — 扫描文件的结果。根据在所有虚拟机上扫描文件的结果生成。对于结果为 SILENT 的检测，不会在检测数据库中创建任何记录。
- hidden: True — 具有此结果的对象不需要 Kaspersky Anti Targeted Attack Platform 模块进一步扫描。
- details — 有关扫描虚拟机中的对象的信息。
  包括以下字段：
  - file — 用于显示的文件的名称 (WCR-form.pdf)。在此记录中，字段包含以下信息：
  - From — 发件人电子邮件地址。
  - Date — 事件的日期和时间。
  - Subj — 邮件主题。
  - images — 有关在虚拟机中扫描对象的信息。
  - verdicts_info — 文件扫描的结果。对于扫描对象的每个虚拟机来说可能都不同。
  - hidden: True — 具有此结果的对象不需要 Kaspersky Anti Targeted Attack Platform 模块进一步扫描。
  - verdict — 在虚拟机上扫描文件的结果。对于结果为 SILENT 的检测，不会在检测数据库中创建任何记录。
  - image — 执行文件的镜像。
  - filesize — 文件的大小。
  - md5 — 文件的 MD5 哈希。
  - tracing mode: all_events — 文件启动后执行的操作的记录。
  - suspicious log [] — 文件执行的恶意操作的记录。

	该字段没有值，因为该文件没有执行任何恶意操作。 • network activity — 由文件发起的网络活动。 • http [] — 该文件未发出任何 HTTP 请求。 • dns [] — 该文件未发出任何 DNS 请求。 "suspicious log"和"network activity"字段仅记录恶意活动的事实。如果您想查看警报的详细信息，您可以在应用程序 Web 界面中进行查看。 • priority — 扫描的优先级 可能的值是 1 表示高、100 表示标准、150 表示后台扫描。 • md5_list — 扫描时生成警报的文件的 MD5 哈希值。 • file_list — 扫描时生成警报的文件的名称。 • sb_names_map — 在应用程序 Web 界面上的警报详细信息中显示的文件名。
2024-06-11 02:38:44.841529 info apt-history: New sb_detect for file alert: {id: 2720, victim: default, state: new, md5: f0429d4845208857cd303df968ef545e}	Sandbox 组件处理结果的信息保存在应用程序数据库中。记录以供内部使用。这并不表示应用程序的检测数据库中存在检测。

管理 Kaspersky Endpoint Agent for Windows

Kaspersky Endpoint Agent 是一款安装在企业 IT 基础架构中的单个设备上的应用程序。应用程序持续监控在这些设备上运行的进程、活动的网络连接和正在被修改的文件。

Kaspersky Endpoint Agent 可让受保护设备与其他卡巴斯基解决方案进行交互，以检测复杂的威胁，例如针对性攻击。

配置 Kaspersky Endpoint Agent 与 Kaspersky Anti Targeted Attack Platform 的集成后，应用程序将运行任务、应用来自 Kaspersky Anti Targeted Attack Platform 的参数，并将遥测数据从受保护设备发送到 KATA Central Node 服务器。有关 Kaspersky Endpoint Agent 与 Kaspersky Anti Targeted Attack Platform 集成时可以执行的操作的更多详细信息，请参阅*应用程序的操作原理*部分。

有关管理 Kaspersky Endpoint Agent 的详细信息，请参阅应用程序的在线帮助：

- 应用程序激活
- 安装和删除应用程序。
- 使用 Kaspersky Security Center 管理控制台管理 Kaspersky Endpoint Agent 设置和 Kaspersky Security Center Web Console：
  - 管理防御
  - 管理任务
  - 打开设置窗口
  - 配置安全设置
  - 配置 Kaspersky Endpoint Agent 与代理服务器的连接
  - 将 Kaspersky Security Center 配置为代理服务器以激活 Kaspersky Endpoint Agent
  - 在 Kaspersky Endpoint Agent 中配置 KSN 使用
  - 在 Kaspersky Endpoint Agent 中配置存储设置
  - 配置故障诊断
- 使用命令行界面管理 Kaspersky Endpoint Agent：
  - 激活管理
  - 认证管理
  - 配置跟踪
  - 配置 Kaspersky Endpoint Agent 进程转储的创建
  - 查看有关隔离设置和被隔离对象的信息
  - 针对隔离对象的操作

- 运行 Kaspersky Endpoint Agent 数据库和模块更新
- 启动、停止和查看当前应用程序状态
- 应用程序的密码保护
- 利用 PPL 技术保护应用程序服务
- 管理自我防御设置
- 管理标准 IOC 扫描任务
- 根据 YARA 规则管理文件和进程扫描
- 创建内存转储
- 创建磁盘转储

管理 Kaspersky Endpoint Security for Windows

Kaspersky Endpoint Security 是一款安装在企业 IT 基础架构中的单个设备上的应用程序。应用程序持续监控在这些设备上运行的进程、活动的网络连接和正在被修改的文件。有关计算机上事件的信息（遥测）将被发送到 Kaspersky Anti Targeted Attack Platform 服务器。Kaspersky Endpoint Security 还会向 Kaspersky Anti Targeted Attack Platform 服务器发送有关应用程序检测到的威胁的信息以及有关处理这些威胁的结果的信息。

配置 Kaspersky Endpoint Security 与 Kaspersky Anti Targeted Attack Platform 的集成后，应用程序将运行任务、应用来自 Kaspersky Anti Targeted Attack Platform 的参数，并将遥测数据从受保护设备发送到 KATA Central Node 服务器。有关 Kaspersky Endpoint Security 与 Kaspersky Anti Targeted Attack Platform 集成时可以执行哪些操作的更多详细信息，请参阅*应用程序的操作原理*部分。

有关管理 Kaspersky Endpoint Security 的详细信息，请参阅应用程序的在线帮助：

- 安装和删除应用程序。
- 应用程序许可。

  要与 Kaspersky Anti Targeted Attack Platform 集成，除了 Kaspersky Endpoint Security 激活密钥之外，您还必须添加 Kaspersky Endpoint Detection and Response (KATA) 附加密钥。有关应用程序许可的详细信息，请参阅 Kaspersky Endpoint Security 在线帮助→与 EDR (KATA) 集成。
- 与 EDR (KATA) 集成。
- 配置遥测。
- 管理隔离区。
- 用于管理 Detection and Response KATA EDR 的命令：与 EDR (KATA) 集成。

管理 Kaspersky Endpoint Security for Linux

Kaspersky Endpoint Security for Linux 是一款安装在运行 Linux 操作系统的单个设备上的应用程序，这些设备是企业 IT 基础架构的一部分。应用程序持续监控在这些设备上运行的进程、活动的网络连接和正在被修改的文件。有关计算机上事件的信息（遥测）将被发送到 Kaspersky Anti Targeted Attack Platform 服务器。Kaspersky Endpoint Security for Linux 还会向Kaspersky Anti Targeted Attack Platform 服务器发送有关应用程序检测到的威胁的信息以及有关处理这些威胁的结果的信息。

配置 Kaspersky Endpoint Security 与 Kaspersky Anti Targeted Attack Platform 的集成后，应用程序将运行任务、应用来自 Kaspersky Anti Targeted Attack Platform 的参数，并将遥测数据从受保护设备发送到 KATA Central Node 服务器。有关 Kaspersky Endpoint Security 与 Kaspersky Anti Targeted Attack Platform 集成时可以执行哪些操作的更多详细信息，请参阅*应用程序的操作原理*部分。

有关管理 Kaspersky Endpoint Security for Linux 的详细信息，请参阅应用程序的在线帮助：

- 安装、移除和更新应用程序。
- 使用命令行管理应用程序：
  - 授权许可密钥管理：授权任务（授权许可，ID：9）。
  - 与 Kaspersky Anti Targeted Attack Platform 集成：与 Kaspersky Endpoint Detection and Response(KATA) 任务集成（KATAEDR，ID：24）。
- 使用Kaspersky Security Center Web Console 和 Kaspersky Security Center 云控制台管理应用程序:
  - 授权许可密钥管理：要了解更多详细信息，请参阅*在 Web 控制台中管理任务→创建任务*和*任务设置→添加密钥*。
  - 与 Kaspersky Anti Targeted Attack Platform 集成：要了解更多详细信息，请参阅*在 Web 控制台中管理策略→创建策略*和*策略设置→与 Kaspersky Endpoint Detection and Response(KATA) 集成*。

要与 Kaspersky Anti Targeted Attack Platform 集成，您无需在 Kaspersky Endpoint Security for Linux 中添加额外的授权许可密钥。

管理 Kaspersky Endpoint Security for Mac

Kaspersky Endpoint Security for Mac 是一款安装在运行 macOS 操作系统的单个设备上的应用程序，这些设备是企业 IT 基础架构的一部分。应用程序持续监控在这些设备上运行的进程、活动的网络连接和正在被修改的文件。有关计算机上事件的信息（遥测）将被发送到 Kaspersky Anti Targeted Attack Platform 服务器。Kaspersky Endpoint Security for Mac 还会向Kaspersky Anti Targeted Attack Platform 服务器发送有关应用程序检测到的威胁的信息以及有关处理这些威胁的结果的信息。

配置 Kaspersky Endpoint Security for Mac 与 Kaspersky Anti Targeted Attack Platform 的集成后，应用程序将运行任务、应用来自 Kaspersky Anti Targeted Attack Platform 的参数，并将遥测数据从受保护设备发送到 KATA Central Node 服务器。有关 Kaspersky Endpoint Security for Mac 与 Kaspersky Anti Targeted Attack Platform 集成时可以执行哪些操作的更多详细信息，请参阅*应用程序的操作原理*部分。

有关管理 Kaspersky Endpoint Security for Mac 的详细信息，请参阅应用程序的在线帮助。

- 安装、移除和更新应用程序。
- 应用程序许可。

  要与 Kaspersky Anti Targeted Attack Platform 集成，除了 Kaspersky Endpoint Security 激活密钥之外，您还必须添加 Kaspersky Endpoint Detection and Response (KATA) 附加密钥。有关应用程序许可的更多详细信息，请参阅 Kaspersky Endpoint Security 帮助 → 应用程序的高级配置 →Endpoint Detection and Response(KATA)。
- 使用命令行管理应用程序:
- 使用 Kaspersky Security Center Web Console 和云控制台远程管理应用程序:
  - 有关授权许可密钥管理的详细信息，请参阅以下部分：创建任务 → 配置添加密钥任务设置。
  - 有关与 Kaspersky Anti Targeted Attack Platform 集成的详细信息，请参阅以下部分：创建策略 → 配置检测和响应设置 → 配置 Endpoint Detection and Response (KATA)。

备份和恢复数据

您可以创建备份副本，并在出现故障或需要重新安装 Kaspersky Anti Targeted Attack Platform 时从中恢复数据。您可以在基于不同操作系统的 Kaspersky Anti Targeted Attack Platform 实例之间恢复数据。例如，您可以将基于 Ubuntu 的 Kaspersky Anti Targeted Attack Platform 的数据恢复到基于 Astra Linux 的 Kaspersky Anti Targeted Attack Platform，反之亦然。

要创建 Central Node 服务器的备份副本，您可以通过 SSH 或终端连接到该服务器。

该流程的示意图如下图所示。



备份和恢复数据

您要恢复数据的应用程序的版本必须与执行备份的服务器上的应用程序的版本相同。如果应用程序版本不匹配，则启动恢复时会显示错误消息，并终止恢复进程。

备份和恢复 Central Node 服务器的数据

此场景描述了在 Central Node 服务器上创建和从备份恢复数据的过程。

Central Node 服务器上的数据备份和恢复涉及以下步骤：

1. **创建备份副本**

   您可以使用管理员菜单或在技术支持模式下创建备份副本。

   如何在管理员菜单中创建备份副本

   Kaspersky Anti Targeted Attack Platform 的备份副本仅包含数据库（警报数据库、VIP 身份详细信息、从扫描中排除的数据列表、通知）和 Central Node 或 PCN 设置。

   1. 登录到您要通过 SSH 或终端进行备份的服务器的管理控制台。
   2. 出现提示时，输入管理员账户的用户名和密码。
      显示应用程序组件管理员菜单。
   3. 在应用程序管理员菜单部分的列表中，选择**系统管理**部分。

4. 按下“**Enter**”。
   这将打开操作选择窗口。

5. 在操作列表中，选择**备份/恢复设置**。

6. 按下“**Enter**”。
   这将打开**备份/恢复设置**窗口。

7. 在操作列表中，选择**新建**。

8. 按下“**Enter**”。
   这将打开**备份设置**窗口。

9. 单击**备份**。

备份副本已创建。

如何在技术支持模式下创建备份副本

1. 登录到您要通过 SSH 或终端进行备份的服务器的管理控制台。

2. 出现提示时，输入管理员账户的用户名和密码。
   显示应用程序组件管理员菜单。

3. 在应用程序管理员菜单部分的列表中，选择**“技术支持模式”**部分。

4. 按下“**Enter**”。
   这将打开技术支持模式确认窗口。

5. 确认您想要在技术支持模式下管理应用程序。为此，请选择**是**并按**Enter**。

6. 运行以下命令：

```
sudo kata-run.sh kata-backup-restore backup
```

您还可以为此命令指定一个或多个参数 (请参阅下表)。

您也可以使用 `-h` 命令接收有关使用参数的提示。

创建备份副本的参数

必需的参数	参数	描述
是	`-b <路径>`	在指定路径创建备份副本， 其中 <path> 是要创建备份副本的目录的绝对路径或相对路径。
否	`-c`	保存备份副本之前清除目录。
否	`-d <存储文件数>`	指定目录中存储的最大备份文件数，其中 <number> 是文件数。
否	`-e`	将文件保存在存储中。
否	`-q`	将文件保存在隔离区中。
否	`-a`	保存等待重新扫描的文件。
否	`-s`	保存 Sandbox 工件。

否	-n	保存 Central Node 或 PCN 设置。
No	-l <文件路径>	将命令执行结果保存到文件中，其中<文件路径>是事件日志文件的名称，包括文件的绝对路径或相对路径。

如果未定义其他设置，备份副本仅包含数据库（警报数据库、VIP 状态详细信息、从扫描中排除的数据列表、通知）。

示例：

创建备份副本的命令：

```
sudo kata-run.sh kata-backup-restore backup -b <路径> -c -d <存储文件数> -e -q -a -s -n -l <文件路径>
```

2 将备份副本保存到硬盘

要将备份副本保存在计算机硬盘上，请运行以下命令：

scp <用于在管理员菜单和服务器管理控制台中工作的账户的名称>@<服务器的 IP 地址>:<备份文件的名称，格式为：data_kata_<创建备份副本的日期和时间>.tar>

示例：

用于将于 2020 年 4 月 10 日 10 时 00 分 00 秒在“admin”账户下的 IP 地址为 10.0.0.10 的 Central Node 服务器上创建的备份副本下载到计算机硬盘的命令：

```
scp admin@10.0.0.10:data_kata_2020_04_10T10_00_00.tar
```

备份副本保存到您的计算机硬盘上的当前目录中。

3 重新安装应用程序

删除并重新安装 Kaspersky Anti Targeted Attack Platform。

4 将备份副本上传至服务器

通过运行以下命令将备份副本上传到 Central Node 服务器：

scp <备份文件的名称，格式为：data_kata_<备份副本创建的日期和时间>.tar> <用于在管理员菜单和服务器管理控制台中工作的账户名称>@<服务器的 IP 地址>:

示例：

用于将于 2020 年 4 月 10 日 10 时 00 分 00 秒创建的备份副本上传到“admin”账户下的 IP 地址为 10.0.0.10 的 Central Node 服务器的命令：

```
scp data_kata_2020_04_10T10_00_00.tar admin@10.0.0.10:
```

备份副本将上传至 Central Node 服务器的当前目录。

5 从备份副本恢复数据

您可以使用管理员菜单或在技术支持模式下从 Central Node 服务器上的备份副本恢复数据。

如何在管理员菜单中恢复数据

1. 登录到您要通过 SSH 或终端恢复其数据的服务器的管理控制台。
2. 出现提示时，输入应用程序组件管理员账户的用户名和密码。
   显示应用程序组件管理员菜单。
3. 在应用程序管理员菜单部分的列表中，选择**系统管理**部分。
4. 按下“**Enter**”。
   这将打开操作选择窗口。

5. 在操作列表中，选择**备份/恢复设置**。

6. 按下“**Enter**”。
   这将打开**备份/恢复设置**窗口。

7. 在包含应用程序备份副本的文件列表中，选择要从中恢复服务器设置的文件。
   如果必要的文件未列出，请将包含备份副本的文件上传到服务器。

8. 按下“**Enter**”。
   这将打开操作选择窗口。

9. 在操作列表中，选择“**恢复 <备份文件的名称，格式为：data_kata_<备份副本的创建日期和时间>.tar>**”

10. 按下“**Enter**”。
    这将打开操作确认窗口。

11. 单击**恢复**。
    从备份副本恢复服务器数据的过程开始。当数据恢复过程完成后，应用程序组件的管理员菜单将显示。

12. 在应用程序管理员菜单部分的列表中，选择**“技术支持模式”**部分。

13. 按顺序运行以下命令：

```
private_key=$(console-settings-updater get
/kata/configuration/product/web_backend | python -c "import json, sys; data =
json.load(sys.stdin); print(data['server_certificate']['private_key'])")
certificate=$(console-settings-updater get
/kata/configuration/product/web_backend | python -c "import json, sys; data =
json.load(sys.stdin); print(data['server_certificate']
['certificate'].encode('unicode_escape').decode('utf-8'))")
console-settings-updater set --merge /kata/configuration/product/nta_core "
{\"server_certificate\": {\"private_key\": \"$private_key\"}}"
console-settings-updater set --merge /kata/configuration/product/nta_core "
{\"server_certificate\": {\"certificate\": \"$certificate\"}}"
console-settings-updater set --merge /kata/configuration/product/nta_syncer "
{\"server_certificate\": {\"private_key\": \"$private_key\"}}"
console-settings-updater set --merge /kata/configuration/product/nta_syncer "
{\"server_certificate\": {\"certificate\": \"$certificate\"}}"
```

服务器数据将被从所选文件中恢复。

如果创建备份副本的服务器和从备份副本恢复数据的服务器上的网络接口名称相同，则会自动恢复从 SPAN 端口接收镜像流量的设置。

如何在技术支持模式下恢复数据

1. 登录到您要通过 SSH 或终端恢复其数据的服务器的管理控制台。

2. 出现提示时，输入应用程序管理员账户的用户名和密码。
   显示应用程序组件管理员菜单。

3. 在应用程序管理员菜单部分的列表中，选择**“技术支持模式”**部分。

4. 按下“**Enter**”。

   这将打开技术支持模式确认窗口。

5. 确认您想要在技术支持模式下管理应用程序。为此，请选择**是**并按**Enter**。

6. 通过运行以下命令启动数据恢复过程：

   ```
   sudo kata-run.sh kata-backup-restore restore
   ```

   您还可以为此命令指定一个或多个参数（请参阅下表）。

   您也可以使用 `-h` 命令接收有关使用参数的提示。

7. 按顺序运行以下命令：

   ```
   private_key=$(console-settings-updater get
   /kata/configuration/product/web_backend | python -c "import json, sys; data =
   json.load(sys.stdin); print(data['server_certificate']['private_key'])")
   certificate=$(console-settings-updater get
   /kata/configuration/product/web_backend | python -c "import json, sys; data =
   json.load(sys.stdin); print(data['server_certificate']
   ['certificate'].encode('unicode_escape').decode('utf-8'))")
   console-settings-updater set --merge /kata/configuration/product/nta_core "
   {\"server_certificate\": {\"private_key\": \"$private_key\"}}"
   console-settings-updater set --merge /kata/configuration/product/nta_core "
   {\"server_certificate\": {\"certificate\": \"$certificate\"}}"
   console-settings-updater set --merge /kata/configuration/product/nta_syncer "
   {\"server_certificate\": {\"private_key\": \"$private_key\"}}"
   console-settings-updater set --merge /kata/configuration/product/nta_syncer "
   {\"server_certificate\": {\"certificate\": \"$certificate\"}}"
   ```

   服务器数据将被从所选文件中恢复。

数据恢复参数

必需的参数	参数	命令描述
是	`-r <路径>`	从包含备份副本的文件中恢复数据， 其中 <path> 是备份文件的完整路径。
否	`-l <文件路径>`	将命令执行结果保存到文件中，其中<文件路径>是事件日志文件的名称，包括文件的绝对路径或相对路径。

示例：

从备份副本恢复数据的命令：

```
sudo kata-run.sh kata-backup-restore restore -r <路径> -l <文件路径>
```

如果创建备份副本的服务器和从备份副本恢复数据的服务器上的网络接口名称相同，则会自动恢复从 SPAN 端口接收镜像流量的设置。

服务器设置的备份副本不包含记录的镜像网络流量的 PCAP 文件。您可以通过从连接的存储的 /data/volumes/dumps 目录复制 PCAP 文件来自行保存和恢复它们。恢复数据后，您必须连接外部存储。

如果在其上创建备份副本的 Central Node 服务器的硬件配置与您计划在其上恢复服务器设置的服务器的硬件配置不同，您需要在恢复后重新配置应用程序扩展设置。

备份和恢复作为集群部署的 Central Node 服务器的数据

此方案描述了在作为集群部署的 Central Node 服务器上备份和恢复数据的过程。

在作为集群部署的 Central Node 服务器上备份和恢复数据涉及以下步骤：

1. **创建备份副本**

   您可以使用管理员菜单或在技术支持模式下创建备份副本：

   如何在管理员菜单中创建备份副本

   Kaspersky Anti Targeted Attack Platform 的备份副本仅包含数据库（警报数据库、VIP 身份详细信息、从扫描中排除的数据列表、通知）和 Central Node 或 PCN 设置。

   1. 通过 SSH 或使用终端进入任何正常运行的集群服务器的管理控制台。
   2. 出现提示时，输入管理员账户的用户名和密码。
      显示应用程序组件管理员菜单。
   3. 在应用程序管理员菜单部分的列表中，选择**系统管理**部分。
   4. 按下“**Enter**”。
      这将打开操作选择窗口。
   5. 在操作列表中，选择**备份/恢复设置**。
   6. 按下“**Enter**”。
      这将打开**备份/恢复设置**窗口。
   7. 在操作列表中，选择**新建**。
   8. 按下“**Enter**”。
      这将打开**备份设置**窗口。
   9. 单击**备份**。

   备份副本已创建。

   如何在技术支持模式下创建备份副本

   1. 通过 SSH 或使用终端进入任何正常运行的集群服务器的管理控制台。
   2. 出现提示时，输入应用程序组件管理员账户的用户名和密码。
      显示应用程序组件管理员菜单。
   3. 在应用程序管理员菜单部分的列表中，选择**“技术支持模式”**部分。

4. 按下“**Enter**”。

   这将打开技术支持模式确认窗口。

5. 确认您想要在技术支持模式下管理应用程序。为此，请选择**是**并按**Enter**。

6. 运行以下命令：

   ```
   sudo kata-run.sh kata-backup-restore backup
   ```

   您还可以为此命令指定一个或多个参数（请参阅下表）。

   您也可以使用 `-h` 命令接收有关使用参数的提示。

创建备份副本的参数

必需的参数	参数	描述
是	`-b <路径>`	在指定路径创建备份副本， 其中 <path> 是要创建备份副本的目录的绝对路径或相对路径。
否	`-c`	保存备份文件之前清除目录。
否	`-d <存储文件数>`	指定目录中存储的最大文件数，其中 <number> 是文件数。
否	`-n`	保存 Central Node 或 PCN 设置。
No	`-l <文件路径>`	将命令执行结果保存到文件中，其中<文件路径>是事件日志文件的名称，包括文件的绝对路径或相对路径。

如果未定义其他设置，备份副本仅包含数据库（警报数据库、VIP 状态详细信息、从扫描中排除的数据列表、通知）。

示例：

创建备份副本的命令：

```
sudo kata-run.sh kata-backup-restore backup -b <路径> -c -d <存储文件数> -e -q -a -s -n -l <文件路径>
```

2 将备份副本保存到硬盘

要将备份副本保存在计算机硬盘上，请运行以下命令：

`scp <用于在管理员菜单和服务器管理控制台中工作的账户的名称>@<服务器的 IP 地址>:<备份文件的名称，格式为：data_kata_<创建备份副本的日期和时间>.tar>`

示例：

用于将于 2020 年 4 月 10 日 10 时 00 分 00 秒在“admin”账户下的 IP 地址为 10.0.0.10 的 Central Node 服务器上创建的备份副本下载到计算机硬盘的命令：

```
scp admin@10.0.0.10:data_kata_2020_04_10T10_00_00.tar
```

备份副本保存到您的计算机硬盘上的当前目录中。

3 重新安装应用程序

删除并重新安装 Kaspersky Anti Targeted Attack Platform。

安装应用程序时，您需要为寻址服务器指定与应用程序备份副本中指定的相同的网络掩码。如果值不匹配，则嵌入式 Sensor 在应用程序恢复后会遇到错误。如果需要，您可以恢复该组件。

安装后，您必须向应用程序添加与创建备份副本的服务器上相同类型的授权许可密钥（KATA、KATA + NDR、KEDR）。这对于恢复备份副本中保存的所有 Central Node、PCN 或 SCN 设置是必要的。

4 将备份副本上传至服务器

通过运行以下命令将备份副本上传到 Central Node 服务器：

`scp <备份文件的名称，格式为：data_kata_<备份副本创建的日期和时间>.tar> <用于在管理员菜单和服务器管理控制台中工作的账户名称>@<服务器的 IP 地址>:`

示例：

用于将于 2020 年 4 月 10 日 10 时 00 分 00 秒创建的备份副本上传到“admin”账户下的 IP 地址为 10.0.0.10 的 Central Node 服务器的命令：

```
scp data_kata_2020_04_10T10_00_00.tar admin@10.0.0.10:
```

备份副本将上传至 Central Node 服务器的当前目录。

5 从备份副本恢复数据

您可以使用管理员菜单或在技术支持模式下从 Central Node 服务器上的备份副本恢复数据：

如何在管理员菜单中恢复数据

1. 通过 SSH 或使用终端进入任何正常运行的集群服务器的管理控制台。
2. 出现提示时，输入应用程序组件管理员账户的用户名和密码。
   显示应用程序组件管理员菜单。
3. 在应用程序管理员菜单部分的列表中，选择**系统管理**部分。
4. 按下“**Enter**”。
   这将打开操作选择窗口。
5. 在操作列表中，选择**备份/恢复设置**。
6. 按下“**Enter**”。
   这将打开**备份/恢复设置**窗口。
7. 在包含应用程序备份副本的文件列表中，选择要从中恢复服务器设置的文件。
   如果必要的文件未列出，请将包含备份副本的文件上传到服务器。
8. 按下“**Enter**”。
   这将打开操作选择窗口。
9. 在操作列表中，选择“**恢复 <备份文件的名称，格式为：data_kata_<备份副本的创建日期和时间>.tar>**”
10. 按下“**Enter**”。
    这将打开操作确认窗口。
11. 单击**恢复**。
    从备份副本恢复服务器数据的过程开始。当数据恢复过程完成后，应用程序组件的管理员菜单将显示。
12. 在应用程序管理员菜单部分的列表中，选择**“技术支持模式”**部分。
13. 按顺序运行以下命令：

```
private_key=$(console-settings-updater get
/kata/configuration/product/web_backend | python -c "import json, sys; data =
json.load(sys.stdin); print(data['server_certificate']['private_key'])")
certificate=$(console-settings-updater get
/kata/configuration/product/web_backend | python -c "import json, sys; data =
json.load(sys.stdin); print(data['server_certificate']
['certificate'].encode('unicode_escape').decode('utf-8'))")
console-settings-updater set --merge /kata/configuration/product/nta_core "
{\"server_certificate\": {\"private_key\": \"$private_key\"}}"
console-settings-updater set --merge /kata/configuration/product/nta_core "
{\"server_certificate\": {\"certificate\": \"$certificate\"}}"
console-settings-updater set --merge /kata/configuration/product/nta_syncer "
{\"server_certificate\": {\"private_key\": \"$private_key\"}}"
console-settings-updater set --merge /kata/configuration/product/nta_syncer "
{\"server_certificate\": {\"certificate\": \"$certificate\"}}"
```

服务器数据将被从所选文件中恢复。

如果创建备份副本的服务器和从备份副本恢复数据的服务器上的网络接口名称相同，则会自动恢复从 SPAN 端口接收镜像流量的设置。

如果网络接口名称不匹配，执行上述说明的第 11 步后，系统将提示您选择用于从 SPAN 端口接收镜像流量的网络接口。

如何在技术支持模式下恢复数据

1. 通过 SSH 或使用终端进入任何正常运行的集群服务器的管理控制台。
2. 出现提示时，输入应用程序管理员账户的用户名和密码。

   显示应用程序组件管理员菜单。
3. 在应用程序管理员菜单部分的列表中，选择**“技术支持模式”**部分。
4. 按下“**Enter**”。

   这将打开技术支持模式确认窗口。
5. 确认您想要在技术支持模式下管理应用程序。为此，请选择**是**并按**Enter**。
6. 通过运行以下命令启动数据恢复过程：

   ```
   sudo kata-run.sh kata-backup-restore restore
   ```

   您还可以为此命令指定一个或多个参数（请参阅下表）。

   您也可以使用 `-h` 命令接收有关使用参数的提示。
7. 按顺序运行以下命令：

   ```
   private_key=$(console-settings-updater get
   /kata/configuration/product/web_backend | python -c "import json, sys; data =
   json.load(sys.stdin); print(data['server_certificate']['private_key'])")
   ```

```
certificate=$(console-settings-updater get
/kata/configuration/product/web_backend | python -c "import json, sys; data =
json.load(sys.stdin); print(data['server_certificate']
['certificate'].encode('unicode_escape').decode('utf-8'))")
console-settings-updater set --merge /kata/configuration/product/nta_core "
{\"server_certificate\": {\"private_key\": \"$private_key\"}}"
console-settings-updater set --merge /kata/configuration/product/nta_core "
{\"server_certificate\": {\"certificate\": \"$certificate\"}}"
console-settings-updater set --merge /kata/configuration/product/nta_syncer "
{\"server_certificate\": {\"private_key\": \"$private_key\"}}"
console-settings-updater set --merge /kata/configuration/product/nta_syncer "
{\"server_certificate\": {\"certificate\": \"$certificate\"}}"
```

服务器数据将被从所选文件中恢复。

数据恢复参数

必需的参数	参数	命令描述
是	`-r <路径>`	从包含备份副本的文件中恢复数据， 其中 <path> 是备份文件的完整路径。
否	`-l <文件路径>`	将命令执行结果保存到文件中，其中<文件路径>是事件日志文件的名称，包括文件的绝对路径或相对路径。

示例：

从备份副本恢复数据的命令：

```
sudo kata-run.sh kata-backup-restore restore -r <路径> -l <文件路径>
```

如果创建备份副本的服务器和从备份副本恢复数据的服务器上的网络接口名称相同，则会自动恢复从 SPAN 端口接收镜像流量的设置。

如果网络接口名称不匹配，执行上述说明的第 6 步后，系统将提示您选择用于从 SPAN 端口接收镜像流量的网络接口。

服务器设置的备份副本不包含记录的镜像网络流量的 PCAP 文件。您可以通过从连接的外部存储器的 /data/volumes/dumps 目录复制 PCAP 文件来自行保存和恢复它们。恢复数据后，您必须连接外部存储。

如果在其上创建备份副本的 Central Node 服务器的硬件配置与您计划在其上恢复服务器设置的服务器的硬件配置不同，您需要在恢复后重新配置应用程序扩展设置。

分布式解决方案和多租户模式下 Central Node 服务器的数据备份和恢复

此场景描述了在分布式解决方案或多租户模式下部署的 Central Node 服务器上备份和恢复数据的过程。

要在使用分布式解决方案和多租户模式时备份和恢复数据，您必须连接到层次结构中的每个 Central Node 服务器，并按照以下说明的步骤进行操作。

备份和恢复以分布式解决方案或多租户模式部署的 Central Node 服务器上的数据涉及以下步骤：

1. **创建备份副本**

   您可以使用管理员菜单或在技术支持模式下创建备份副本：

   如何在管理员菜单中创建备份副本

   > Kaspersky Anti Targeted Attack Platform 的备份副本仅包含数据库（警报数据库、VIP 身份详细信息、从扫描中排除的数据列表、通知）和 Central Node 或 PCN 设置。

   1. 登录到您要通过 SSH 或终端进行备份的服务器的管理控制台。
   2. 出现提示时，输入管理员账户的用户名和密码。
      显示应用程序组件管理员菜单。
   3. 在应用程序管理员菜单部分的列表中，选择**系统管理**部分。
   4. 按下“**Enter**”。
      这将打开操作选择窗口。
   5. 在操作列表中，选择**备份/恢复设置**。
   6. 按下“**Enter**”。
      这将打开**备份/恢复设置**窗口。
   7. 在操作列表中，选择**新建**。
   8. 按下“**Enter**”。
      这将打开**备份设置**窗口。
   9. 单击**备份**。

   备份副本已创建。

   如何在技术支持模式下创建备份副本

   1. 登录到您要通过 SSH 或终端进行备份的服务器的管理控制台。
   2. 出现提示时，输入管理员账户的用户名和密码。
      显示应用程序组件管理员菜单。
   3. 在应用程序管理员菜单部分的列表中，选择**“技术支持模式”**部分。
   4. 按下“**Enter**”。
      这将打开技术支持模式确认窗口。
   5. 确认您想要在技术支持模式下管理应用程序。为此，请选择**是**并按**Enter**。

6. 运行以下命令：

```
sudo kata-run.sh kata-backup-restore backup
```

您还可以为此命令指定一个或多个参数（请参阅下表）。

您也可以使用 `-h` 命令接收有关使用参数的提示。

创建备份副本的参数

必需的参数	参数	描述
是	`-b <路径>`	在指定路径创建备份副本， 其中 <path> 是要创建备份副本的目录的绝对路径或相对路径。
否	`-c`	保存备份副本之前清除目录。
否	`-d <存储文件数>`	指定目录中存储的最大备份文件数，其中 <number> 是文件数。
否	`-e`	将文件保存在存储中。
否	`-q`	将文件保存在隔离区中。
否	`-a`	保存等待重新扫描的文件。
否	`-s`	保存 Sandbox 工件。
否	`-n`	保存 Central Node 或 PCN 设置。
No	`-l <文件路径>`	将命令执行结果保存到文件中，其中<文件路径>是事件日志文件的名称，包括文件的绝对路径或相对路径。

如果未定义其他设置，备份副本仅包含数据库（警报数据库、VIP 状态详细信息、从扫描中排除的数据列表、通知）。

示例：

创建备份副本的命令：

```
sudo kata-run.sh kata-backup-restore backup -b <路径> -c -d <存储文件数> -e -q -a -s -n -l <文件路径>
```

2 将备份副本保存到硬盘

要将备份副本保存在计算机硬盘上，请运行以下命令：

`scp <用于在管理员菜单和服务器管理控制台中工作的账户的名称>@<服务器的 IP 地址>:<备份文件的名称，格式为：data_kata_<创建备份副本的日期和时间>.tar>`

示例：

用于将于 2020 年 4 月 10 日 10 时 00 分 00 秒在“admin”账户下的 IP 地址为 10.0.0.10 的 Central Node 服务器上创建的备份副本下载到计算机硬盘的命令：

```
scp admin@10.0.0.10:data_kata_2020_04_10T10_00_00.tar
```

备份副本保存到您的计算机硬盘上的当前目录中。

3 重新安装应用程序

删除并重新安装 Kaspersky Anti Targeted Attack Platform。

数据只能从备份恢复到具有 Central Node 角色的服务器。如果在开始之前为服务器分配 PCN 或 SCN 角色，则恢复过程将失败。

4 将备份副本上传至服务器

通过运行以下命令将备份副本上传到 Central Node 服务器：

`scp <备份文件的名称，格式为：data_kata_<备份副本创建的日期和时间>.tar> <用于在管理员菜单和服务器管理控制台中工作的账户名称>@<服务器的 IP 地址>:`

示例：

用于将于 2020 年 4 月 10 日 10 时 00 分 00 秒创建的备份副本上传到“admin”账户下的 IP 地址为 10.0.0.10 的 Central Node 服务器的命令：

```
scp data_kata_2020_04_10T10_00_00.tar admin@10.0.0.10:
```

备份副本将上传至 Central Node 服务器的当前目录。

5 从备份副本恢复数据

您可以使用管理员菜单或在技术支持模式下从 Central Node 服务器上的备份副本恢复数据：

如何在管理员菜单中恢复数据

1. 登录到您要通过 SSH 或终端恢复其数据的服务器的管理控制台。
2. 出现提示时，输入应用程序组件管理员账户的用户名和密码。
   显示应用程序组件管理员菜单。
3. 在应用程序管理员菜单部分的列表中，选择**系统管理**部分。
4. 按下“**Enter**”。
   这将打开操作选择窗口。
5. 在操作列表中，选择**备份/恢复设置**。
6. 按下“**Enter**”。
   这将打开**备份/恢复设置**窗口。
7. 在包含应用程序备份副本的文件列表中，选择要从中恢复服务器设置的文件。
   如果必要的文件未列出，请将包含备份副本的文件上传到服务器。
8. 按下“**Enter**”。
   这将打开操作选择窗口。
9. 在操作列表中，选择“**恢复 <备份文件的名称，格式为：data_kata_<备份副本的创建日期和时间>.tar>**”
10. 按下“**Enter**”。
    这将打开操作确认窗口。
11. 单击**恢复**。
    从备份副本恢复服务器数据的过程开始。当数据恢复过程完成后，应用程序组件的管理员菜单将显示。
12. 在应用程序管理员菜单部分的列表中，选择**“技术支持模式”**部分。
13. 按顺序运行以下命令：

```
private_key=$(console-settings-updater get
/kata/configuration/product/web_backend | python -c "import json, sys; data =
json.load(sys.stdin); print(data['server_certificate']['private_key'])")
```

```
certificate=$(console-settings-updater get
/kata/configuration/product/web_backend | python -c "import json, sys; data =
json.load(sys.stdin); print(data['server_certificate']
['certificate'].encode('unicode_escape').decode('utf-8'))")
console-settings-updater set --merge /kata/configuration/product/nta_core "
{\"server_certificate\": {\"private_key\": \"$private_key\"}}"
console-settings-updater set --merge /kata/configuration/product/nta_core "
{\"server_certificate\": {\"certificate\": \"$certificate\"}}"
console-settings-updater set --merge /kata/configuration/product/nta_syncer "
{\"server_certificate\": {\"private_key\": \"$private_key\"}}"
console-settings-updater set --merge /kata/configuration/product/nta_syncer "
{\"server_certificate\": {\"certificate\": \"$certificate\"}}"
```

服务器数据将被从所选文件中恢复。

如果创建备份副本的服务器和从备份副本恢复数据的服务器上的网络接口名称相同，则会自动恢复从 SPAN 端口接收镜像流量的设置。

如何在技术支持模式下恢复数据

1. 登录到您要通过 SSH 或终端恢复其数据的服务器的管理控制台。
2. 出现提示时，输入应用程序管理员账户的用户名和密码。
   显示应用程序组件管理员菜单。
3. 在应用程序管理员菜单部分的列表中，选择**“技术支持模式”**部分。
4. 按下“**Enter**”。
   这将打开技术支持模式确认窗口。
5. 确认您想要在技术支持模式下管理应用程序。为此，请选择**是**并按**Enter**。
6. 通过运行以下命令启动数据恢复过程：
   ```
   sudo kata-run.sh kata-backup-restore restore
   ```
   您还可以为此命令指定一个或多个参数（请参阅下表）。
   您也可以使用 `-h` 命令接收有关使用参数的提示。
7. 按顺序运行以下命令：
   ```
   private_key=$(console-settings-updater get
   /kata/configuration/product/web_backend | python -c "import json, sys; data =
   json.load(sys.stdin); print(data['server_certificate']['private_key'])")
   certificate=$(console-settings-updater get
   /kata/configuration/product/web_backend | python -c "import json, sys; data =
   json.load(sys.stdin); print(data['server_certificate']
   ['certificate'].encode('unicode_escape').decode('utf-8'))")
   console-settings-updater set --merge /kata/configuration/product/nta_core "
   {\"server_certificate\": {\"private_key\": \"$private_key\"}}"
   console-settings-updater set --merge /kata/configuration/product/nta_core "
   {\"server_certificate\": {\"certificate\": \"$certificate\"}}"
   ```

```
console-settings-updater set --merge /kata/configuration/product/nta_syncer "
{\"server_certificate\": {\"private_key\": \"$private_key\"}}"
console-settings-updater set --merge /kata/configuration/product/nta_syncer "
{\"server_certificate\": {\"certificate\": \"$certificate\"}}"
```

服务器数据将被从所选文件中恢复。

数据恢复参数

必需的参数	参数	命令描述
是	`-r <路径>`	从包含备份副本的文件中恢复数据， 其中 <path> 是备份文件的完整路径。
否	`-l <文件路径>`	将命令执行结果保存到文件中，其中<文件路径>是事件日志文件的名称，包括文件的绝对路径或相对路径。

示例：

从备份副本恢复数据的命令：

```
sudo kata-run.sh kata-backup-restore restore -r <路径> -l <文件路径>
```

如果创建备份副本的服务器和从备份副本恢复数据的服务器上的网络接口名称相同，则会自动恢复从 SPAN 端口接收镜像流量的设置。

如果在其上创建备份副本的 Central Node 服务器的硬件配置与您计划在其上恢复服务器设置的服务器的硬件配置不同，您需要在恢复后重新配置应用程序扩展设置。

恢复数据后，您不需要将 SCN 重新连接到 PCN：PCN 连接设置和连接的 SCN 列表将从备份副本中恢复。

服务器设置的备份副本不包含记录的镜像网络流量的 PCAP 文件。您可以通过从连接的存储的 /data/volumes/dumps 目录复制 PCAP 文件来自行保存和恢复它们。恢复数据后，您必须连接外部存储。

导出数据的内容

Kaspersky Anti Targeted Attack Platform 可能包含用户数据和其他机密信息。Kaspersky Anti Targeted Attack Platform 管理员在创建备份副本，更换安装应用程序的设备，或在其他可能需要永久删除数据的情况下，必须采取措施确保此数据的安全。Kaspersky Anti Targeted Attack Platform 管理员负责访问存储在应用程序服务器上的数据。

您可以创建以下数据的备份副本：

- 应用程序数据库。
- 存储中的对象。
- 重新扫描期间生成的警报档案。
- Sandbox 工件。

- 配置文件。
- Central Node 设置。

从备份恢复数据之前，上面列出的数据在您恢复应用程序的 Central Node 服务器上被清除。

导出以创建备份副本的数据内容和数量

数据类型	导出的数据	应用程序运行模式	部署方式
• Central Node 设置，包括服务器的 TLS 证书。 • PCN 连接设置 • 已连接的 SCN 列表 • Central Node 上的应用程序数据库： • 网络流量事件 • 警报和警报的 VIP 身份 • 任务及任务执行结果 • 策略 • 用户定义的 TAA (IOA) 规则和排除项 • IDS 排除项 • IOC 文件 • 扫描排除规则 • 有关存储中文件的信息 • 被隔离的对象的信息 • 具有 Endpoint Agent 的计算机列表 • 设备清查 • 分配给设备的标签 • 在设备操作系统中注册的用户账户列表 • 设备上的可执行文件列表 • 设备的地址空间 • 有关网络交互图上设备位置的信息 • 常规报告和报告模板 • NDR 报告和报告模板 • 用户账户数据 • 网络会话数据 • 拓扑图 • 通知	Central Node 设置（如果已选择）。 默认为应用程序数据库。	独立 Central Node 服务器。	所有部署方法。
PCN 设置，包括服务器的 TLS 证书。	自定义	分布式解决方案和多租户模式。	所有部署方法。
SCN 设置，包括服务器的 TLS 证书。	自定义 适用于独立的 Central Node 服务器。	分布式解决方案和多租户模式。	所有部署方法。

数据类型	导出的数据	应用程序运行模式	部署方式
PCN 上的应用程序据库： • 网络流量事件 • 警报和警报的 VIP 身份 • 任务执行结果 • 策略 • 用户定义的 TAA (IOA) 规则和排除项 • IDS 排除项 • IOC 文件 • 被从扫描中排除的数据列表 • 有关存储中文件的信息 • 被隔离的对象的信息 • 具有 Endpoint Agent 组件的计算机列表 • 设备清查 • 分配给设备的标签 • 在设备操作系统中注册的用户账户列表 • 设备上的可执行文件列表 • 设备的地址空间 • 有关网络交互图上设备位置的信息 • 常规报告和报告模板 • NDR 报告和报告模板 • 用户账户数据 • 网络会话数据 • 拓扑图 • 通知	默认	分布式解决方案和多租户模式。	所有部署方法。
配置文件，MDR 集成文件除外。	是	所有模式。	所有部署方法。
备份	自定义	所有模式。	非高可用性版本。
Sandbox 工件。	自定义	所有模式。	非高可用性版本。
重新扫描期间生成的警报档案。	自定义	所有模式。	非高可用性版本。
创建应用程序的备份副本时在扫描队列中的文件。	无。	所有模式。	所有部署方法。
授权许可密钥。	无。	所有模式。	所有部署方法。
事件数据库。	无。	所有模式。	所有部署方法。
网络接口设置。	无。	所有模式。	所有部署方法。
SPAN 流量转储。	无。	所有模式。	所有部署方法。

升级 Kaspersky Anti Targeted Attack Platform

在安装应用程序升级包之前，建议首先为每个要更新的 Central Node 服务器的当前状态创建备份，并从应用程序管理员菜单将其下载到硬盘。如果安装应用程序升级包失败，或者需要重新安装 Kaspersky Anti Targeted Attack Platform，您可以使用应用程序的备份副本。
我们还建议您了解要升级到的版本的限制。

您无法通过升级从应用程序的非高可用性版本迁移到高可用性版本，如果您使用的是应用程序的非高可用性版本，则只能在升级期间安装非高可用性版本，反之亦然。

升级应用程序涉及以下步骤：

1. 升级 Sandbox 组件。
   应用程序没有升级组件的程序。您必须安装该组件的 7.0.3 版本。

   安装该组件后，您需要设置同时运行的虚拟机的最大数量。默认值为 48。

   在 VMware ESXi 虚拟机上安装组件时，必须设置*Sandbox 组件计算*部分中所述的配置。

2. 升级 Central Node 组件。
   您可以通过以下方式之一升级组件：

   - 从版本 6.1 到版本 7.0.3。
     在这种情况下，请按照以下说明之一进行操作：升级安装在服务器上的 Central Node 或升级作为集群安装的 Central Node。

     6.1 之前的版本无法升级到 7.0.3 版本。如果您使用的是应用程序旧版本，则必须按以下顺序将 Central Node 升级到版本 6.1：3.7 → 3.7.1、3.7.1 → 3.7.2、3.7.2 → 4.0、4.0 → 4.1、4.1 → 5.0、5.0 → 5.1、5.1 → 6.0、6.0 → 6.0.2、6.0.2 → 6.1。

   - 如果您正在使用 Central Node 7.0 版本，则需要将其升级到 7.0.1 版本，然后再升级到 7.0.3 版本。
   - 如果您正在使用该组件的 7.0.1 版本，则需要将其升级到 7.0.3 版本。

   如果您已将 PCN 升级到 7.0.3 版本，并且**不打算**在六个月或更长时间内将应用程序升级到 7.1.1 版本，我们强烈建议您在升级后运行 fix_old_slots.sh 脚本，以防止 PCN 服务器磁盘空间耗尽。您可以通过联系技术支持服务获取脚本文件及其使用说明。

   7.0 Central Node 服务器的硬件要求与组件先前版本的硬件要求不同。我们强烈建议确保您的服务器配置满足*"Central Node 组件计算"*部分中列出的要求。

3. 升级安装在独立服务器上的 Sensor 组件。

   应用程序没有升级组件的程序。您必须安装该组件的 7.0.3 版本。

   请注意，安装 Sensor 组件 7.0.3 版本后，Sensor 组件 7.0.1 版本保存到外部存储的网络流量转储文件仍保留在外部存储中，但您无法在应用程序 Web 界面中查看或下载它们。

4. 升级 Endpoint Agent 组件：

   - Kaspersky Endpoint Agent for Windows。

     如果将该解决方案与 Kaspersky Security for Windows Server 一起使用，您可以从 Kaspersky Security for Windows Server 迁移到包含内置代理的 Kaspersky Endpoint Security for Windows 版本 12.1 或更高版本。有关迁移的更多信息，请参阅Kaspersky Endpoint Security for Windows帮助。

   - Kaspersky Endpoint Security for Windows。

   - Kaspersky Endpoint Security for Linux。
   - Kaspersky Endpoint Security for Mac。

将 Kaspersky Anti Targeted Attack Platform 从版本 6.1 更新到版本 7.0.3 的特殊注意事项

1. 在将 Kaspersky Anti Targeted Attack Platform 升级到 7.0.3 版后，您必须再次添加授权许可密钥。
2. 应用程序（包括应用程序的高可用性版本）运行中发生短暂中断被认为可以接受。
3. 如果 Kaspersky Secure Mail Gateway 解决方案用被作 Sensor 组件，则会保存与其集成的设置。
4. Sandbox 组件数据**未**保存。我们建议在更新 Sandbox 之前删除自定义操作系统镜像，并在更新后上传它们。
5. Central Node 7.0.3 与早期版本的 Sensor 和 Sandbox 组件**不**兼容。

将服务器上安装的 Central Node 从版本 6.1 升级到 7.0.3

在安装应用程序升级包之前，建议首先为每个要更新的 Central Node 服务器的当前状态创建备份，并从应用程序管理员菜单将其下载到硬盘。如果安装应用程序升级包失败，或者需要重新安装 Kaspersky Anti Targeted Attack Platform，您可以使用应用程序的备份副本。
我们还建议您了解要升级到的版本的限制。

7.0 Central Node 服务器的硬件要求与组件先前版本的硬件要求不同。我们强烈建议确保您的服务器配置满足*"Central Node 组件计算"*部分中列出的要求。

如果您使用的是分布式解决方案和多租户模式，则必须先完成安装升级的准备步骤，然后才能继续升级。

升级以升级包形式提供。该软件包包含在应用程序分发包中。

要升级服务器上安装的 Central Node：

1. 移除与正在更新的 Central Node 分开安装的 Sandbox 和 Sensor 组件。

   下面描述的所有步骤都必须在使用 sudo -i 命令提升用户权限后在技术支持模式下的服务器上执行。

2. 将应用程序升级包放置在 Central Node 服务器的 `/data` 目录中。

3. 通过 SSH 或终端登录到要执行升级的 Central Node 服务器的管理控制台。

4. 确保 /dev/sda2 文件系统有超过 100 GB 的可用空间。

5. 如果不使用来自 SPAN 端口的镜像流量处理（包括使用 KEDR 授权许可密钥的应用程序），请执行以下命令：
   ```
   kata-enable-span
   ```

   如果禁用来自 SPAN 端口的镜像流量处理，升级将失败。

6. 解压升级存档：
   ```
   tar xvf /data/kata-upgrade-7.0.3.520-x86_64_en-ru.tar.gz -C /data/
   ```

7. 通过运行以下命令安装升级包：
   ```
   cd /data/upgrade/
   ./run_kata_upgrade.py
   ```
   显示用户名输入窗口。

8. 在显示的窗口中，在“**用户名**”字段中，输入具有管理员权限的用户的名称，选择“**确定**”按钮并按“**Enter**”。
   默认值：**admin**。

9. 在显示的窗口中，在“**密码**”字段中，输入具有管理员权限的用户的密码，选择“**确定**”按钮并按“**Enter**”。
   这将打开一个窗口，用于输入更新存档的路径。

10. 这将打开一个窗口；在该窗口中，在“**数据目录**”字段中，输入更新存档的路径，选择“**确定**”按钮并按 **Enter**。
    默认值：**/data/upgrade**

11. 在显示的窗口中，选择 NDR 功能的本地化语言。
    与 NDR 功能相关的应用程序部分将以所选语言显示。
    一段时间后，控制台将显示一条消息，提示您关闭服务器电源。

12. 显示提示关闭服务器电源的消息后，请运行以下命令：
    ```
    poweroff
    ```

13. 挂载 Kaspersky Anti Targeted Attack Platform 7.0.3 基于 Ubuntu 的 iso 映像 (kata-cn-7.0.3.520-inst.x86_64_en-ru.iso)。如果您使用基于 Astra Linux 操作系统的 Kaspersky Anti Targeted Attack Platform，请按照以下“说明”创建 iso 镜像。

14. 从已安装 iso 镜像的设备启动。

15. 在 GRUB 菜单中，选择**升级 KATA 7.0**。

16. 按照向导的剩余步骤完成服务器上的升级。

    Central Node 组件被升级。

升级后，您必须通过 SSH 或终端重新登录 Central Node 服务器管理控制台。

如果您已将 PCN 升级到 7.0.3 版本，并且**不打算**在六个月或更长时间内将应用程序升级到 7.1.1 版本，我们强烈建议您在升级后运行 fix_old_slots.sh 脚本，以防止 PCN 服务器磁盘空间耗尽。您可以通过联系技术支持服务获取脚本文件及其使用说明。

升级到 7.0 版本后，分布式解决方案或多租户模式中使用的 Central Node 组件可能会丢失嵌入式 Sensor。

要消除限制：

1. 通过 SSH 或使用终端登录到您想要升级嵌入的 Sensor 的 Central Node 服务器的管理控制台。
2. 系统提示时，输入管理员用户名和安装组件期间指定的密码。
   显示应用程序组件管理员菜单。
3. 在应用程序管理员菜单中，选择技术支持模式。
4. 按 ENTER。
5. 这将打开技术支持模式确认窗口。
6. 确认您想要在技术支持模式下管理应用程序。为此，请选择“是”并按 ENTER。
7. 运行以下命令：

```
docker service update --cap-add=CAP_DAC_OVERRIDE --cap-add=CAP_IPC_LOCK --cap-add=CAP_SYS_PTRACE kata_product_main_1_preprocessor_span
```

嵌入式 Sensor 已恢复。

将作为集群安装的 Central Node 从版本 6.1 升级到版本 7.0.3

在安装应用程序升级包之前，建议首先为每个要更新的 Central Node 服务器的当前状态创建备份，并从应用程序管理员菜单将其下载到硬盘。如果安装应用程序升级包失败，或者需要重新安装 Kaspersky Anti Targeted Attack Platform，您可以使用应用程序的备份副本。
我们还建议您了解要升级到的版本的限制。

7.0 Central Node 服务器的硬件要求与组件先前版本的硬件要求不同。我们强烈建议确保您的服务器配置满足*“Central Node 组件计算”*部分中列出的要求。

升级以升级包形式提供。该软件包包含在应用程序分发包中。

如果您使用的是分布式解决方案和多租户模式，则必须先完成安装升级的准备步骤，然后才能继续升级。

准备在分布式解决方案和多租户模式下安装升级

如果您使用的是分布式解决方案和多租户模式，则在将应用程序从 6.1 版本升级到 7.0.3 版本之前，需要执行以下操作：

1. 升级 PCN 之前，必须断开连接到此 PCN 的所有 SCN 服务器。应用程序升级完成后，PCN 服务器与升级前属于同一租户。

2. 如果要在 SCN 服务器上更新应用程序，请在更新之前断开该 SCN 服务器与 PCN 的连接。

   应用程序在独立的 Central Node 服务器上得到更新。升级应用应用程序后，您可以为服务器分配SCN角色，并选择 SCN 服务器所属的租户。

   在 Kaspersky Anti Targeted Attack Platform 6.1 版中，断开 SCN 与 PCN 的连接是一项可逆操作。将应用程序升级到 7.0.3 版本后，您可以将 SCN 重新连接到 PCN。从 7.0 版本开始，断开 SCN 与 PCN 的连接将变得不可逆，并且无法再将 SCN 重新连接到任何 PCN 服务器。

   应用程序更新完成后，默认情况下，所有拥有**管理员**角色的用户被授予访问 PCN 服务器和所有 SCN 服务器的 Web 界面的权限。

   默认情况下，具有“**高级安全官**”和“**安全官**”角色的用户可以访问升级前可以访问的相同服务器的 Web 界面。

   Kaspersky Anti Targeted Attack Platform 可能包含用户数据和其他机密信息。Kaspersky Anti Targeted Attack Platform 管理员必须在升级应用程序时或在其他可能需要永久删除数据的情况下采取措施确保该数据的安全。Kaspersky Anti Targeted Attack Platform 管理员负责访问存储在应用程序服务器上的数据。

完成准备步骤后，您可以按照以下说明之一升级 PCN 和 SCN 服务器：升级安装在服务器上的 Central Node 或升级作为集群安装的 Central Node。

升级安装在独立服务器上的 Sensor

该应用程序没有标准的升级过程。您需要安装组件版本 7.0、7.0.1 或 7.0.3。

请注意，安装 Sensor 组件版本 7.0.3 后，您无法查看或下载 Sensor 组件版本 7.0.1 运行期间保存到外部存储的网络流量转储文件。

安装该组件时适用以下建议：

1. 以方便的格式保存 Sensor 组件的设置；例如，您可以制作屏幕截图。如果您使用 BPF 和 Regexp 流量过滤，我们建议将过滤规则保存到文件中。

2. 安装 Sensor 组件。

3. 将已安装的 Sensor 组件连接到 Central Node 组件。

4. 手动恢复您保存的 Sensor 组件设置。

5. 连接外部存储。

在应用程序 7.0、7.0.1 或 7.0.3 版本的 Web 界面中，您无法下载使用 Sensor 组件 6.1 版本保存到外部存储的流量转储。

升级 Kaspersky Anti Targeted Attack Platform 时保留的信息内容和数量

下表列出了 Kaspersky Anti Targeted Attack Platform 从版本 6.1 升级到版本 7.0 时保留的内容和数据量的信息。

将应用程序从版本 6.1 升级到版本 7.0 时保存的内容和数据量

数据类型	升级期间保存的数据

将 Kaspersky Anti Targeted Attack Platform 从 7.0 版更新至 7.0.1 版

在安装应用程序升级包之前，建议首先为每个要更新的 Central Node 服务器的当前状态创建备份，并从应用程序管理员菜单将其下载到硬盘。如果安装应用程序升级包失败，或者需要重新安装 Kaspersky Anti Targeted Attack Platform，您可以使用应用程序的备份副本。
我们还建议您了解要升级到的版本的限制。

如果您使用分布式解决方案和多租户模式，则需要按照以下步骤升级每个 Central Node，而无需断开 SCN 与 PCN 的连接。

SCN 与 PCN 的断开是不可逆的，您无法将 SCN 重新连接到任何 PCN 服务器。

升级以升级包形式提供。该软件包包含在应用程序分发包中。

要更新 Central Node：

1. 如果 Central Node 安装在服务器上：

   a. 将应用程序升级包放置在 Central Node 服务器的 `/data` 目录中。

   b. 通过 SSH 或终端登录到要执行升级的 Central Node 服务器的管理控制台。

2. 如果 Central Node 作为集群安装

   a. 将应用程序升级包放在 Docker swarm 中具有管理者角色的 Central Node 集群服务器上的 `/data` 目录中。要查看角色，请使用 `$ docker node ls` 命令。

   b. 通过 SSH 或终端进入相关服务器的管理控制台。

3. 确保 /dev/sda2 文件系统有超过 100 GB 的可用空间。

4. 解压更新存档：

   ```
   tar xvf /data/kata-upgrade-7.0.1.500-x86_64_en-ru.tar.gz -C /data/
   ```

5. 通过运行以下命令安装升级包：

   ```
   cd /data/upgrade/
   ./run_kata_upgrade.py --patch-version 701
   ```

   显示用户名输入窗口。

6. 在显示的窗口中，在“**用户名**”字段中，输入具有管理员权限的用户的名称，选择“**确定**”按钮并按“**Enter**”。

   默认值：**admin**。

7. 在显示的窗口中，在“**密码**”字段中，输入具有管理员权限的用户的密码，选择“**确定**”按钮并按“**Enter**”。

   这将打开一个窗口，用于输入更新存档的路径。

8. 这将打开一个窗口；在该窗口中，在“**数据目录**”字段中，输入更新存档的路径，选择“**确定**”按钮并按 **Enter**。

   默认值：**/data/upgrade**

9. 在显示的窗口中，选择 NDR 功能的本地化语言。

   与 NDR 功能相关的应用程序部分将以所选语言显示。

Central Node 组件被升级。

更新完成后，我们建议重新启动所有更新的 Central Node。如果 Central Node 作为集群安装，我们建议逐一重新启动所有集群服务器。

将 Kaspersky Anti Targeted Attack Platform 从 7.0.1 版更新至 7.0.3 版

在安装应用程序升级包之前，建议首先为每个要更新的 Central Node 服务器的当前状态创建备份，并从应用程序管理员菜单将其下载到硬盘。如果安装应用程序升级包失败，或者需要重新安装 Kaspersky Anti Targeted Attack Platform，您可以使用应用程序的备份副本。
我们还建议您了解要升级到的版本的限制。

如果您使用分布式解决方案和多租户模式，则需要按照以下步骤升级每个 Central Node，而无需断开 SCN 与 PCN 的连接。

SCN 与 PCN 的断开是不可逆的，您无法将 SCN 重新连接到任何 PCN 服务器。

升级以升级包形式提供。该软件包包含在应用程序分发包中。

要更新 Central Node：

1. 如果 Central Node 安装在服务器上：

   a. 将应用程序升级包放置在 Central Node 服务器的 `/data` 目录中。

   b. 通过 SSH 或终端登录到要执行升级的 Central Node 服务器的管理控制台。

2. 如果 Central Node 作为集群安装

   a. 将应用程序升级包放在 Docker swarm 中具有管理者角色的 Central Node 集群服务器上的 `/data` 目录中。要查看角色，请使用 `$ docker node ls` 命令。

   b. 通过 SSH 或终端进入相关服务器的管理控制台。

3. 确保 /dev/sda2 文件系统有超过 100 GB 的可用空间。

4. 解压更新存档：

   ```
   tar xvf /data/kata-upgrade-7.0.3.520-x86_64_en-ru.tar.gz -C /data/
   ```

5. 通过运行以下命令安装升级包：

   ```
   cd /data/upgrade/
   ./run_kata_upgrade.py --patch-version 703
   ```

   显示用户名输入窗口。

6. 在显示的窗口中，在“**用户名**”字段中，输入具有管理员权限的用户的名称，选择“**确定**”按钮并按“**Enter**”。

   默认值：**admin**。

7. 在显示的窗口中，在“**密码**”字段中，输入具有管理员权限的用户的密码，选择“**确定**”按钮并按“**Enter**”。

   这将打开一个窗口，用于输入更新存档的路径。

8. 这将打开一个窗口；在该窗口中，在“**数据目录**”字段中，输入更新存档的路径，选择“**确定**”按钮并按 **Enter**。

   默认值：**/data/upgrade**

9. 在显示的窗口中，选择 NDR 功能的本地化语言。

   与 NDR 功能相关的应用程序部分将以所选语言显示。

Central Node 组件被升级。

更新完成后，我们建议重新启动所有更新的 Central Node。如果 Central Node 作为集群安装，我们建议逐一重新启动所有集群服务器。

升级 Central Node 集群后，警报表可能不会显示 IDS 技术生成的新警报。我们建议按照以下说明的步骤检查表中是否显示新警报。

要查看警报表中是否显示新警报，请执行以下操作：

1. 通过 SSH 或终端登录到 Central Node 集群中任何服务器的管理控制台。
2. 通过运行以下命令检查所有集群服务是否正在运行且稳定（最近 10 分钟内未重新启动）：
   ```
   docker ps --format "table {{.Image}} | {{.Status}}"
   ```
3. 如果集群的所有服务都稳定，则通过发出以下请求生成测试警报：
   ```
   curl "http://eicar.com/counter.php?act=1&uid=1&id=234"
   ```
4. 在“**高级安全官**”用户账户下登录应用程序 Web 界面。
5. 在应用程序 Web 界面窗口中选择**警报**部分。
   这将打开警报表。
6. 检查警报表是否包含针对地址为 http://eicar.com/counter.php?act=1&uid=1&id=234 的网络事件的新警报。

如果表中缺少警报，请按照说明中的步骤修复限制。

要消除限制：

1. 通过 SSH 或终端，登录到启用了 SPAN 镜像流量处理的集群服务器的管理控制台。
2. 通过运行以下命令提高用户的权限。
   ```
   sudo -i
   ```
3. 运行以下命令：
   ```
   docker service update --force kata_product_main_1_ids_alert_syncer
   ```
4. 按照上述说明的第 3 步至第 6 步检查警报表中是否存在新警报。

限制已移除。

如果表中缺少测试警报，请联系技术支持。

使用 Kaspersky Anti Targeted Attack Platform API KATA 和 KEDR

您可以配置 Kaspersky Anti Targeted Attack Platform 与外部系统的集成，以管理威胁响应操作、扫描存储在这些系统中的文件、以及向外部系统提供对有关所有警报和事件的信息的访问。

API 方法调用仅适用于被授权的外部系统。对于授权，应用程序管理员必须创建将外部系统与应用程序集成的请求。然后，管理员必须在 Kaspersky Anti Targeted Attack Platform 的 Web 界面中处理该请求。

如果您已将 Central Node 和 Sensor 组件部署为集群，则可以使用以下选项之一配置与外部系统的高可用性集成：

- 使用轮询调度算法功能。
- 配置外部系统，以便在发生超时时外部系统可在集群服务器的 IP 地址之间切换。

要使用轮询调度算法功能配置与外部系统的高可用性集成：

1. 在 Central Node 集群对应域名的 DNS 服务器上配置轮询调度算法。
2. 在邮件服务器设置中指定此域名。

与外部系统的集成是基于域名配置的。外部系统将与集群中的随机服务器进行通信。如果该服务器出现故障，外部系统将与集群中另一台健康的服务器进行通信。

将外部系统与 Kaspersky Anti Targeted Attack Platform 集成

要开始使用 API，您需要将外部系统与 Kaspersky Anti Targeted Attack Platform 集成。外部系统必须在 Kaspersky Anti Targeted Attack Platform 服务器上完成授权。

若要将外部系统与 Kaspersky Anti Targeted Attack Platform 集成：

1. 生成一个用于在 Kaspersky Anti Targeted Attack Platform 中授权的外部系统的唯一标识符 – `sensorId`。
2. 为外部系统服务器生成证书。
3. 在 Kaspersky Anti Targeted Attack Platform 中创建来自外部系统的包含 `sensorId` 的任何请求。例如，您可以创建在 Kaspersky Anti Targeted Attack Platform 中扫描外部系统对象的请求。

   Kaspersky Anti Targeted Attack Platform 的 Web 界面将显示来自外部系统的授权请求。联系应用程序管理员以处理请求。

如果您需要更改外部系统服务器证书，请重复将外部系统与 Kaspersky Anti Targeted Attack Platform 集成的步骤。

请求扫描对象

要创建扫描对象的请求，请使用 HTTP POST方法。例如，您可以使用 cURL 命令行实用程序创建请求。

您可以使用附加开关来设置执行 cURL 命令的参数（请参见下表）。

有关 cURL 命令开关的更多信息，请参阅 cURL 文档。

命令语法

```
curl --cert <TLS 证书文件路径> --key <私钥文件路径> -X POST "<Central Node 组件服务器的URL>:<端口，默认为 443>/kata/scanner/v1/sensors/<sensorId>/scans?sensorInstanceId=<sensorInstanceId>" -F "content=<要扫描的文件的路径>" -F scanId=<扫描请求 ID> -F "objectType=file"
```

如果请求得到成功处理，将显示OK状态。

设置

参数	类型	描述
sensorId	UUID	用于 Kaspersky Anti Targeted Attack Platform 授权的外部系统的唯一 ID。
content	file	扫描对象的内容。
scanId	string	扫描请求的唯一 ID。它必须在外部系统中生成。它不能包含空格或特殊字符。请勿使用文件名作为扫描请求 ID。 如果未定义此参数，则无法查看扫描结果。
objectType	string	扫描对象的类型。 参数的可能值：文件。
sensorInstanceId	string	外部系统实例的唯一 ID。组合成一个集群的服务器也被视为外部系统的实例。此参数是可选的。

返回值

返回码	描述
200	扫描对象的请求已成功创建。
401	需要授权。
429	超过的请求数。稍后重复该请求。
500	内部服务器错误。稍后重复该请求。

输入具有开关的命令的示例

```
curl --cert /root/cert.pem --key /root/server.key -
X POST "https://10.10.10.1:443/kata/scanner/v1/sensors/dd11a1ee-a00b-111c-b11a-11001b1f1111/scans?
sensorInstanceId=instance1" -F "content=@/tmp/test" -F scanId=1 -F "objectType=file"
```

请求扫描结果

要创建接收扫描结果的请求，请使用 HTTP GET方法。例如，您可以使用 cURL 命令行实用程序创建请求。

您可以使用附加开关来设置执行 cURL 命令的参数（请参见下表）。

有关 cURL 命令开关的更多信息，请参阅 cURL 文档。

命令语法

`curl --cert <TLS 证书文件路径> --key <私钥文件路径> -X GET "<Central Node 组件服务器的 URL>:<端口，默认 443>/kata/scanner/v1/sensors/<sensorId>/scans/state?sensorInstanceId=<sensorInstanceId>&state=<您想要在扫描结果中显示的一个或多个扫描状态>"`

如果请求发送成功，则会显示扫描对象的请求列表以及扫描这些对象的结果。扫描结果将按您在`state`参数中指定的状态进行筛选。例如，如果您在扫描结果请求中指定`state=processing,detect`，则应用程序将仅显示正在被处理或应用程序在其中检测到威胁的对象扫描请求。

设置

参数	类型	描述
`sensorId`	string	用于 Kaspersky Anti Targeted Attack Platform 授权的外部系统的唯一 ID。
`state`	array（字符串元素类型）	对象扫描状态。定义此参数后，将按状态筛选扫描结果。 指示一种或多种状态，以逗号分隔。 可以使用以下参数值： • `detect` • `not detected` • `processing` • `timeout` • `error`
`sensorInstanceId`	string	外部系统实例的唯一 ID。组合成一个集群的服务器也被视为外部系统的实例。此参数是可选的。

Response

HTTP 代码：200

格式：JSON

```
type Response []Scans

type Scans struct {
ScanID integer `json:"scanId"`
State array `json:"state"`
}
```

返回值

返回码	描述
204	没有内容。
404	未找到指定 ID 的扫描结果。
500	内部服务器错误。稍后重复该请求。

如果要在扫描结果中显示所有对象扫描状态时输入带有开关的命令的示例

```
curl --cert /root/cert.pem --key /root/server.key -X GET "https://10.10.10.1:443/kata/scanner/v1/sensors/dd11a1ee-a00b-111c-b11a-11001b1f1111/scans/state?
sensorInstanceId=instance1&state=detect,not%20detected,processing,error,timeout"
```

请求删除扫描结果

要创建删除一个或多个对象的扫描结果的请求，请使用 DELETE 方法。例如，您可以使用 cURL 命令行实用程序创建请求。

命令语法

`curl --cert <TLS 证书文件的路径> --key <私钥文件的路径> -X DELETE "<具有 Central Node 组件的服务器的 URL>:<端口，默认为 443>/kata/scanner/v1/sensors/<sensorId>/scans/<scanId>"`

如果请求得到成功处理，对象扫描结果将被删除。“OK”状态将显示。

设置

参数	类型	描述
sensorId	string	用于 Kaspersky Anti Targeted Attack Platform 授权的外部系统的唯一 ID。
scanId	string	对象扫描请求的唯一 ID。如果未定义此参数，则将删除所有对象的扫描结果。

返回值

返回码	描述
200	删除扫描结果的请求已成功创建。
401	需要授权。
404	未找到指定 ID 的扫描结果。
500	内部服务器错误。稍后重复该请求。

命令输入示例

```
curl --cert /root/cert.pem --key /root/server.key -
X DELETE "https://10.10.10.1:443/kata/scanner/v1/sensors/dd11a1ee-a00b-111c-b11a-11001b1f1111/scans/1"
```

请求显示对象扫描限制

要创建请求以显示应用程序对扫描对象的限制（例如，按大小），请使用 HTTP GET方法。例如，您可以使用 cURL 命令行实用程序创建请求。

命令语法

`curl --cert <TLS 证书文件的路径> --key <私钥文件的路径> -X GET "<具有 Central Node 组件的服务器的 URL>:<端口，默认为 443>/kata/scanner/v1/sensors/<sensorId>/scans/filters`

如果请求得到成功处理，将显示应用程序的对象扫描限制。例如，`maxObjectSize`限制是您可以提交进行扫描的对象的最大允许大小。

设置

参数	类型	描述
sensorId	string	用于 Kaspersky Anti Targeted Attack Platform 授权的外部系统的唯一 ID。

Response

HTTP 代码：200

格式：JSON

```
type Response struct {
MaxObjectSize integer `json:"maxObjectSize"`
Version string `json:"version"`
}
```

返回值

返回码	描述
401	需要授权。
500	内部服务器错误。稍后重复该请求。

命令输入示例

```
curl --cert /root/cert.pem --key /root/server.key -X GET "https://10.10.10.1:443/kata/scanner/v1/sensors/dd11a1ee-a00b-111c-b11a-11001b1f1111/scans/filters"
```

外部系统可用来接收应用程序警报信息的 API

Kaspersky Anti Targeted Attack Platform 提供一个 API，允许外部系统访问有关应用程序所有警报的信息，而不仅仅是扫描这些外部系统中存储的对象的结果。

为了仅接收满足特定条件的警报信息，您可以在请求参数中指定筛选器。

> 应用程序不会根据先前的请求自动发送有关新警报的信息。必须发送新请求才能接收最新信息。

分布式解决方案中操作的特殊注意事项

如果应用程序在分布式解决方案模式下运行，必须为要从其接收警报信息的每个 PCN 和 SCN 服务器单独配置与外部系统的集成。此限制是由于 PCN 服务器的 Web 界面显示所有警报信息，但警报数据库仅存储已在该特定服务器上注册的那些警报。

请求显示警报信息

要创建请求以显示有关 Kaspersky Anti Targeted Attack Platform 警报的信息，请使用 HTTP `GET`方法。例如，您可以使用 cURL 命令行实用程序创建请求。

命令语法

`curl --cert <TLS 证书文件的路径> --key <私钥文件的路径> -X GET "<Central Node 组件服务器的 URL>:<端口，默认为 443>/kata/scanner/v1/sensors/<sensorId>/detects?detect_type=<用于生成警报的一种或多种技术>&limit=<响应请求中的警报数量>&token=<请求 ID>"`

如果请求处理成功，您将在外部系统的服务器上看到 Kaspersky Anti Targeted Attack Platform 生成的警报列表。

设置

参数	类型	描述
`sensorId`	string	用于 Kaspersky Anti Targeted Attack Platform 授权的外部系统的唯一 ID。
`detect_type`	Array	创建警报的技术。您可以指定以逗号分隔的技术列表。 可能值: • `am` – 反恶意软件引擎 • `sb` – Sandbox • `yara` – YARA • `url_reputation` – URL 信誉 • `ids` – 入侵检测系统 如果未指定该参数，则提供有关所有警报的信息。
`limit`	整数	为了响应请求而为其提供信息的对象的数量。允许的值：1 到 10000 之间的整数。 默认值为 `1000`。
`token`	string	请求 ID。如果指定该参数，则重复请求不会显示之前请求获得的警报信息。这有助于避免在重复请求时出现有关相同警报的重复信息。 如果未指定此参数，则提供有关所有警报的信息。

Response

HTTP 代码：200

格式：JSON

```
type Response struct {
Detects array `json:"detects"`
Token string `json:"token"`
}
```

返回值

返回码	描述
400	参数不正确。
429	超过的请求数。
401	需要授权。
500	内部服务器错误。稍后重复该请求。

输入具有开关的命令的示例

```
curl --cert /root/cert.pem --key /root/server.key -X GET "https://10.10.10.1:443/kata/scanner/v1/sensors/dd11a1ee-a00b-111c-b11a-11001b1f1111/detects?detect_type=am,sb&limit=100&token=7b226f6666736574223a20307d"
```

传输数据的范围

下表列出了为每个检测传输的信息。

警报传输的信息范围

参数	值	描述
alertID	整数值。	警报 ID。
eventTimeStamp	日期和时间。	事件时间。
detectTimestamp	日期和时间。	Kaspersky Anti Targeted Attack Platform 数据库中记录警报信息的时间。
importance	以下值之一： • 高 • 中 • 低	警报重要性。
objectSource	以下值之一： • web • mail • endpoint • external • dns	检测到的对象的来源。
technology	以下值之一： • am – 反恶意软件引擎 • sb – Sandbox • yara – YARA • url_reputation – URL 信誉 • ids – 入侵检测系统	用于检测对象的技术。

参数	值	描述
objectType	以下值之一： • file。 • URL。 • host（对于远程域或主机）。	检测对象的类型。
object	取决于检测对象的类型。	检测对象的数据。
detection	取决于用于检测对象的技术。	有关检测到的威胁的数据。
details	取决于检测到的对象的来源。	有关检测到的对象的环境数据。

有关检测到的对象的数据

下表列出了检测到的对象的传输数据范围，具体取决于对象的类型。

有关检测到的对象的数据

	参数	数据类型	描述	示例
file	processedObject.MD5	MD5	被发送进行扫描的文件或复合对象的 MD5 哈希值。	1839a1e9621c58dadf782e131df3821f
	processedObject.SHA256	SHA256	被发送进行扫描的文件或复合对象的 SHA256 哈希值。	7bbfc1d690079b0c591e146c4294305da1cee857e12db40f431
	processedObject.fileName	string	被发送进行扫描的文件或复合对象的名称。	EICAR-CURE.com
	processedObject.fileType	string	被发送进行扫描的文件或复合对象的类型。	GeneralTxt
	processedObject.fileSize	整数	被发送进行扫描的文件或复合对象的大小（以字节为单位）。	184
	detectedObject.MD5	MD5	在其中检测到威胁的文件（简单对象或复合对象中的文件）的 MD5 哈希值。	1839a1e9621c58dadf782e131df3821f
	detectedObject.fileName	string	在其中检测到威胁的文件（简单对象或复合对象中的文件）的名称。	EICAR-CURE.com
	detectedObject.fileSize	整数	在其中检测到威胁的文件（简单对象或复合对象中的文件）的大小（以字节为单位）。	184
URL	detectedObject	string	检测到的对象的 URL。	http://example.com/link
host	detectedObject	Array	检测到的对象所属的域列表。 对于URL技术以及具有 objectSource=dns 参数的对象，该列表可以包含多个域。	example.org，example.net

有关检测到的威胁的数据

下表列出了检测到的威胁的传输数据范围，具体取决于用于生成警报的技术。

有关检测到的威胁的数据

technology	参数	描述	数据类型	示例
以下技术之一： • 反恶意软件引擎。 • YARA。 • 入侵检测系统。	detect	检测到的威胁的列表。	Array	HEUR:Trojan.Win32.Generic, Trojan-DDoS.Win32.Macri.avy, UDS:DangerousObject.Multi.Generic
	dataBaseVersion	用于扫描文件的数据库的版本。	整数	201811190706
Sandbox	detect	检测到的威胁的列表。	Array	HEUR:Trojan.Win32.Generic, Trojan-DDoS.Win32.Macri.avy, UDS:DangerousObject.Multi.Generic
	image	扫描文件的虚拟机镜像的名称。	string	Win7
	dataBaseVersion	数据库版本采用以下格式：<被用于扫描文件的应用程序数据库的版本> / <IDS 模块数据库的版本>。	整数	201902031107/ 201811190706
URL 信誉	detect	检测对象的 URL 信誉类别列表（适用于URL或host类型的对象）。	Array	钓鱼主机、恶意主机、僵尸网络 C&C (Backdoor.Win32.Mokes)

有关检测到的对象的环境数据

下表列出了有关检测到的对象的环境的传输数据的范围，具体取决于对象的来源。

有关检测到的对象的环境数据

对象的来源	参数	描述	数据类型	示例
web	sourceIP	建立连接的计算机的 IP 地址。	IP 地址	192.0.2.0
	sourceHostname	建立连接的计算机的名称。	string	example.com
	destinationIp	与其建立了连接的计算机的 IP 地址。	IP 地址	198.51.100.0
	destinationPort	与其建立连接的计算机的端口。	整数	3128
	URL	被访问的 Web 资源的 URL。 IDS 技术检测没有此参数。 对于 URL 技术检测，此参数与 detectedObject 参数具有相同的值。	string	https://example.com:443/
	method	HTTP 请求方法。	string	Connect
	referrer	从起进行重定向的 URL。	string	https://example.com:443/
	agentString	HTTP 请求的用户代理标头，包含客户端应用程序的名称和版本。	string	Mozilla/4.0
mail	mailFrom	发件人的电子邮件地址。	string	sender@example.com
	mailTo	以逗号分隔的收件人电子邮件地址列表。	Array	recipient1@example.com，recipient2@example.com
	subject	邮件主题。	string	'您是赢家'
	messageId	电子邮件 ID。	string	1745028736.156014.1542897410859.JavaMail.svc_jira_pool
• endpoint • external	hostName	生成检测的计算机的名称。	string	computername.example.com
	IP	生成检测的计算机的 IP 地址。	IP 地址	198.51.100.0

对象的来源	参数	描述	数据类型	示例
dns	sourceIp	发起 DNS 连接的计算机的 IP 地址。	IP 地址	192.0.2.0
	destinationIp	与其建立 DNS 连接的计算机（通常是 DNS 服务器）的 IP 地址。	IP 地址	198.51.100.0
	destinationPort	与其建立 DNS 连接的计算机（通常是 DNS 服务器）的端口。	整数	3128
	dnsMessageType	DNS 消息类型： • Request • Response	string	Request
	dnsRequestType	以下 DNS 请求类型之一： • A。 • AAA。 • CNAME。 • MX。	string	MX
	domainToBeResolved	来自 DNS 请求的域名。	string	example.com

外部系统可用来接收应用程序事件信息的 API

Kaspersky Anti Targeted Attack Platform 为外部系统提供 API，可用于访问有关应用程序注册的事件的信息。

若要仅接收满足特定条件的事件的信息，您可以在请求参数中指定筛选器。

应用程序不会根据先前的请求自动发送有关新事件的信息。必须发送新请求才能接收最新信息。

新事件信息在这些事件出现在 Kaspersky Anti Targeted Attack Platform 数据库中后的两个小时内即可检索到。

分布式解决方案中操作的特殊注意事项

如果应用程序在分布式解决方案模式下运行，必须为要从其接收事件的每个 PCN 和 SCN 服务器单独配置与外部系统的集成。此限制是由于 PCN 服务器的 Web 界面显示有关所有事件的信息，但事件数据库仅存储已在该特定服务器上注册的事件。

查询事件信息的请求

要创建获取事件信息的请求，请使用 HTTP GET 方法。

您可以使用附加开关来设置执行 cURL 命令的参数（请参见下表）。

有关 cURL 命令开关的更多信息，请参阅 cURL 文档。

在第一次请求时，Kaspersky Anti Targeted Attack Platform 会创建一个*ContinuationToken*（以下也称为"令牌"）。应用程序在创建令牌时会发送系统中可用的事件。创建新令牌时，Kaspersky Anti Targeted Attack Platform 会发送创建此令牌时系统中可用的事件。

令牌包含有关最后传输的数据的信息。如果您想接收上次请求后记录的事件，则必须保存创建的令牌并在以后的请求中使用它。

命令语法

对于第一个请求：

```
curl --cert <TLS 证书文件的路径> --key <私钥文件的路径> -X GET "<Central Node 组件服务器的URL>:<端口，默认为 443>/kata/events_api/v1/<external_system_id>/events"
```

如果请求处理成功，会显示有关请求的事件和令牌值的信息。

对于后续请求：

```
curl --cert <TLS 证书文件的路径> --key <私钥文件的路径> -X GET "<Central Node 组件服务器的URL>:<端口，默认为 443>/kata/events_api/v1/<external_system_id>/events&continuation_token=<第一个请求收到的令牌值>"
```

如果请求处理成功，会显示自上次请求以来收到的事件的信息。

您可以通过指定最大收集时间和事件数量以及事件筛选参数来创建输出事件信息的请求：

```
curl --cert <TLS 证书文件的路径> --key <私钥文件的路径> -X GET "<Central Node 组件服务器的URL>:<端口，默认为 443>/kata/events_api/v1/<external_system_id>/events?filter=<事件筛选器>&max_timeout=<最大事件收集时间>&max_events=<最大事件数>&continuation_token=<第一个请求收到的令牌值>"
```

如果您为第一个请求指定了筛选参数的值，则不必在后续请求中指定它：筛选参数会从上一个请求中保存下来，并且在后续请求中没有传递新参数时使用。如果您不想使用筛选，请不要指定该参数的值。

设置

参数	类型	描述
`external_system_id`	UUID	用于 Kaspersky Anti Targeted Attack Platform 授权的外部系统的唯一 ID。
`filter`	string	事件筛选设置。这些是使用事件查询语言设置的。
`max_timeout`	int	最大事件收集时间。按以下格式指定：PT<整数值>S。例如，PT300S。服务器发送在指定时间内收集的事件的信息。 默认值为 5 分钟。除非请求中另有指定，否则使用该值。 最大事件收集时间不得超过 5 分钟。如果指定的值大于 5 分钟，Central Node 服务器将返回错误。 等待事件的实际总时间可能会增加。

参数	类型	描述
max_events	int	最大事件数 如果请求中未指定值，Kaspersky Anti Targeted Attack Platform 将根据安装了 Endpoint Agent 组件的主机数量来计算该值。 典型配置的值示例： • 对于 1000 台主机：64000。 • 对于 5000 台主机：128000。 • 对于 10000 台主机：208000。 • 对于 15000 名主机：288000。 • 对于 30000 台主机：528000。 请求中指定的值不得超过这些限制。
continuation_token	string	令牌值。

输入带有参数的命令的示例

```
curl --cert <TLS 证书文件的路径> --key <私钥文件的路径> -X GET "https://10.10.0.22:443/kata/events_api/v1/c440a37b-5c01-4505-a30e-3d23b20dd609/events"
```

```
curl --cert <TLS 证书文件的路径> --key <私钥文件的路径> -X GET "https://10.10.0.22:443/kata/events_api/v1/c440a37b-5c01-4505-a30e-3d23b20dd609/events?
filter=EventType=='threatdetect' OR
EventType=='threatprocessingresult'&max_timeout=PT300S&max_events=64000&continuation_token=
CiQyZDcyNjNiOS0zZmNlLTQxNzktYTdhOC03N2E0ZmUwNjNjMTkSBAgAEAoSBAgBEAMSBAgCEAsSBAgDEAcSBAgEEAgSBAgFEAkSBAgGEAQSBAg
HEAUSBAgIEAcSBAgJEAMYiYyCmvIw"
```

如果参数值包含特殊字符，则必须使用 URL 编码或
请求中的`--data-urlencode`选项。

带有 URL 编码参数的命令示例

```
curl --cert <TLS 证书文件的路径> --key <私钥文件的路径> GET "https://10.10.0.22:443/kata/events_api/v1/c440a37b-5c01-4505-a30e-3d23b20dd609/events?
filter=EventType=='threatdetect' OR
EventType=='threatprocessingresult'&max_timeout=PT300S&max_events=64000&continuation_token=
CiQ%3Dcy%7ENiOS0zZmNlLTQxNzktYTdhOC03N2E0Z40%wNjNjMTkSBAgAEAoSBAgB%5EMSB%3CEAsSBAgDEAcSBAgEEAgSBAgFEAkSBAgGEAQSBAg
HEAUSBAgIEAcSBAgJEAMYiYyCmvIw"
```

带有使用`--data-urlencode`选项的参数的命令示例

```
curl --cert <TLS 证书的路径> --key <私钥文件的路径> --GET -d "max_events=64000" -d "max_timeout=PT300S" -d
"filter=EventType=='threatdetect'" --data-urlencode "continuation_token=
CiQ?Dcy~NiOS0zZmNlLTQxNzktYTdhOC03N2E0Z@wNjNjMTkSBAgAEAoSBAgB^MSB?CEAsSBAgDEAcSBAgEEAgSBAgFEAkSBAgGEAQSBAg
HEAUSBAgIEAcSBAgJEAMYiYyCmvIw" https://10.10.0.22:443/kata/events_api/v1/c440a37b-5c01-4505-a30e-
3d23b20dd609/events
```

Response

HTTP 代码：200

格式：JSON

```
type Response struct {
Events array `json:"events"`
ContinuationToken string `json:"continuationToken"`
}
```

返回值

返回码	描述
400	参数不正确。
401	需要授权。
500, 502, 503, 504	内部服务器错误。稍后重复该请求。

用于筛选事件的查询语言

事件筛选查询语言支持以下函数和运算符：

- 函数： `in`。
- 字符串或布尔值的比较运算符：
  - `==`
  - `!=`
- 数字和变量的比较运算符：
  - AND
  - OR
  - NOT
  - ==
  - !=
  - >
  - >=

- <
- <=

您可以在事件筛选字段部分中查看可用于筛选事件的字段列表。

如果您想要接收有关不同类型事件的信息，必须为每种类型的事件创建单独的请求。

```
EventType=='threatdetect' OR EventType=='threatprocessingresult'
```

支持数字和字符串常量。字符串常量必须带单引号：`'example'`。通配符 * 和 ? 支持字符串常量。如果您不想使用这些字符作为通配符，则必须对它们进行转义：`\*`，`\?`。另外，在字符串常量中，必须对特殊字符进行转义。

用于筛选事件的字段

下表列出了用于筛选事件的字段。

如果字段值包含特殊字符，则必须使用 URL 编码或请求中的`--data-urlencode`选项。

用于筛选事件的字段列表

字段名称	类型	描述
hostName	string	主机名称。
HostIp	string	主机的 IP 地址。
EventType	string	事件类型。可能值: • process — 进程已开始。 • process_terminate — 进程已终止。 • module — 模块已加载。 • connection — 远程连接。 • applock — 防护规则。 • blockdocument — 文档被阻止。 • filechange — 文件已修改。 • windowsevent — 系统事件日志。 • registry — 注册表已修改。 • portlisten — 监听的端口。 • driver — 驱动程序已加载。 • threatdetect — 警报。 • threatprocessingresult — 警报处理结果。 • amsiscan — AMSI 扫描。 • process_interpretated_file_run — 文件的已解释运行。 • process_console_interactive_input — 在控制台上交互式输入命令。
UserName	string	用户名称。
OsFamily	string	操作系统系列。
OsVersion	string	主机上使用的操作系统版本。
Ioa.Rules.Id	string	TAA (IOA) 规则 ID。
Ioa.Rules.Name	string	有关使用 Targeted Attack Analyzer 技术进行文件分析的结果的信息：用于创建警报的 TAA (IOA) 规则的名称。
Ioa.Rules.Techniques	string	MITRE 技术
Ioa.Rules.Tactics	string	MITRE tactic

字段名称	类型	描述
loa.Severity	string	分配给使用此 TAA (IOA) 规则生成的事件的重要性级别。 可能值: • 低 • 中 • 高
loa.Confidence	string	置信度取决于规则引起误报的可能性。 可能值: • 低 • 中 • 高
FileCreationTime	integer	文件创建时间。
DllCreationTime	integer	DLL 创建时间。
DroppedCreationTime	integer	被修改文件的创建时间。
InterpretedFileCreationTime	integer	被解释文件的创建时间。
FileName	string	文件名。
DllName	string	DLL 名称。
DroppedName	string	被修改文件的名称。
BlockedName	string	被阻止文件的名称。
InterpretedFileName	string	被解释文件的名称。
FilePath	string	文件所在目录的路径。
DllPath	string	DLL 所在目录的路径。
DroppedPath	string	修改后的文件所在目录的路径。
BlockedPath	string	被阻止文件所在目录的路径。
InterpretedFilePath	string	被解释文件所在目录的路径。
FileFullName	string	文件的完整路径。包括目录路径和文件名。
DllFullName	string	DLL 的完整路径。包括目录路径和文件名。
DroppedFullName	string	被修改文件的完整路径。包括目录路径和文件名。
BlockedFullName	string	被阻止文件的完整路径。包括目录路径和文件名。
DetectedName	string	被检测文件的完整路径。包括目录路径和文件名。
OriginalFileName	string	原始文件的完整路径。包括目录路径和文件名。
InterpretedFileFullName	string	被解释文件的完整路径。包括目录路径和文件名。
FileModificationTime	integer	文件修改时间。
DllModificationTime	integer	DLL 修改时间。
DroppedModificationTime	integer	被修改时间的修改时间。
InterpretedFileModificationTime	integer	被解释时间的修改时间。
FileSize	integer	文件大小。
DllSize	integer	DLL 大小。
DroppedSize	integer	修改后的文件的大小。
InterpretedFileSize	integer	被解释文件的大小。
Md5	string	文件的 MD5 哈希。
DllMd5	string	DLL 的 MD5 哈希
DroppedMd5	string	被修改文件的 MD5 哈希。
InterpretedMd5	string	被解释文件的 MD5 哈希。
DetectedMd5	string	检测到的文件的 MD5 哈希。

字段名称	类型	描述
Sha256	string	文件的 SHA256 哈希。
DLLSha256	string	DLL 的 SHA256 哈希。
DroppedSha256	string	被修改文件的 SHA256 哈希。
BlockedSha256	string	被阻止文件的 SHA256 哈希。
InterpretedSha256	string	被解释文件的 SHA256 哈希。
DetectedSha256	string	检测到的文件的 SHA256 哈希。
HijackingPath	string	放置在标准搜索路径上的目录中的恶意 DLL，以使操作系统在原始 DLL 之前加载它。
LogonRemoteHost	string	发起远程访问的主机的 IP 地址。
RealUserName	string	用户在系统中注册时被分配的用户名称。
EffectiveUserName	string	用于登录系统的用户名。
Environment	string	环境变量。
ProcessType	integer	进程类型。可能值: • 1 – exec • 2 – fork • 3 – vfork • 4 – clone
LinuxOperationResult	string	操作结果。可能值: • success • failed
SystemPid	integer	进程 ID。
ParentFileFullName	string	父进程文件的路径。
ParentMd5	string	父进程文件的 MD5 哈希。
ParentSha256	string	父进程文件的 SHA256 哈希。
StartupParameters	string	进程启动选项。
ParentSystemPid	integer	父进程 ID。
ParentStartupParameters	string	父进程启动设置。
Method	string	HTTP 请求方法。
Direction	string	连接方向。可能值: • inbound • outbound
LocalIp	string	进行远程连接尝试的本地计算机的 IP 地址。
LocalPort	integer	尝试进行远程连接的本地计算机的端口。
RemoteHostName	string	作为远程连接尝试目标的计算机的名称。
RemoteIp	string	作为远程连接尝试目标的计算机的 IP 地址。
RemotePort	integer	作为远程连接尝试目标的计算机的端口。
URI	string	对其发出 HTTP 请求的资源的地址。
KeyName	string	注册表项路径。
ValueName	string	注册表值名称。
ValueData	string	注册表值数据。
RegistryOperationType	integer	注册表操作的类型。可能值: • 0 – 注册表项已创建。 • 1 – 注册表项已删除。 • 2 – 注册表已修改。 • 3 – 注册表项被重命名。
PreviousKeyName	string	以前的注册表项路径。

字段名称	类型	描述
PreviousValueData	string	注册表值的先前名称。
System.EventID.value	string	在 Windows 日志中的安全事件类型 ID。
LinuxEventType （该字段被用于获取 Linux 和 macOS 操作系统的事件日志中记录的事件类型）	string	事件类型。可能值: • MemberAddedToGroup — 用户账户已创建。 • UserAccountDeleted — 用户账户已删除。 • GroupCreated — 组已创建。 • GroupDeleted — 组已修改。 • MemberAddedToGroup — 用户账户已添加到组。 • UserPasswordChanged — 用户账户密码已更改。 • LinuxAuth — 在 Linux 或 macOS 中执行的身份验证。 • LinuxSessionStart — Linux 或 macOS 会话已启动。 • LinuxSessionEnd — Linux 或 macOS 会话已结束。 • ServiceStart — 服务已启动。 • ChangeAccountExpirationDate — 账户到期日期已更改。 • OperatingSystemShuttingDown — 操作系统已关闭。 • OperatingSystemStarted — 操作系统已启动。 • ModifyPromiscouslyMode — 混杂模式已修改。 • AuditdConfigurationChanged — 审核设置已修改。
System.Channel.value	string	日志名称。
System.EventRecordID.value	string	日志中的条目 ID。
System.Provider.Name.value	string	记录事件的系统的 ID。
EventData.Data.TargetDomainName.value	string	远程计算机的域名。
EventData.Data.ObjectName.value	string	发起事件的对象的名称。
EventData.Data.PackageName.value	string	启动事件的数据包的名称。
EventData.Data.ProcessName.value	string	启动事件的进程的名称。
VerdictName	string	检测到的对象的名称。
RecordId	integer	被触发的规则 ID。
ProcessingMode	string	扫描模式。可能值: • Default — 默认。 • OnDemand — 按需。 • OnAccess — 访问时。 • OnExecute — 执行时。 • OnDownload — 下载时。 • OnStartup — 应用程序启动时。 • OnMail — 发送消息时。 • OnPostpone — 已推迟扫描。 • OnDisinfect — 清除时。 • OnVulnerability — 扫描漏洞时。 • OnFirstLaunch — 首次启动时。 • OnEngineLoad — 系统启动时。 • OnQuarantineRescan — 重新扫描存储中的对象时。 • OnWebRequest — 根据网络请求。 • OnAmsiScan — AMSI 扫描时。 • OnSystemWatcherScan — 分析应用程序行为时。
DetectedName	string	对象的名称。
DetectedObjectType	string	对象的类型。可能值: • 未知。 • 文件。 • LogicalDrive — 逻辑驱动器。 • PhysicalDisk — 物理磁盘。 • SystemMemory — 系统内存。 • MemoryProcess — 进程内存。 • MemoryModule — 内存模块。 • MailMsgRef — 电子邮件消息的引用标题。 • MailMsgMime — MIME 附件。 • MailMsgBody — 电子邮件正文。 • MailMsgAttach — 电子邮件附件。 • StartUp — 启动对象。 • Folder — 目录。 • Script — 脚本。 • Url — URL 地址。 • AmsiStream — AMSI 扫描流。

字段名称	类型	描述
ThreatStatus	string	发现模式。可能值: • Untreated — 对象未处理。 • Untreatable — 对象无法被处理。 • NotFound — 对象未找到。 • Disinfected — 对象被清除。 • Deleted — 对象已删除。 • Quarantined — 对象被移至隔离区。 • AddByUser — 用户添加的对象。 • 未知。 • AddToExclude — 对象被添加到排除项。 • Terminated — 处理终止。 • Clear — 对象未受感染。 • FalseAlarm — 误报。 • RolledBack — 回滚到之前的状态。 • IpNotBlocked — IP 地址未被阻止。 • IpBlocked — IP 地址被阻止。 • IpCannotBeBlocked — 无法阻止 IP 地址。 • IpBlockIsNotRequired — 不需要 IP 地址阻止。
UntreatedReason	string	对象处理状态。可能值: • None — 没有数据。 • NonCurable — 对象无法被清除。 • Locked — 对象被锁定。 • ReportOnly — 应用程序在*仅报告*模式下。 • NoRights — 无执行该操作的权利。 • Canceled — 处理已取消。 • WriteProtect — 对象受写入保护。 • TaskStopped — 处理任务中断。 • Postponed — 操作被推迟。 • NonOverwritable — 对象不能被覆写。 • CopyFailed — 无法创建对象的副本。 • WriteError — 数据写入错误。 • OutOfSpace — 磁盘空间不足。 • ReadError — 数据读取错误。 • DeviceNotReady — 设备未准备好。 • ObjectNotFound — 未找到对象。 • WriteNotSupported — 不支持数据写入。 • CannotBackup — 无法创建对象的备份。 • SystemCriticalObject — 对象对于系统至关重要。 • AlreadyProcessed — 对象已处理。
InteractiveInputText	string	解释器命令。
ObjectContent	string	被发送以进行扫描的脚本内容。
ObjectContentType	integer	脚本的内容类型。可能值: • 1 – 文本 • 2 – 二进制代码
FileOperationType	integer	文件操作的类型。可能值: • 1 – 文件已创建 • 2 – 文件已修改 • 3 – 文件已重命名 • 4 – 文件属性被修改 • 5 – 文件已删除 • 6 – 文件已读取
PreviousFileName	string	文件先前所在目录的路径。
PreviousFileFullName	string	文件的全名，包括文件先前所在目录的路径和/或先前的文件名。
DroppedFileType	integer	被修改文件的类型。可能值: • 0 – 未知 • 1 – 其他文件 • 2 – PE 镜像 • 3 – PE DLL • 4 – PE 资源 • 5 – .NET 资源文件 • 6 – ELF 文件

用于管理威胁响应操作的 API

Kaspersky Anti Targeted Attack Platform 提供用于执行威胁响应操作的 API。执行操作的命令在 Central Node 服务器处被接收，然后被转发到 Endpoint Agent 组件。

您可以使用外部系统在具有 Endpoint Agent 组件的主机上执行以下操作：

- 管理主机网络隔离
- 管理防止规则
- 运行应用程序

上述所有操作均可在使用 Kaspersky Endpoint Agent for Windows 或 Kaspersky Endpoint Security for Windows 作为 Endpoint Agent 组件的主机上使用。

如果 Kaspersky Endpoint Security for Linux 作为 Endpoint Agent 组件使用，您可以管理网络隔离并运行应用程序。

请求获取具有 Endpoint Agent 组件的主机列表

要创建对具有 Endpoint Agent 组件的主机的信息请求，请使用 GET HTTP 方法。

命令语法

GET "<Central Node 服务器的 URL>:<端口，默认为 443>/kata/response_api/v1/<external_system_id>/sensors"

如果请求处理成功，则会显示具有 Endpoint Agent 组件的主机列表。

您可以创建对主机信息的请求，并按主机的 IP 地址、名称或 ID 进行筛选。您可以指定一个、多个或所有这些筛选器。

> 指定主机名时，请牢记筛选器区分大小写。

GET "<Central Node 服务器的 URL>:<端口，默认为 443>/kata/response_api/v1/<external_system_id>/sensors?ip=<主机的 IP 地址>&host=<主机名称>&sensor_id=<sensor_id >"

如果成功处理请求，将显示有关带有 Endpoint Agent 组件的选定主机的信息。

设置

参数	类型	描述
external_system_id	UUID	用于 Kaspersky Anti Targeted Attack Platform 授权的外部系统的唯一 ID。
sensor_id	UUID	具有 Endpoint Agent 组件的主机的唯一 ID。
ip	string	具有 Endpoint Agent 组件的主机的 IP 地址。
host	string	具有 Endpoint Agent 组件的主机的名称。

输入带有参数的命令的示例

```
GET "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/sensors"
```

```
GET "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/sensors?
ip=10.16.40.243&host=host4&sensor_id=DF64838B-B518-414B-B769-2B8BE341A2F0"
```

Response

HTTP 代码：200

格式：JSON

```
type Response Sensors

type Server struct {
Version string `json:"version"`
},

type Sensors struct {
SensorID UUID `json:"sensorId"`
HostIP string `json:"hostIp"`
LastAccessTimestamp `json:"lastAccessTimestamp"`
Version string `json:"version"`
SelfDefenseState boolean `json:"selfDefenseState"`
LicenseStatus string `json:"licenseStatus"`
OSFamily string `json:"osFamily"`
OSName string `json:"osName"`
Capabilities array `json:"capabilities"`

}
```

返回值

返回码	描述
400	需要授权。
401	参数不正确。
500, 502, 503, 504	内部服务器错误。稍后重复该请求。

请求有关网络隔离以及具有 Kaspersky Endpoint Agent 组件的主机是否存在防止规则的信息

HTTP 方法 GET 用于创建请求以显示有关网络隔离以及具有 Endpoint Agent 组件的主机是否存在防止规则的信息。

命令语法

```
GET "<Central Node 服务器的 URL>:<端口，默认为
443>/kata/response_api/v1/<external_system_id>/settings?sensor_id=
<sensor_id>&settings_type=<network_isolation 或预防>"
```

如果请求得到成功处理，则会显示具有 Endpoint Agent 组件的主机列表，其中列出了在处理请求时应用了防止规则或网络隔离规则的主机。

设置

参数	类型	描述
`external_system_id`	UUID	用于 Kaspersky Anti Targeted Attack Platform 授权的外部系统的唯一 ID。
`sensor_id`	UUID	具有 Endpoint Agent 组件的主机的唯一 ID。
`settings_type`	enum	规则类型：network_isolation 或预防。

使用开关输入命令的示例

```
GET "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?
sensor_id=DF64838B-B518-414B-B769-2B8BE341A2F0&settings_type=network_isolation"
```

Response

HTTP 代码：200

格式：JSON

```
type Response []Settings

type Settings struct {
ExcludedRules array `json:"excludedRules"`
AutoTurnoffTimeoutInSec int `json:"autoTurnoffTimeoutInSec"`
}
```

返回值

返回码	描述
400	需要授权。
401	参数不正确。
404	未找到具有 Endpoint Agent 组件的指定主机。
500, 502, 503, 504	内部错误。稍后重复该请求。

主机网络隔离管理

要使用 API 隔离具有 Endpoint Agent 组件的主机，建议按照以下步骤与 Kaspersky Anti Targeted Attack Platform 进行交互：

1. **创建获取具有 Endpoint Agent 组件的主机列表的请求**
2. **创建请求以获取有关已启用网络隔离的主机的信息**
3. **创建以下之一对具有 Endpoint Agent 组件的主机的操作请求：**
   - 启用网络隔离
   - 禁用网络隔离
   - 将排除项添加到现有网络隔离规则

您可以在应用程序的 Web 界面中管理创建的网络隔离规则。

请求启用网络隔离

要为选定的主机启用网络隔离，您必须添加网络隔离规则。要创建请求，请使用 HTTP POST 方法。

命令设置以 JSON 格式在请求正文中传递。

命令语法

```
curl -k --cert <TLS 证书文件路径> --key <私钥文件路径> -X POST "<Central Node 服务器的 URL>:
<端口，默认为 443>/kata/response_api/v1/<external_system_id>/settings?sensor_id=
<sensor_id>&settings_type=network_isolation" -H 'Content-Type: application/json' -d '

{

"settings": {

"autoTurnoffTimeoutInSec": <网络隔离时间段>}

}

'
```

如果请求得到成功处理，则添加网络隔离规则。添加规则后，所选主机的网络隔离将变为活动状态。

在创建请求时指定的一段时间后，网络隔离将变为非活动状态。网络隔离规则本身不会被删除。如有必要，您可以删除选定的规则。

要禁用网络隔离，您必须创建请求以禁用所选规则。

设置

参数	类型	描述
external_system_id	UUID	用于 Kaspersky Anti Targeted Attack Platform 授权的外部系统的唯一 ID。
sensor_id	UUID	具有 Endpoint Agent 组件的主机的唯一 ID。
autoTurnoffTimeoutInSec	integer	网络隔离处于活动状态的时间段。 允许范围 - 1 到 9999 小时。网络隔离时间以秒为单位指定。例如，如果要启用主机网络隔离两个小时，则必须指定 7200 秒。

输入具有开关的命令的示例

```
curl -k --cert <TLS 证书文件路径> --key <私钥文件路径> -X POST
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?sensor_id=DF64838B-
B518-414B-B769-2B8BE341A2F0&settings_type=network_isolation" -H 'Content-Type: application/json' -d '
{
"settings": {
"autoTurnoffTimeoutInSec": 7200}
}
'
```

Response

HTTP 代码：200

格式：JSON

```
type Response []Settings

type Settings struct {
ExcludedRules array `json:"excludedRules"`
AutoTurnoffTimeoutInSec integer `json:"autoTurnoffTimeoutInSec"`
}
```

返回值

返回码	描述
400	参数不正确。
401	需要授权。
404	未找到具有 Endpoint Agent 组件的指定主机。
500, 502, 503, 504	内部服务器错误。稍后重复该请求。

如果要编辑已创建的网络隔离规则的设置，您必须创建新请求以添加具有新设置的规则。

请求禁用网络隔离

要禁用选定主机的网络隔离，您必须创建禁用网络隔离规则的请求。HTTP 方法 DELETE 用于创建请求。

命令语法

```
curl -k --cert <TLS 证书文件路径> --key <私钥文件路径> -X DELETE "<Central Node 服务器的URL>:<端口，默认为 443>/kata/response_api/v1/<external_system_id>/settings?sensor_id=<sensor_id>&settings_type=network_isolation"
```

如果请求处理成功，则网络隔离规则被禁用。

设置

参数	类型	描述
external_system_id	UUID	用于 Kaspersky Anti Targeted Attack Platform 授权的外部系统的唯一 ID。
sensor_id	UUID	具有 Endpoint Agent 组件的主机的唯一 ID。

输入带有 DELETE 参数的命令的示例

```
curl -k --cert <TLS 证书文件路径> --key <私钥文件路径> -X DELETE
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?sensor_id=DF64838B-
B518-414B-B769-2B8BE341A2F0&settings_type=network_isolation"
```

要验证网络隔离是否已被禁用，请使用 HTTP GET 方法请求任务信息。

输入带有 GET 参数的命令的示例

```
curl -k --cert <TLS 证书文件路径> --key <私钥文件路径> -X GET "https://10.10.0.22:443/kata/response_api/v1/15301050-
0490-4A41-81EA-B0391CF21EF3/settings?sensor_id=DF64838B-B518-414B-B769-
2B8BE341A2F0&settings_type=network_isolation"| python -m json.tool
```

如果网络隔离被禁用，Kaspersky Anti Targeted Attack Platform 将按以下格式向外部系统返回响应：

```
{
"error": "未找到"
}
```

返回值

返回码	描述
400	参数不正确。
401	需要授权。
404	未找到具有 Endpoint Agent 组件的指定主机。
500, 502, 503, 504	内部服务器错误。稍后重复该请求。

请求将排除项添加到网络隔离规则

要将排除项添加到之前创建的网络隔离规则中，您必须创建添加排除项的请求。要创建请求，请使用 HTTP POST 方法。

命令设置以 JSON 格式在请求正文中传递。

命令语法

```
curl -k --cert <TLS 证书文件路径> --key <私钥文件路径> -X POST "<Central Node 服务器的 URL>:
<端口，默认为 443>/kata/response_api/v1/<external_system_id>/settings?sensor_id=
<sensor_id>&settings_type=network_isolation" -H 'Content-Type：application/json' -d '

{
"settings":
{"excludedRules": [
{
"direction": "<outbound、inbound 或 both>",
"protocol": <IP 协议编号>,
"remoteIpv4Address": "<具有 Endpoint Agent 组件的主机的 IP 地址，该组件的流量不得被阻止>",
"localPortRange":
{
"fromPort": <端口号>,
"toPort": <端口号>
}
}
,
{
"direction": "<outbound、inbound 或 both>",
"protocol": <IP 协议编号>,
"remoteIpv4Address": "<具有 Endpoint Agent 组件的主机的 IP 地址，该组件的流量不得被阻止>",
"remotePortRange":
{
"fromPort": <端口号>,
"toPort": <端口号>
}
}
,
{
"direction": "<outbound、inbound 或 both>",
"protocol": <IP 协议编号>,
"remoteIpv4Address": "<具有 Endpoint Agent 组件的主机的 IP 地址，该组件的流量不得被阻止>"
}
]
,
"autoTurnoffTimeoutInSec": <网络隔离时长>
}
}
'
```

如果请求处理成功，则会添加网络隔离规则的排除项。

设置

参数	类型	描述
external_system_id	UUID	用于 Kaspersky Anti Targeted Attack Platform 授权的外部系统的唯一 ID。

sensor_id	UUID	具有 Endpoint Agent 组件的主机的唯一 ID。
direction	array	不得被阻止的网络流量方向。可能值: • inbound • outbound • both 如果您没有为此参数指定值，则默认值为"both"，这意味着应用程序在两个方向上传输流量。
protocol	integer	由互联网号码分配机构 (IANA) 分配的 IP 协议号。 如果不指定此参数的值，则默认情况下，网络隔离将应用于所有协议。
remoteIpv4Address	string	具有 Endpoint Agent 组件的主机的 IP 地址，其流量不得被阻止
remotePortRange	string	目的端口。 仅当您选择了网络流量的出站方向时，才可以指定目标端口。无法为双向流量指定端口范围。
localPortRange	string	从其发起连接的端口。 仅当您选择了网络流量的入站方向时，才可以指定目标端口。无法为双向流量指定端口范围。
autoTurnoffTimeoutInSec	integer	网络隔离处于活动状态的时间段。 允许范围 - 1 到 9999 小时。网络隔离时间以秒为单位指定。例如，如果要启用主机网络隔离两个小时，则必须指定 7200 秒。

输入具有开关的命令的示例

```
curl -k --cert <TLS 证书文件路径> --key <私钥文件路径> -X POST
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?sensor_id=DF64838B-
B518-414B-B769-2B8BE341A2F0&settings_type=network_isolation" -H 'Content-Type: application/json' -d '
{
"settings":
{"excludedRules": [
{
"direction": "inbound",
"protocol": 6,
"remoteIpv4Address": "10.16.41.0",
"localPortRange":
{
"fromPort": 3389,
"toPort": 3389
}
}
,
{
"direction": "outbound",
"remoteIpv4Address": "10.16.41.1",
"remotePortRange":
{
"fromPort": 13957,
"toPort": 55409
}
}
,
{
"direction": "both",
"protocol": 6,
"remoteIpv4Address": "10.16.41.2"
}
]
,
"autoTurnoffTimeoutInSec": 7200
}
}
'
```

Response

HTTP 代码：200

格式：JSON

```
type Response []Settings
type Settings struct {
ExcludedRules array `json:"excludedRules"`
AutoTurnoffTimeoutInSec integer `json:"autoTurnoffTimeoutInSec"`
}
type ExcludedRules struct {
Direction array `json:"direction"`
Protocol integer `json:"autoTurnoffTimeoutInSec"`
RemotePortRange string `json:"remotePortRange"`
LocalPortRange string `json:"localPortRange"`
}
```

返回值

返回码	描述
`400`	参数不正确。
`401`	需要授权。
`404`	未找到具有 Endpoint Agent 组件的指定主机。
`500, 502, 503, 504`	内部服务器错误。稍后重复该请求。

如果要编辑已创建的排除项的设置，您必须创建一个新请求以添加具有新设置的排除项。

管理防止规则

您可以使用防止规则来阻止文件或进程在具有 Endpoint Agent 组件的选定主机或所有主机上运行。例如，您可以阻止某些您认为不安全的应用程序。该应用程序通过使用 MD5 和 SHA256 哈希算法基于文件哈希识别文件。通过外部系统创建的防止规则可以包含多个文件哈希。

您可以使用外部系统来管理为单个主机或同时为所有主机创建的所有防止规则。当您通过外部系统为选定主机创建防止规则时，Kaspersky Anti Targeted Attack Platform 会将应用于该主机的所有防止规则替换为具有新参数的防止规则。例如，如果您通过应用程序的 Web 界面为选定主机添加了多个防止规则，随后通过外部系统添加了一条防止规则，则在 Web 界面中添加的所有防止规则都将替换为通过外部系统添加的规则。

当通过外部系统创建的防止规则的参数被修改时，应用程序仅保存新参数。例如，如果您添加了一条包含多个文件的哈希值的防止规则，并且想要向该规则添加另一个哈希值，则必须创建一个请求来添加防止规则并指定您之前有防御的所有哈希值，加上新的哈希值。

所描述的场景也与应用于所有主机的防止规则相关。

要使用 API 创建防止规则，建议按照以下步骤与 Kaspersky Anti Targeted Attack Platform 进行交互：

1. **创建获取具有 Endpoint Agent 组件的主机列表的请求**
2. **创建请求以获取已具有防止规则的主机的信息。**
3. **创建请求执行以下防止规则操作之一：**
   - 创建规则
   - 删除规则

添加的防止规则显示在应用程序的 Web 界面中的**防止**部分，**防止规则**子部分。

如果要通过外部系统为所有主机创建防止规则，您必须首先确保服务器上不存在同一文件的防止规则，或者规则没有被应用于一台或多台主机。如果您想要通过外部系统为选定的主机创建防止规则，则此先决条件也很重要：您必须确保服务器上不存在同一文件的防止规则，并且没有应用于所有主机。否则，服务器将向外部系统返回错误，其中包含已应用防止规则的主机列表。

如果通过外部系统创建的防止规则包含多个文件哈希，则错误信息仅提及导致错误的第一个文件。其他防重复规则的信息不显示。

要修改之前通过 Web 界面或外部系统创建的防止规则，您必须创建请求以添加具有更新参数的防止规则。

请求创建防止规则

要创建请求，请使用 HTTP POST 方法。命令设置以 JSON 格式在请求正文中传递。

命令语法

```
curl -k --cert <TLS 证书文件路径> --key <私钥文件路径> -X POST "<Central Node 服务器的 URL>:<端口，默认为 443>/kata/response_api/v1/<external_system_id>/settings?sensor_id=<sensor_id 或全部，如果要为所有主机创建防止规则>&settings_type=prevention" -H 'Content-Type: application/json' -d '

{

"settings": {

"objects": [

{

"file": {

"<sha256 or md5>": "<要阻止启动的文件的 SHA256 或 MD5 哈希>"

}

},

{

"file": {

"<sha256 or md5>": "<要阻止启动的文件的 SHA256 或 MD5 哈希>"

}

}

]

}

}
```

'

如果请求处理成功，则防止规则被添加。防止规则在添加后立即生效。

如有必要，您可以删除防止规则。

设置

参数	类型	描述
external_system_id	UUID	用于 Kaspersky Anti Targeted Attack Platform 授权的外部系统的唯一 ID。
sensor_id	UUID	具有 Endpoint Agent 组件的主机的唯一 ID。
objects	string	您想要阻止运行的对象的类型。 参数的可能值：file。
sha256 or md5	string	SHA256 或 MD5 具有您想要阻止运行的对象。

输入具有开关的命令的示例

```
curl -k --cert <TLS 证书文件路径> --key <私钥文件路径> -X POST
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?
sensor_id=all&settings_type=prevention" -H 'Content-Type: application/json' -d '
{
"settings": {
"objects": [
{
"file": {
"sha256": "830195824b742ee59390bc5b9302688c778fc95a64e7d597e28a74c03a04dd63"
}
},
{
"file": {
"md5": "d8e577bf078c45954f4531885478d5a9"
}
}
]
}
}
'
```

Response

HTTP 代码：200

格式：JSON

```
type Response []Objects

type Objects struct {
type file struct {
SHA256 string `json:"sha256"`
},
type file struct {
MD5 string `json:"md5"`
}
}
```

返回值

返回码	描述
400	参数不正确。
401	需要授权。
404	未找到具有 Endpoint Agent 组件的指定主机。
500, 502, 503, 504	内部服务器错误。稍后重复该请求。

请求删除防止规则

您可以使用具有空白值的新请求或具有 DELETE 参数的请求来删除防止规则。POST 和 DELETE HTTP 方法用于创建请求。

新请求的命令语法

命令设置以 JSON 格式在请求正文中传递。

```
curl -k --cert <TLS 证书文件路径> --key <私钥文件路径> -X POST "<Central Node 服务器的 URL>:<端口，默认为 443>/kata/response_api/v1/<external_system_id>/settings?sensor_id=<sensor_id 或全部，如果要删除所有主机的防止规则>&settings_type=prevention" -H 'Content-Type: application/json' -d '

{

"settings": {

"objects": []
```

```
}

}

'
```

带有 DELETE 参数的命令语法

```
curl -k --cert <TLS 证书文件路径> --key <私钥文件路径> -X DELETE "<Central Node 服务器的URL>:<端口，默认为 443>/kata/response_api/v1/<external_system_id>/settings?sensor_id=<sensor_id 或全部，如果要删除所有主机的防止规则>&settings_type=prevention"
```

设置

参数	类型	描述
external_system_id	UUID	用于 Kaspersky Anti Targeted Attack Platform 授权的外部系统的唯一 ID。
sensor_id	UUID	具有 Endpoint Agent 组件的主机的唯一 ID。

新请求的命令示例

```
curl -k --cert <TLS 证书文件路径> --key <私钥文件路径> -X POST
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?
sensor_id=all&settings_type=prevention" -H 'Content-Type: application/json' -d '

{

"settings": {

"objects": []

}

}

'
```

输入带有 DELETE 参数的命令的示例

```
curl -k --cert <TLS 证书文件路径> --key <私钥文件路径> -X DELETE
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?
sensor_id=all&settings_type=prevention"
```

如果请求得到成功处理，则阻止规则被删除。

要验证防止规则是否已被删除，请使用 HTTP GET 方法请求有关防止规则的信息。

输入带有 GET 参数的命令的示例

```
curl -k --cert <TLS 证书文件路径> --key <私钥文件路径> -X GET "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?sensor_id=all&settings_type=prevention"| python -m json.tool
```

如果防止规则被删除，Kaspersky Anti Targeted Attack Platform 将按以下格式向外部系统返回响应：

```
{
"error": "未找到"
}
```

返回值

返回码	描述
400	参数不正确。
401	需要授权。
404	未找到具有 Endpoint Agent 组件的指定主机。
500, 502, 503, 504	内部服务器错误。稍后重复该请求。

管理应用程序运行任务

要使用 API 管理应用程序运行任务，建议按照以下步骤与 Kaspersky Anti Targeted Attack Platform 进行交互：

1. **创建有关任务设置、创建时间和完成状态信息的请求**
2. **创建请求执行以下任务操作之一：**
   - 创建任务
   - 删除任务

添加的任务显示在应用程序的 Web 界面中的**任务**部分。

请求获取有关任务的信息

要创建获取有关任务的信息的请求，请使用 HTTP GET 方法。

命令语法

```
GET "<Central Node 服务器的 URL>:<端口，默认为 443>/kata/response_api/v1/<external_system_id>/tasks/<task_id>?settings=<true 或 false>"
```

如果请求处理成功，则会显示有关任务的设置、创建时间和完成状态的信息。

设置

设置	类型	描述
external_system_id	UUID	用于 Kaspersky Anti Targeted Attack Platform 授权的外部系统的唯一 ID。
sensor_id	UUID	具有 Endpoint Agent 组件的主机的唯一 ID。
task_id	UUID	任务的唯一 ID。
settings	boolean	可能值: • true。 如果输入此值，将显示有关任务的设置、创建时间和完成状态的信息。 • false。 如果输入此值，将显示有关任务的创建时间和完成状态的信息。

输入具有开关的命令的示例

```
GET https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/tasks/2EEB4CBC-10C6-4DC4-BE0A-72A75CDB0BE8?settings=<true 或 false>
```

Response

HTTP 代码：200

格式：JSON

```
type Response struct {
State `json:"state"`
LatestStartDateTime `json:"latestStartDateTime"`
type Task struct {
type Schedule struct {
StartNow boolean `json:"startNow"`
ExecCommand string `json:"execCommand"`
}
}
}
```

返回值

返回码	描述
400	参数不正确。
401	需要授权。

返回码	描述
409	指定 ID 的任务已经存在。
500, 502, 503, 504	内部服务器错误。稍后重复该请求。

请求创建任务

HTTP POST 方法用于请求运行 Kaspersky Anti Targeted Attack Platform 应用程序。命令设置以 JSON 格式在请求正文中传递。

命令语法

```
curl -k --<TLS证书文件路径> --key <私钥文件路径> -X POST "<Central Node 服务器的 URL>:<端口，默认443>/kata/response_api/v1/<external_system_id>/tasks/<task_id>?sensor_id=<sensor_id>&task_type=run_process" -H 'Content-Type：application/json' -d '

{

"task": {

"shedule": {"startNow": <true 或 false>},

"execCommand": "<要运行的应用程序的名称>",

"cmdLineParameters": "<运行文件或命令的其他选项>",

"workingDirectory": "<工作目录>"

}

}

'
```

如果成功处理请求，则会创建运行应用程序任务。

设置

参数	类型	描述
external_system_id	UUID	用于 Kaspersky Anti Targeted Attack Platform 授权的外部系统的唯一 ID。
sensor_id	UUID	具有 Endpoint Agent 组件的主机的唯一 ID。
task_id	UUID	任务的唯一 ID。

输入具有开关的命令的示例

```
curl -k --example.cert --example.key -X POST "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/tasks/2EEB4CBC-10C6-4DC4-BE0A-72A75CDB0BE8?sensor_id=DF64838B-B518-414B-B769-2B8BE341A2F0&task_type=run_process" -H 'Content-Type: application/json' -d '
{

"task": {

"schedule": {"startNow": true},

"execCommand": "Example.exe",

"cmdLineParameters": "C:\Windows\System32\",

"workingDirectory": "/all"

}

}

'
```

Response

HTTP 代码：200

格式：JSON

```
type Response struct {
State `json:"state"`
LatestStartDateTime `json:"latestStartDateTime"`
type Task struct {
type Schedule struct {
StartNow boolean `json:"startNow"`
ExecCommand string `json:"execCommand"`
}
}
}
```

返回值

返回码	描述
400	参数不正确。
401	需要授权。

返回码	描述
404	未找到具有指定 ID 的任务。
500, 502, 503, 504	内部服务器错误。稍后重复该请求。

如果要编辑已创建任务的设置，则必须创建新请求以添加具有新设置的任务。

请求删除任务

要创建删除 Kaspersky Anti Targeted Attack Platform 任务的请求，请使用 HTTP DELETE 方法。

命令语法

```
curl -k --<TLS 证书文件路径> --key <私钥文件路径> -X DELETE "<Central Node 服务器的 URL>:<端口，默认为 443>/kata/response_api/v1/<external_system_id>/tasks/<task_id>"
```

如果成功处理请求，则会删除应用程序运行任务。

设置

参数	类型	描述
external_system_id	UUID	用于 Kaspersky Anti Targeted Attack Platform 授权的外部系统的唯一 ID。
task_id	UUID	任务的唯一 ID。

输入带有 DELETE 参数的命令的示例

```
curl -k --example.cert --example.key -X DELETE "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/tasks/2EEB4CBC-10C6-4DC4-BE0A-72A75CDB0BE8"
```

如果请求得到成功处理，则阻止规则被删除。

要验证任务是否已被删除，请使用 HTTP GET 方法请求有关任务的信息。

输入带有 GET 参数的命令的示例

```
curl -k --example.cert --example.key -X GET "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/tasks/2EEB4CBC-10C6-4DC4-BE0A-72A75CDB0BE8?settings=false"| python -m json.tool
```

如果任务被删除，Kaspersky Anti Targeted Attack Platform 将按以下格式向外部系统返回响应：

```
{
"error": "未找到"
}
```

返回值

返回码	描述
400	参数不正确。
401	需要授权。
404	未找到具有指定 ID 的任务。
500, 502, 503, 504	内部服务器错误。稍后重复该请求。

使用 Kaspersky Anti Targeted Attack Platform API NDR

REST API 服务器为外部系统提供对 NDR 功能的访问，它在 Central Node 服务器上运行并使用 REST (Representational State Transfer) 架构风格处理请求。使用 HTTPS 向 REST API 服务器发出请求。您可以在“**设置→连接服务器**”下配置 REST API 服务器（包括用受信任证书替换默认的自签名证书）。

JSON 格式用于表示请求和响应中的数据。

包含基于 REST 架构风格的请求描述的文档作为“在线帮助指南”发布在“卡巴斯基在线帮助”页面上。本文档是英文版的开发者指南。开发人员指南还提供了被发送到 REST API 服务器的请求中可用的可调用元素的示例代码和详细描述。

打开描述对 REST API 服务器的请求的文档，版本 3

打开描述对 REST API 服务器的请求的文档，版本 4

外部系统可以使用 Kaspersky Anti Targeted Attack Platform API 来：

- 接收有关应用程序已知设备的信息。
- 添加、修改和删除设备。
- 接收有关已注册的网络流量事件（NDR 事件）的信息。
- 将 NDR 事件发送到 Kaspersky Anti Targeted Attack Platform（代码为 4000005400 的系统事件类型用于注册事件）。
- 接收有关检测到的漏洞的信息。
- 接收应用程序消息和审计记录。
- 接收有关允许规则的信息。
- 启用、禁用和删除允许规则。
- 接收与设备相关的风险信息。
- 接收有关地址空间的信息。
- 将网络拓扑图报告发送至 Kaspersky Anti Targeted Attack Platform。
- 发送、接收和删除有关设备上用户的信息。
- 发送和接收有关设备上的应用程序和补丁的信息。
- 发送和删除有关设备上的可执行文件的信息。
- 发送设备日志的内容。

- 接收以下应用程序数据：
  - 包含应用程序组件的服务器列表
  - 监控点及其参数列表
  - 支持的协议栈及其参数列表
  - NDR 事件类型及其参数列表
  - 技术现状及运作模式
  - 应用程序版本和已安装更新的发布日期
  - 有关添加的授权许可密钥的信息
  - 应用程序本地化语言

向 REST API 服务器版本 4 发出请求时，所有列出的操作均可用。向 REST API 服务器版本 3 发出请求时，其中一些操作不受支持。

使用 Kaspersky Anti Targeted Attack Platform API 的外部系统通过连接器连接到 Central Node 组件。连接器使用证书来建立安全连接。对于您想要向 REST API 服务器发送请求的每个外部系统，您需要在 Kaspersky Anti Targeted Attack Platform 中创建一个单独的连接器。

外部系统必须使用身份验证令牌才能连接到 Kaspersky Anti Targeted Attack Platform。Kaspersky Anti Targeted Attack Platform 根据外部系统的请求发出身份验证令牌，令牌使用为该系统创建的连接器的证书。身份验证令牌的有效期为 10 小时。外部系统可以通过特殊请求更新身份验证令牌。

包含身份验证令牌操作查询描述的文档作为在线帮助指南发布在“卡巴斯基在线帮助”页面上。本文档是英文版的开发者指南。

打开描述身份验证令牌操作查询的文档，版本 3

打开描述身份验证令牌操作查询的文档，版本 4

Kaspersky Anti Targeted Attack Platform API 允许通过以下方式与外部系统进行交互：

- 基于 REST 架构风格的交互
- 通过 WebSocket 协议进行交互

外部系统可以使用 WebSocket 协议在 Kaspersky Anti Targeted Attack Platform API 中进行交互，以创建对应用程序收到的修改值的订阅。

确保使用 Kaspersky Anti Targeted Attack Platform API 时的安全性

外部系统通过建立加密的 HTTPS 连接，使用 Kaspersky Anti Targeted Attack Platform API 访问应用程序的功能。Kaspersky Anti Targeted Attack Platform 的 Central Node 组件颁发的证书用于保护连接的安全。该组件为外部系统用于连接服务器的连接器颁发证书。

必须在 Kaspersky Anti Targeted Attack Platform 中为每个外部系统创建单独的连接器。只有使用由 Central Node 组件颁发并保存在该连接器的通信数据包中的特定证书才能通过连接器建立连接。如果外部系统提供来自不同连接器、Kaspersky Anti Targeted Attack Platform 的不同 Central Node 组件或用于其他连接的证书（例如，Sensor 组件的证书），则无法建立连接。

建立加密连接后，外部系统必须为连接器请求一个*身份验证令牌*，外部系统将在发送到 Central Node REST API 服务器的请求中使用该令牌。

身份验证令牌在签发后 10 小时内有效。如果令牌需要使用更长时间，则外部系统必须在令牌过期之前请求延长时间。

有关 Kaspersky Anti Targeted Attack Platform API 支持的请求和方法的信息，请参阅 Kaspersky Anti Targeted Attack Platform API 的文档。

在处理来自外部系统的请求时，Kaspersky Anti Targeted Attack Platform 使用审计日志记录有关尝试执行以下操作的信息：

- 接收身份验证令牌。
- 延长身份验证令牌的有效期。
- 将设备添加到设备表中。
- 编辑设备信息。
- 删除设备。
- 查询审计日志（加载 Web 服务器后第一次通过连接器读取审计条目时）。

创建并使用 Kaspersky Anti Targeted Attack Platform API 的连接器

为了实现外部系统与 Kaspersky Anti Targeted Attack Platform API 之间的交互，您需要为该系统添加一个连接器。创建连接器时，您必须指明连接器的**一般**系统类型。

当添加连接器并为此连接器创建新的通信数据包时，Central Node 会生成一个通信数据包，您需要使用该数据包使连接器工作。

通信数据包是一个包含以下文件的存档：

- certificates.pfx 文件包含 Central Node 证书的加密公钥和 Central Node 为连接器颁发的证书（带有私钥）。文件内容使用添加连接器时或为此连接器创建新的通信数据包时设置的密码加密。

- metadata.json 文件包含连接器的配置数据。数据以 JSON 格式呈现。

必须使用列出的文件通过连接器连接外部系统。要解密 certificates.pfx 文件并应用其包含的证书和密钥，您可以使用处理此格式的文件的标准方法（例如， `openssl` 命令）。连接器工作以及向 REST API 服务器发送请求需要 metadata.json 文件中指定的地址。

通信数据包中的证书和配置数据一直有效，直到创建新的通信数据包或者从应用程序中移除连接器为止。

有关应用程序的信息源

卡巴斯基网站上的 Kaspersky Anti Targeted Attack Platform 网页

在 Kaspersky Anti Targeted Attack Platform 页面上，您可以找到有关该应用程序、其功能和特点的一般信息。

Kaspersky Anti Targeted Attack Platform 网页中包含在线商店的链接。在在线商店中，您可以购买应用程序或续费授权许可。

知识库中的 Kaspersky Anti Targeted Attack Platform 网页

*知识库*是技术支持网站上的一个部分。

在知识库中的 Kaspersky Anti Targeted Attack Platform 页面上，您可以阅读文章，这些文章提供有关购买，安装和使用该程序的常见问题的有用信息，建议和解答。

知识库文章不仅可以回答与 Kaspersky Anti Targeted Attack Platform 相关的问题，还可以回答与卡巴斯基其他应用程序相关的问题。知识库文章还可能包含技术支持的新闻。

在论坛上讨论卡巴斯基软件

如果您的问题不需要立即回答，您可以在我们的论坛上与卡巴斯基专家和其他用户一起讨论。

在论坛上，您可以查看现有主题、发表评论以及创建新的讨论主题。

联系技术支持服务

本节描述获得技术支持的方法和可用的条款。

如何获得技术支持

如果您无法在程序文档或其中一个Kaspersky Anti Targeted Attack Platform 信息源中找到问题的解决方案，建议您联系技术支持。技术支持人员将解答您有关安装和使用 Kaspersky Anti Targeted Attack Platform 的问题。

卡巴斯基在 Kaspersky Anti Targeted Attack Platform 的整个生命周期内提供支持（请参阅产品生命周期页面）。与技术支持联系之前，请阅读技术支持规则。

您可以通过以下方式之一联系技术支持：

- 访问技术支持网站。
- 通过 Kaspersky CompanyAccount 门户向技术支持发送请求。

通过 Kaspersky CompanyAccount 获得技术支持

Kaspersky CompanyAccount 是一个面向使用卡巴斯基软件的公司提供的门户。Kaspersky CompanyAccount 门户是为了通过网络请求方便用户和卡巴斯基专家之间的互动。Kaspersky CompanyAccount 门户允许监控卡巴斯基员工在线请求处理的进度并保留电子请求的历史记录。

您可以让您的组织机构中所有的员工在 Kaspersky CompanyAccount 注册一个账户。一个单一账户可让您集中管理注册员工发送给卡巴斯基的电子请求，也可以通过 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。

词汇表

Central Node

应用程序组件。扫描数据、分析对象的行为，并将分析结果发布到应用程序的 Web 界面上。

CSRF 攻击

跨站请求伪造（也称为“XSRF 攻击”）。利用 HTTP 协议的漏洞攻击网站用户。这种攻击使得黑客能够打着授权用户的幌子在易受攻击的网站中执行操作。例如，在易受攻击的网站中，黑客可以打着授权用户的幌子秘密地向外部支付系统的服务器发送请求，以便将资金转移到黑客的账户。

Endpoint Agent 组件

应用程序组件。安装在运行 Microsoft Windows、Linux 和 macOS 操作系统的企业 IT 基础架构的工作站和服务器上。持续监控在这些计算机上运行的进程、活动的网络连接和被修改的文件。

ICAP 客户端

Kaspersky Anti Targeted Attack Platform 通过其接收流量的系统。

ICAP 数据

由 ICAP 协议（互联网内容适配协议）接收的数据。该协议允许筛选和修改 HTTP 请求和 HTTP 响应的数据。例如，它允许扫描数据中的病毒、阻止垃圾邮件以及拒绝访问个人资源。ICAP 客户端通常是通过 ICAP 协议与 ICAP 服务器交互的代理服务器。在 ICAP 服务器上处理完此数据后，Kaspersky Anti Targeted Attack Platform 会从组织的代理服务器接收数据。

IOA

攻击指标。对公司 IT 基础架构内对象可疑行为的描述，可能表明该组织受到有针对性的攻击。

IOC

入侵指标。有关恶意对象或恶意活动的一组数据。

IOC 文件

IOC 文件包含一组与事件指标进行比较的指标。如果比较的指标匹配，应用程序将该事件视为检测并创建警报。如果扫描检测到对象数据与多个 IOC 文件之间的精确匹配，则警报的可能性会增加。

Kaspersky Anti Targeted Attack Platform

保护企业 IT 基础架构和及时检测诸如*零日攻击*、*针对性攻击*，以及被称为*高级持续性威胁*（以下也称为"*APT*"）的复杂针对性攻击等威胁的解决方案。

Kaspersky Secure Mail Gateway

用于保护传入和传出的电子邮件免受恶意对象和垃圾邮件的影响，以及用于邮件内容筛选的一种解决方案。该解决方案可让您部署虚拟邮件网关并将其集成到现有的企业邮件基础架构中。虚拟邮件网关上预安装了操作系统、邮件服务器和卡巴斯基反病毒应用程序。

Kaspersky Threat Intelligence Portal

卡巴斯基信息系统 包含并显示文件和 URL 地址的信誉信息。

KATA

Kaspersky Anti Targeted Attack。Kaspersky Anti Targeted Attack Platform 的功能块，用于检测企业 IT 基础架构周边的威胁。

KEDR

Kaspersky Endpoint Detection and Response。Kaspersky Anti Targeted Attack Platform 的功能块，为组织的局域网提供保护。

Kerberos 身份验证

一种在客户端和服务器之间建立连接之前进行相互验证的机制，允许通过不受保护的网络进行通信。该机制基于使用由受信任的身份验证中心向用户颁发的票证。

Keytab 文件

一个包含被允许使用 Kerberos 身份验证的客户端对的唯一名称（主体）和从用户密码派生的加密密钥的文件。支持 Kerberos 的系统使用 keytab 文件来验证用户身份，而无需输入密码。

KPSN 的本地信誉数据库

存储在卡巴斯基私有安全网络服务器上但不存储在卡巴斯基安全网络服务器上的对象（文件或 URL）的信誉数据库。本地信誉数据库由 KPSN 管理员管理。

MIB（管理信息库）

用于管理通过 SNMP 协议传输的对象的虚拟数据库。

MITRE 技术

MITRE ATT&CK （对抗策略、技术和常识）数据库包含基于真实攻击分析的黑客行为描述。它是以表格形式表示的已知黑客技术的结构化列表。

NTP 服务器

使用网络时间协议的精确时间服务器。

OpenIOC

一种基于 XML 的开放性标准，用于描述包含超过 500 种不同入侵指标的入侵指标。

Sandbox

应用程序组件。启动操作系统的虚拟镜像。在这些操作系统中启动文件并跟踪每个操作系统中文件的行为，以检测恶意活动以及针对企业 IT 基础架构的针对性攻击的迹象。

Sensor

应用程序组件。接收数据。

SIEM 系统

安全信息和事件管理系统。用于管理组织安全系统中的信息和事件的解决方案。

SPAN

交换端口分析器。用于将流量从一个端口镜像到另一个端口的技术。

Syslog

发送和记录 UNIX™ 和 GNU/Linux 平台上使用的系统中发生的事件相关消息的标准。

TAA（IOA）规则

企业 IT 基础架构中对象的可疑行为的一种迹象，会导致 Kaspersky Anti Targeted Attack Platform 将事件视为检测并创建警报。TAA (IOA) 规则包含攻击迹象的描述和建议的对策。

TLS 加密

两台服务器之间连接的加密，可确保因特网上服务器之间数据的安全传输。

VIP 身份

具有特殊访问权限的检测的状态。例如，具有**安全官**角色的用户无法查看 VIP 身份的警报。

YARA

应用程序模块。使用由 Kaspersky Anti Targeted Attack Platform 用户创建的 YARA 规则数据库扫描文件和对象，以发现对企业 IT 基础架构的针对性攻击的迹象。

YARA 规则

一种公开可用的恶意软件分类，其中包含对企业 IT 基础架构的针对性攻击和入侵的迹象的签名，由 Kaspersky Anti Targeted Attack Platform 用于扫描文件和对象。

中间人攻击

中间人。对组织的 IT 基础结构的攻击，其中黑客劫持两个接入点之间的通信链路，将其进行传输，并在必要时修改这些接入点之间的连接。

入侵检测系统

应用程序模块。扫描 Internet 流量是否存在入侵企业 IT 基础构架的迹象。

最终用户授权许可协议

您与 AO卡巴斯基之间达成的有约束力的协议，其中明确了用户使用该应用程序的条款。

分布式解决方案

安装有 Central Node 组件的服务器的两层架构。此架构分配主控制服务器 *（主 Central Node (PCN)）*和从属服务器 *（从属 Central Node (SCN)）*。

卡巴斯基安全网络（KSN）

提供对卡巴斯基在线知识库的访问的云服务基础结构，其中包含有关文件信誉、网络资源和软件的信息。使用来自卡巴斯基安全网络的数据可确保卡巴斯基应用程序能够更快地响应威胁，提高某些保护组件的性能，并降低误报的可能性。

卡巴斯基私有安全网络

允许卡巴斯基反病毒应用程序用户访问卡巴斯基安全网络数据库、而无需不从他们的计算机发送数据到卡巴斯基安全网络服务器的一种解决方案。

反恶意软件引擎

应用程序核心。使用反病毒数据库扫描文件和对象以查找企业 IT 基础架构中的病毒和其他威胁。

后门程序

黑客在受感染计算机上植入的一种程序，目的是将来能够访问该计算机。

备用数据流

NTFS 文件系统的数据流（备用数据流）用于文件的其他属性或信息。

NTFS 文件系统中的每个文件都包含一组流。主流包含文件内容。其他（备用）流用于元数据。可以创建、删除、单独保存、重命名流，甚至可以作为一个进程运行。

黑客可以使用替代流来隐藏传输或从计算机接收数据。

多租户

Kaspersky Anti Targeted Attack Platform 被用来同时保护多个组织或同一组织分支机构的基础架构的运行模式。

恶意 Web 地址

分发恶意软件的资源的 URL。

新一代威胁

一种企业 IT 基础架构威胁，能够覆盖、修改、加密或扭曲其代码，以至于安全系统无法再检测到与签名相匹配的位置。

服务主体名称 (SPN)

网络上用于 Kerberos 身份验证的服务的唯一 ID。

检测

应用程序的单个模块或组件扫描对象的结果。

租户

为其提供 Kaspersky Anti Targeted Attack Platform 解决方案的单个组织或组织的分支机构。

签名

包含已知威胁描述的信息保护数据库中的代码。

网络钓鱼 URL 地址

资源的 URL 地址，旨在获得对用户机密数据的未授权访问。网络钓鱼的目的通常是窃取各种财务数据。

警报

使用 Kaspersky Anti Targeted Attack Platform 模块和技术扫描对象后进行的一次或一组检测的记录。显示在警报表中。

转储

在指定时刻进程的工作内存或系统整个 RAM 的内容。

追踪

应用程序以调试模式运行；执行每个命令后，应用程序停止并显示该步骤的结果。

通信信道带宽

特定通信信道中信息传输的最高速度。

针对性攻击

针对特定个人或组织的攻击。与旨在感染尽可能多台计算机的计算机病毒的大规模攻击不同，针对性攻击的目的是感染特定组织的网络，甚至是企业 IT 基础架构内的单独服务器。可以编写专门的木马程序来分阶段进行针对性攻击。

针对性攻击分析器

应用程序模块。使用 TAA (IOA) 规则分析和监控公司 LAN 计算机上安装的软件的网络活动。搜索 Kaspersky Anti Targeted Attack Platform 的用户应注意的网络活动的迹象，以及对企业 IT 基础架构的针对性攻击的迹象。

镜像流量

从一个交换机端口重定向到同一交换机（本地镜像）或远程交换机（远程镜像）的另一个端口的流量副本。网络管理员可以配置应该镜像哪部分流量以传输到 Kaspersky Anti Targeted Attack Platform。

Kaspersky Anti Targeted Attack Platform 支持从聚合设备接收镜像流量：网络包代理或网络轻触。如果要对来自聚合设备的流量应用过滤，则必须调整 Kaspersky Anti Targeted Attack Platform 的硬件要求。为了确定解决方案的实际硬件要求，我们建议先进行试点部署。

零日攻击

一种利用软件零日漏洞攻击企业 IT 基础架构的攻击。这些是黑客在软件供应商发布补丁之前发现和利用的软件漏洞。

零日漏洞

黑客在软件供应商有机会发布包含修补程序代码的补丁之前发现并利用的软件漏洞。

高级持续性威胁（APT）

针对企业 IT 基础架构的高级针对性攻击，可同时使用不同的方法渗透网络，隐藏于网络并获得对机密数据的无障碍访问。

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文件夹中的 legal_notices.txt 文件内。

商标声明

注册商标和服务标志分别属于其各自的所有者。

Adobe、Flash 是 Adobe 公司在美国和/或其他国家/地区的注册商标或商标。

AMD 是 Advanced Micro Devices, Inc. 的商标或注册商标。

Apple、Mac、Macintosh、macOS 和 Safari 是 Apple Inc. 的商标。

Ubuntu® 是 Canonical Ltd 的注册商标。

Cisco 是 Cisco Systems, Inc. 和/或其附属公司在美国和某些其他国家/地区的注册商标或商标。

Citrix 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。

Docker 和 Docker 徽标是 Docker, Inc. 在美国和/或其他国家/地区的商标或注册商标。Docker, Inc. 和其他方也可能拥有本文使用的其他术语中描述的商标的权利。

Google、Google Chrome、 Android 是 Google LLC 的商标。

Intel、 Core 和 Xeon 是英特尔公司或其子公司的商标。

Linux 是 Linus Torvalds 在美国和其他国家/地区的注册商标。

Microsoft、Active Directory、Excel、Internet Explorer、PowerPoint、PowerShell、Win32、Windows、Windows PowerShell、 Windows Server 和 Windows XP 是 Microsoft 集团公司的商标。

Mozilla™ 和 Firefox™ 是 Mozilla 基金会在美国和其他国家/地区的商标。

NVIDIA 是 NVIDIA 公司的注册商标。

OpenSSL 是 OpenSSL 软件基金会的商标。

Java 是 Oracle 和/或其附属公司的注册商标。

Python 是 Python 软件基金会的商标或注册商标。

CentOS 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。

Schneider Electric 是 Schneider Electric 的商标。

Siemens 是 Siemens AG 的注册商标。

Debian 是 Software in the Public Interest, Inc. 的注册商标。

UNIX 是在美國和其他國家/地區的註冊商標，透過 X/Open Company Limited 獨家授權。